

Authentication with Privacy *and* Security

—the maths behind attribute-based credentials—

Greg Alpar

greg.alpar@ou.nl

Open Universiteit, Radboud Universiteit

August 25 and September 1, 2018

Open Universiteit
www.ou.nl



Who is this guy?

- ▶ Maths and maths teaching (MSc) – ELTE
- ▶ Mathematics for Industry (MTD, PDEng) – TU/e
- ▶ Computer Science (PhD) – RU
- ▶ Assistant Professor (UD) – OU (, RU)

- ▶ Number Theory, Abstract algebra
- ▶ Coding theory, Cryptography
- ▶ Privacy

- ▶ ABC Technology Workshop

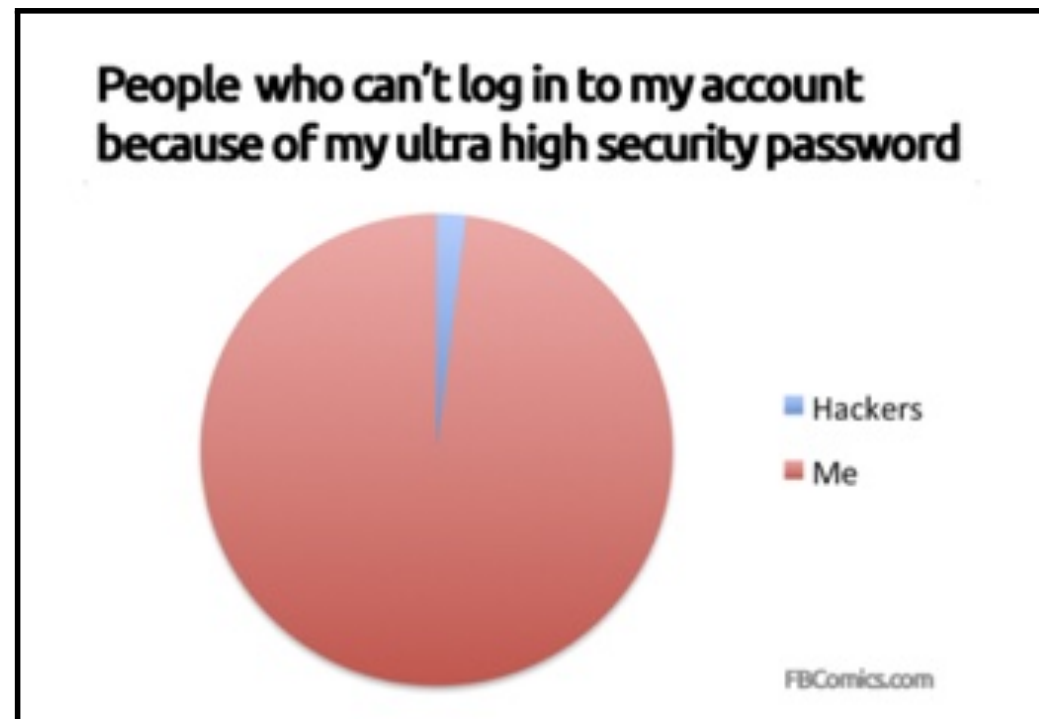
- ▶ Open Maths – Comenius Grant (Innovative University Education)

Attribute-based credentials



Problems with online logins

- ▶ User unfriendly
- ▶ Often insecure
- ▶ Often identifying





Problems with online logins

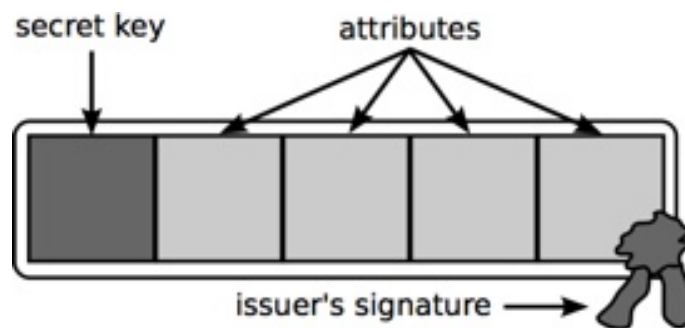
or they are:

- ▶ Always identifying
- ▶ Highly centralized & traceable

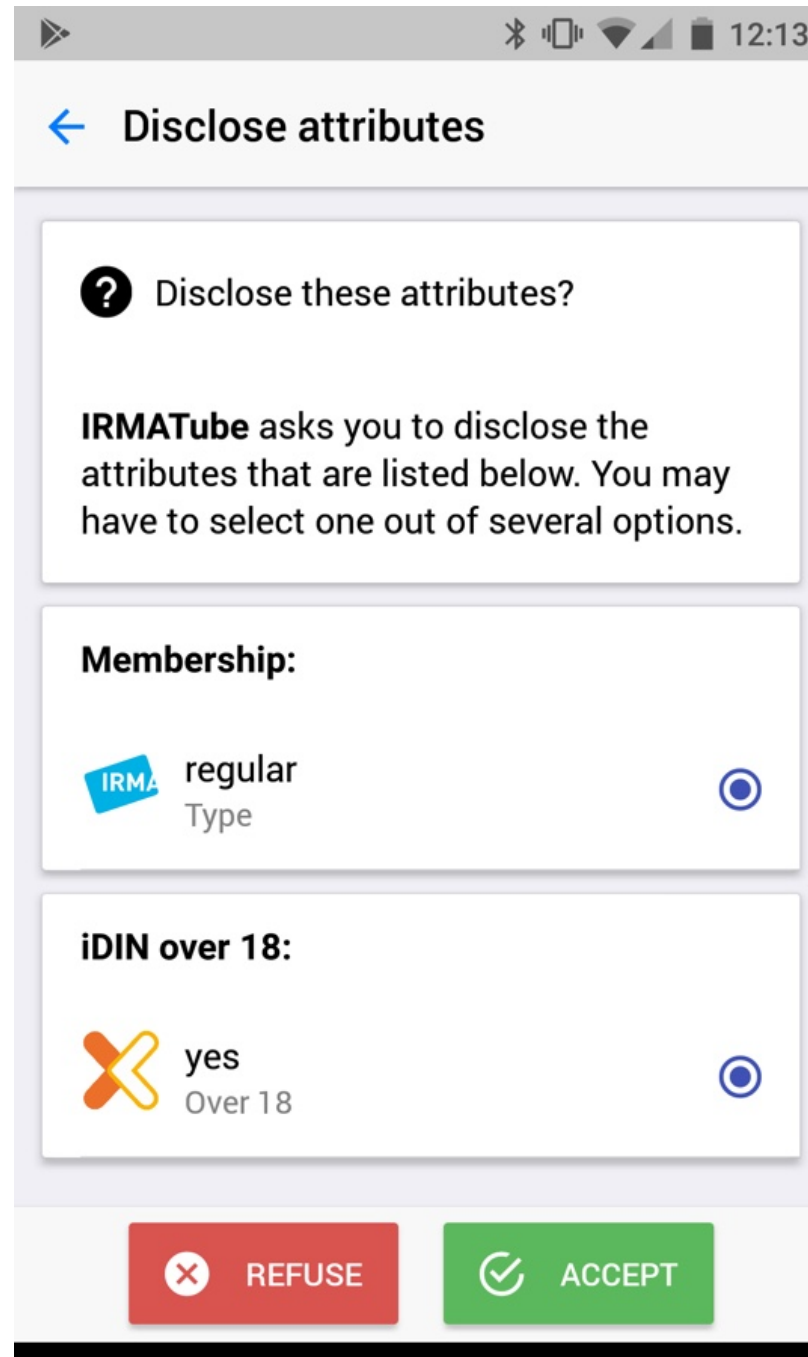
Attribute-based credentials to the rescue!

What is this ABC?

- ▶ Attribute-Based Credentials (**ABCs**)
- ▶ Specifically IBM's Identity mixer (Idemix) based on the **Camenisch–Lysyanskaya signature**
- ▶ A credential is a cryptographic container
 - ▶ Signature: authenticity, integrity, 'verifiability'
 - ▶ ...on a block of messages, called **attributes**
 - ▶ **Randomisation** (blind)
 - ▶ **Selective disclosure**



Demo time




The screenshot shows a mobile application interface with a status bar at the top displaying Bluetooth, signal, and battery icons, and the time 12:13. The app's title bar is light gray with a blue back arrow and the text "Disclose attributes". The main content area is white and contains a question "Disclose these attributes?" with a question mark icon. Below this, a text block explains that IRMATube asks for disclosure of attributes listed below, requiring selection of one option. The first section, "Membership:", features a blue "IRMA" logo and the text "regular Type" next to a selected radio button. The second section, "iDIN over 18:", features an orange "X" logo and the text "yes Over 18" next to a selected radio button. At the bottom, there are two buttons: a red "REFUSE" button with a white 'X' icon and a green "ACCEPT" button with a white checkmark icon.

← Disclose attributes


? Disclose these attributes?



IRMATube asks you to disclose the attributes that are listed below. You may have to select one out of several options.

Membership:

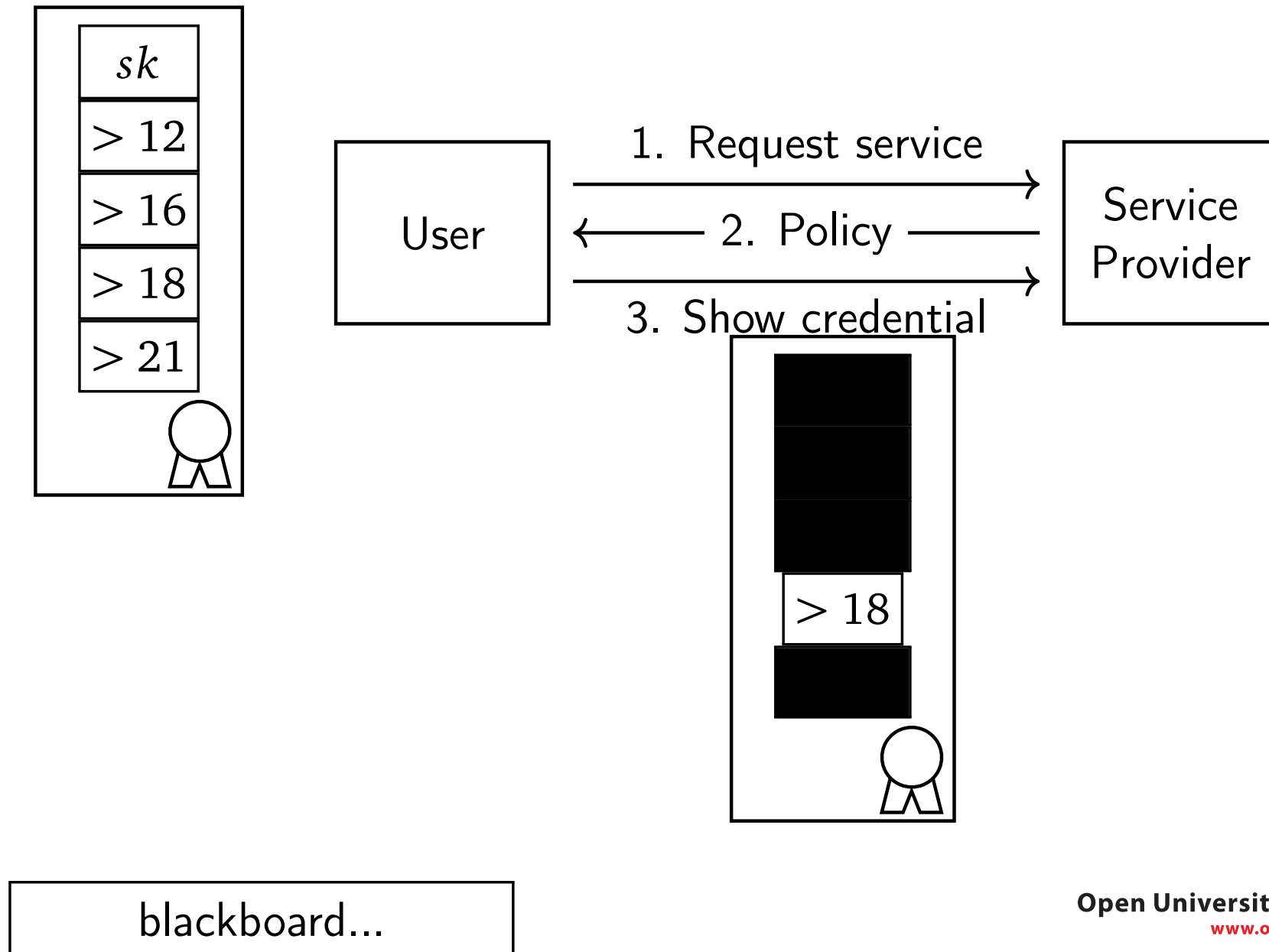
 regular
Type ☒

iDIN over 18:

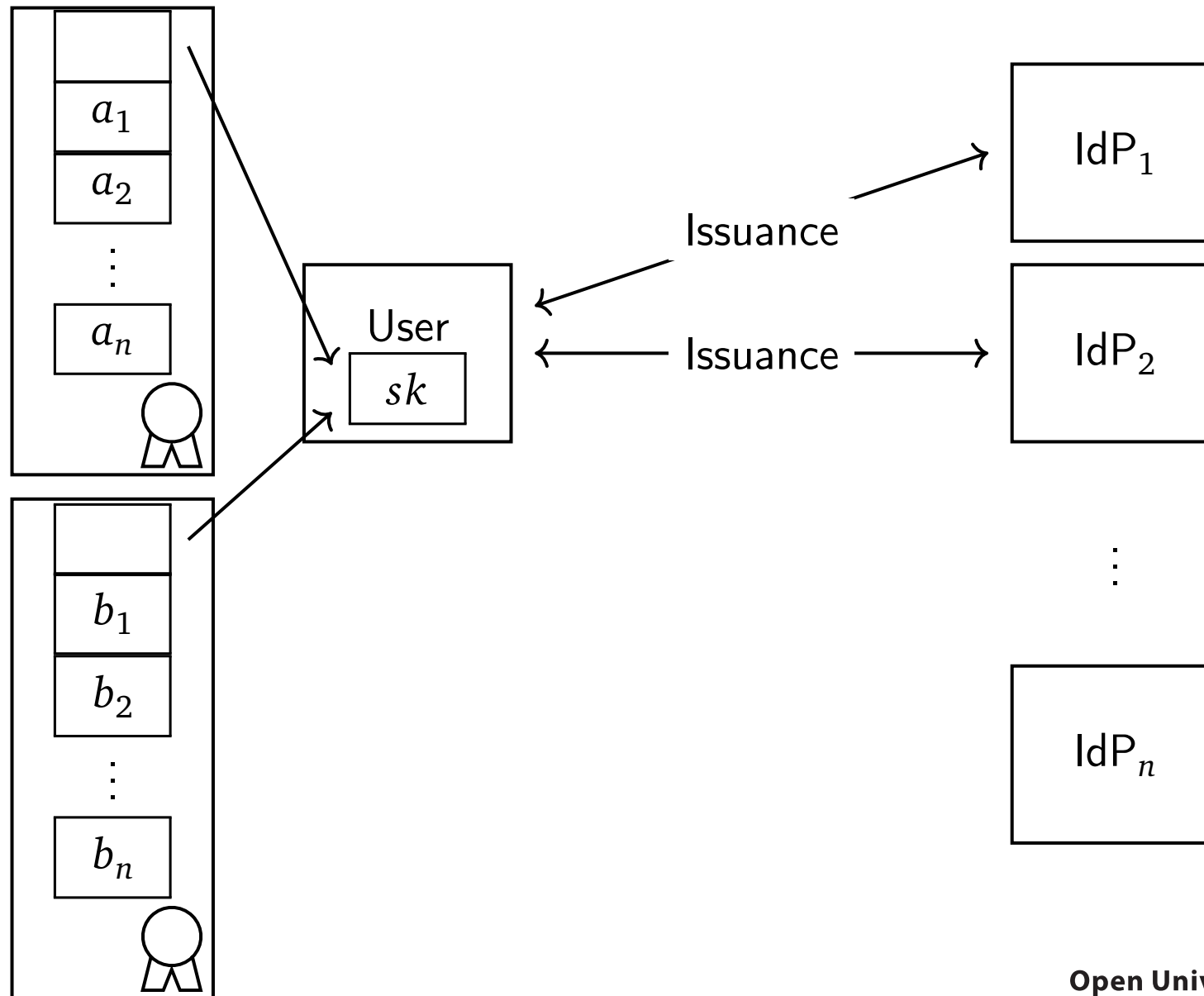
 yes
Over 18 ☒

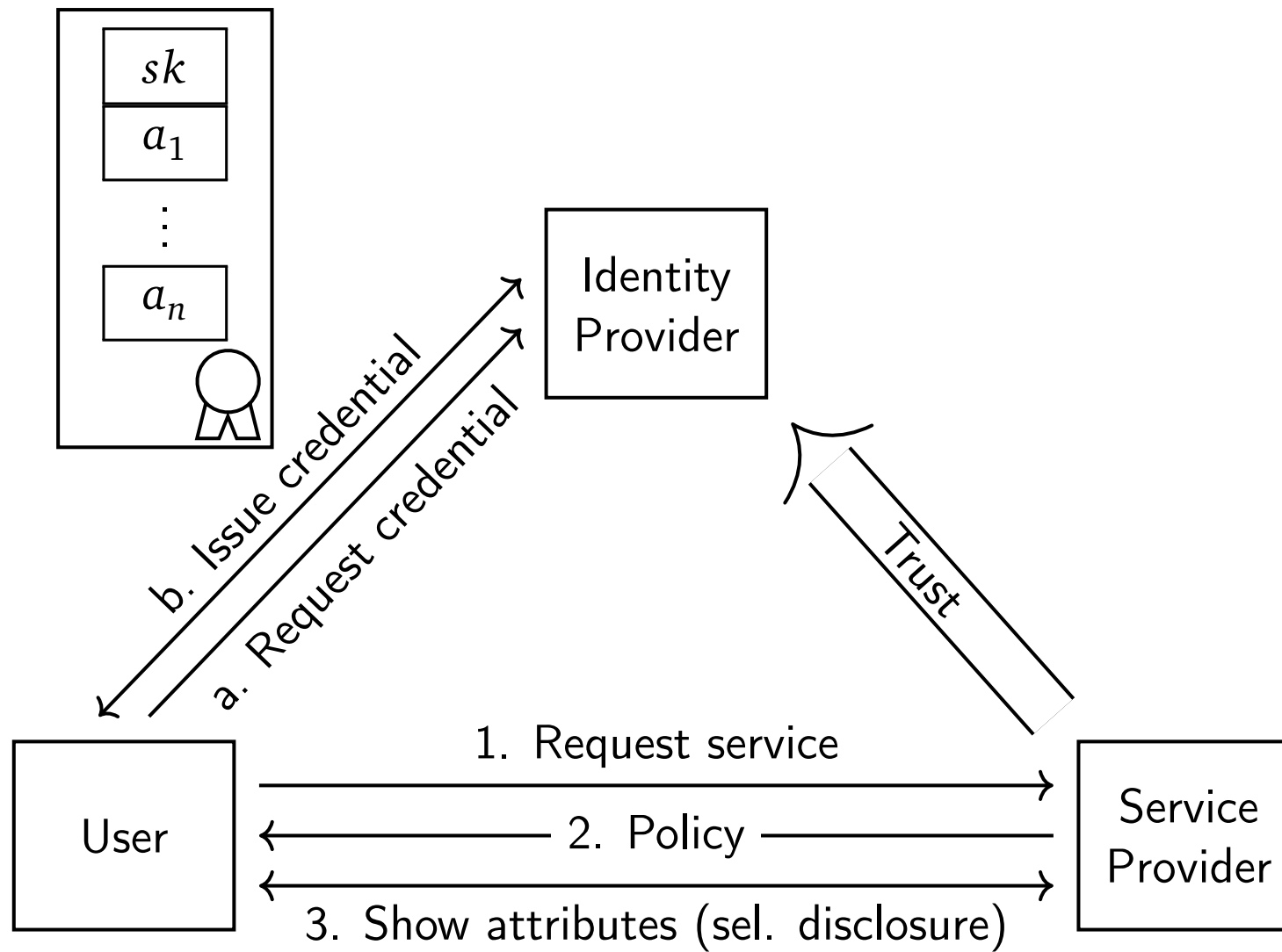
Attribute-based credential – selective disclosure



ABC issuing



An ABC system



ABC summary

- ▶ Independence between issuing and showing: time and protocol
- ▶ Credential: **security** for the system
 - ▶ Authenticity
 - ▶ Integrity
 - ▶ Non-transferability
- ▶ Credential: **privacy** for the user
 - ▶ Selective disclosure
 - ▶ Issuer unlinkability (*even the issuer can not identify a non-identifying attribute when it is disclosed*)
 - ▶ Multi-show unlinkability (*it is impossible to distinguish whether two of the same non-identifying, disclosed attributes belong to the same user*)
- ▶ ...and all of this with **elegant mathematics!**

T H A N K Y O U !