IRMA, as simple as ABC

OUrsi

Fabian van den Broek

fabian.vandenbroek@ou.nl

Open University of the Netherlands & Radboud Universiteit Nijmegen

7 February 2017

Open Universiteit
www.ou.nl

IRMA,
as simple as
ABC

I Reveal My Attributes,
as simple as
ABC

I Reveal My Attributes

=

ABC

Open Universiteit
www.ou.nl

I Reveal My Attributes

=

Attribute Based Credentials

Some attributes of the speaker

Some attributes of the speaker

- Studied Computer science
- PhD-thesis on Mobile communication security
- Post docs on smart grid security and attribute based credentials
- From 1 Jan. researcher at OU
- research subjects:
  - security of mobile telephony
  - security of smart grids
  - attribute based credentials

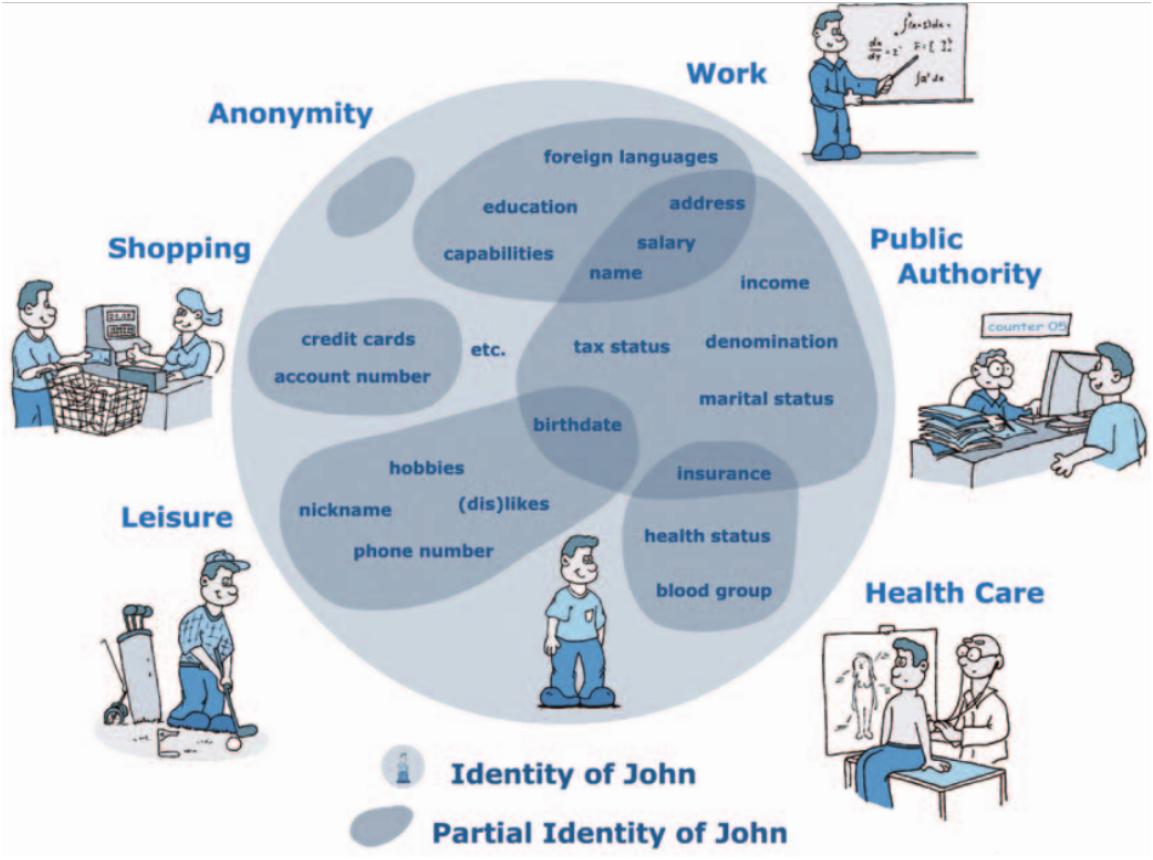
Open Universiteit
www.ou.nl

Some attributes of the speaker

- Studied Computer science
- PhD-thesis on Mobile communication security
- Post docs on smart grid security and attribute based credentials
- From 1 Jan. researcher at OU
- research subjects:
  - security of mobile telephony
  - security of smart grids
  - attribute based credentials
- male,
- married, with children,
- over 18 years old,
- under 65 years old,
- bloodtype: `[redacted]`,
- living in Nijmegen,
- etc.

Open Universiteit
www.ou.nl

Identities versus attributes



[FIDIS] project

Open Universiteit
www.ou.nl

Identities versus attributes

Open Universiteit
www.ou.nl

Identities versus attributes

- Identity management revolves around identities
  - Often uniquely identifying numbers, such as social security number, or passport number
  - high-value targets for profiling & identity fraud
    (this also holds for pseudonyms)

Identities versus attributes

- Identity management revolves around identities
  - Often uniquely identifying numbers, such as social security number, or passport number
  - high-value targets for profiling & identity fraud (this also holds for pseudonyms)
- A more flexible identity ecosystem uses attributes
  - 'over 18', 'over 21', 'over 65', 'under 15', 'female', 'male'
  - 'student', 'doctor', 'lawyer', 'top secret clearance'
  - 'NL-citizen', 'resident of Nijmegen'
  - 'home address', 'owner of bankaccount nr. . . . '

Identities versus attributes

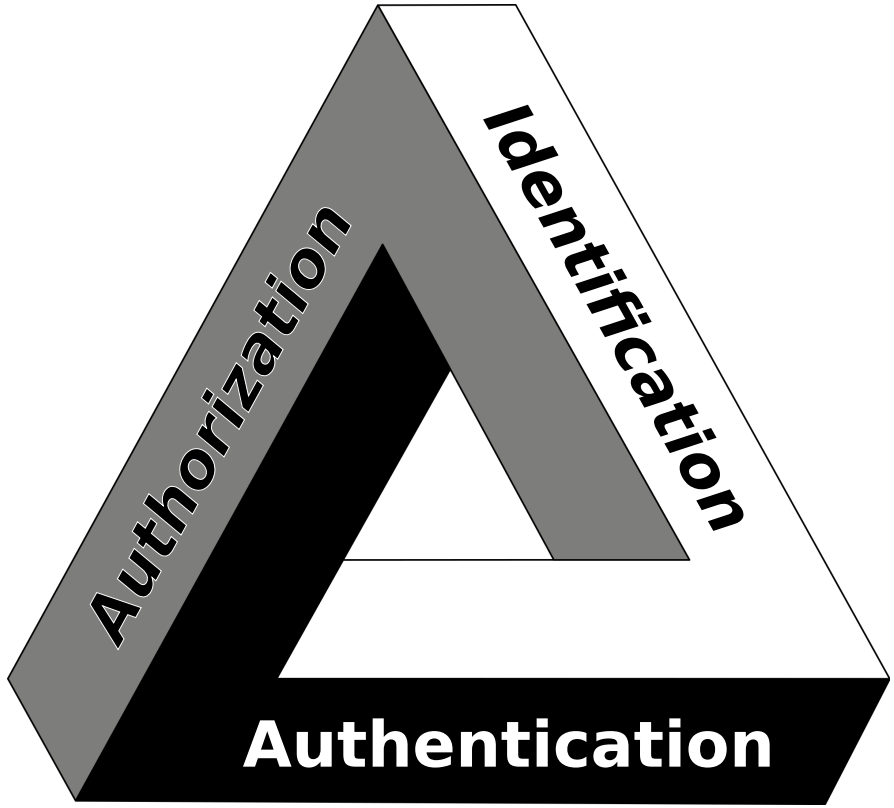
- Identity management revolves around identities
  - Often uniquely identifying numbers, such as social security number, or passport number
  - high-value targets for profiling & identity fraud (this also holds for pseudonyms)
- A more flexible identity ecosystem uses attributes
  - 'over 18', 'over 21', 'over 65', 'under 15', 'female', 'male'
  - 'student', 'doctor', 'lawyer', 'top secret clearance'
  - 'NL-citizen', 'resident of Nijmegen'
  - 'home address', 'owner of bankaccount nr. . . . '
- Attributes may be identifying (like social security number, bank account, phone number) or non-identifying

Identities versus attributes

- Identity management revolves around identities
  - Often uniquely identifying numbers, such as social security number, or passport number
  - high-value targets for profiling & identity fraud (this also holds for pseudonyms)
- A more flexible identity ecosystem uses attributes
  - 'over 18', 'over 21', 'over 65', 'under 15', 'female', 'male'
  - 'student', 'doctor', 'lawyer', 'top secret clearance'
  - 'NL-citizen', 'resident of Nijmegen'
  - 'home address', 'owner of bankaccount nr. ...'
- Attributes may be identifying (like social security number, bank account, phone number) or non-identifying

Your **identity** is the collection of attributes that hold for you

Goal of ABCs

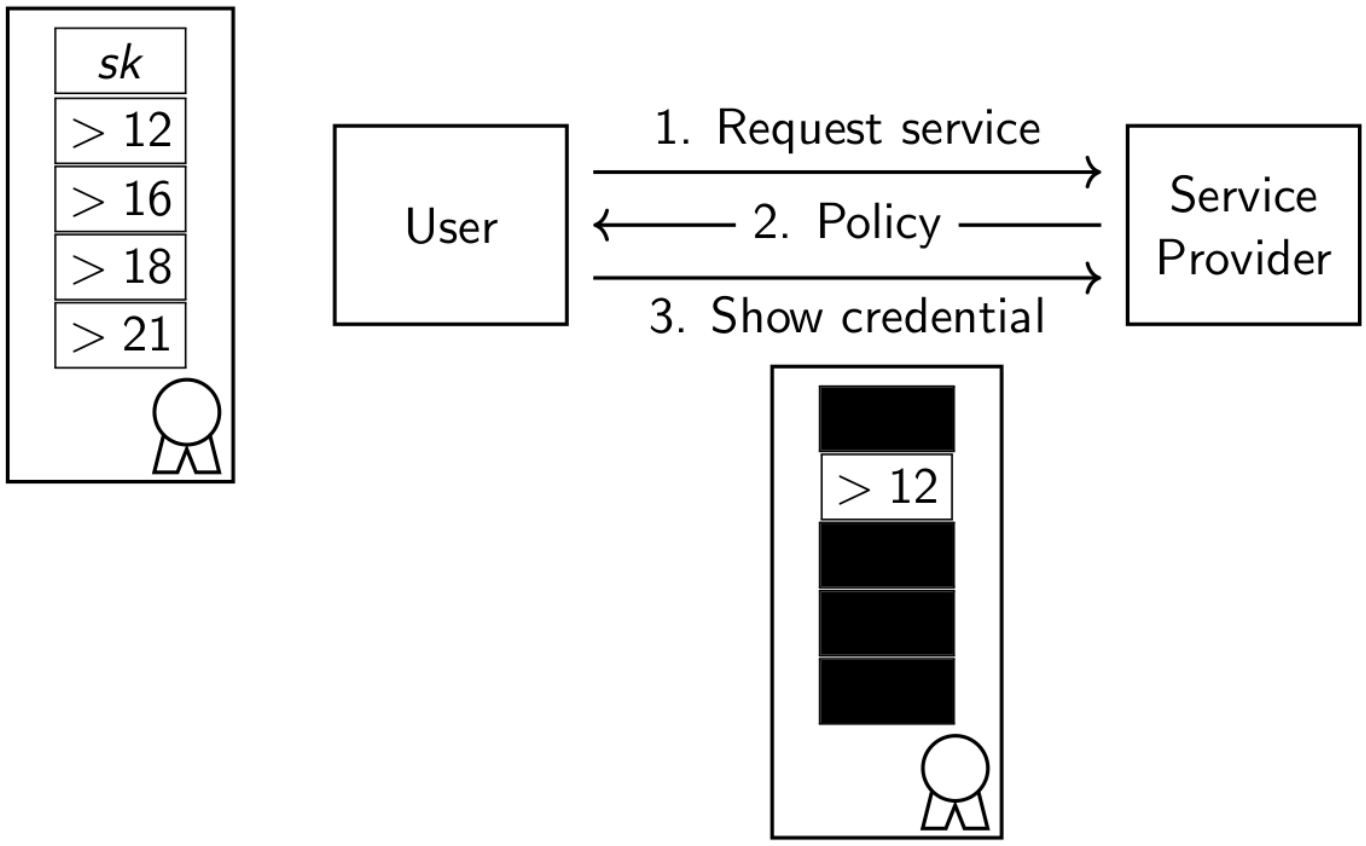


Open Universiteit
www.ou.nl

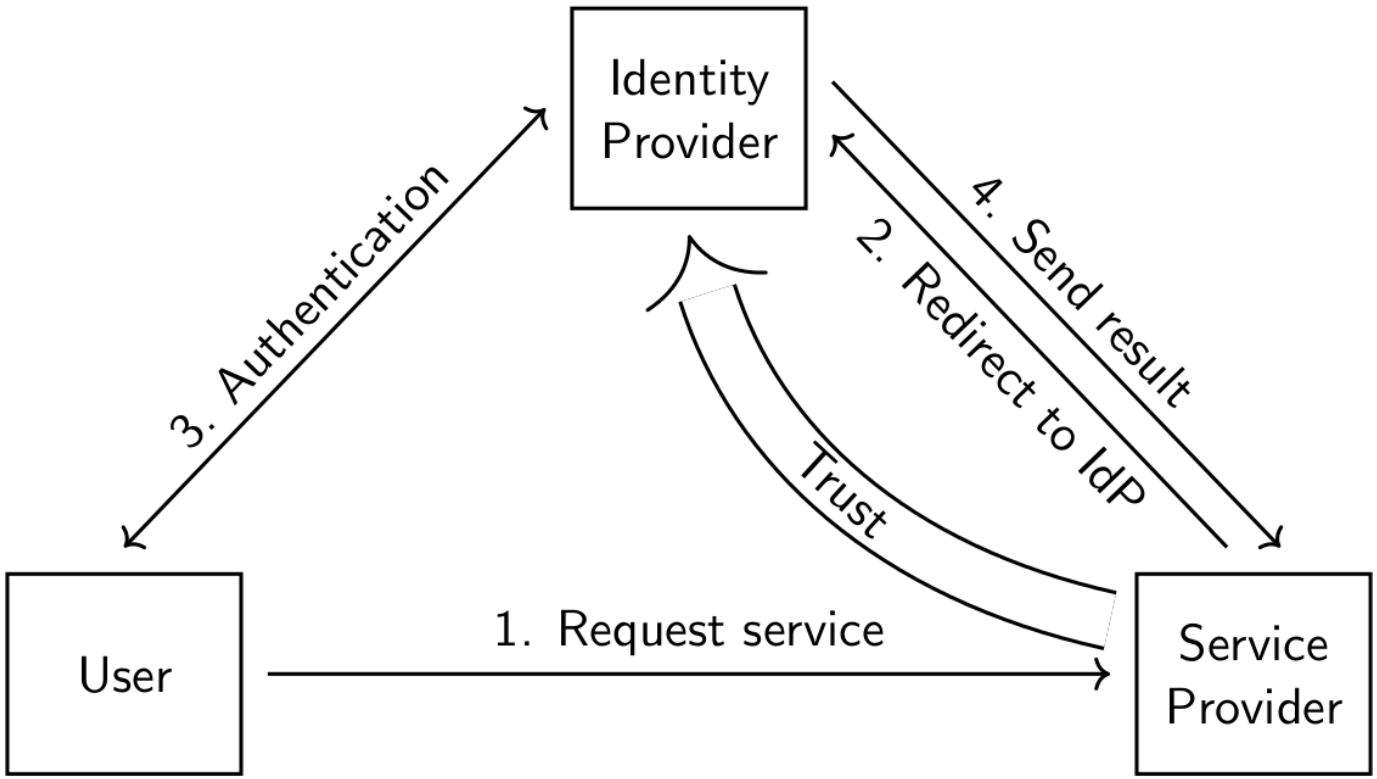
Goal of ABCs

Open Universiteit
www.ou.nl

IRMA overview

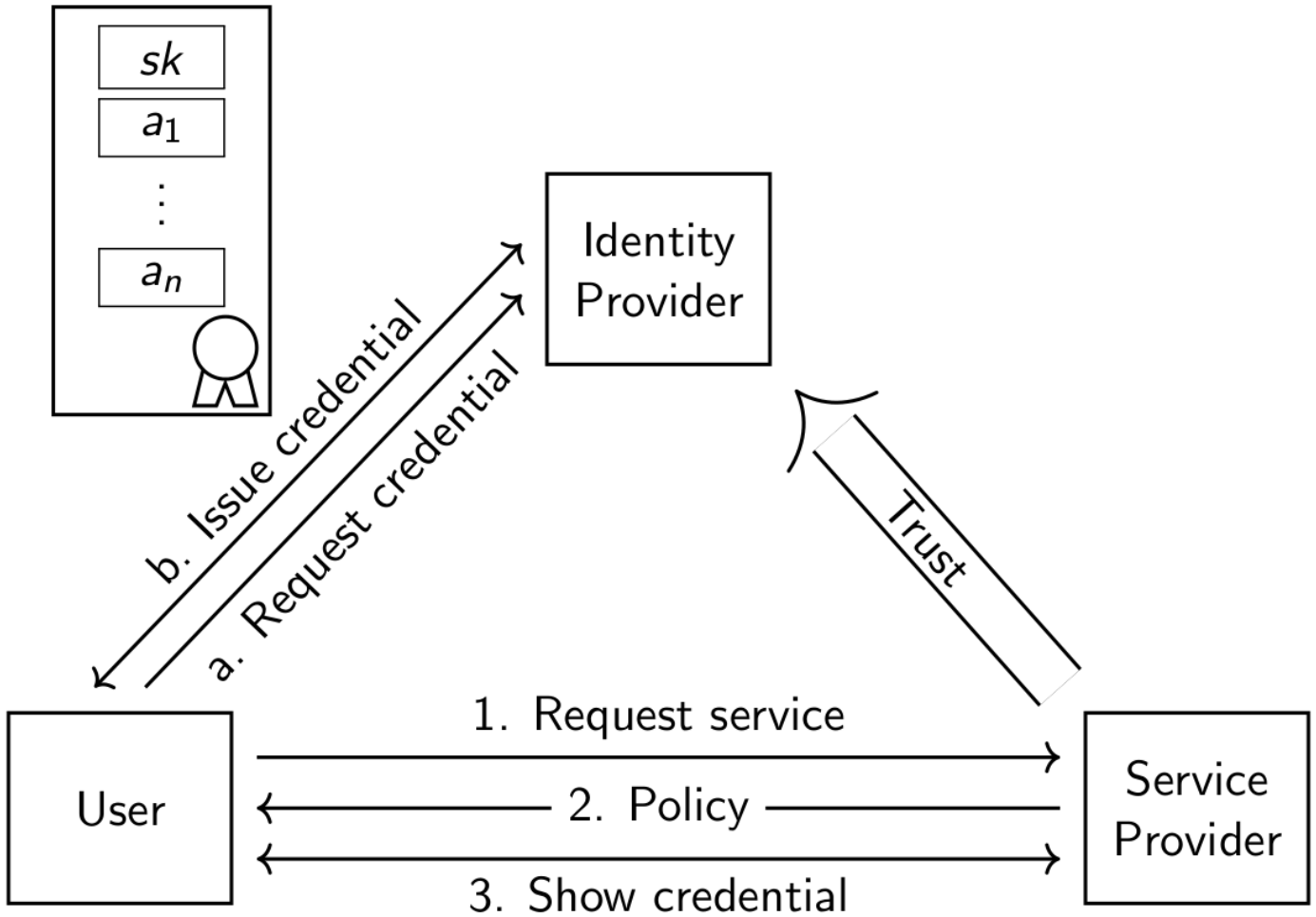


Standard centralized solution



Open Universiteit
www.ou.nl

IRMA is a decentral solution



Essentials of IRMA = I Reveal My Attributes

Open Universiteit
www.ou.nl

Essentials of IRMA = I Reveal My Attributes

- An IRMA user can selectively disclose different attributes about him/her self, depending on the situation
  - privacy-by-design, via data minimalisation and user-control

Open Universiteit
www.ou.nl

Essentials of IRMA = I Reveal My Attributes

- An IRMA user can selectively disclose different attributes about him/her self, depending on the situation
  - privacy-by-design, via data minimalisation and user-control
- Attributes are issued by (different, relevant) authorities, and are verified by service providers

Open Universiteit
www.ou.nl

Essentials of IRMA = I Reveal My Attributes

- An IRMA user can selectively disclose different attributes about him/her self, depending on the situation
  - privacy-by-design, via data minimalisation and user-control
- Attributes are issued by (different, relevant) authorities, and are verified by service providers
- Attributes are reliable via a digital signature of the issuer
  - they also carry a validity date

Open Universiteit
www.ou.nl

Essentials of IRMA = I Reveal My Attributes

- An IRMA user can selectively disclose different attributes about him/her self, depending on the situation
  - privacy-by-design, via data minimalisation and user-control
- Attributes are issued by (different, relevant) authorities, and are verified by service providers
- Attributes are reliable via a digital signature of the issuer
  - they also carry a validity date
- Attributes are stored locally, under direct control of the user
  - storage on mobile phone is most convenient
  - attributes are cryptographically bound to the user, and are non-transferrable

Open Universiteit
www.ou.nl

Requirements for attribute-bases systems

Requirements for attribute-bases systems

- Authentic: the attributes I show where given to me by a specific issuer and are unchanged
  - realised via signatures

Open Universiteit
www.ou.nl

Requirements for attribute-bases systems

- Authentic: the attributes I show where given to me by a specific issuer and are unchanged
  - realised via signatures

- Non-transferability: my little nephew should not be able to get my "over 18" attribute (and go to XXX sites)
  - realised via binding to my private key

Open Universiteit
www.ou.nl

Requirements for attribute-bases systems

- Authentic: the attributes I show where given to me by a specific issuer and are unchanged
  - realised via signatures
- Non-transferability: my little nephew should not be able to get my "over 18" attribute (and go to XXX sites)
  - realised via binding to my private key
- Issuer-unlinkability: the issuers should not be able to track where I use which attribute
  - typically realised via blind(able) signature

Requirements for attribute-bases systems

- Authentic: the attributes I show where given to me by a specific issuer and are unchanged
  - realised via signatures
- Non-transferability: my little nephew should not be able to get my "over 18" attribute (and go to XXX sites)
  - realised via binding to my private key
- Issuer-unlinkability: the issuers should not be able to track where I use which attribute
  - typically realised via blind(able) signature
- Multi-show unlinkability: service providers should not be able to connect usage (at different providers)
  - realised via zero-knowledge proofs, or via "self-blinding"

Requirements for attribute-bases systems

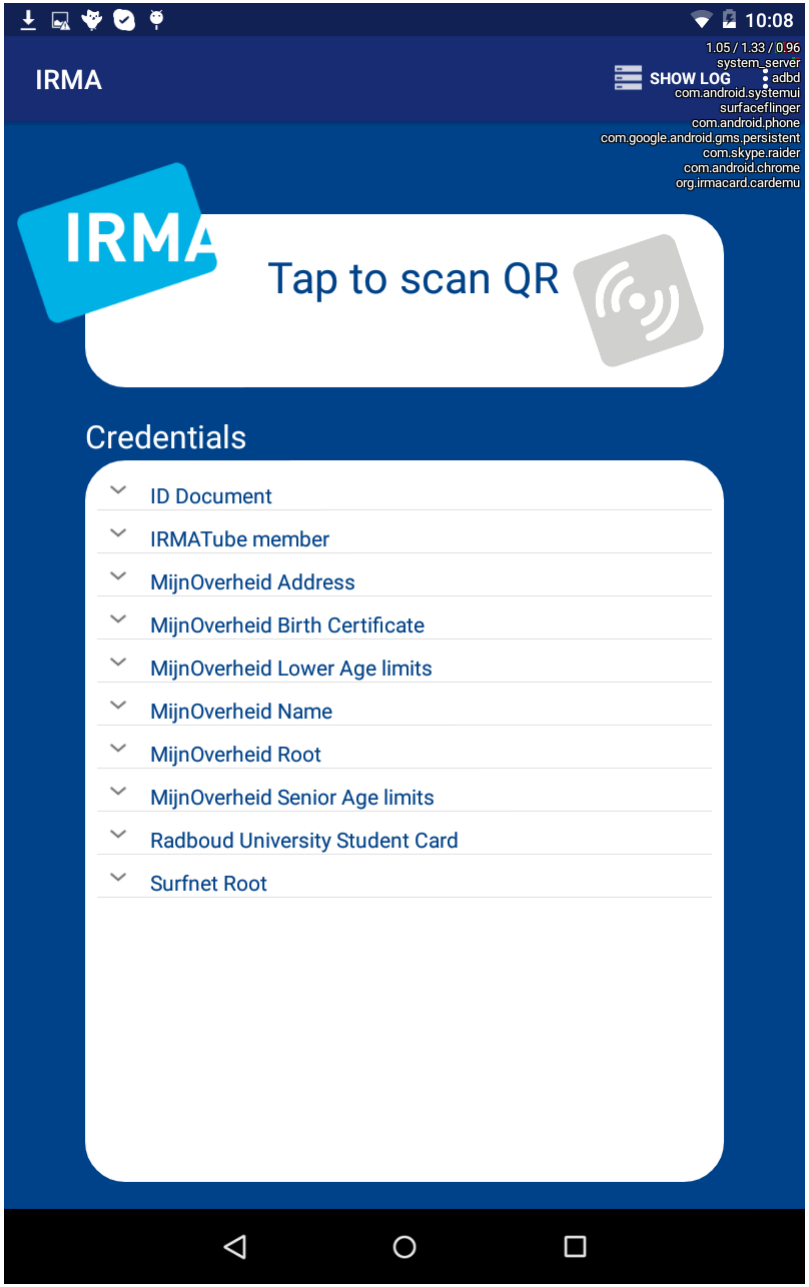
- Authentic: the attributes I show where given to me by a specific issuer and are unchanged
  - realised via signatures
- Non-transferability: my little nephew should not be able to get my "over 18" attribute (and go to XXX sites)
  - realised via binding to my private key
- Issuer-unlinkability: the issuers should not be able to track where I use which attribute
  - typically realised via blind(able) signature
- Multi-show unlinkability: service providers should not be able to connect usage (at different providers)
  - realised via zero-knowledge proofs, or via "self-blinding"
- Revocation: rogue attributes (via stolen/lost cards) should be blockable.
  - partly in conflict with previous requirements

Open Universiteit
www.ou.nl

When I got involved with IRMA

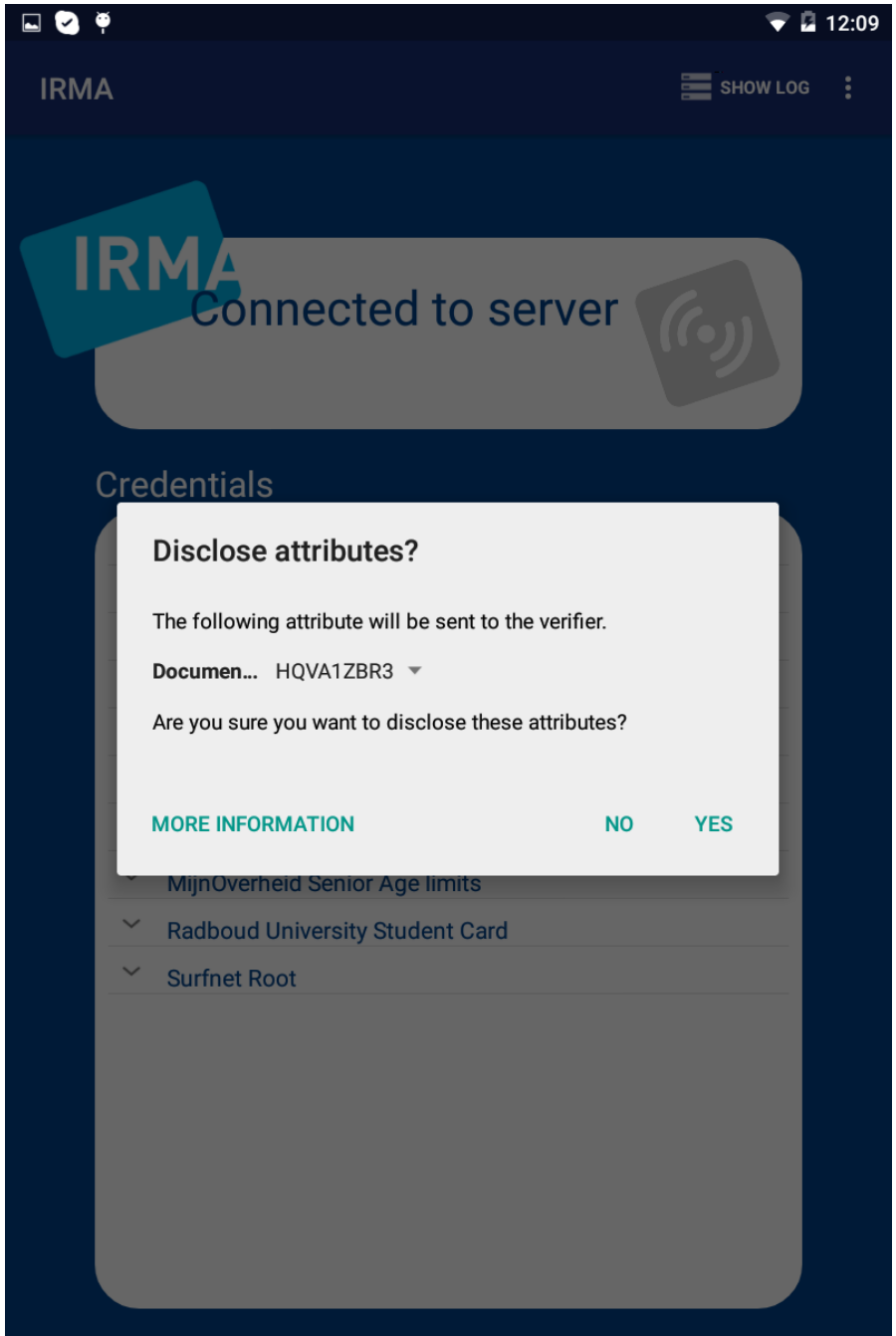
Open Universiteit
www.ou.nl

and we moved to:



Open Universiteit
www.ou.nl

Demo time



Open Universiteit
www.ou.nl

IRMA carrier comparison

A smartcard offers:

- Secure key storage
- Strong(er) offline user binding

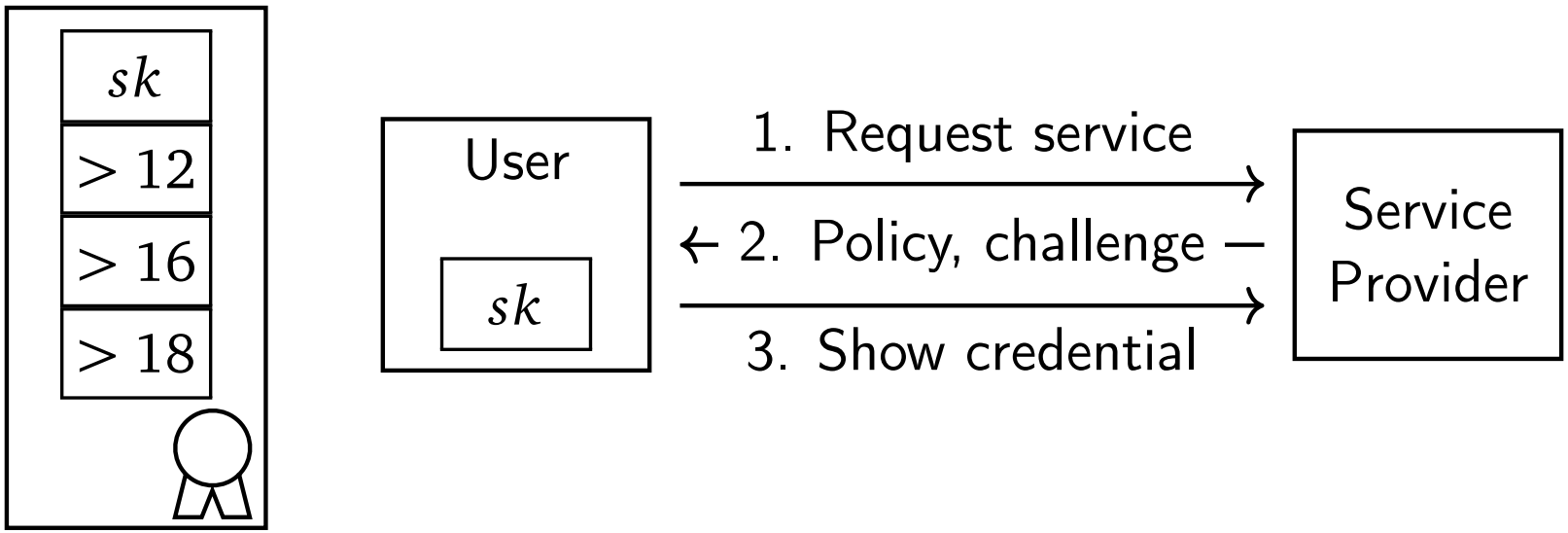
- A horrible user experience
- Poor computational power
- No Internet connectivity

A smartphone offers:

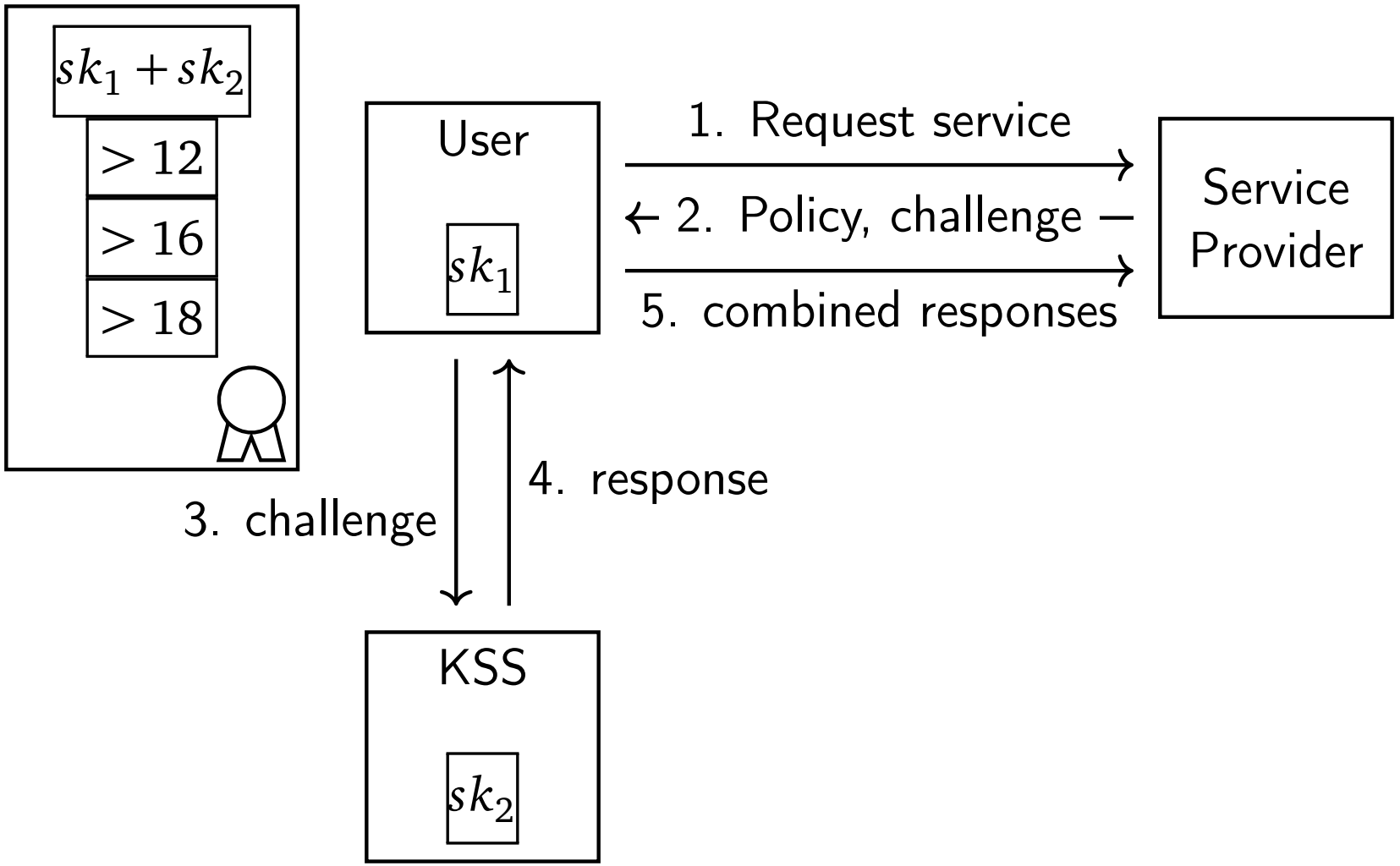
- Weak key storage
- Weak offline user binding

- Nicer user experience
- Stronger keys, faster performance, unlimited attributes, etc.
- Online issuance & verification, updatability, etc.

Securing the private key



Securing the private key



Open Universiteit
www.ou.nl

The Key Share Server

has tremendous benefits:

- Securing the key?

Open Universiteit
www.ou.nl

The Key Share Server

has tremendous benefits:

- Securing the key
- Strong revocation

Open Universiteit
www.ou.nl

The Key Share Server

has tremendous benefits:

- Securing the key
- Strong revocation
- Limited logging

Open Universiteit
www.ou.nl

The Key Share Server

has tremendous benefits:

- Securing the key
- Strong revocation
- Limited logging
- Limited monitoring

Open Universiteit
www.ou.nl

The Key Share Server

has tremendous benefits:

- Securing the key
- Strong revocation
- Limited logging
- Limited monitoring

Open Universiteit
www.ou.nl

The Key Share Server

has tremendous benefits:

- Securing the key
- Strong revocation
- Limited logging
- Limited monitoring

but also has some downsides:

- Introducing a central server

Open Universiteit
www.ou.nl

The Key Share Server

has tremendous benefits:

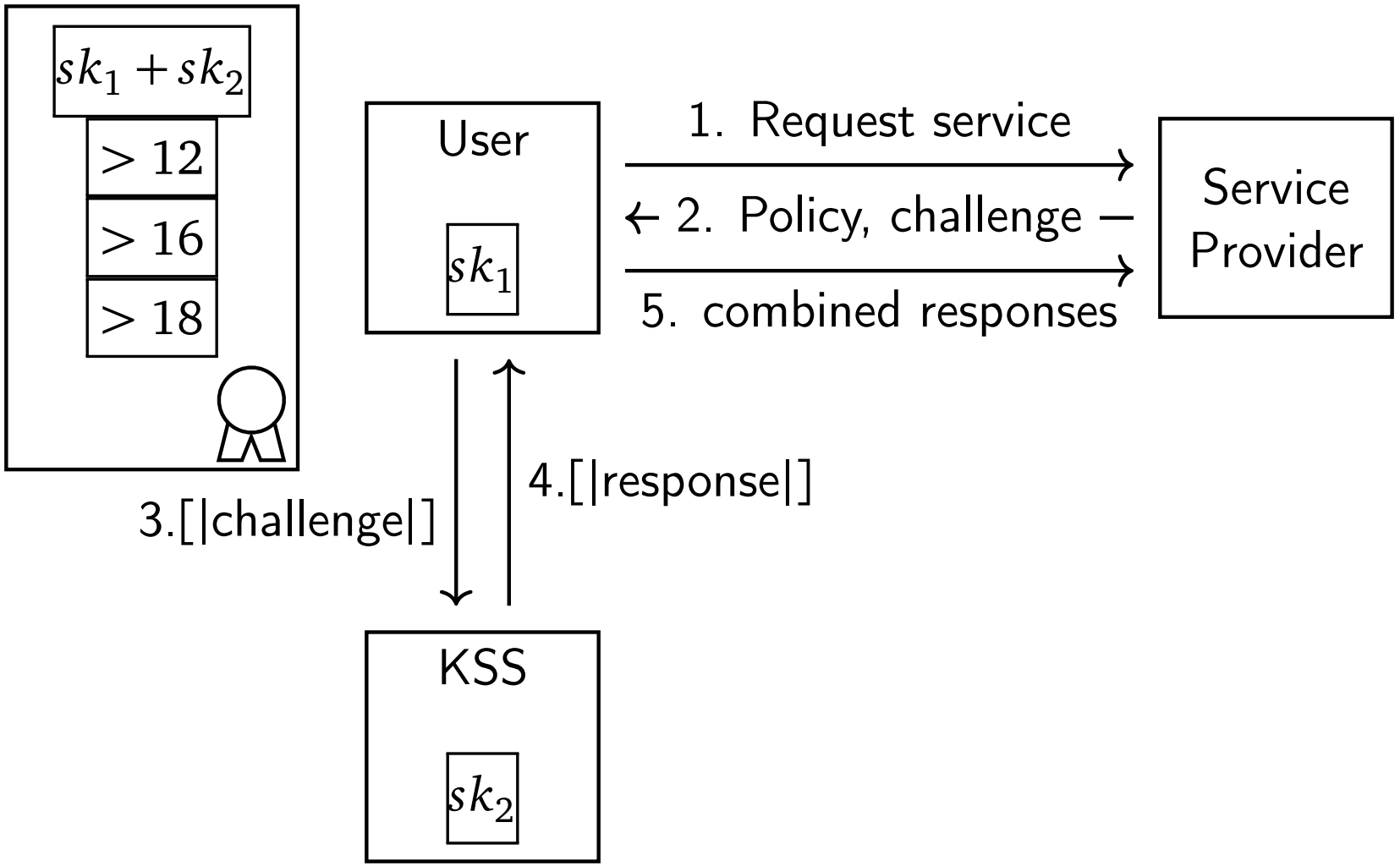
- Securing the key
- Strong revocation
- Limited logging
- Limited monitoring

but also has some downsides:

- Introducing a central server
- What does the KSS learn?

Open Universiteit
www.ou.nl

The Key Share Server



Open Universiteit
www.ou.nl

Improvements

The move to a phone allows for several other improvements:

- Extended enrolment scenario's
- Attribute based signatures
- Online credential store

Open Universiteit
www.ou.nl

Enrolment

New enrolment options:

1. Self-enrolment

Open Universiteit
www.ou.nl

Enrolment

New enrolment options:

1. Self-enrolment
   - 1.1 Passport + SIM
   - 1.2 iDIN
   - 1.3 Combining

Open Universiteit
www.ou.nl

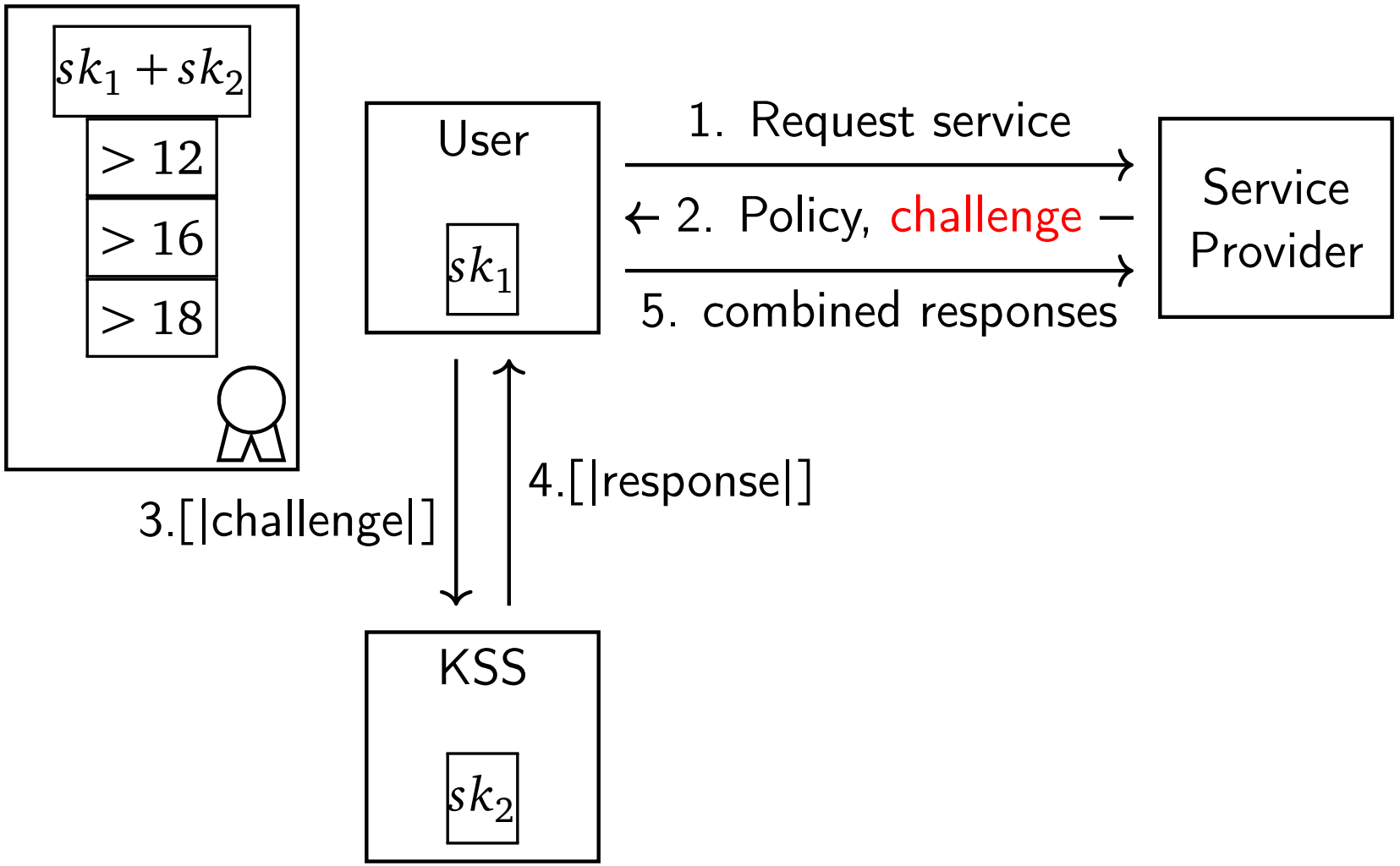
Enrolment

New enrolment options:

1. Self-enrolment
   - 1.1 Passport + SIM
   - 1.2 iDIN
   - 1.3 Combining
2. Desk-enrolment

Open Universiteit
www.ou.nl

Atttibute based signatures



Open Universiteit
www.ou.nl

Atttibute based signatures

The challenge could also be a document hash!

Atttibute based signatures

The challenge could also be a document hash!

Standard digital signatures show access to private key

Atttibute based signatures

The challenge could also be a document hash!

Standard digital signatures show access to private key
The certificate binds the signature to a person

Atttibute based signatures

The challenge could also be a document hash!

Standard digital signatures show access to private key
The certificate binds the signature to a person

Attribute-based signatures can show much more information!

Atttibute based signatures

The challenge could also be a document hash!

Standard digital signatures show access to private key
The certificate binds the signature to a person

Attribute-based signatures can show much more information!
e.g. signed by a docter with speciality ..., >18, a sergeant, etc.

Credential store

- The meta-information of credentials was hard-coded on the smartcard.

Credential store

- The meta-information of credentials was hard-coded on the smartcard.
- On the phone we can get up-to-date information from a server.

Credential store

- The meta-information of credentials was hard-coded on the smartcard.
- On the phone we can get up-to-date information from a server.
- This meta-information includes:

Credential store

- The meta-information of credentials was hard-coded on the smartcard.
- On the phone we can get up-to-date information from a server.
- This meta-information includes:
  - Issuer

Open Universiteit
www.ou.nl

Credential store

- The meta-information of credentials was hard-coded on the smartcard.
- On the phone we can get up-to-date information from a server.
- This meta-information includes:
  - Issuer
  - Issuer Public Key

Open Universiteit
www.ou.nl

Credential store

- The meta-information of credentials was hard-coded on the smartcard.
- On the phone we can get up-to-date information from a server.
- This meta-information includes:
  - Issuer
  - Issuer Public Key
  - Public Key validity date

Open Universiteit
www.ou.nl

Credential store

- The meta-information of credentials was hard-coded on the smartcard.
- On the phone we can get up-to-date information from a server.
- This meta-information includes:
  - Issuer
  - Issuer Public Key
  - Public Key validity date
  - Old Public Keys

Open Universiteit
www.ou.nl

Credential store

- The meta-information of credentials was hard-coded on the smartcard.
- On the phone we can get up-to-date information from a server.
- This meta-information includes:
  - Issuer
  - Issuer Public Key
  - Public Key validity date
  - Old Public Keys
  - Labels for attributes

Open Universiteit
www.ou.nl

Credential store

- The meta-information of credentials was hard-coded on the smartcard.
- On the phone we can get up-to-date information from a server.
- This meta-information includes:
  - Issuer
  - Issuer Public Key
  - Public Key validity date
  - Old Public Keys
  - Labels for attributes
  - ...

Open Universiteit
www.ou.nl

Future work

Upcoming pilots:

- Tippiq
- GP
- Schiphol
- Radboud
- ...

Open Universiteit
www.ou.nl

Future work

Upcoming pilots:

- Tippiq
- GP
- Schiphol
- Radboud
- ...

Engineering:

- Attribute-based signatures
- Convenience tooling
- Attribute typing
- Local verification

Open Universiteit
www.ou.nl

Future work

Upcoming pilots:

- Tippiq
- GP
- Schiphol
- Radboud
- ...

Engineering:

- Attribute-based signatures
- Convenience tooling
- Attribute typing
- Local verification

Research:

- ABCs for mobile networks
- ...

Open Universiteit
www.ou.nl

Thank you

Open Universiteit
www.ou.nl