eID-developments

PI.lab dag, 11 dec, 2015

Bart Jacobs
bart@cs.ru.nl
11 dec. 2015

iCIS | Digital Security
Radboud University

Outline

iCIS | Digital Security
Radboud University

Where we are, sofar

Background

Background

- The NL government is in the process of introducing a new national electronic identity — abbreviated as eID
  - the system is called Idensys

iCIS | Digital Security
Radboud University

Background

- The NL government is in the process of introducing a new national electronic identity — abbreviated as eID
  - the system is called Idensys
- A Privacy Impact Assement (PIA) of Idensys has appeared
  - written by consultancy firm *Mazars*
  - to be precise: the PIA is from july'15, about Idensys 0.8

iCIS | Digital Security
Radboud University

Background

- The NL government is in the process of introducing a new national electronic identity — abbreviated as eID
  - the system is called Idensys
- A Privacy Impact Assement (PIA) of Idensys has appeared
  - written by consultancy firm *Mazars*
  - to be precise: the PIA is from july'15, about Idensys 0.8
- The current speaker has published a PI.lab blog about this
  - the title is: "An Assessment of a Privacy Impact Assessment: Idensys under review" — but the text is in Dutch

pilab.nl/index.php/2015/11/09/
an-assessment-of-a-privacy-impact-assessment-idensys-under-review/
?lang=nl

iCIS | Digital Security
Radboud University

Background

- The NL government is in the process of introducing a new national electronic identity — abbreviated as eID
  - the system is called Idensys
- A Privacy Impact Assement (PIA) of Idensys has appeared
  - written by consultancy firm *Mazars*
  - to be precise: the PIA is from july'15, about Idensys 0.8
- The current speaker has published a PI.lab blog about this
  - the title is: "An Assessment of a Privacy Impact Assessment: Idensys under review" — but the text is in Dutch

pilab.nl/index.php/2015/11/09/an-assessment-of-a-privacy-impact-assessment-idensys-under-review/?lang=nl

  - Not everyone was amused . . . especially not by the (harsh) tone

iCIS | Digital Security
Radboud University

One-page summary of the blog

One-page summary of the blog

- eID-topic has been hijacked by the Ministry of Economic Affairs
  - the basis of Idensys is e-Herkenning, an existing system for authentication between companies, giving non-privacy by design
  - commercial interests of a few companies are leading
  - privacy parlance is empty ritual

One-page summary of the blog

- eID-topic has been hijacked by the Ministry of Economic Affairs
  - the basis of Idensys is e-Herkenning, an existing system for authentication between companies, giving non-privacy by design
  - commercial interests of a few companies are leading
  - privacy parlance is empty ritual
- Idensys does not even satisfy its own requirements
  - interoperability does not exist, via differences of pseudonyms
  - crucial claims like end-to-end-encryption are false & misleading
  - intermediate parties can monitor and charge every transaction

iCIS | Digital Security
Radboud University

One-page summary of the blog

- eID-topic has been hijacked by the Ministry of Economic Affairs
  - the basis of Idensys is e-Herkenning, an existing system for authentication between companies, giving non-privacy by design
  - commercial interests of a few companies are leading
  - privacy parlance is empty ritual
- Idensys does not even satisfy its own requirements
  - interoperability does not exist, via differences of pseudonyms
  - crucial claims like end-to-end-encryption are false & misleading
  - intermediate parties can monitor and charge every transaction
- PIA has prominent positive conclusions; critique is hidden
  - privacy hotspots are recognised, but this is "the best possible"
  - false security claims are not exposed

One-page summary of the blog

- eID-topic has been hijacked by the Ministry of Economic Affairs
  - the basis of Idensys is e-Herkenning, an existing system for authentication between companies, giving non-privacy by design
  - commercial interests of a few companies are leading
  - privacy parlance is empty ritual
- Idensys does not even satisfy its own requirements
  - interoperability does not exist, via differences of pseudonyms
  - crucial claims like end-to-end-encryption are false & misleading
  - intermediate parties can monitor and charge every transaction
- PIA has prominent positive conclusions; critique is hidden
  - privacy hotspots are recognised, but this is "the best possible"
  - false security claims are not exposed
- The blog calls for a comparison between centralised and decentralised architectures — as a basis for a conscious choice

Where we are, sofar

Important underlying architectural choice

Important underlying architectural choice

Where is identity information of users stored?

- **centralised**: under control of intermediate parties
- **decentralised**: under control of the users

iCIS | Digital Security
Radboud University

Important underlying architectural choice

Where is identity information of users stored?

- **centralised**: under control of intermediate parties
- **decentralised**: under control of the users

Two concrete realisation of these architectures:

- centralised: Idensys
- decentralised: IRMA

iCIS | Digital Security
Radboud University

Important underlying architectural choice

Where is identity information of users stored?

- **centralised**: under control of intermediate parties
- **decentralised**: under control of the users

Two concrete realisation of these architectures:

- centralised: Idensys
- decentralised: IRMA

Our aim is to give a conceptual analysis of the two architectures — and not to go into the details

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider

Decentralised: everyting goes via the User

iCIS | Digital Security
Radboud University

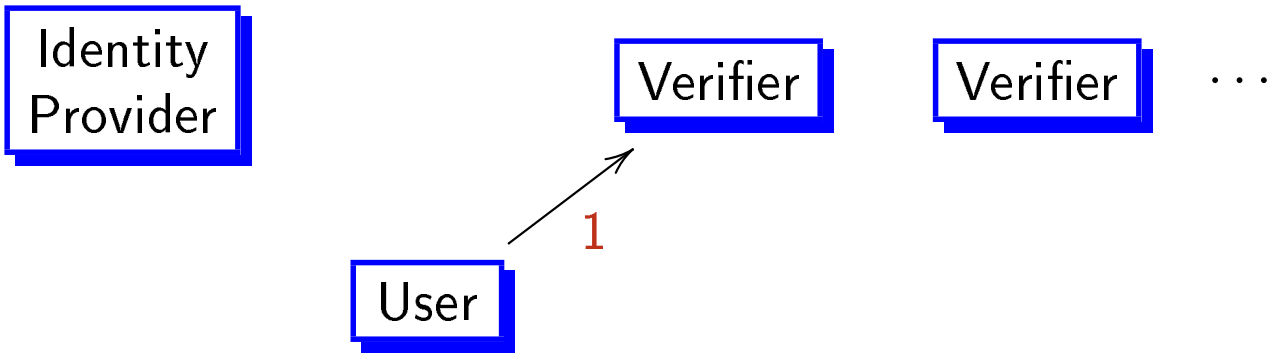
Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider

Decentralised: everyting goes via the User

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider

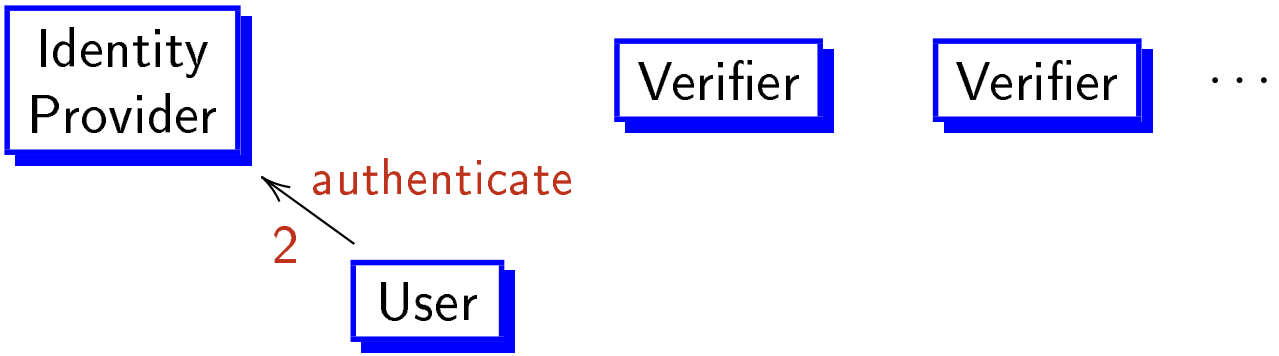


Decentralised: everyting goes via the User

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider

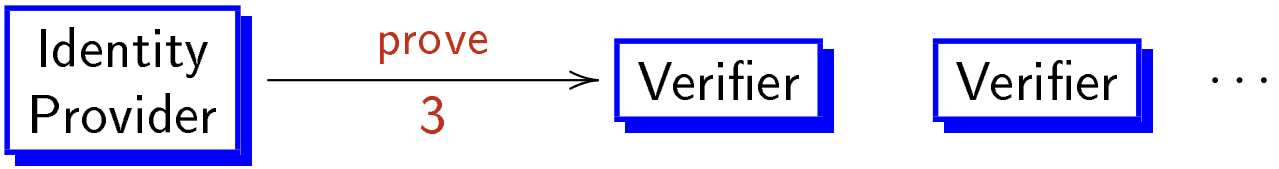


Decentralised: everyting goes via the User

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

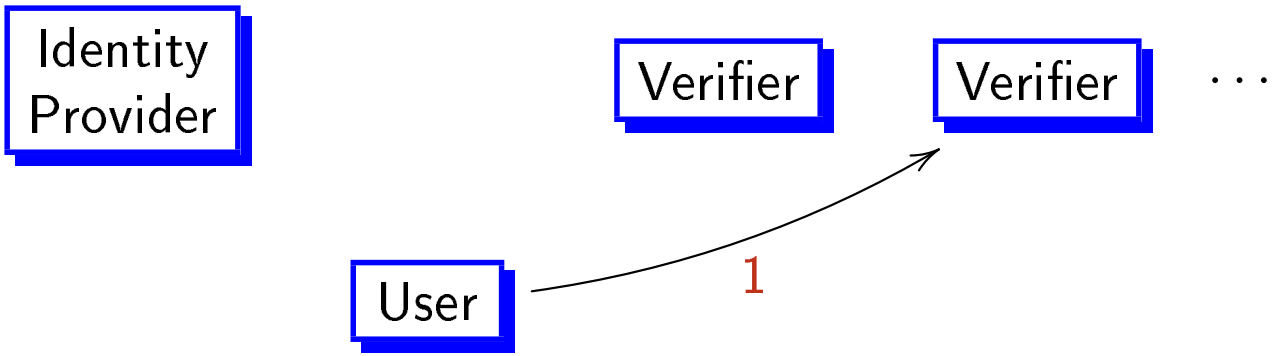
Centralised: everything goes via the Identity Provider



Decentralised: everyting goes via the User

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider

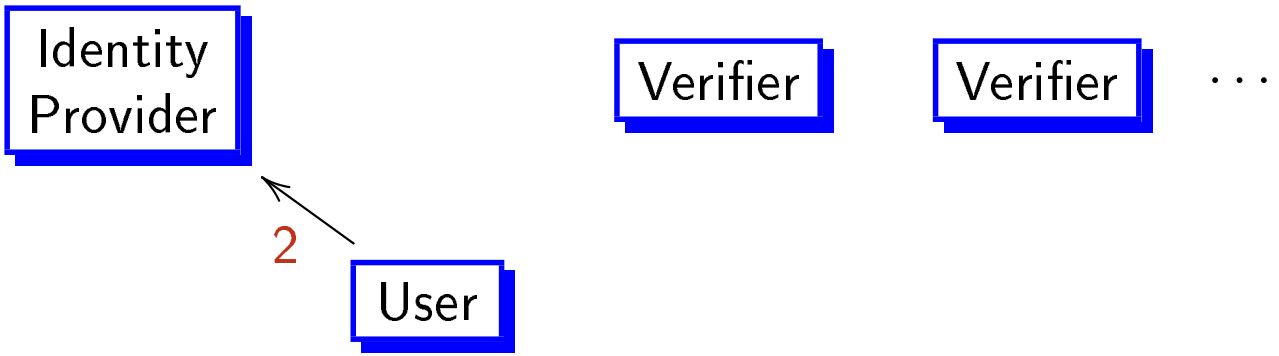


Decentralised: everyting goes via the User

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider

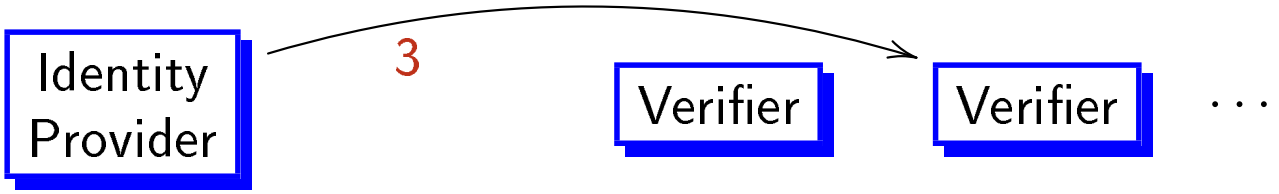


Decentralised: everyting goes via the User

iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider

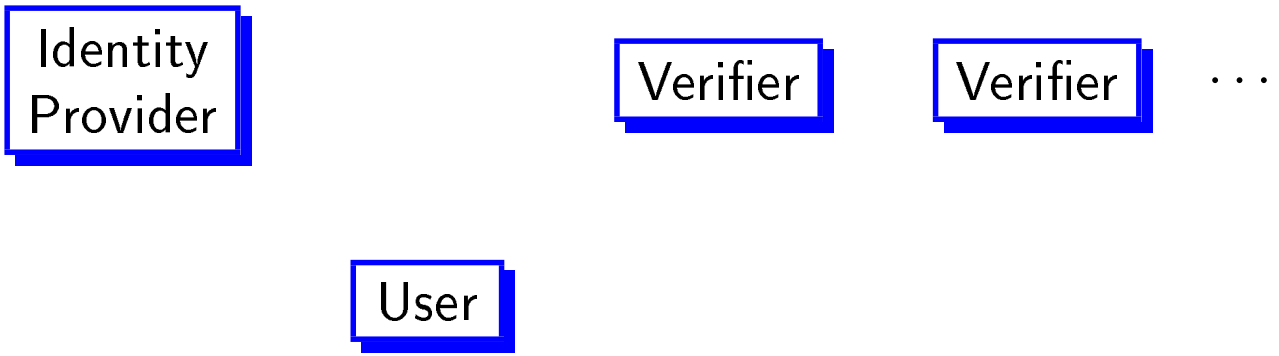


Decentralised: everyting goes via the User

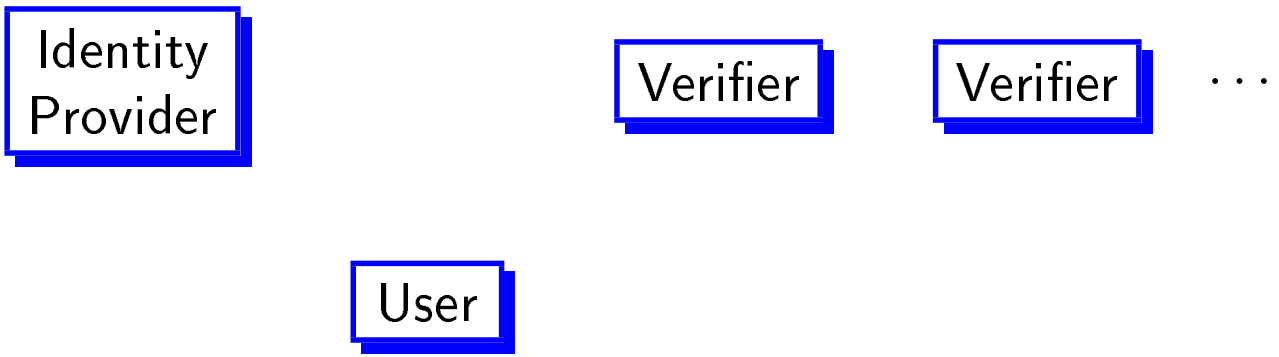
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider



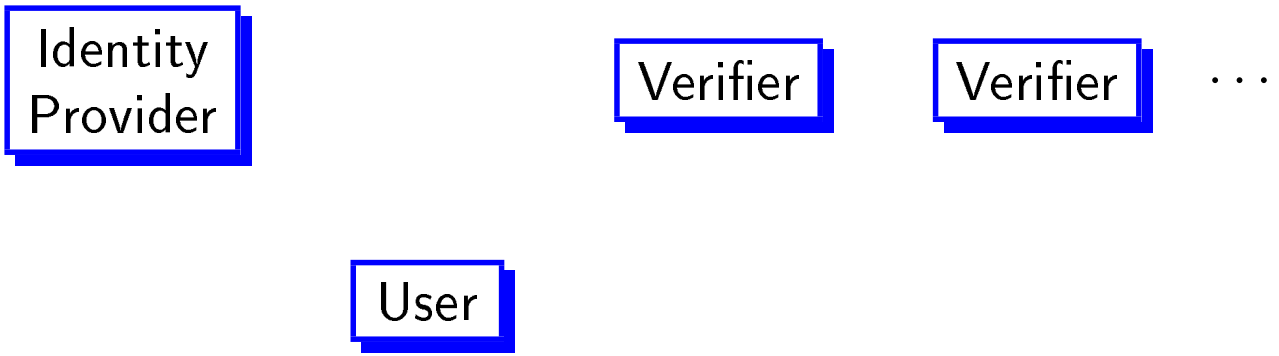
Decentralised: everyting goes via the User



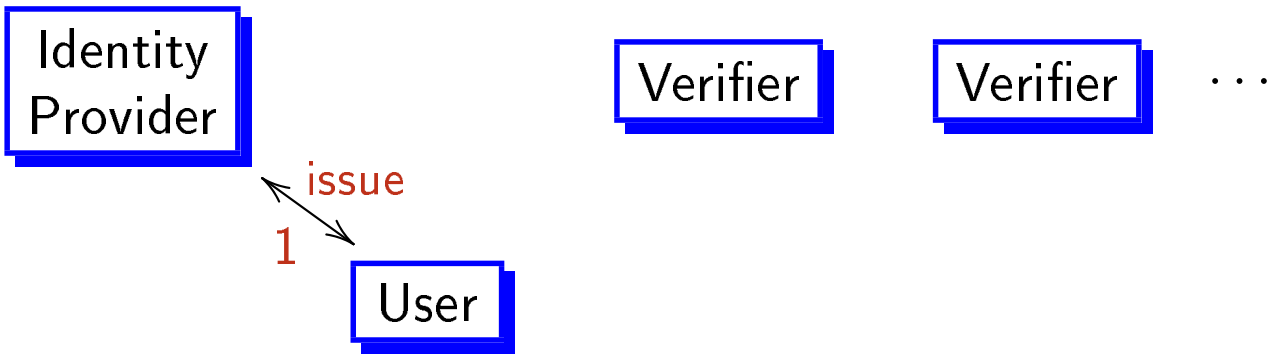
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider



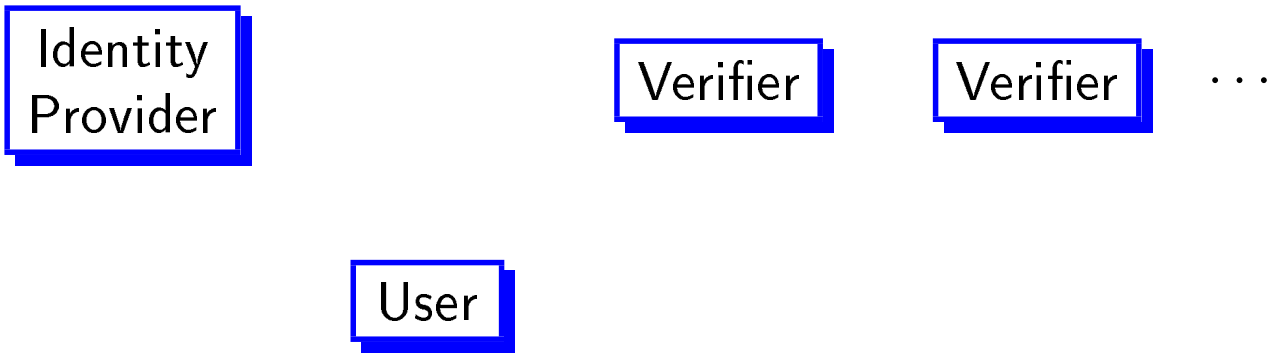
Decentralised: everyting goes via the User



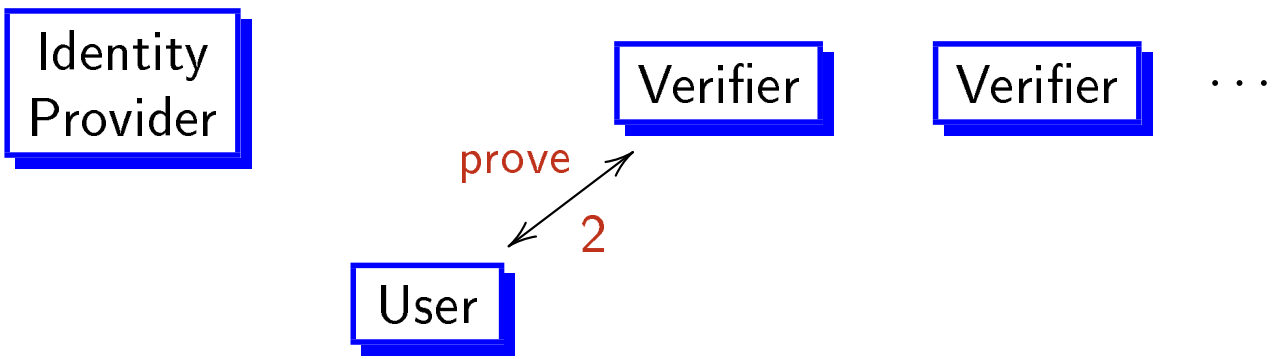
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider



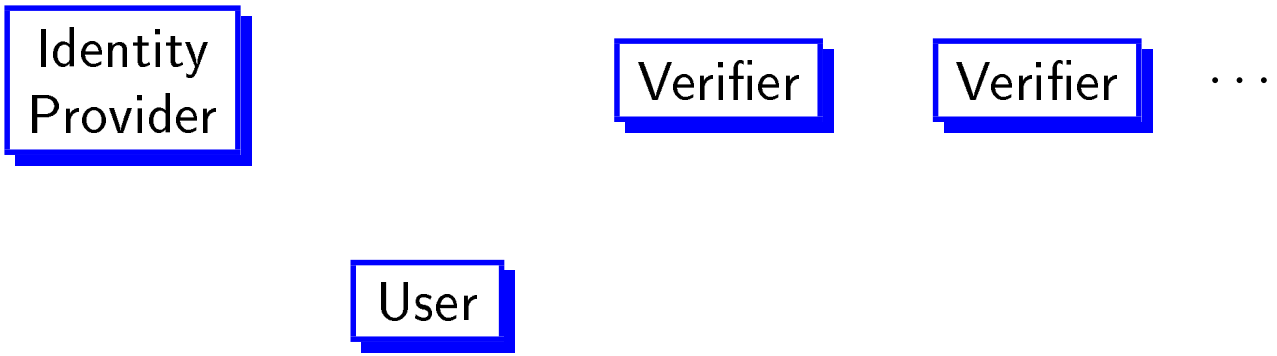
Decentralised: everyting goes via the User



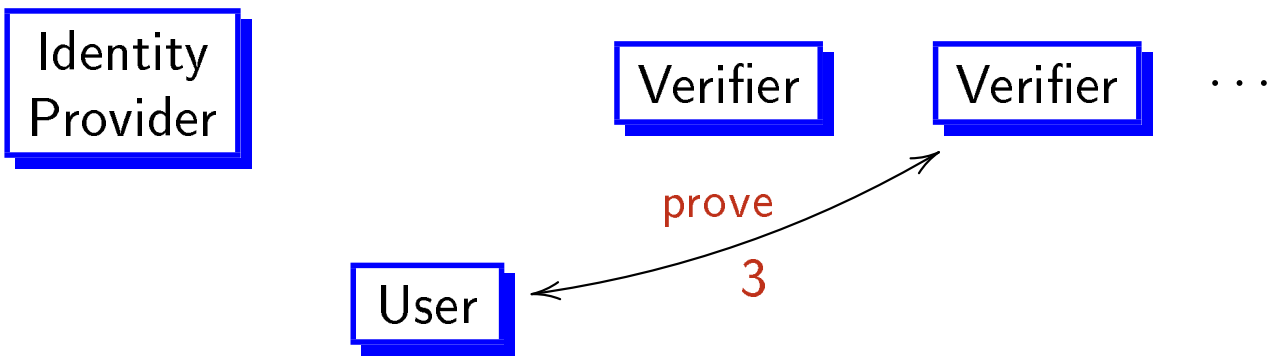
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider



Decentralised: everyting goes via the User



iCIS | Digital Security
Radboud University

Observation I

Observation I

The centralised approach reduces users to authenticators

Observation I

The centralised approach reduces users to authenticators

- The underlying idea is: you only have to prove who you are, we know all the rest and will handle all your contacts

iCIS | Digital Security
Radboud University

Observation I

The centralised approach reduces users to authenticators

- The underlying idea is: you only have to prove who you are, we know all the rest and will handle all your contacts
  - the blog speaks of a pimp architecture

iCIS | Digital Security
Radboud University

Observation I

The centralised approach reduces users to authenticators

- The underlying idea is: you only have to prove who you are, we know all the rest and will handle all your contacts
  - the blog speaks of a pimp architecture
  - alternative framing: a concierge who exlusively owns all keys of a building: only he can let you into an appartment

iCIS | Digital Security
Radboud University

Observation I

The centralised approach reduces users to authenticators

- The underlying idea is: you only have to prove who you are, we know all the rest and will handle all your contacts
  - the blog speaks of a pimp architecture
  - alternative framing: a concierge who exlusively owns all keys of a building: only he can let you into an appartment
- These central parties thus know everything, in two forms:
  - they know all your properties, which they can show to verifiers
  - they know where you go when

iCIS | Digital Security
Radboud University

Observation I

The centralised approach reduces users to authenticators

- The underlying idea is: you only have to prove who you are, we know all the rest and will handle all your contacts
  - the blog speaks of a pimp architecture
  - alternative framing: a concierge who exlusively owns all keys of a building: only he can let you into an appartment
- These central parties thus know everything, in two forms:
  - they know all your properties, which they can show to verifiers
  - they know where you go when
- Moreover, the central parties can also act on user's behalve
  - authenticity and integrity of messages to verifiers is problematic

iCIS | Digital Security
Radboud University

Observation I

The centralised approach reduces users to authenticators

- The underlying idea is: you only have to prove who you are, we know all the rest and will handle all your contacts
  - the blog speaks of a pimp architecture
  - alternative framing: a concierge who exlusively owns all keys of a building: only he can let you into an appartment
- These central parties thus know everything, in two forms:
  - they know all your properties, which they can show to verifiers
  - they know where you go when
- Moreover, the central parties can also act on user's behalve
  - authenticity and integrity of messages to verifiers is problematic
- Authentication devices for users can be simple

Observation II

Observation II

The decentralised approach imposes responsabilities on users

iCIS | Digital Security
Radboud University

Observation II

The decentralised approach imposes responsabilities on users

- Users have to collect and maintain all identity information

iCIS | Digital Security
Radboud University

Observation II

The decentralised approach imposes responsabilities on users

- Users have to collect and maintain all identity information
- They will have to use more complicated authentication devices

iCIS | Digital Security
Radboud University

Observation II

The decentralised approach imposes responsabilities on users

- Users have to collect and maintain all identity information
- They will have to use more complicated authentication devices
  - but these devices can perform truely end-to-end security
  - that is, between user and verifier
    (and not just between pimp and verifier, like in Idensys)

iCIS | Digital Security
Radboud University

Observation II

The decentralised approach imposes responsabilities on users

- Users have to collect and maintain all identity information
- They will have to use more complicated authentication devices
  - but these devices can perform truely end-to-end security
  - that is, between user and verifier
    (and not just between pimp and verifier, like in Idensys)
- Users will have to re-construct their identity information in case of loss, theft, or renewal of these devices
  - they will also have to revoke the data on their old device

iCIS | Digital Security
Radboud University

Observation III

Observation III

The centralised parties are über-powerful hotspots

iCIS | Digital Security
Radboud University

Observation III

The centralised parties are über-powerful hotspots

- They are informational hotspots
  - they control and monitor all information flows
  - they can profile users, for anomaly detection and for commercial reasons (advertisement, price discrimination, . . .)

iCIS | Digital Security
Radboud University

Observation III

The centralised parties are über-powerful hotspots

- They are informational hotspots
  - they control and monitor all information flows
  - they can profile users, for anomaly detection and for commercial reasons (advertisement, price discrimination, . . .)
- They are financial hotspots
  - they can charge users for authentication devices and services
  - they can charge verifiers for each authentication transaction

iCIS | Digital Security
Radboud University

Observation III

The centralised parties are über-powerful hotspots

- They are informational hotspots
  - they control and monitor all information flows
  - they can profile users, for anomaly detection and for commercial reasons (advertisement, price discrimination, . . .)
- They are financial hotspots
  - they can charge users for authentication devices and services
  - they can charge verifiers for each authentication transaction
- The dream-position for the information giants of the world
  - think of Baidu, Google, Facebook etc. in such a role
  - the fear of verifiers, as expressed by bol.com

iCIS | Digital Security
Radboud University

Observation IV

Observation IV

The decentralised business model is soft

Observation IV

The decentralised business model is soft

- Users and verifiers interact directly, so charging transactions and profiling is more difficult

iCIS | Digital Security
Radboud University

Observation IV

The decentralised business model is soft

- Users and verifiers interact directly, so charging transactions and profiling is more difficult
- Letting users pay all costs is not a good way to attract customers

iCIS | Digital Security
Radboud University

Observation IV

The decentralised business model is soft

- Users and verifiers interact directly, so charging transactions and profiling is more difficult
- Letting users pay all costs is not a good way to attract customers
- Charging for verifier support services is the main option
  - offer authentication services, like payment services, to verifiers
  - this undermines the privacy-friendly character to some extent

iCIS | Digital Security
Radboud University

Observation IV

The decentralised business model is soft

- Users and verifiers interact directly, so charging transactions and profiling is more difficult
- Letting users pay all costs is not a good way to attract customers
- Charging for verifier support services is the main option
  - offer authentication services, like payment services, to verifiers
  - this undermines the privacy-friendly character to some extent
- The public sector will thus have to play a steering role
  - or data protection authorities, or possibly judges, eventually

Which architecture would they prefer in . . .

Which architecture would they prefer in . . .

- **Russia** and **China**?

Which architecture would they prefer in . . .

- **Russia** and **China**?
  - the centralised one of course — since it facilitates oppression

Which architecture would they prefer in . . .

- **Russia** and **China**?
  - the centralised one of course — since it facilitates oppression
- **The United States**?

iCIS | Digital Security
Radboud University

Which architecture would they prefer in . . .

- **Russia** and **China**?
  - the centralised one of course — since it facilitates oppression
- **The United States**?
  - the centralised one — for commercial reasons

iCIS | Digital Security
Radboud University

Which architecture would they prefer in . . .

- **Russia** and **China**?
  - the centralised one of course — since it facilitates oppression
- **The United States**?
  - the centralised one — for commercial reasons
- **The Netherlands**?

iCIS | Digital Security
Radboud University

Which architecture would they prefer in . . .

- **Russia** and **China**?
  - the centralised one of course — since it facilitates oppression
- **The United States**?
  - the centralised one — for commercial reasons
- **The Netherlands**?
  - the centralised one — see later

iCIS | Digital Security
Radboud University

Which architecture would they prefer in . . .

- **Russia** and **China**?
  - the centralised one of course — since it facilitates oppression
- **The United States**?
  - the centralised one — for commercial reasons
- **The Netherlands**?
  - the centralised one — see later
- In a society that values a balance of power (oh so naive)?

iCIS | Digital Security
Radboud University

Which architecture would they prefer in . . .

- **Russia** and **China**?
  - the centralised one of course — since it facilitates oppression
- **The United States**?
  - the centralised one — for commercial reasons
- **The Netherlands**?
  - the centralised one — see later
- In a society that values a balance of power (oh so naive)?
  - the decentralised one!

iCIS | Digital Security
Radboud University

Where we are, sofar

Parliamentary subcommittee: 25 nov. 2015

MP Oosenbrug asks about central versus decentral

MP Oosenbrug asks about central versus decentral

Minister Plasterk answers

MP Oosenbrug asks about central versus decentral

Minister Plasterk answers

Dan heb je twee modellen. Het ene model is dat je dat decentraal organiseert. Dus je hebt alle informatie op een drager staan, op een telefoon of op een kaartje, of wat dan ook, en dan is die makelaar puur een doorgeefluik.

The Minister's reasoning, continued

[...] wanneer je het decentraal maakt, dan ben je volledig van het middel afhankelijk, en de keuze zoals wij die hebben gemaakt is om te zeggen: wij kunnen het niet helemaal overzien, we denken nu aan een chipje op je paspoort of op je rijbewijs of op je bankpas, of misschien een appje op je telefoon. Ik was gisteren bij een bedrijf [...] Er zijn allerlei technische mogelijkheden, en we zouden niet bij dat stelsel op voorhand ons aan één techniek willen verbinden, en dat pleit er uiteindelijk voor, in de afweging zoals we hem hebben gemaakt, om die makelaar, dus ook de inhoud te laten dragen, zodat we dus met tokens, en sleutels en Google brillen, en weet ik wat voor dingen er nog komen, allemaal bij die informatie zouden kunnen. Maar ik ben het er mee eens, dat is wel een reële keuze.

The Minister's reasoning, continued

[...] wanneer je het decentraal maakt, dan ben je volledig van het middel afhankelijk, en de keuze zoals wij die hebben gemaakt is om te zeggen: wij kunnen het niet helemaal overzien, we denken nu aan een chipje op je paspoort of op je rijbewijs of op je bankpas, of misschien een appje op je telefoon. Ik was gisteren bij een bedrijf [...] Er zijn allerlei technische mogelijkheden, en we zouden niet bij dat stelsel op voorhand ons aan één techniek willen verbinden, en dat pleit er uiteindelijk voor, in de afweging zoals we hem hebben gemaakt, om die makelaar, dus ook de inhoud te laten dragen, zodat we dus met tokens, en sleutels en Google brillen, en weet ik wat voor dingen er nog komen, allemaal bij die informatie zouden kunnen. Maar ik ben het er mee eens, dat is wel een reële keuze.

(The MPs accepted this answer without any further discussion.)

So what is the Minister's argument?

So what is the Minister's argument?

(1) With a decentral set-up, you are completely dependent on the authentication token — a phone, or card, or whatever

iCIS | Digital Security
Radboud University

So what is the Minister's argument?

(1) With a decentral set-up, you are completely dependent on the authentication token — a phone, or card, or whatever

(2) We do not want to commit to one technique (for user authentication), so we put all information centrally (at the 'makelaar')

iCIS | Digital Security
Radboud University

So what is the Minister's argument?

(1) With a decentral set-up, you are completely dependent on the authentication token — a phone, or card, or whatever

(2) We do not want to commit to one technique (for user authentication), so we put all information centrally (at the 'makelaar')

"But, I agree, there is a real choice!" — and it has already been made!

iCIS | Digital Security
Radboud University

Weighing the Minister's (only) argument

Weighing the Minister's (only) argument

The decentral architecture is technology-dependent

Weighing the Minister's (only) argument

The decentral architecture is technology-dependent

- The central architecture uses one techology for verifier-pimp communication — so it is also technology-dependent

iCIS | Digital Security
Radboud University

Weighing the Minister's (only) argument

The decentral architecture is technology-dependent

- The central architecture uses one techology for verifier-pimp communication — so it is also technology-dependent
  - but several technologies can be used for user-pimp communication

Weighing the Minister's (only) argument

The decentral architecture is technology-dependent

- The central architecture uses one techology for verifier-pimp communication — so it is also technology-dependent
  - but several technologies can be used for user-pimp communication
- The decentral architecture has one technology for user-verifier communication — making it technology-dependent indeed
  - but this technique may be used on several carriers (tokens) — such as a card or phone or whatever

iCIS | Digital Security
Radboud University

Weighing the Minister's (only) argument

The decentral architecture is technology-dependent

- The central architecture uses one techology for verifier-pimp communication — so it is also technology-dependent
  - but several technologies can be used for user-pimp communication
- The decentral architecture has one technology for user-verifier communication — making it technology-dependent indeed
  - but this technique may be used on several carriers (tokens) — such as a card or phone or whatever

This difference is not the most important one!

- certainly because different technologies for user-pimp communication yield incompatible outcomes (pseudonyms) in Idensys
- the argument is weak, and disregards the more fundamental issues

Where we are, sofar

Putting Idensys and IRMA together

Putting Idensys and IRMA together

- The naive combination uses IRMA for user-authentication to Idensys central parties (*authenticatiediensten*)

iCIS | Digital Security
Radboud University

Putting Idensys and IRMA together

- The naive combination uses IRMA for user-authentication to Idensys central parties (*authenticatiediensten*)
  - this destroys all privacy-friendliness of IRMA, since transactions become traceable

iCIS | Digital Security
Radboud University

Putting Idensys and IRMA together

- The naive combination uses IRMA for user-authentication to Idensys central parties (*authenticatiediensten*)
  - this destroys all privacy-friendliness of IRMA, since transactions become traceable
- There are two "machiato" versions (think of "latte" or "cafe")

iCIS | Digital Security
Radboud University

Putting Idensys and IRMA together

- The naive combination uses IRMA for user-authentication to Idensys central parties (*authenticatiediensten*)
  - this destroys all privacy-friendliness of IRMA, since transactions become traceable
- There are two "machiato" versions (think of "latte" or "cafe")

(1) True end-to-end authentication with IRMA token via Idensys

iCIS | Digital Security
Radboud University

Putting Idensys and IRMA together

- The naive combination uses IRMA for user-authentication to Idensys central parties (*authenticatiediensten*)
  - this destroys all privacy-friendliness of IRMA, since transactions become traceable
- There are two "machiato" versions (think of "latte" or "cafe")

(1) True end-to-end authentication with IRMA token via Idensys
  - proposed by Eric Verheul
  - intermediate parties see nothing, but verifiers must do more
  - end-to-end may be required in certain sectors, like health

Putting Idensys and IRMA together

- The naive combination uses IRMA for user-authentication to Idensys central parties (*authenticatiediensten*)
  - this destroys all privacy-friendliness of IRMA, since transactions become traceable
- There are two "machiato" versions (think of "latte" or "cafe")

(1) True end-to-end authentication with IRMA token via Idensys
  - proposed by Eric Verheul
  - intermediate parties see nothing, but verifiers must do more
  - end-to-end may be required in certain sectors, like health

(2) External apostiller check in every IRMA authentication

iCIS | Digital Security
Radboud University

Putting Idensys and IRMA together

- The naive combination uses IRMA for user-authentication to Idensys central parties (*authenticatiediensten*)
  - this destroys all privacy-friendliness of IRMA, since transactions become traceable
- There are two "machiato" versions (think of "latte" or "cafe")

(1) True end-to-end authentication with IRMA token via Idensys
  - proposed by Eric Verheul
  - intermediate parties see nothing, but verifiers must do more
  - end-to-end may be required in certain sectors, like health

(2) External apostiller check in every IRMA authentication
  - the apostiller is needed, but cannot see transaction details
  - it can be used for easy revocation and anti-fraud monitoring
  - current topic of research

iCIS | Digital Security
Radboud University

Where we are, sofar

Main points

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 in the decentral one

  What kind of society do we prefer to live in?
- The NL authorities have made their choice very early on
  - flimsy technical differences are exaggerated now
  - value-laden discussion is avoided altogether
- Who will defend "the public good" in the digital world?
  - a sombre mood is what remains.
  - a lost opportunity for privacy

See the PI.lab blog for more (cheerful) discussion.

iCIS | Digital Security
Radboud University

Finally . . .