Privacy and Identity

Werkconferentie Nijmegen

Bart Jacobs — Radboud University and Privacy by Design foundation
bart@cs.ru.nl
March 12, 2018

iCIS | Digital Security
Radboud University

Dimensions of privacy

Dimensions of privacy

Privacy has many interacting dimensions, such as:

- **Legal**: what are the rules?
- **Ethical**: what do we see as right or wrong?
- **Technical**: how does privacy protection work (or fail)?

iCIS | Digital Security
Radboud University

Dimensions of privacy

Privacy has many interacting dimensions, such as:

- **Legal**: what are the rules?
- **Ethical**: what do we see as right or wrong?
- **Technical**: how does privacy protection work (or fail)?

Plan: briefly talk about privacy & identity, and at a concrete privacy-friendly identity platform IRMA.

iCIS | Digital Security
Radboud University

Dimensions of privacy

Privacy has many interacting dimensions, such as:

- **Legal**: what are the rules?
- **Ethical**: what do we see as right or wrong?
- **Technical**: how does privacy protection work (or fail)?

Plan: briefly talk about privacy & identity, and at a concrete privacy-friendly identity platform IRMA.

- it's value-driven design, connecting principles and solutions
- relevant values: self-sovereignty, transparancy, independence
- catch-phrase: contextual authentication
- governance is a interesting & challenging issue in itself

iCIS | Digital Security
Radboud University

Privacy is keeping information in context (Helen Nissenbaum)

Privacy is keeping information in context (Helen Nissenbaum)

- We naturally live in different contexts
  - home, work, sports club, in church, with friends . . .

Privacy is keeping information in context (Helen Nissenbaum)

- We naturally live in different contexts
  - home, work, sports club, in church, with friends ...
- We naturally want to keep information in context
  - what we tell to our doctor should not end up in a supermarket

Privacy is keeping information in context (Helen Nissenbaum)

- We naturally live in different contexts
  - home, work, sports club, in church, with friends ...
- We naturally want to keep information in context
  - what we tell to our doctor should not end up in a supermarket
- People get upset when contextual integrity is broken
  - recall anger: about selling customer financial data (ING), about speeding data ending up at the police (TomTom), about school children's performances in online tests ending up at publishers

iCIS | Digital Security
Radboud University

Privacy is keeping information in context (Helen Nissenbaum)

- We naturally live in different contexts
  - home, work, sports club, in church, with friends ...
- We naturally want to keep information in context
  - what we tell to our doctor should not end up in a supermarket
- People get upset when contextual integrity is broken
  - recall anger: about selling customer financial data (ING), about speeding data ending up at the police (TomTom), about school children's performances in online tests ending up at publishers
- When explained like this, almost everybody cares about privacy

iCIS | Digital Security
Radboud University

Privacy is keeping information in context (Helen Nissenbaum)

- We naturally live in different contexts
  - home, work, sports club, in church, with friends ...
- We naturally want to keep information in context
  - what we tell to our doctor should not end up in a supermarket
- People get upset when contextual integrity is broken
  - recall anger: about selling customer financial data (ING), about speeding data ending up at the police (TomTom), about school children's performances in online tests ending up at publishers
- When explained like this, almost everybody cares about privacy
- The Google's and Facebook's of this world make us use the same identifier everywhere or track us via Like  and cookies
  - they break-up contexts, and destroy our basic privacy intuitions
  - Mark Zuckerberg: "Having two identities for yourself is a lack of integrity" 

iCIS | Digital Security
Radboud University

Identity Management (IdM)

Identity Management (IdM)

IdM is an area of computer security dealing with o.a.

- **Technicalities** of identification, authentication, authortisation
- **Personalisation**, service adjustment to individual preferences
- **Provisioning**, *i.e.* automatic propagation of changes in identity data, esp. enroll, update, suspend, restore, remove
- **Tracking & tracing** in online scenarios

iCIS | Digital Security
Radboud University

Identity Management (IdM)

IdM is an area of computer security dealing with o.a.

- **Technicalities** of identification, authentication, authortisation
- **Personalisation**, service adjustment to individual preferences
- **Provisioning**, *i.e.* automatic propagation of changes in identity data, esp. enroll, update, suspend, restore, remove
- **Tracking & tracing** in online scenarios

Current trend

- using personal attributes for maximal flexibility
- self-sovereign identity: combining transparancy, fairness, support of the commons, protection for the individual

iCIS | Digital Security
Radboud University

Identity Management (IdM)

IdM is an area of computer security dealing with o.a.

- **Technicalities** of identification, authentication, authortisation
- **Personalisation**, service adjustment to individual preferences
- **Provisioning**, *i.e.* automatic propagation of changes in identity data, esp. enroll, update, suspend, restore, remove
- **Tracking & tracing** in online scenarios

Current trend

- using personal attributes for maximal flexibility
- self-sovereign identity: combining transparancy, fairness, support of the commons, protection for the individual

Challenge: self-sovereignty in a data-driven world

iCIS | Digital Security
Radboud University

Principles of identity management

Principles of identity management

- **Kim Cameron**'s 7 *Laws of Identity* (2005)

- Reformulated by **Christopher Allen** as 10 self-sovereign identity principles (2016)

iCIS | Digital Security
Radboud University

Principles of identity management

- **Kim Cameron**'s 7 *Laws of Identity* (2005)
  - See http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
  - the internet has been designed without "identity" in mind
  - this hampers many applications & has led to ad hoc solutions
- Reformulated by **Christopher Allen** as 10 self-sovereign identity principles (2016)

iCIS | Digital Security
Radboud University

Principles of identity management

- **Kim Cameron**'s 7 *Laws of Identity* (2005)
  - See http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
  - the internet has been designed without "identity" in mind
  - this hampers many applications & has led to ad hoc solutions
- Reformulated by **Christopher Allen** as 10 self-sovereign identity principles (2016)
  - See http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
  - often connected to *blockchains*: both unnecessary and unwise

iCIS | Digital Security
Radboud University

Principles of identity management

- **Kim Cameron**'s 7 *Laws of Identity* (2005)
  - See http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
  - the internet has been designed without "identity" in mind
  - this hampers many applications & has led to ad hoc solutions
- Reformulated by **Christopher Allen** as 10 self-sovereign identity principles (2016)
  - See http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
  - often connected to *blockchains*: both unnecessary and unwise

Common ground: self-control, data minimisation, transparancy, consent, interoperability, protection

iCIS | Digital Security
Radboud University

Principles of identity management

- **Kim Cameron**'s 7 *Laws of Identity* (2005)
  - See http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
  - the internet has been designed without "identity" in mind
  - this hampers many applications & has led to ad hoc solutions
- Reformulated by **Christopher Allen** as 10 self-sovereign identity principles (2016)
  - See http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
  - often connected to *blockchains*: both unnecessary and unwise

Common ground: self-control, data minimisation, transparancy, consent, interoperability, protection

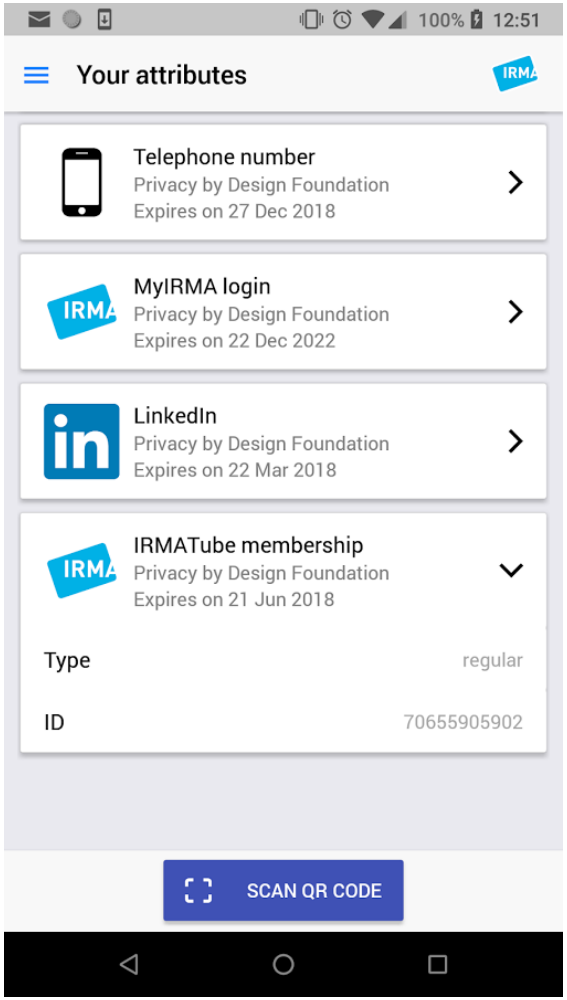
Experience: business-based solutions are not sufficiently trusted to become universal; they put too much emphasis on the privatisation of information and the modeling of users as consumers

iCIS | Digital Security
Radboud University

IRMA basics: reveal only relevant attributes

iCIS | Digital Security
Radboud University

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

iCIS | Digital Security
Radboud University

IRMA history, in two phases

IRMA history, in two phases

- **2008 – now**: scientific research project at Radboud University

- **2016 – now**: technology deployment via non-profit foundation

iCIS | Digital Security
Radboud University

IRMA history, in two phases

- **2008 – now**: scientific research project at Radboud University
  - active research line on attribute-based authentication (via Idemix)
  - 3 PhD theses so far, postdocs too, many publications
  - financial support from: NLnet, Translink, BZK, NWO, KPN
  - prototype implementations on:
    - smart card — at first, but no longer supported
    - smart phone — for Android only

- **2016 – now**: technology deployment via non-profit foundation

iCIS | Digital Security
Radboud University

IRMA history, in two phases

- **2008 – now**: scientific research project at Radboud University
  - active research line on attribute-based authentication (via Idemix)
  - 3 PhD theses so far, postdocs too, many publications
  - financial support from: NLnet, Translink, BZK, NWO, KPN
  - prototype implementations on:
    - smart card — at first, but no longer supported
    - smart phone — for Android only

- **2016 – now**: technology deployment via non-profit foundation
  - https://privacybydesign.foundation set up in fall 2016
  - foundation runs infrastructure, and issues attributes
  - eg. from: iDIN (banks), SURFconext (academia), BIG (health)
  - both Android and iOS apps, with common code-base in **Go**
  - attribute verification pilots are emerging
  - attribute-based signatures will be added soon

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised versus decentralised, schematically

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

Decentralised: everyting goes via the User (think IRMA)

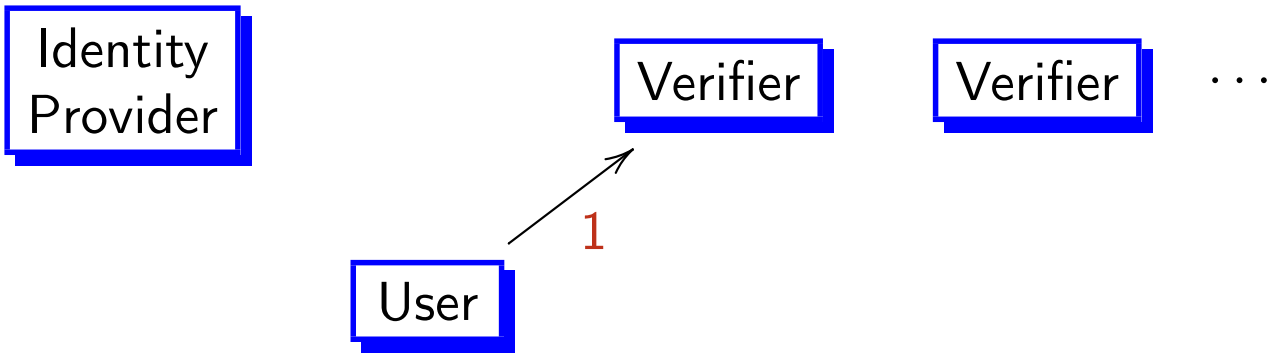
Centralised versus decentralised, schematically

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

Decentralised: everyting goes via the User (think IRMA)

Centralised versus decentralised, schematically

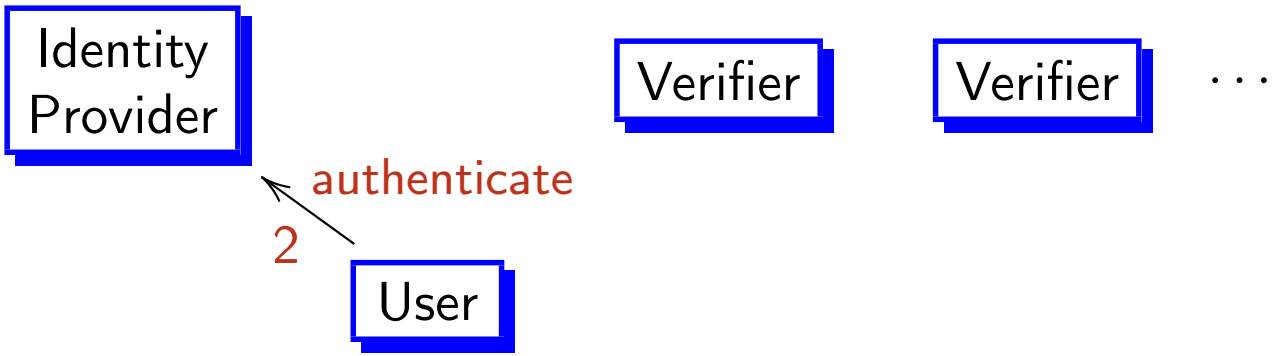
Centralised: everything goes via the Identity Provider (think iDIN)



Decentralised: everyting goes via the User (think IRMA)

Centralised versus decentralised, schematically

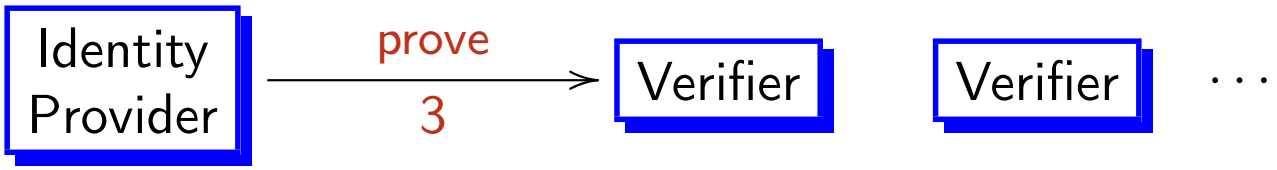
Centralised: everything goes via the Identity Provider (think iDIN)



Decentralised: everyting goes via the User (think IRMA)

Centralised versus decentralised, schematically

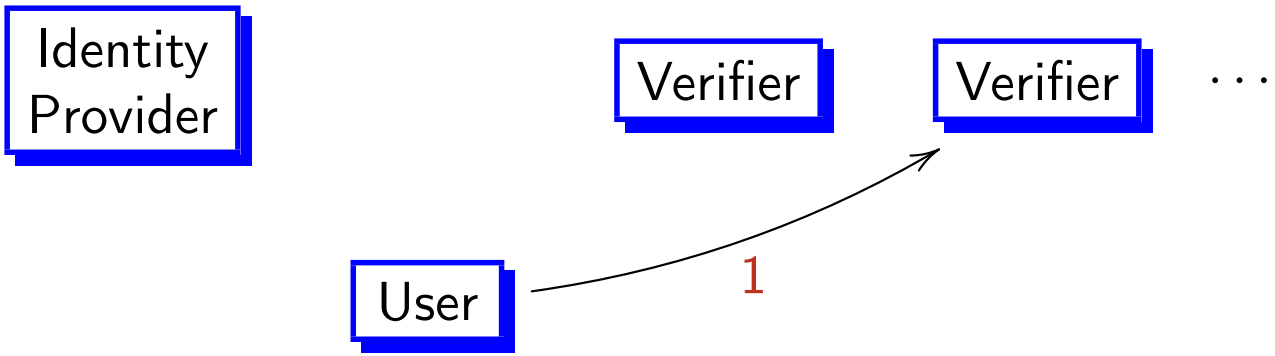
Centralised: everything goes via the Identity Provider (think iDIN)



Decentralised: everyting goes via the User (think IRMA)

Centralised versus decentralised, schematically

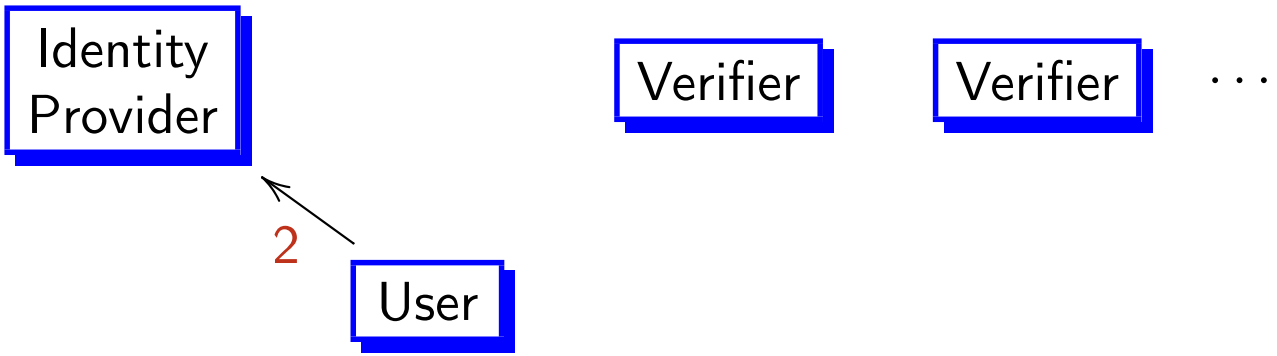
Centralised: everything goes via the Identity Provider (think iDIN)



Decentralised: everyting goes via the User (think IRMA)

Centralised versus decentralised, schematically

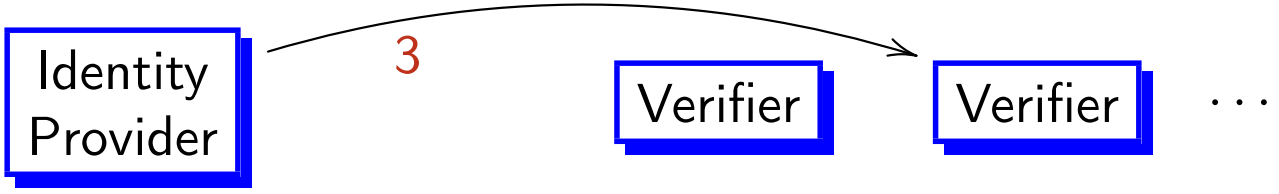
Centralised: everything goes via the Identity Provider (think iDIN)



Decentralised: everyting goes via the User (think IRMA)

Centralised versus decentralised, schematically

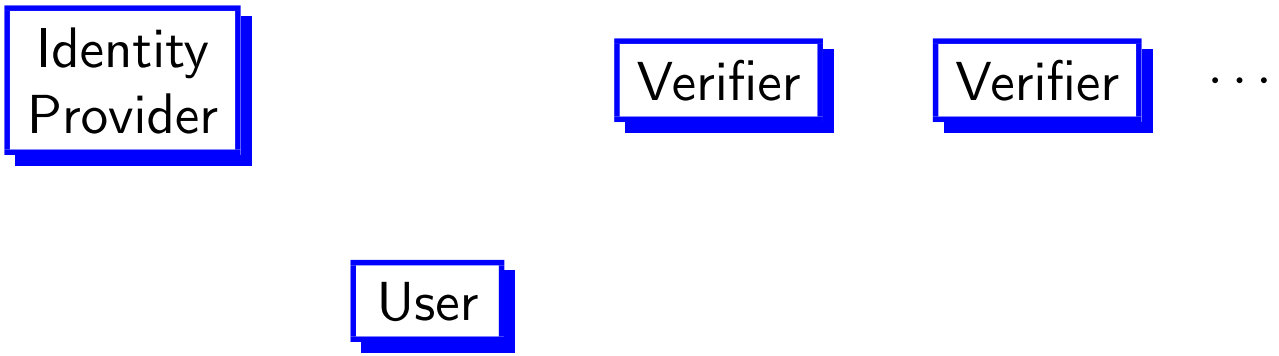
Centralised: everything goes via the Identity Provider (think iDIN)



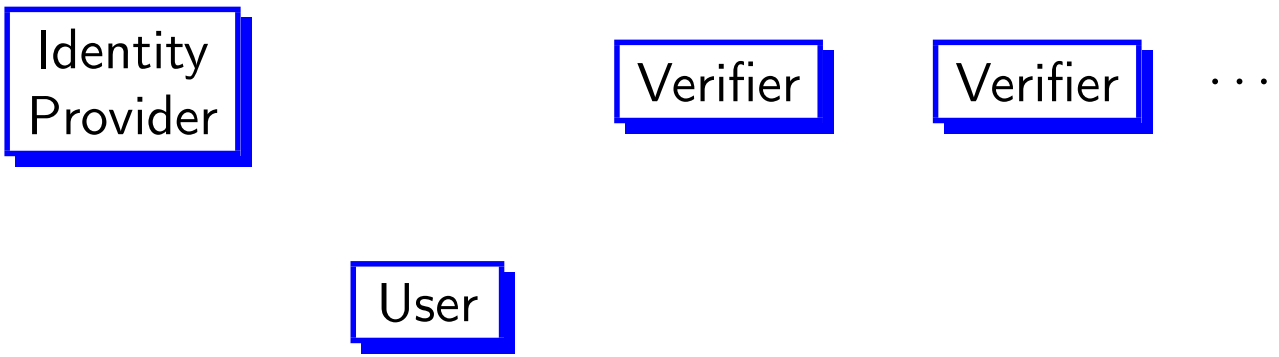
Decentralised: everyting goes via the User (think IRMA)

Centralised versus decentralised, schematically

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

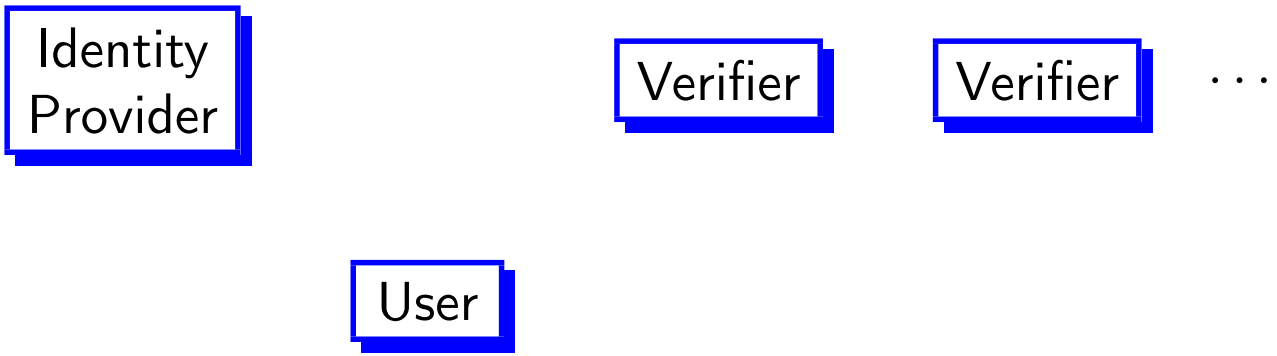


Decentralised: everyting goes via the User (think IRMA)

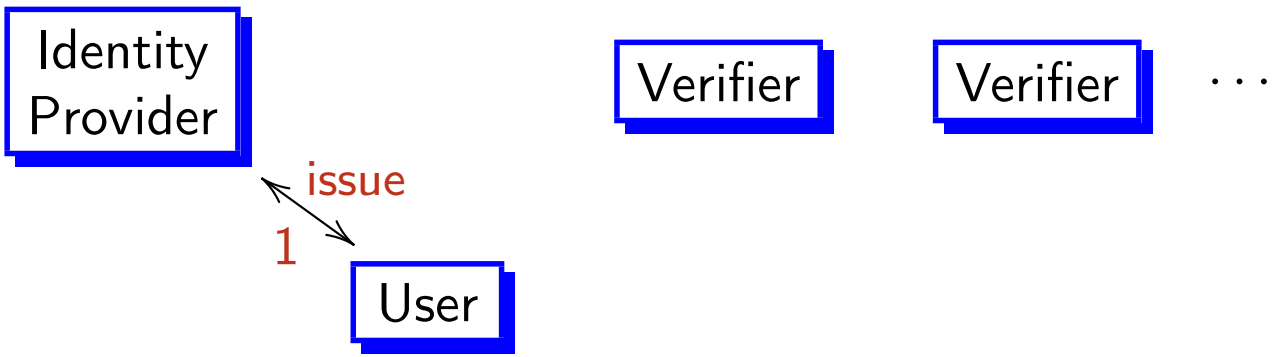


Centralised versus decentralised, schematically

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



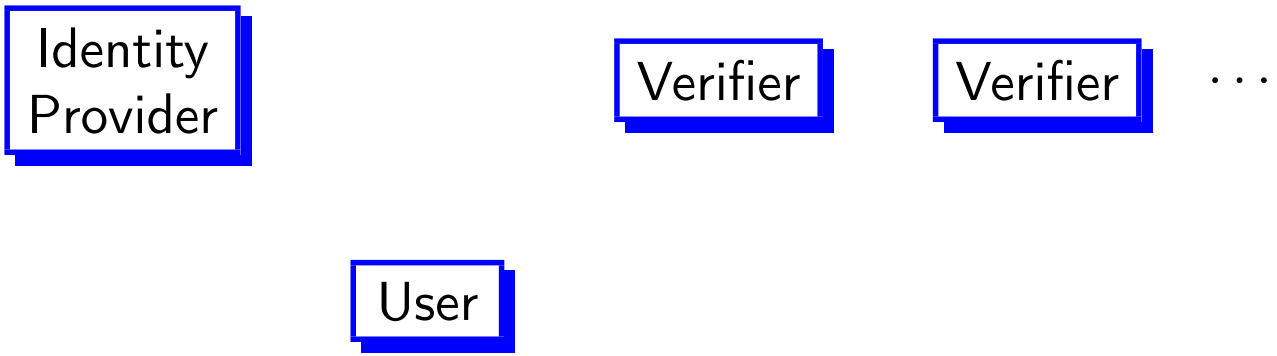
Decentralised: everyting goes via the User (think IRMA)



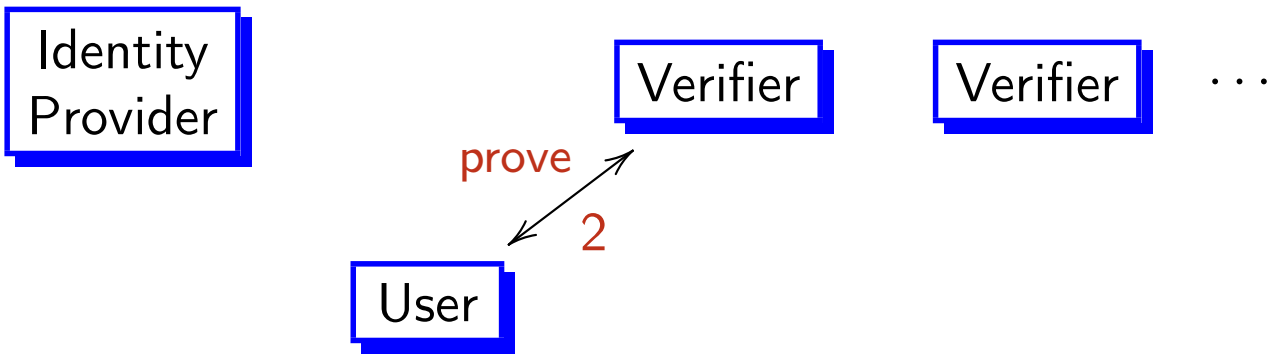
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

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



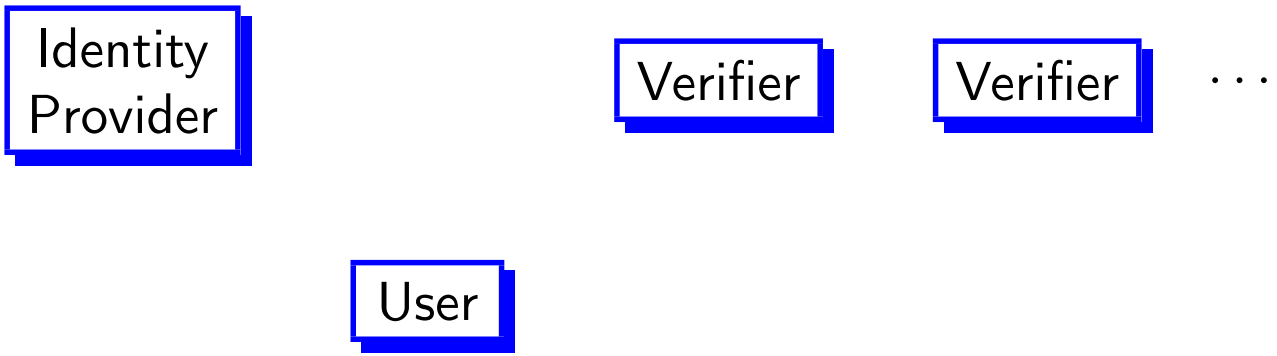
Decentralised: everyting goes via the User (think IRMA)



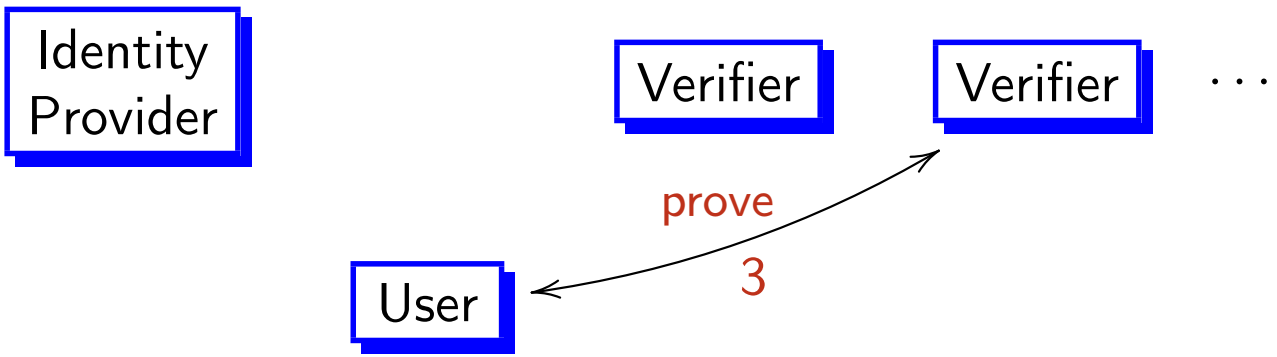
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

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



Decentralised: everyting goes via the User (think IRMA)



iCIS | Digital Security
Radboud University

Main points

Main points

- Information flows and authentication requirements determine power relations in modern societies

Main points

- Information flows and authentication requirements determine power relations in modern societies
- The choice of authentication architecture is extremely sensitive
  - substantial differences exist between central and decentral
  - power and (financial) control are key in the central approach
  - privacy and autonomy are leading values in the decentral one

  What kind of society do we prefer to live in?

iCIS | Digital Security
Radboud University

Main points

- Information flows and authentication requirements determine power relations in modern societies
- The choice of authentication architecture is extremely sensitive
  - substantial differences exist between central and decentral
  - power and (financial) control are key in the central approach
  - privacy and autonomy are leading values in the decentral one

  What kind of society do we prefer to live in?
- IRMA is a decentralised, open source, non-profit, flexible system that is up and running, and being tested by various parties
  - it provides privacy-friendly empowerment of users
  - now organised and run by non-profit foundation

iCIS | Digital Security
Radboud University

Main points

- Information flows and authentication requirements determine power relations in modern societies
- The choice of authentication architecture is extremely sensitive
  - substantial differences exist between central and decentral
  - power and (financial) control are key in the central approach
  - privacy and autonomy are leading values in the decentral one

  What kind of society do we prefer to live in?
- IRMA is a decentralised, open source, non-profit, flexible system that is up and running, and being tested by various parties
  - it provides privacy-friendly empowerment of users
  - now organised and run by non-profit foundation

Interested? Follow twitter.com/IRMA_privacy

iCIS | Digital Security
Radboud University