IRMA as precursor EU-wallet-ID

22/6/2022, EDPS/IPEN, Warsaw

Bart Jacobs — Radboud University, Nijmegen, NL

bart@cs.ru.nl

iCIS | Digital Security
Radboud University

Background

Background

- Professor of computer security & privacy at Nijmegen, NL
  - Member of Royal Netherlands Academy of Arts and Sciences
  - Recipient of Stevin premium 2021, highest award in science in NL
- Active in media, societal debates and parliamentary hearings
- Member of national Cyber Security Board
  - Also former member of: NL intelligence law evaluation committee
  - And of: NL advice committee on Covid apps
- Non-renumerated chair of Privacy by Design foundation — which runs free IRMA app, jointly with SIDN
  - focus on showing there are IT-alternatives based on public values
  - there are choices — and not just what sillicon valley imposes

iCIS | Digital Security
Radboud University

Global platforms

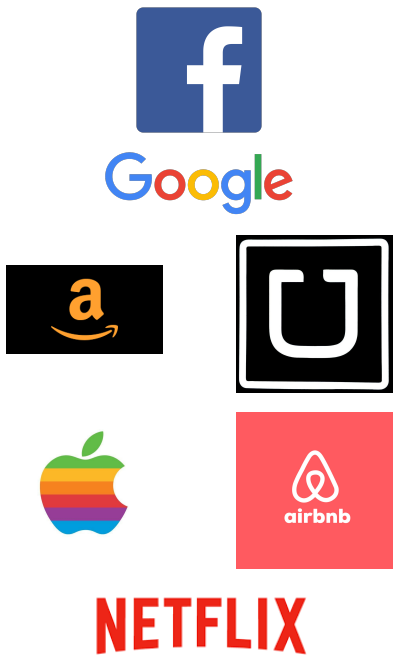
Global platforms

VS	Europe	China

iCIS | Digital Security
Radboud University

Global platforms

VS	Europe	China



etc

Global platforms

VS	Europe	China

etc

iCIS | Digital Security
Radboud University

Global platforms

VS	Europe	China

etc

iCIS | Digital Security
Radboud University

The shared US-CN agenda, versus EU

The shared US-CN agenda, versus EU

- Both US and CN platforms wish to control digital identities
  - they wish to precisely register who is doing what & when online
  - goal: build up detailed profiles

The shared US-CN agenda, versus EU

- Both US and CN platforms wish to control digital identities
  - they wish to precisely register who is doing what & when online
  - goal: build up detailed profiles
- The US platforms have mostly commercial motives
  - but they have been used for political manipulation too

iCIS | Digital Security
Radboud University

The shared US-CN agenda, versus EU

- Both US and CN platforms wish to control digital identities
  - they wish to precisely register who is doing what & when online
  - goal: build up detailed profiles
- The US platforms have mostly commercial motives
  - but they have been used for political manipulation too
- The CN platforms are instrumental in maintaining state control
  - see e.g. their role in "social credit scores"

iCIS | Digital Security
Radboud University

The shared US-CN agenda, versus EU

- Both US and CN platforms wish to control digital identities
  - they wish to precisely register who is doing what & when online
  - goal: build up detailed profiles
- The US platforms have mostly commercial motives
  - but they have been used for political manipulation too
- The CN platforms are instrumental in maintaining state control
  - see e.g. their role in "social credit scores"

These systems work on the basis of a unique identifier (number), per individual, that is used everywhere

- Strong EU sentiment: there are better ways to do this, with more respect for human (digital) rights & dignity

iCIS | Digital Security
Radboud University

Von der Leyen, State of the Union (EP, sept'2020)

iCIS | Digital Security
Radboud University

Von der Leyen, State of the Union (EP, sept'2020)

- "Europe's Digital Decade (2020-2030)"
- Focus on European cloud, AI and on European digital identity
- *That is why the Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used.*
- EU digital wallet-id plans appeared in June 2021 — as eIDAS revision
  - with IRMA as leading example: selective disclosure of attributes

iCIS | Digital Security
Radboud University

Security and identities

Security and identities

- Essential for security : knowing who you are dealing with
  - e.g. in electronic banking
  - or in buying alcoholic drinks
  - or during video calls/conferences (recall EU defence ministers)

iCIS | Digital Security
Radboud University

Security and identities

- Essential for security : knowing who you are dealing with
  - e.g. in electronic banking
  - or in buying alcoholic drinks
  - or during video calls/conferences (recall EU defence ministers)
- Identity requests must be proportional and contextual (by GDPR):
  - for hefty online game a proof of "older than 16" suffices
  - for ordering a book: only address + bank account number
  - for logging into government site: a citizen number, typically

iCIS | Digital Security
Radboud University

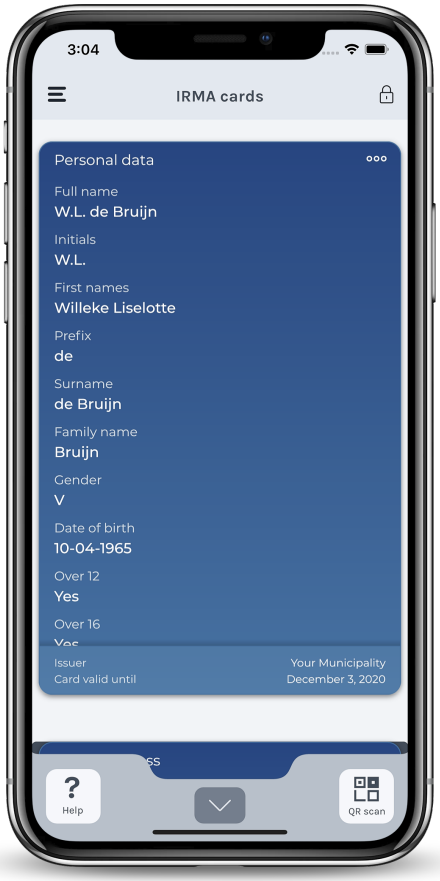
Security and identities

- Essential for security : knowing who you are dealing with
  - e.g. in electronic banking
  - or in buying alcoholic drinks
  - or during video calls/conferences (recall EU defence ministers)
- Identity requests must be proportional and contextual (by GDPR):
  - for hefty online game a proof of "older than 16" suffices
  - for ordering a book: only address + bank account number
  - for logging into government site: a citizen number, typically
- Digital identity supports working of the GDPR
  - authentication, for reliably exercising access rights (art. 15)
  - digital signing, for reliably giving consent (art. 7)

iCIS | Digital Security
Radboud University

IRMA app, for revealing only relevant attributes

IRMA app, for revealing only relevant attributes



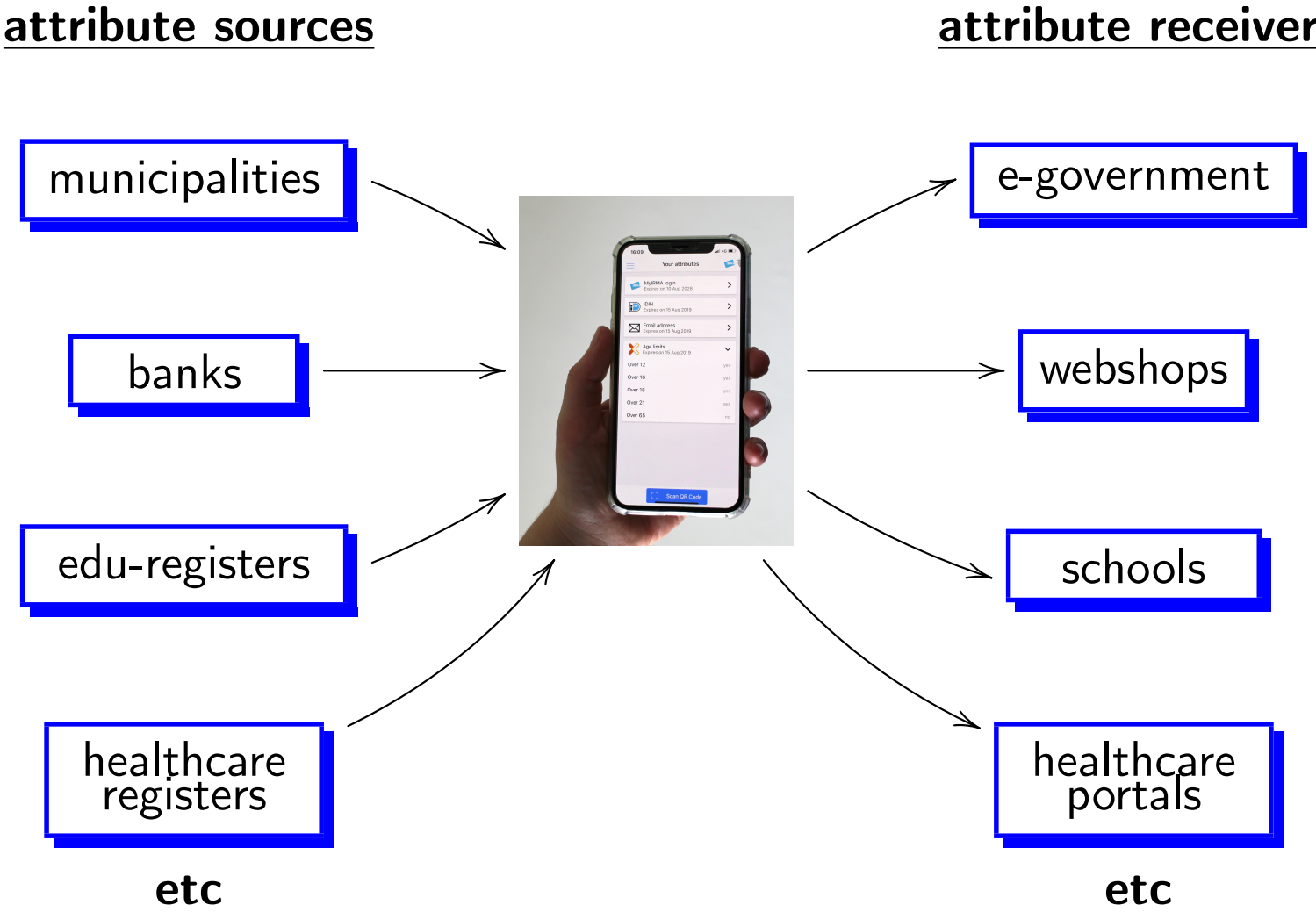
Essentials:

- attributes instead of identities
- collected by user him/herself
- attributes are reliable (digitally signed by source)
- decentralised architecture: attributes only on users own phone
- IRMA is free & open source, up-and-running, with almost $100K$ registrations, worldwide

iCIS | Digital Security
Radboud University

The IRMA app as everyone's personal ID-wallet

The IRMA app as everyone's personal ID-wallet



iCIS | Digital Security
Radboud University

IRMA status

IRMA status

- It's proven technology, up and running $\geq$ 5 years
  - based on zero-knowledge proofs, from IBM's Idemix

iCIS | Digital Security
Radboud University

IRMA status

- It's proven technology, up and running ≥ 5 years
  - based on zero-knowledge proofs, from IBM's Idemix
- User base approaching 100K — with $\geq 1K$ new per week
  - usage esp. in healthcare, local government
  - also e.g. in insurance, for authenticated access (GDPR art. 15)

iCIS | Digital Security
Radboud University

IRMA status

- It's proven technology, up and running ≥ 5 years
  - based on zero-knowledge proofs, from IBM's Idemix
- User base approaching 100K — with $\geq 1K$ new per week
  - usage esp. in healthcare, local government
  - also e.g. in insurance, for authenticated access (GDPR art. 15)
- NO blockchain in IRMA
  - irrelevant, wasteful technology, creating noise in discussions
  - "a solution looking for a problem"

iCIS | Digital Security
Radboud University

IRMA status

- It's proven technology, up and running ≥ 5 years
  - based on zero-knowledge proofs, from IBM's Idemix
- User base approaching 100K — with $\geq 1K$ new per week
  - usage esp. in healthcare, local government
  - also e.g. in insurance, for authenticated access (GDPR art. 15)
- NO blockchain in IRMA
  - irrelevant, wasteful technology, creating noise in discussions
  - "a solution looking for a problem"
- IRMA's open source character sparks much innovative follow-up, e.g.
  - Identity-based email encryption (postguard.eu)
  - Authenticated video calls (irma-meet.nl)
  - Authenticated phone calls (ID-contact.nl)
  - Encrypted file transfer (cryptify.nl)
  - Tweet signing, against fake news ("Twid")
  - New social network with authentication (pubhubs.net)

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised versus decentralised, schematically

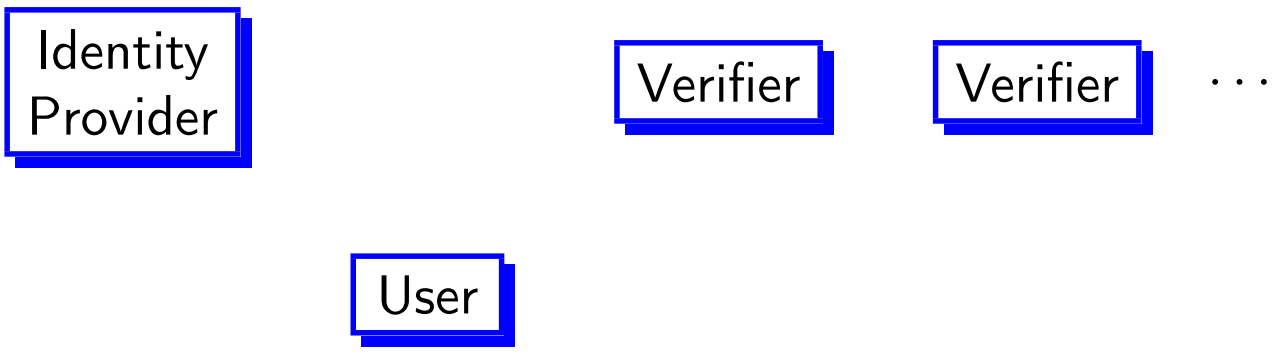
Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)

Decentralised: everyting goes via the User (think IRMA)

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)

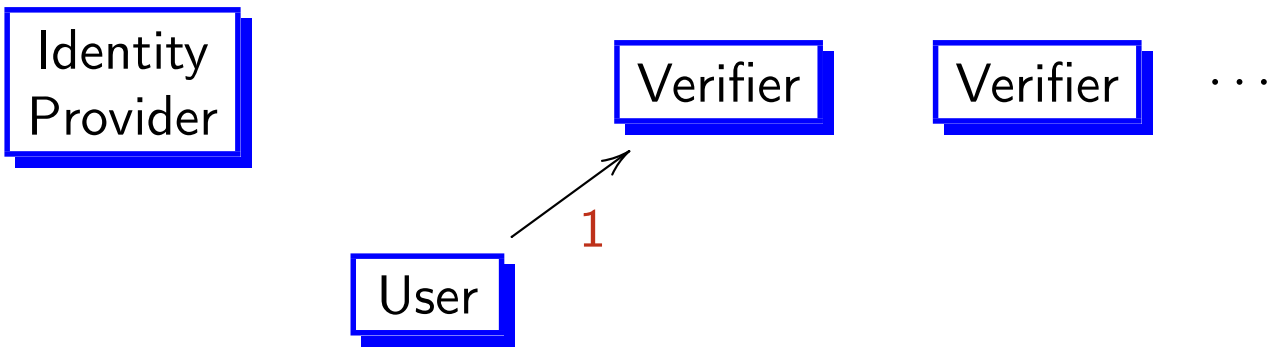


Decentralised: everyting goes via the User (think IRMA)

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)

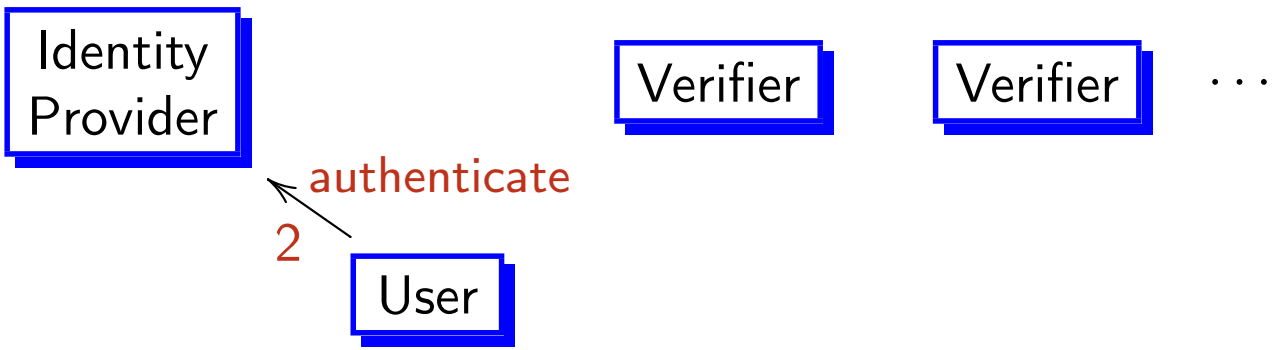


Decentralised: everyting goes via the User (think IRMA)

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)

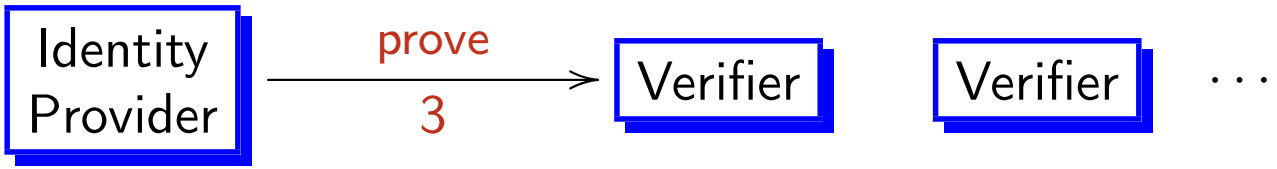


Decentralised: everyting goes via the User (think IRMA)

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)

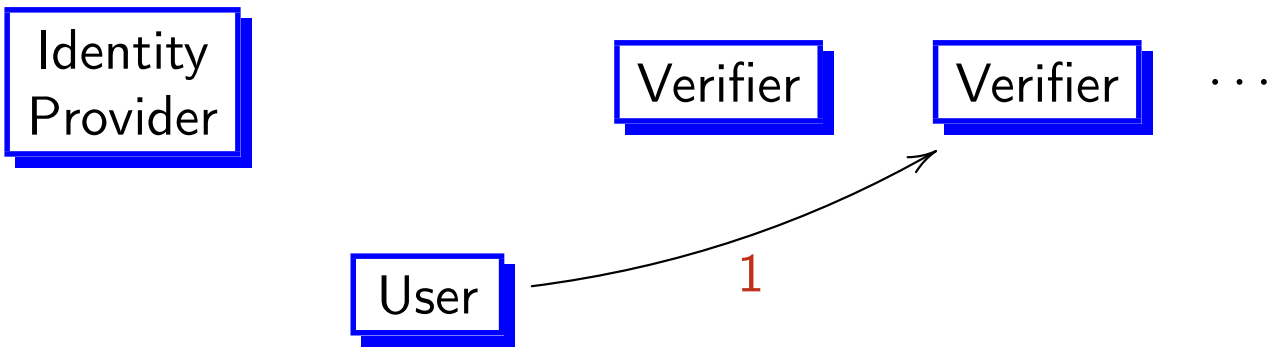


Decentralised: everyting goes via the User (think IRMA)

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)

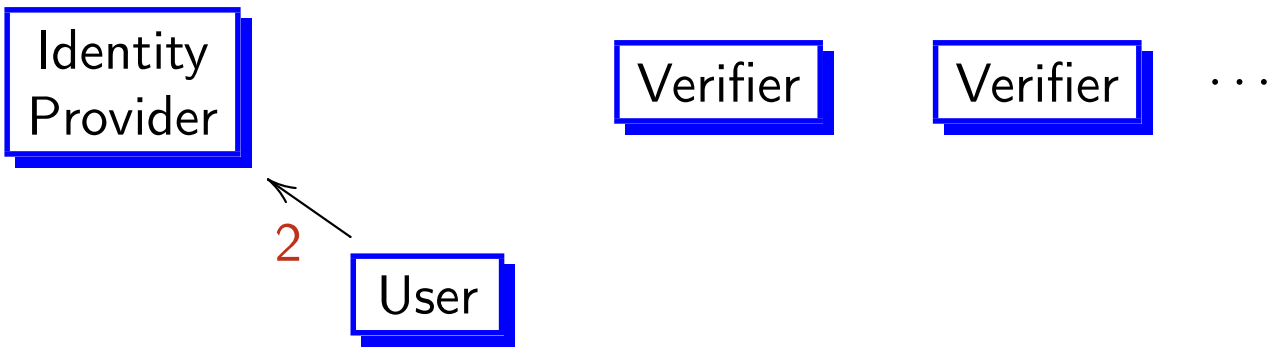


Decentralised: everyting goes via the User (think IRMA)

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)

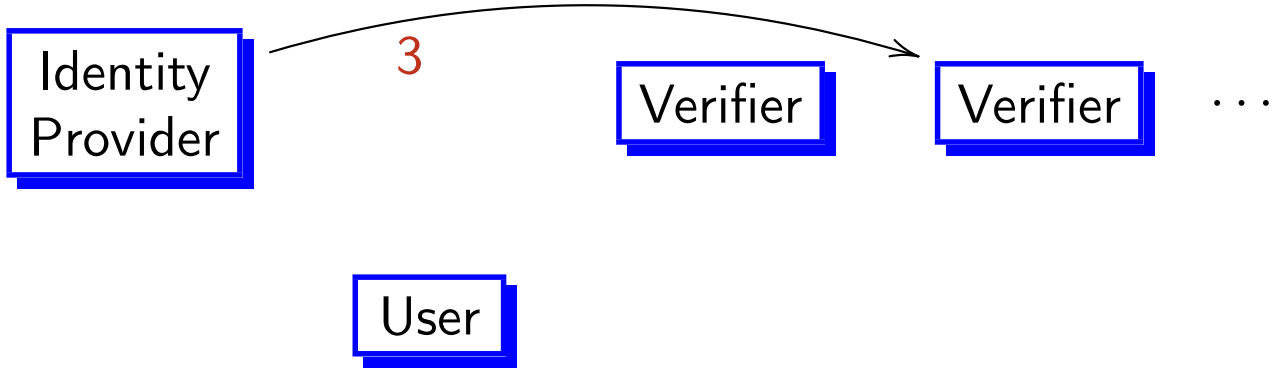


Decentralised: everyting goes via the User (think IRMA)

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)

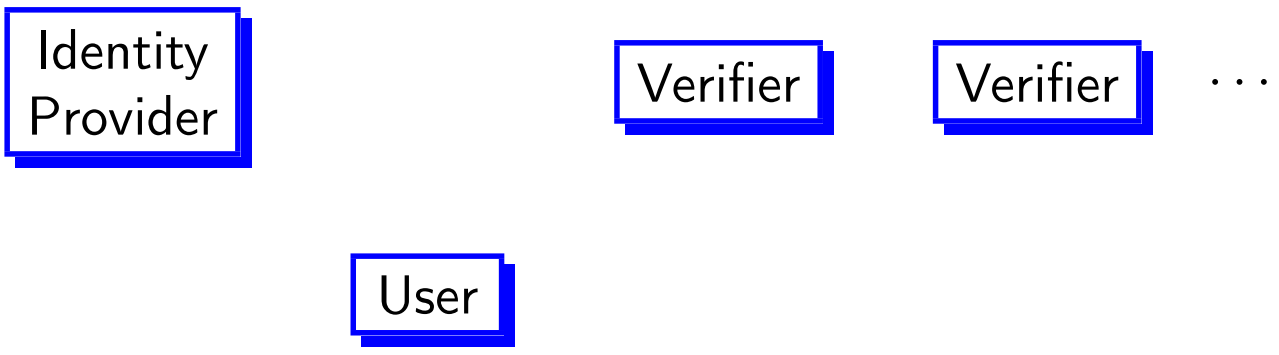


Decentralised: everyting goes via the User (think IRMA)

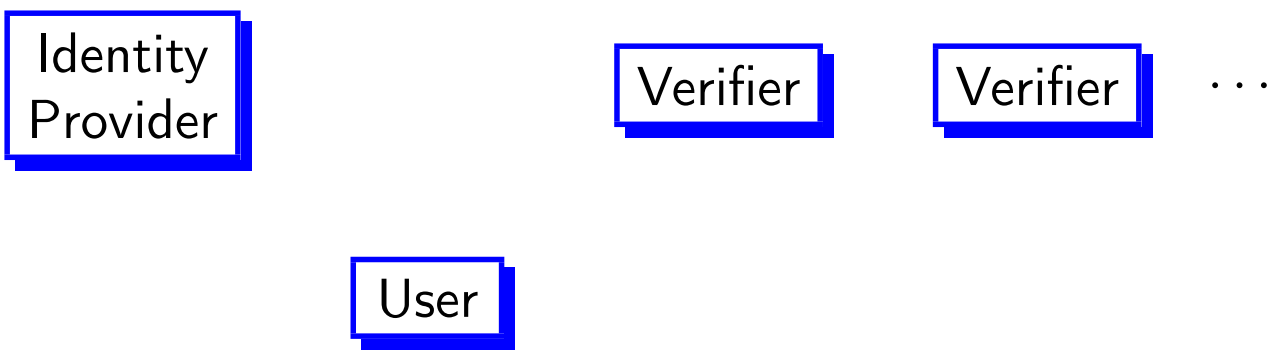
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)



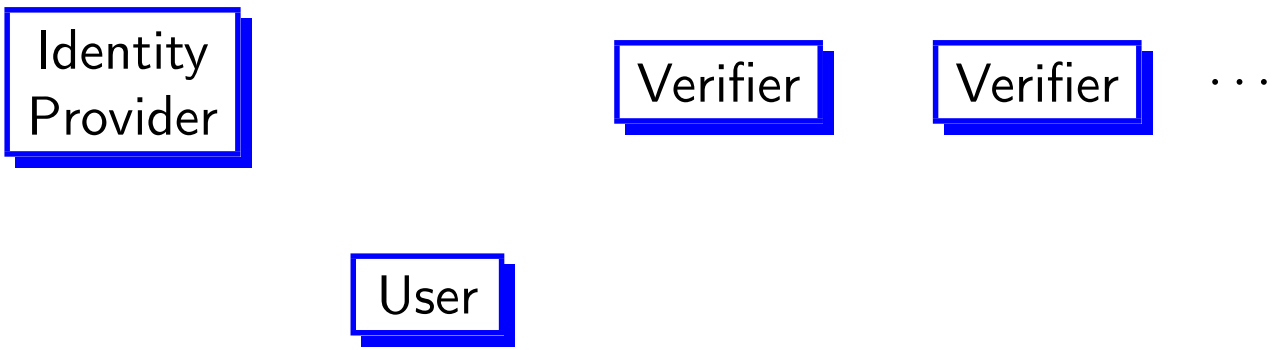
Decentralised: everyting goes via the User (think IRMA)



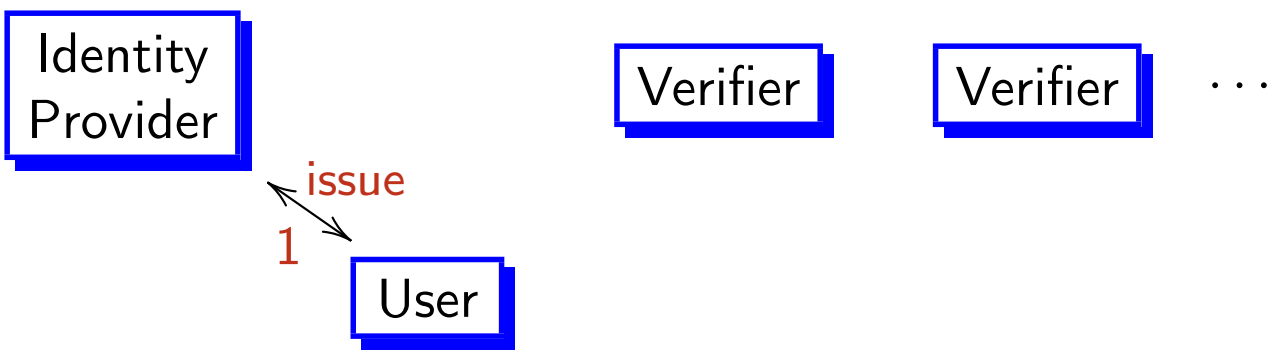
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)



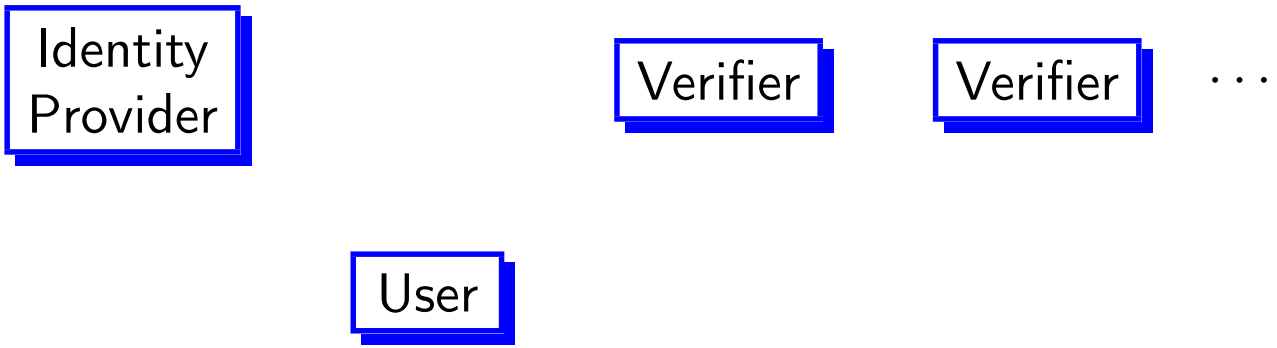
Decentralised: everyting goes via the User (think IRMA)



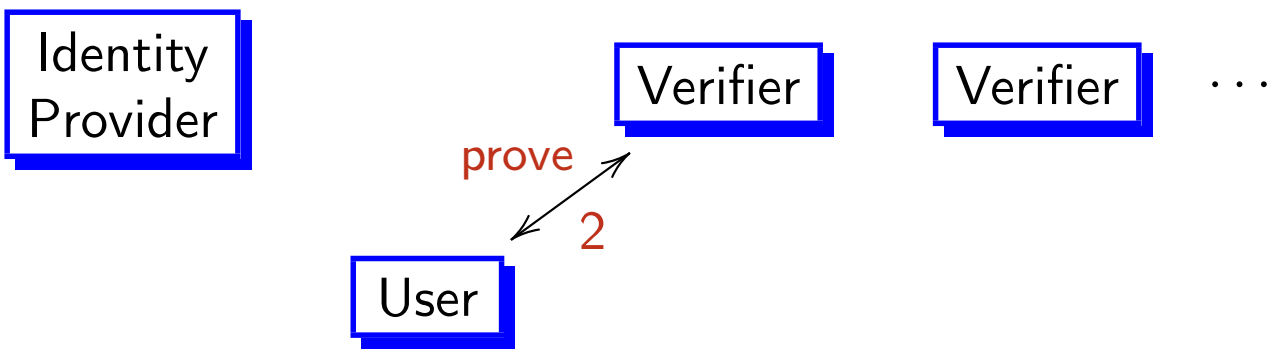
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)

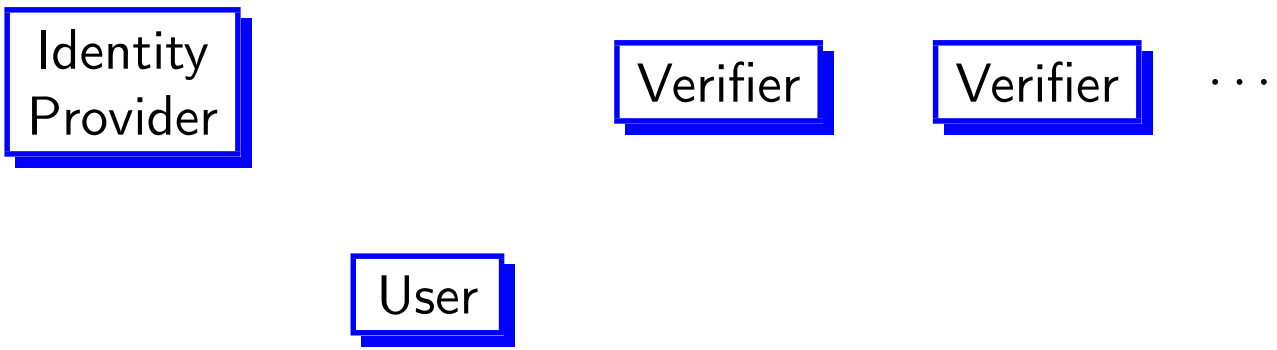


Decentralised: everyting goes via the User (think IRMA)

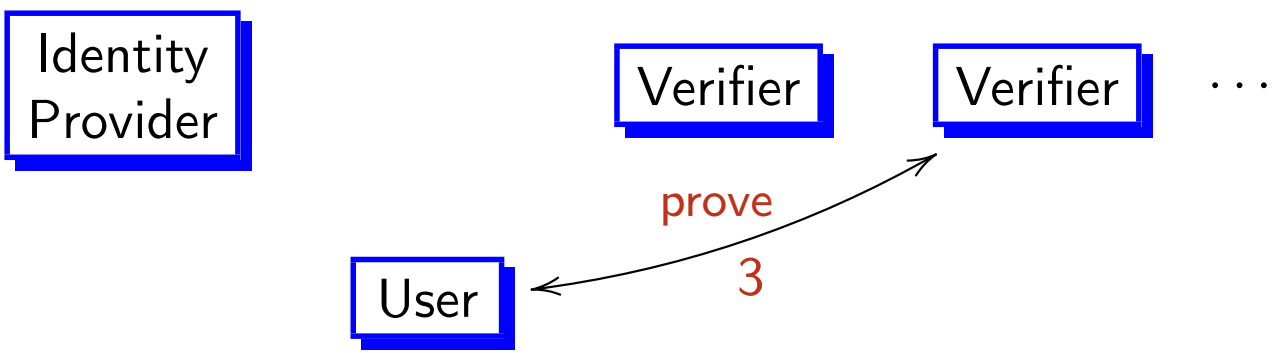


Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)



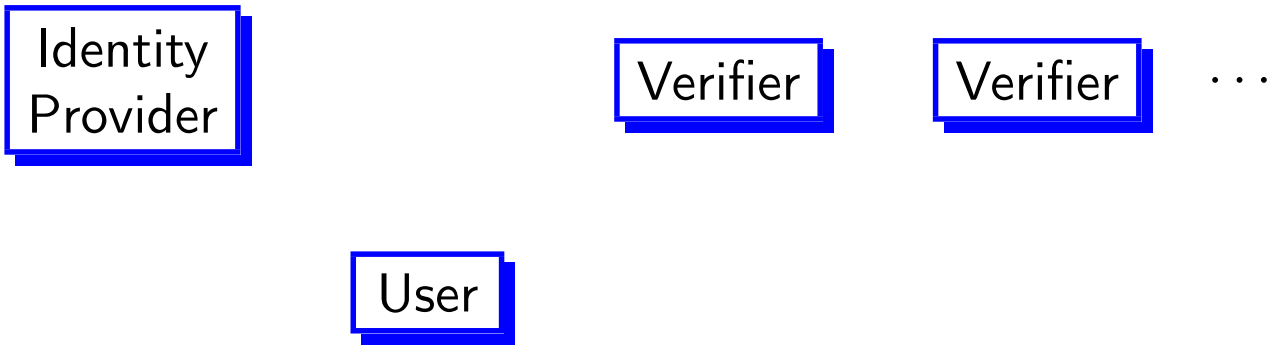
Decentralised: everyting goes via the User (think IRMA)



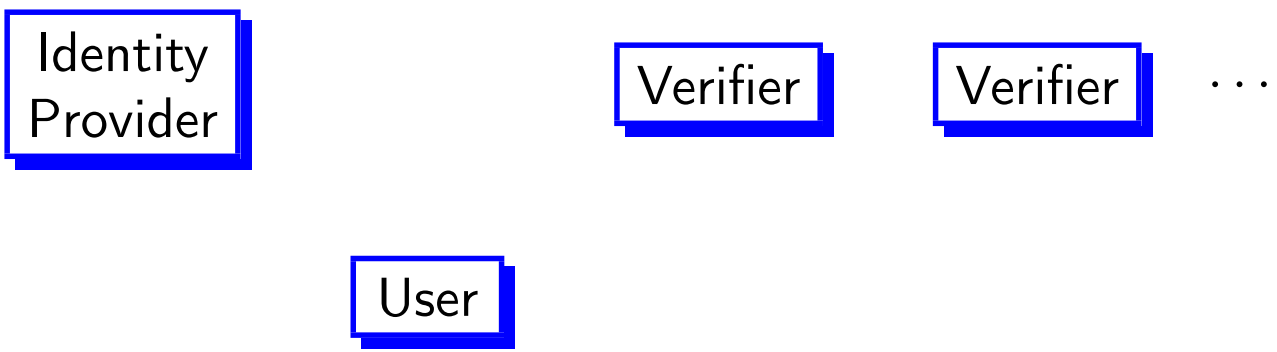
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)



Decentralised: everyting goes via the User (think IRMA)



Note: Data flows determine power relations in modern societies!

Problems with centralised architecture

Problems with centralised architecture

(1) Does centralisation satisfy privacy by design (GDPR art. 25)?
- privacy-friendly (decentralised) alternatives exist
- compliance question (with art. 25) lies on supervisors' plate

iCIS | Digital Security
Radboud University

Problems with centralised architecture

(1) Does centralisation satisfy privacy by design (GDPR art. 25)?
- privacy-friendly (decentralised) alternatives exist
- compliance question (with art. 25) lies on supervisors' plate

(2) The centralised architecture does not scale
- its privacy hotspot grows with every new set of attributes
- Belgium example:
  - Itsme is dominant login, run by banks & telecoms
  - it's centralised, users can be traced, their data is with Itsme
  - plans exist to add drivers licence data — must go to Itsme!!
  - discomfort and doubts are growing
  - problems get worse with diplomas, passport, vaccinations, ...

iCIS | Digital Security
Radboud University

Importance of open source software for wallet-ID

Importance of open source software for wallet-ID

(1) Classic arguments pro open source ("public money for public code")
- transparancy for public trust — like with covid apps
- reuse of code for avoiding vendor lock-in

iCIS | Digital Security
Radboud University

Importance of open source software for wallet-ID

(1) Classic arguments pro open source ("public money for public code")
- transparancy for public trust — like with covid apps
- reuse of code for avoiding vendor lock-in

(2) Geo-political arguments
- to keep big-tech out, esp. from US and CN
- to enable EU to embed EU values in software

iCIS | Digital Security
Radboud University

Importance of open source software for wallet-ID

(1) Classic arguments pro open source ("public money for public code")
- transparancy for public trust — like with covid apps
- reuse of code for avoiding vendor lock-in

(2) Geo-political arguments
- to keep big-tech out, esp. from US and CN
- to enable EU to embed EU values in software

(3) Supervision arguments
- open software gives (additional) incentive to comply
- transparancy of code makes compliance checking easier

iCIS | Digital Security
Radboud University

Supervision challenges with wallet-IDs

Supervision challenges with wallet-IDs

- How to prevent over-asking by verifiers (too many attributes)?
  - GDPR requires goal-binding and data-minimalisation
  - Ideally, goal-binding is part of the disclosure request
  - DPA's should get explicit role in wallet-IDs — and also budget

iCIS | Digital Security
Radboud University

Supervision challenges with wallet-IDs

- How to prevent over-asking by verifiers (too many attributes)?
  - GDPR requires goal-binding and data-minimalisation
  - Ideally, goal-binding is part of the disclosure request
  - DPA's should get explicit role in wallet-IDs — and also budget

- Are assurance levels and data-minimalisation linked?
  - My name may occur multiple times — certainly in IRMA
  - e.g. from trusted official source or from, say, LinkedIn (untrusted)
  - It is an overkill to request official name where nickname suffices
  - does data minimalisation requirement imply minimal assurance level, in disclosure requests?

iCIS | Digital Security
Radboud University

Main points

Main points

- EU wallet-ID can benefit from IRMA's practical experience
  - participation in case studies and reference implementation
- Open source benefits: regulatory, societally, geo-politically
- Decentralised architecture offers privacy-by-design and allows scaling to multiple attributes, without third-party privacy hotspots
- necessary DPA role against over-asking, for public trust

iCIS | Digital Security
Radboud University

Main points

- EU wallet-ID can benefit from IRMA's practical experience
  - participation in case studies and reference implementation
- Open source benefits: regulatory, societally, geo-politically
- Decentralised architecture offers privacy-by-design and allows scaling to multiple attributes, without third-party privacy hotspots
- necessary DPA role against over-asking, for public trust

Required additions to EU wallet plans

(1) Open source as requirement, not as option

(2) Decentralised architecture mandated.

iCIS | Digital Security
Radboud University