THE EU DIGITAL WALLET, AN OPPORTUNITY FOR HIGHER SECURITY AND HIGHER PRIVACY

MARYLINE LAURENT
RST DEPARTMENT, SAMOVAR, TÉLÉCOM SUDPARIS,
INSTITUT POLYTECHNIQUE DE PARIS

ON THE WAY TO A EU DIGITAL WALLET

FOR A HIGHLY SECURE AND TRUSTWORTHY MARKET

Driven by the revision of the EU eIDAS* regulation

Forecast that 80% of European citizens and residents will be equipped with a EU digital wallet by 2030

To access administrative and commercial services across borders

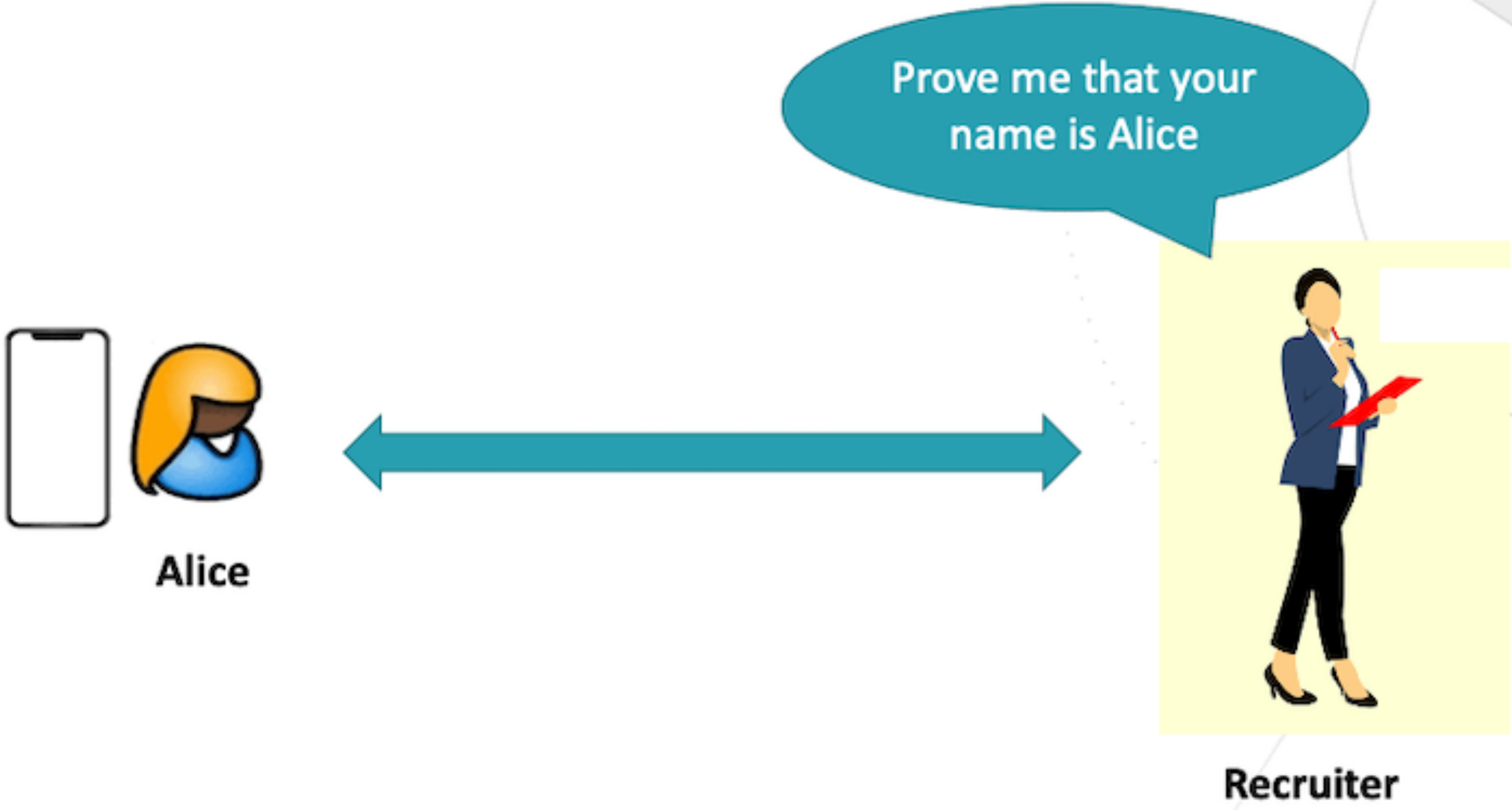
For supporting trust services (electronic signature, timestamping…)

For certifying identities and attributes (to counteract impersonations)

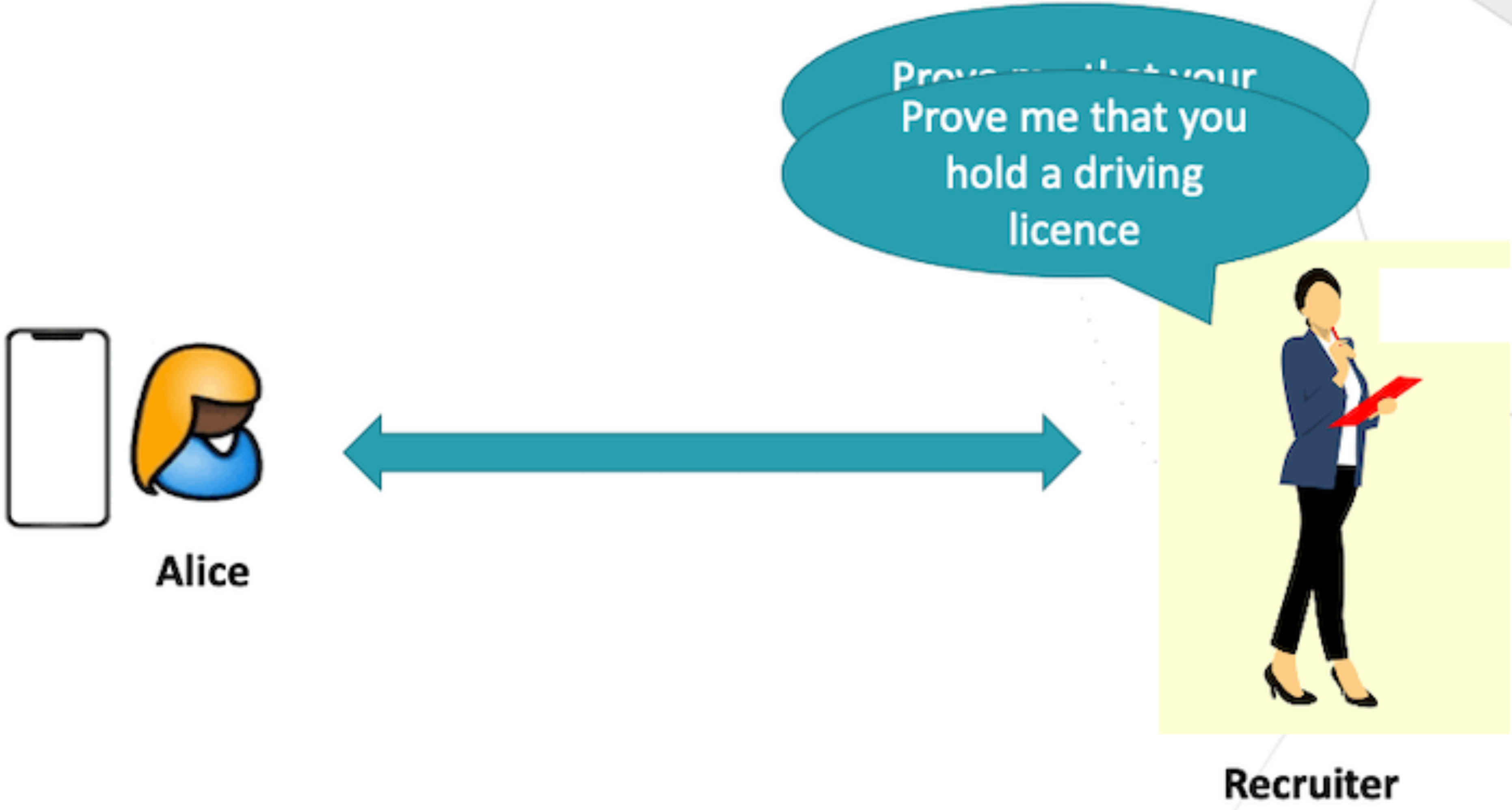
Full study currently conducted by the chair Values and Policies of Personal Information of Institut Mines-Télécom

- eIDAS1: REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- eIDAS2: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final, 3 June 2021

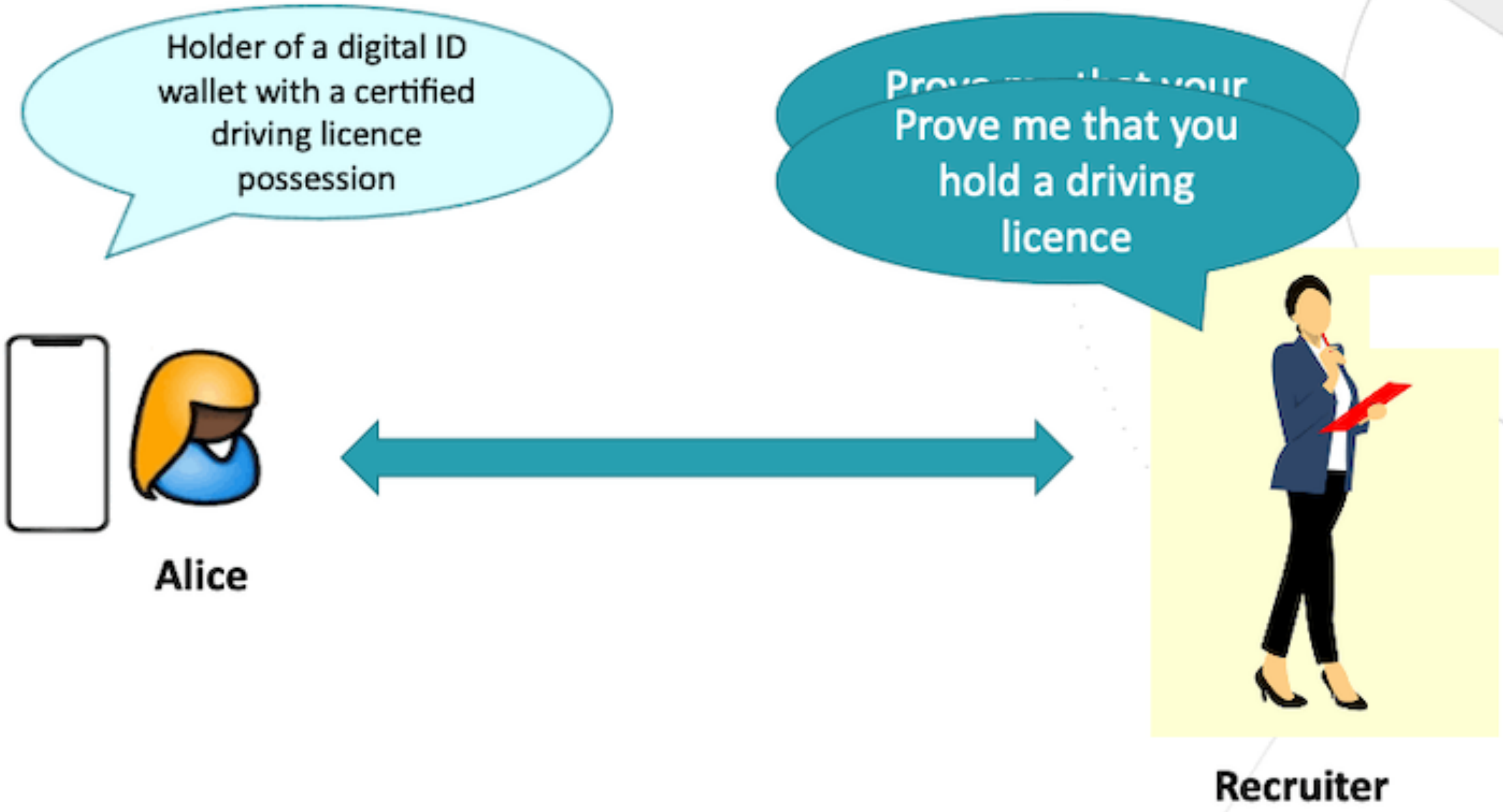
A CASE STUDY



A CASE STUDY

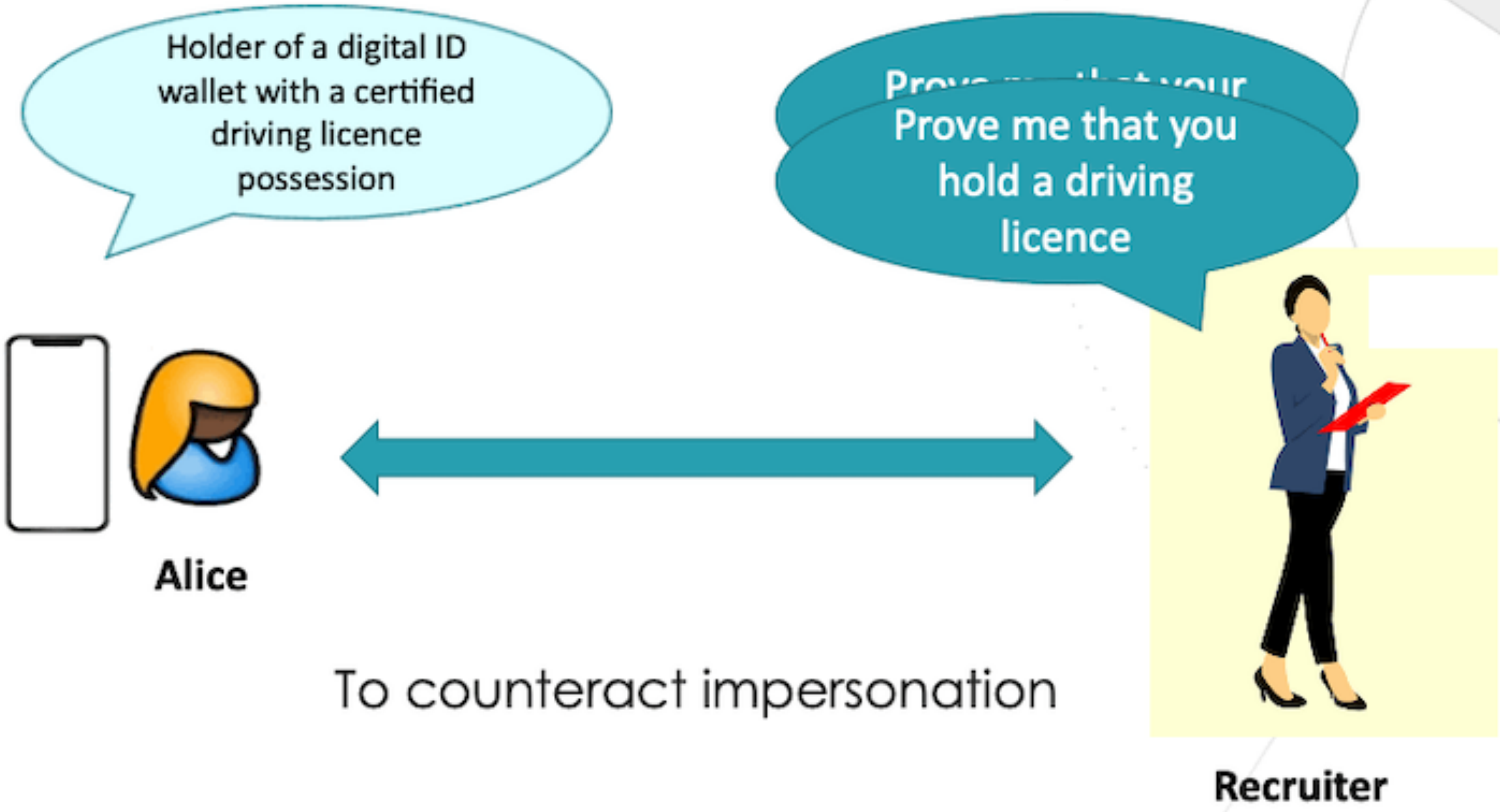

Prove me that your
Prove me that you hold a driving licence
Alice
Recruiter

A CASE STUDY



Holder of a digital ID wallet with a certified driving licence possession
Prove me that you hold a driving licence
Alice
Recruiter

A CASE STUDY



Holder of a digital ID wallet with a certified driving licence possession

Prove me that your

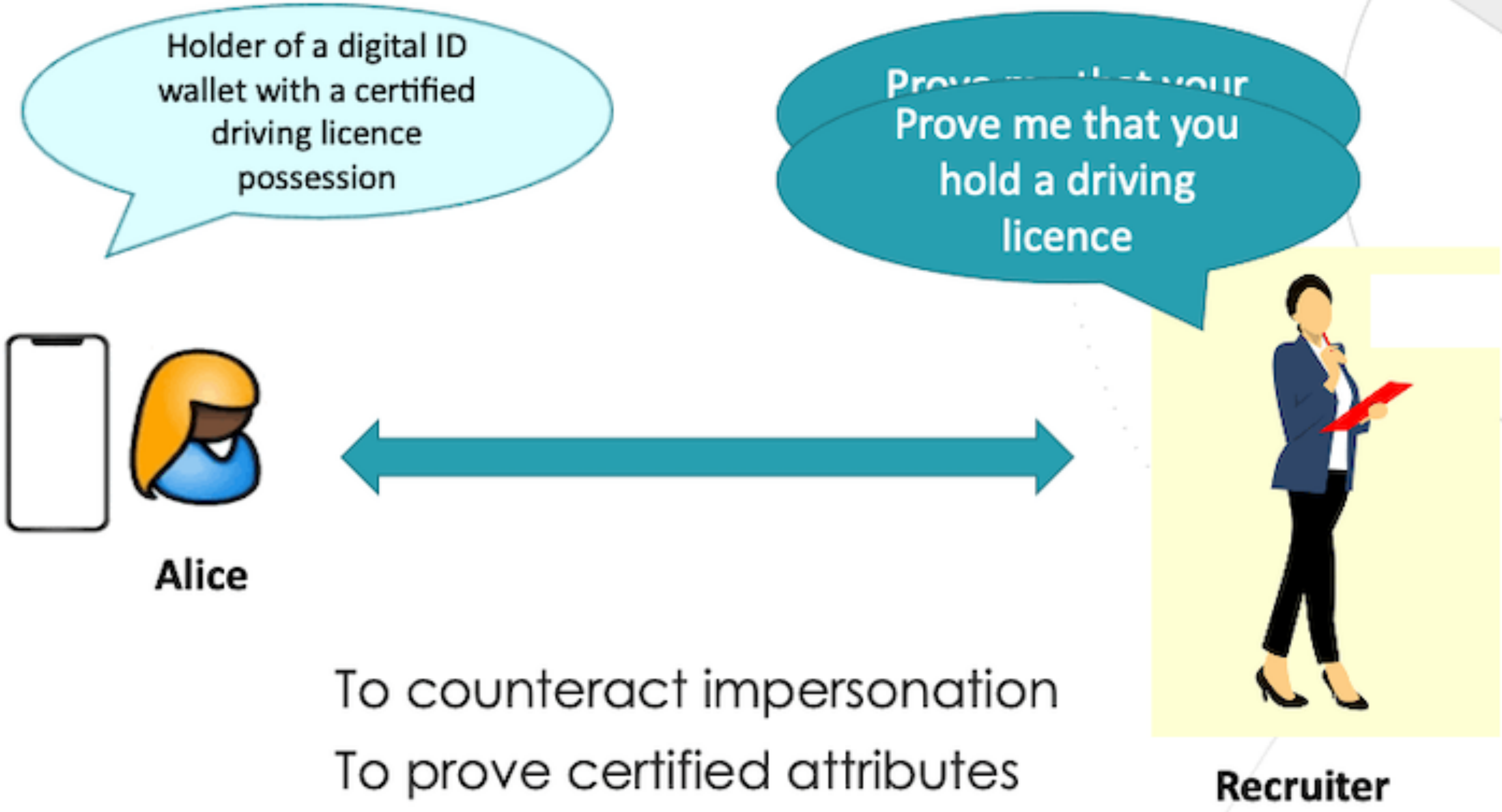
Prove me that you hold a driving licence

Alice

Recruiter

To counteract impersonation

A CASE STUDY


Holder of a digital ID wallet with a certified driving licence possession
Prove me that your
Prove me that you hold a driving licence
Alice
Recruiter

To counteract impersonation

To prove certified attributes

HIGH-IMPACT REQUIREMENTS

TO SUPPORT PERSONAL DATA PROTECTION AND FREEDOMS

Users must remain at the center of his identities and personal data

Users must be able to minimize data… (GDPR)

Users must be able to choose on the offer of wallet providers and software tools

Users must still be able to interact with some services under pseudonyms as most services are using this facility

Alice

Social network platform

HIGH-IMPACT REQUIREMENTS

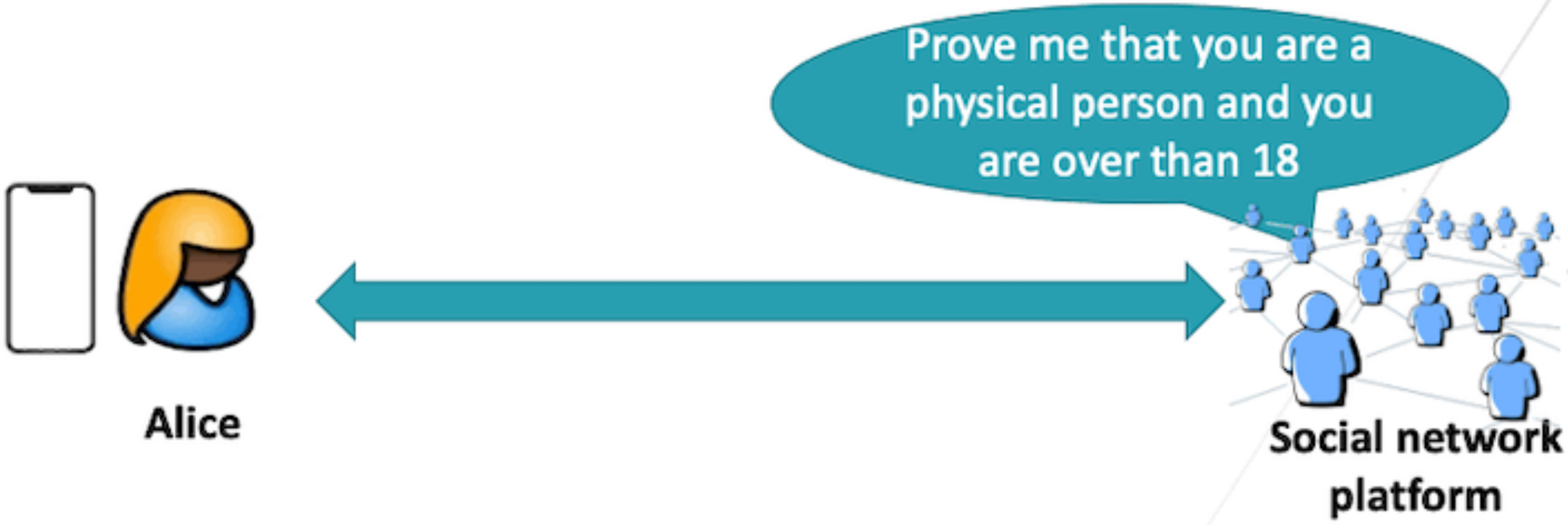
TO SUPPORT PERSONAL DATA PROTECTION AND FREEDOMS

Users must remain at the center of his identities and personal data

Users must be able to minimize data… (GDPR)

Users must be able to choose on the offer of wallet providers and software tools

Users must still be able to interact with some services under pseudonyms as most services are using this facility


Prove me that you are a physical person and you are over than 18
Alice
Social network platform

HIGH-IMPACT REQUIREMENTS

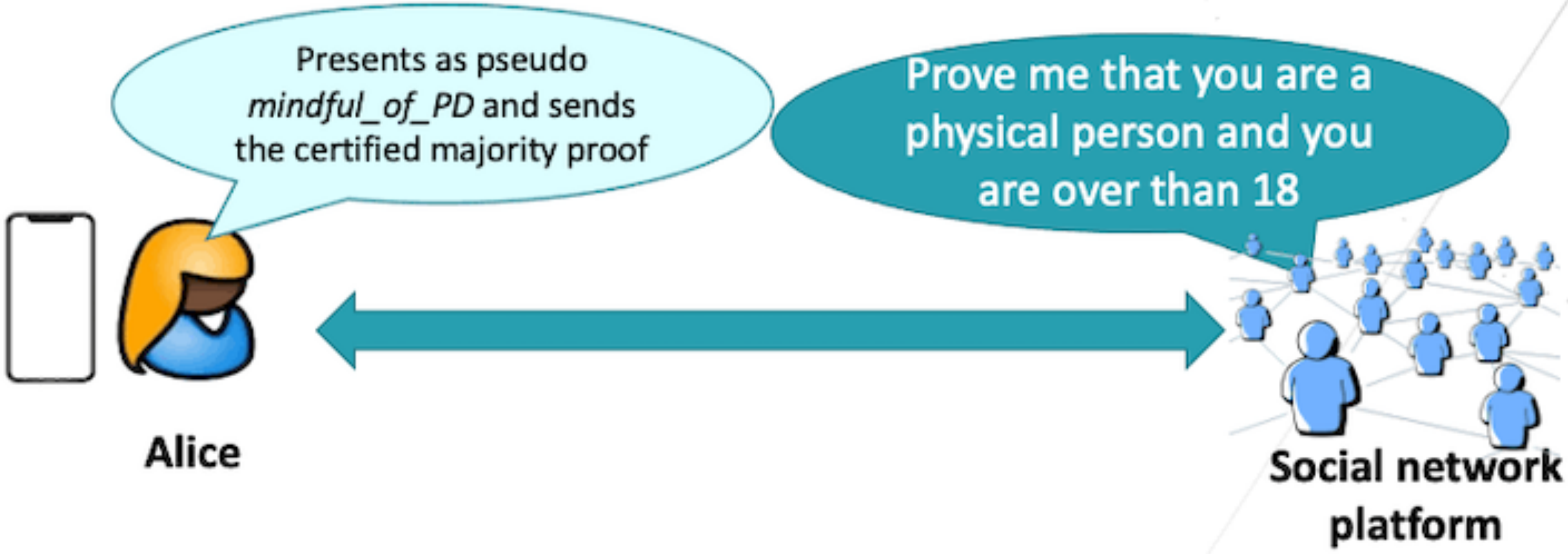
TO SUPPORT PERSONAL DATA PROTECTION AND FREEDOMS

Users must remain at the center of his identities and personal data

Users must be able to minimize data… (GDPR)

Users must be able to choose on the offer of wallet providers and software tools

Users must still be able to interact with some services under pseudonyms as most services are using this facility

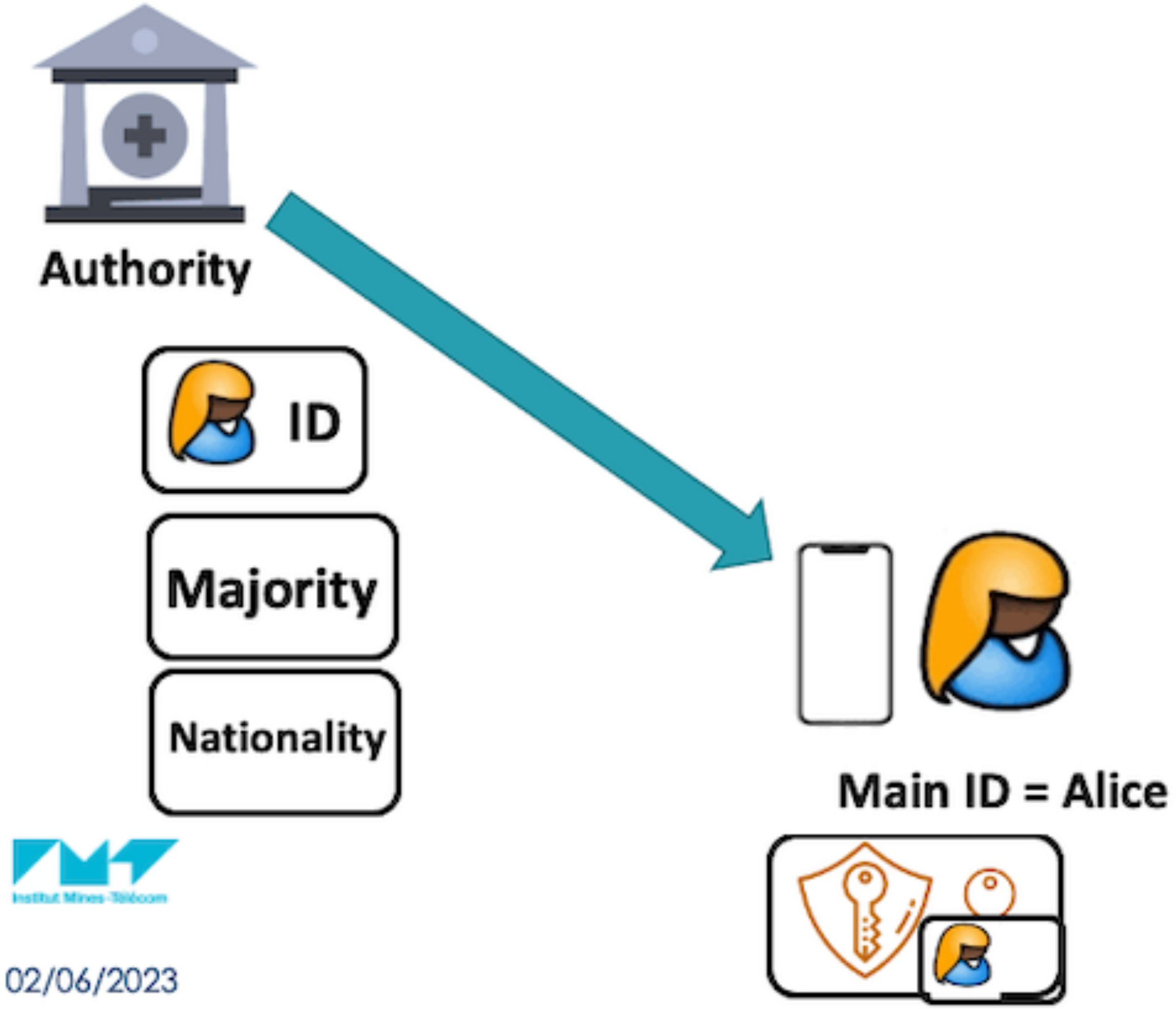

Presents as pseudo *mindful_of_PD* and sends the certified majority proof
Prove me that you are a physical person and you are over than 18
Alice
Social network platform

WHAT IS THE PIMA APPROACH ABOUT?

A solution to support pseudomyms, proof of identity, data minimization, attribute certification

WHAT IS THE PIMA APPROACH ABOUT?

A solution to support pseudomyms, proof of identity, data minimization, attribute certification



Authority

ID

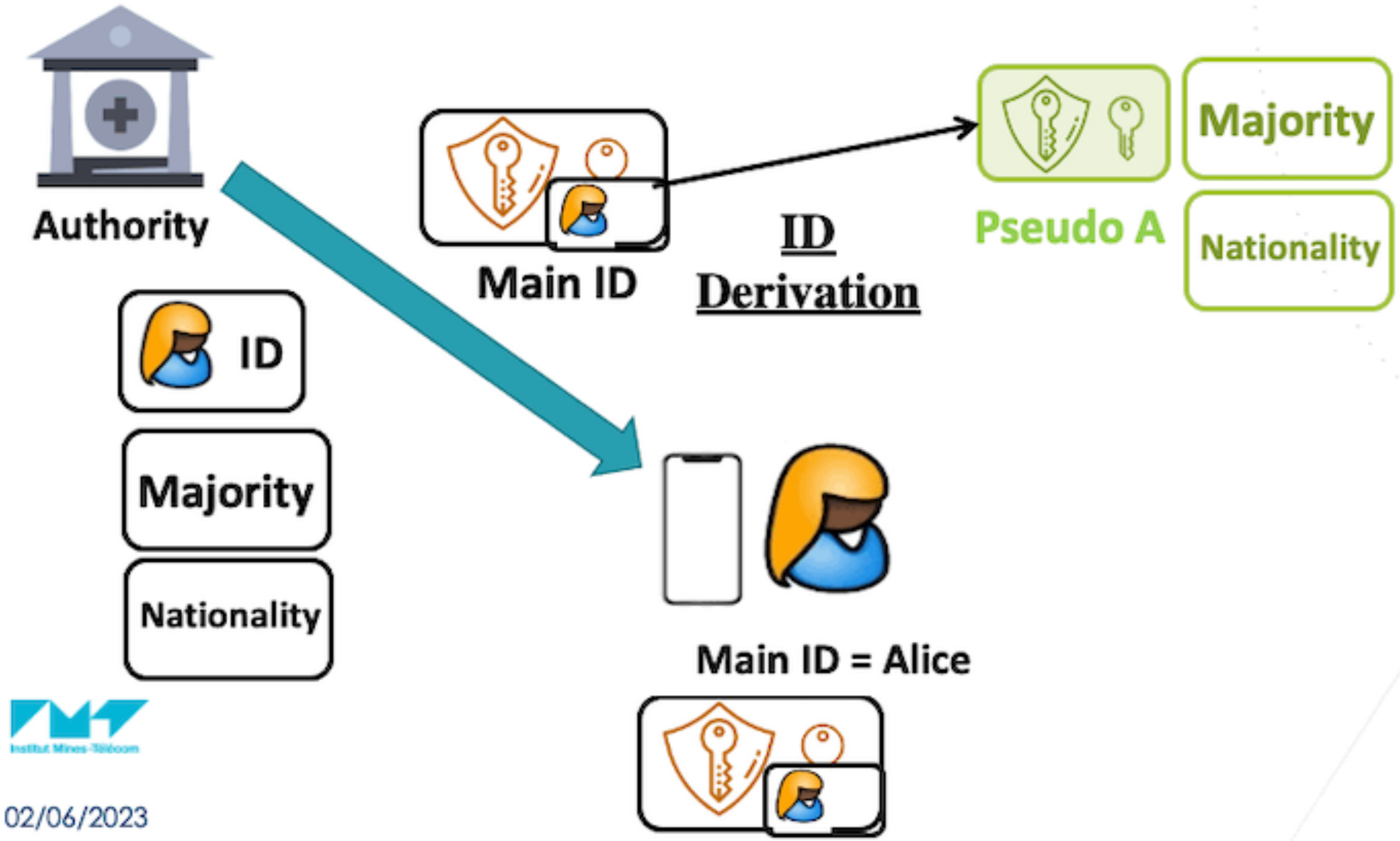
Majority

Nationality

Main ID = Alice

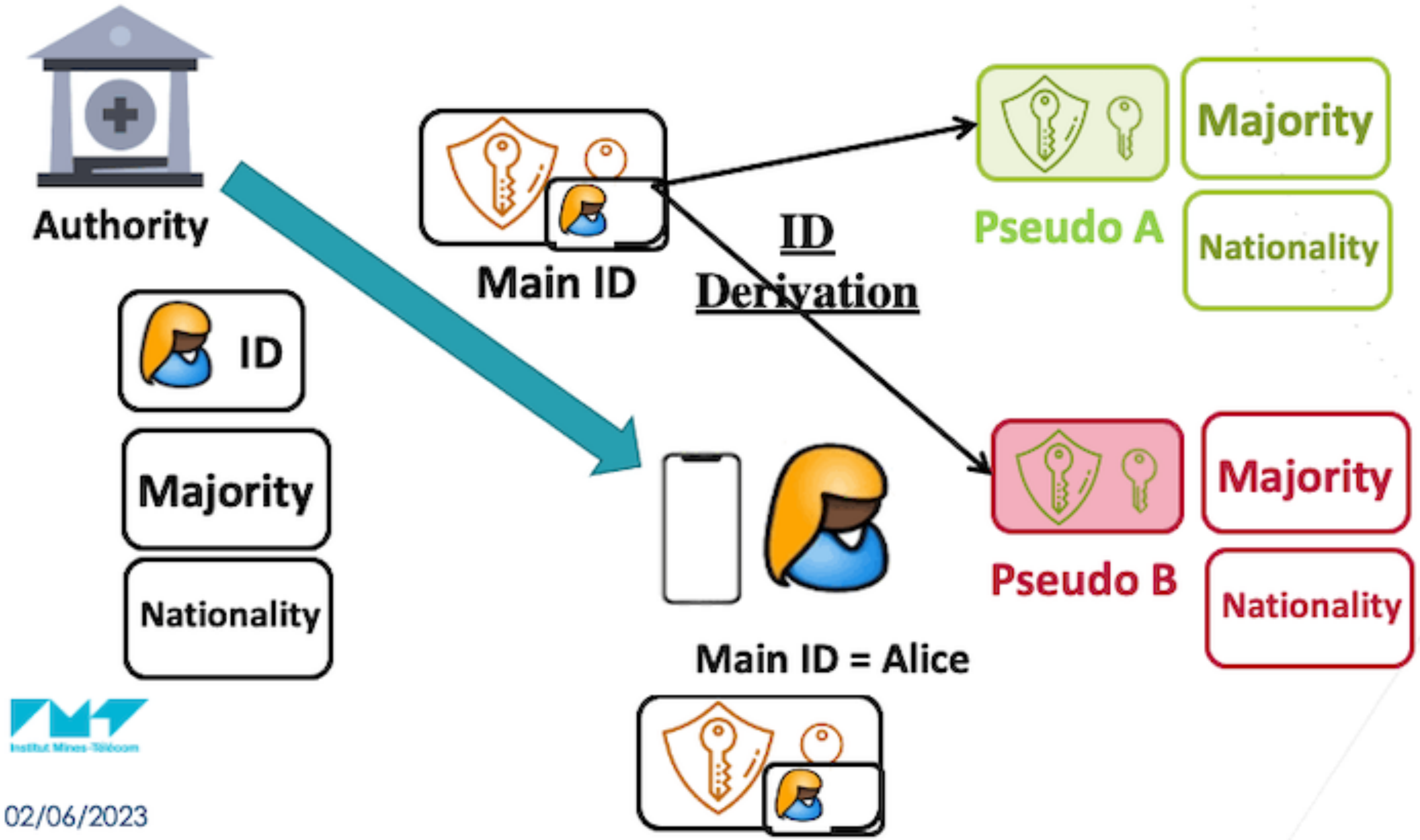
WHAT IS THE PIMA APPROACH ABOUT?

A solution to support pseudomyms, proof of identity, data minimization, attribute certification



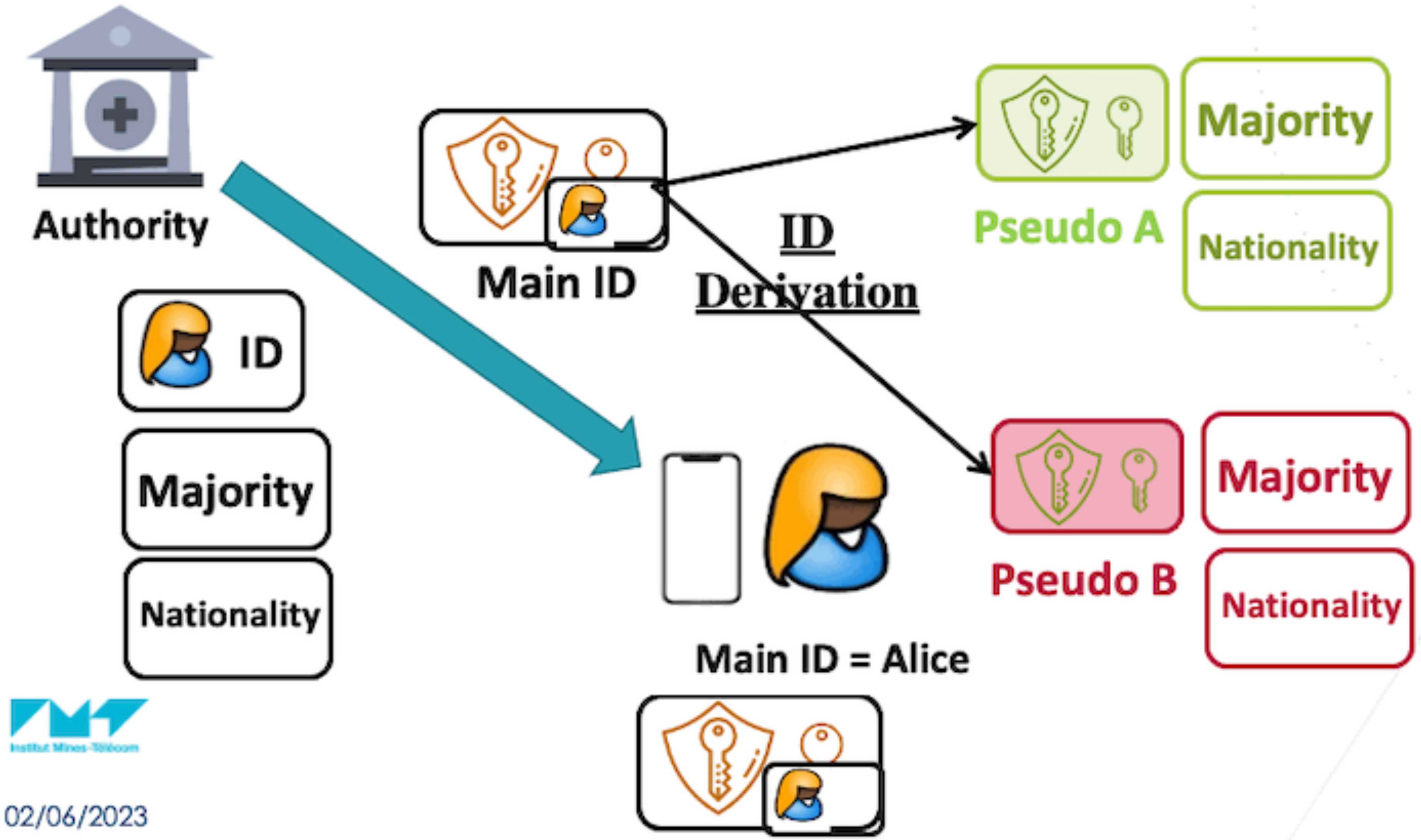
WHAT IS THE PIMA APPROACH ABOUT?

A solution to support pseudomyms, proof of identity, data minimization, attribute certification



WHAT IS THE PIMA APPROACH ABOUT?

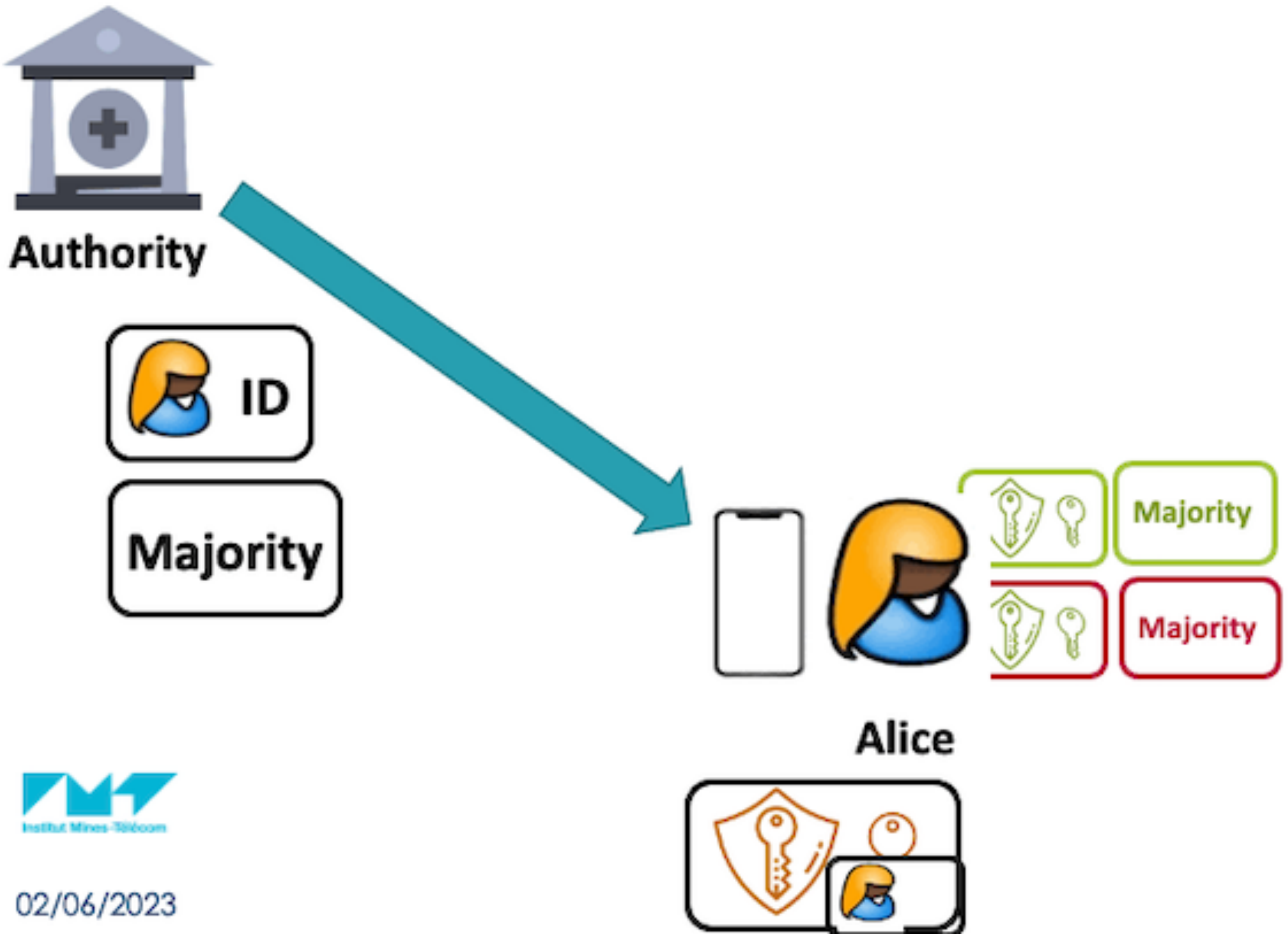
A solution to support pseudomyms, proof of identity, data minimization, attribute certification



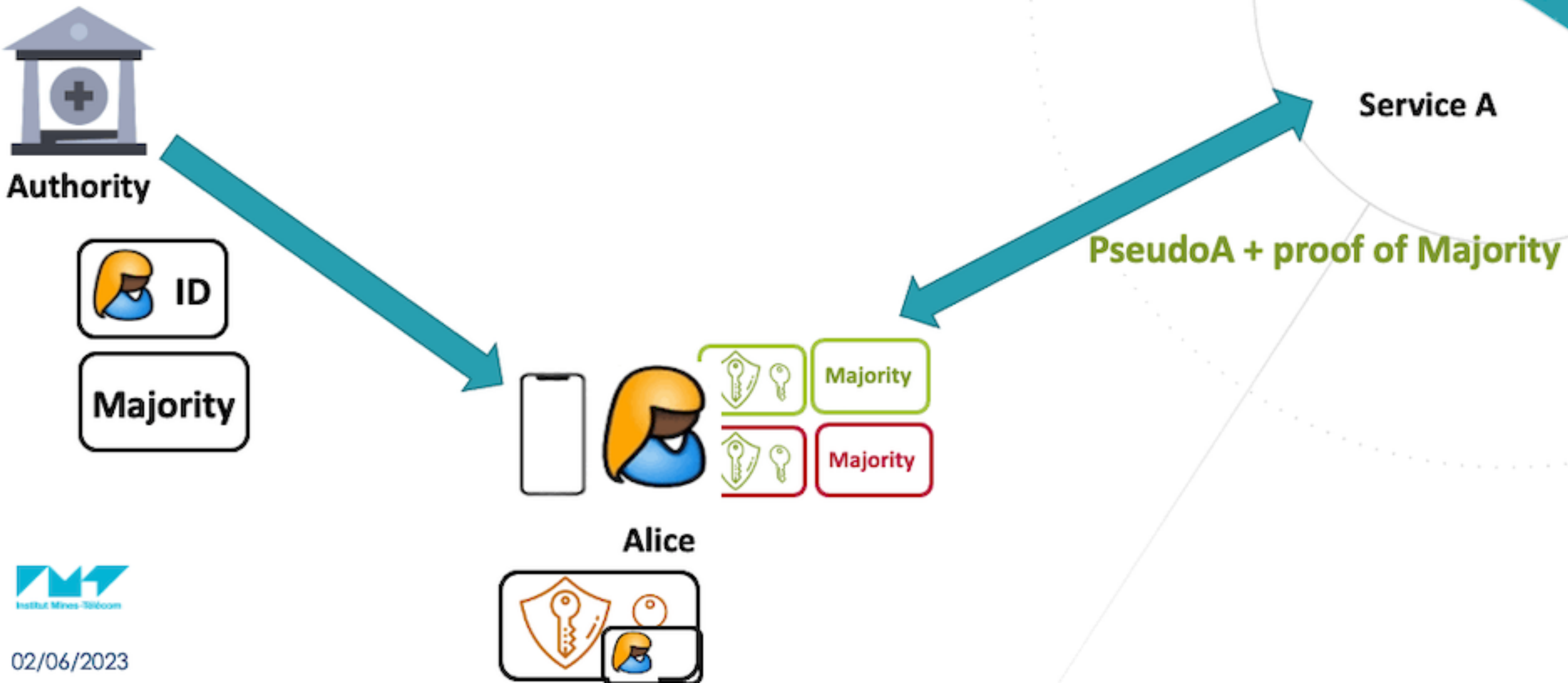
Works carried out within a PhD thesis conducted by Dr. Souha Masmoudi under the co-supervision of Maryline Laurent and Nesrine Kaâniche
Funded by VP-IP chair

Technology behind: Adaptation of the malleable Pointcheval-Sanders signature enabling a user to modify an attribute certificate

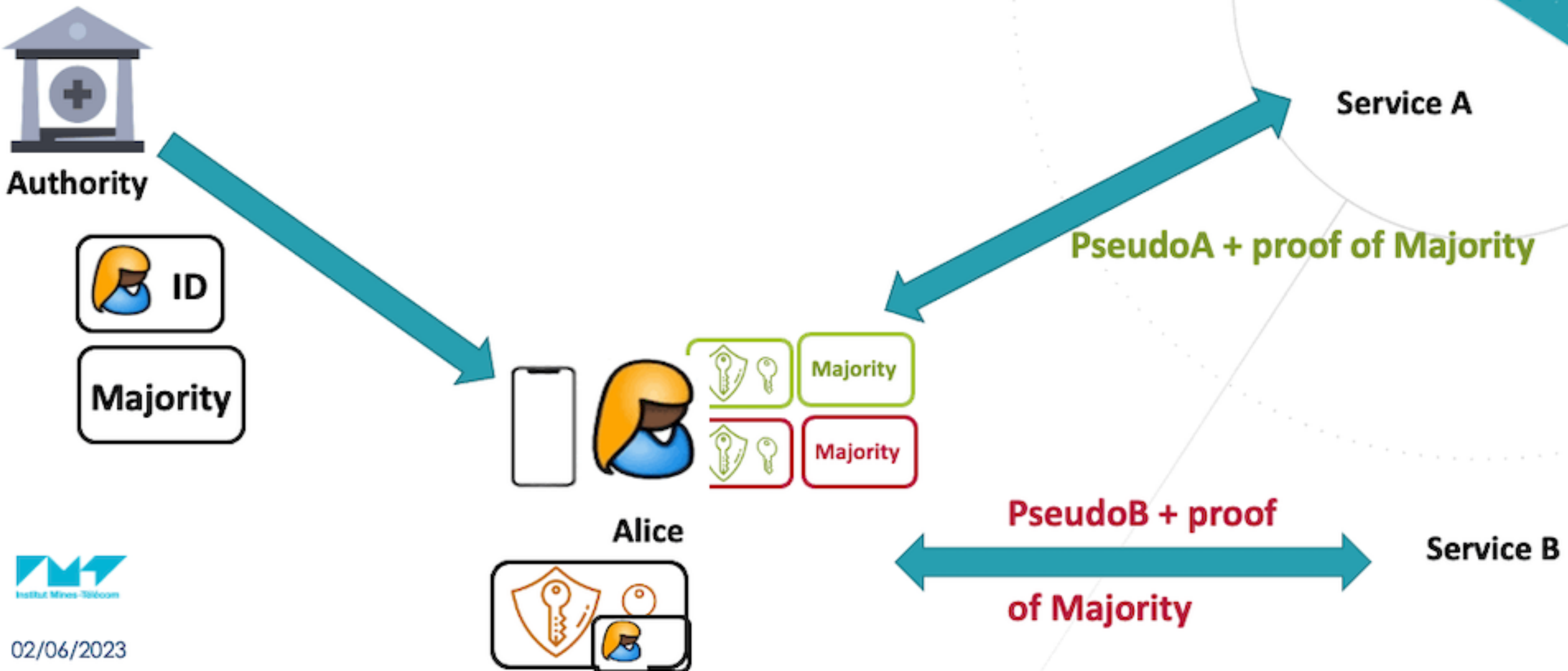
WHAT IS THE PIMA APPROACH ABOUT?



WHAT IS THE PIMA APPROACH ABOUT?



WHAT IS THE PIMA APPROACH ABOUT?



Authority

ID

Majority

Alice

Majority

Majority

Service A

PseudoA + proof of Majority

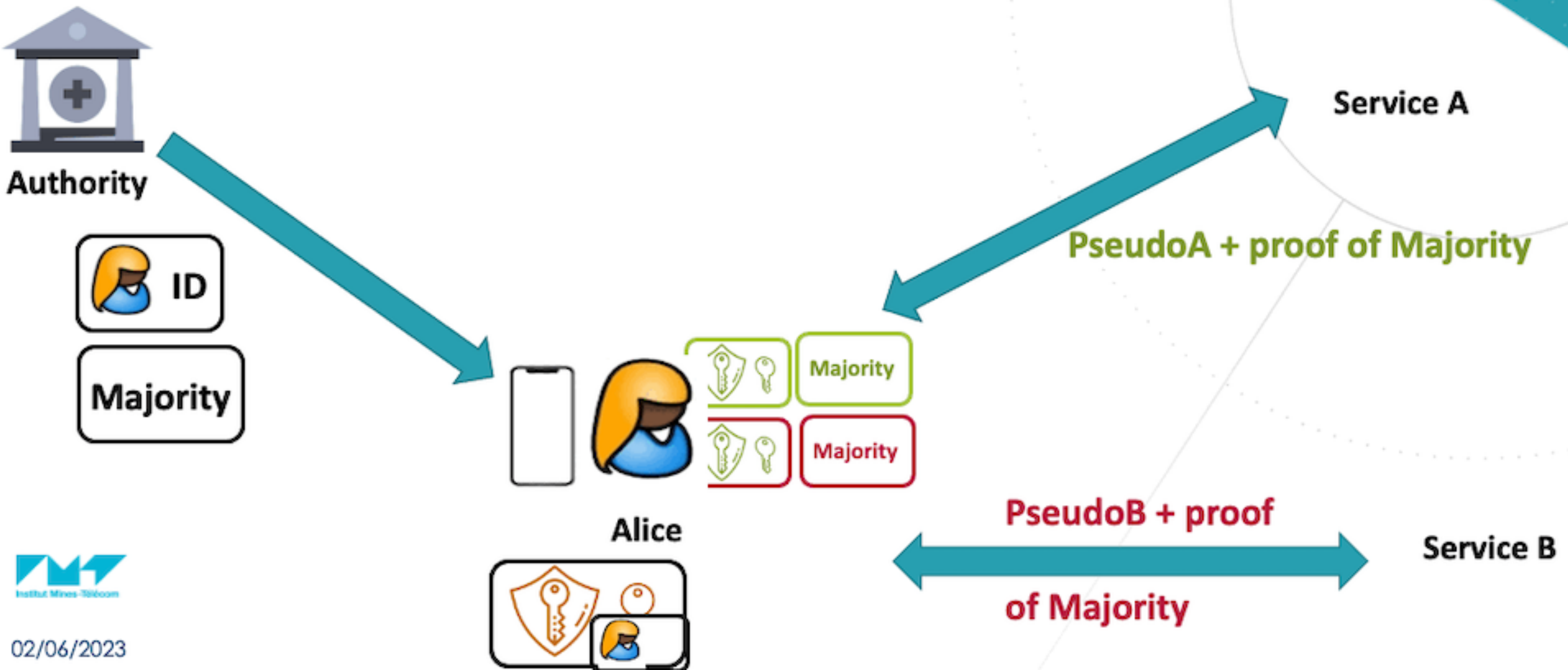
PseudoB + proof

of Majority

Service B

WHAT IS THE PIMA APPROACH ABOUT?

Technical privacy properties:



Authority

ID

Majority

Alice

Majority

Majority

PseudoA + proof of Majority

Service A

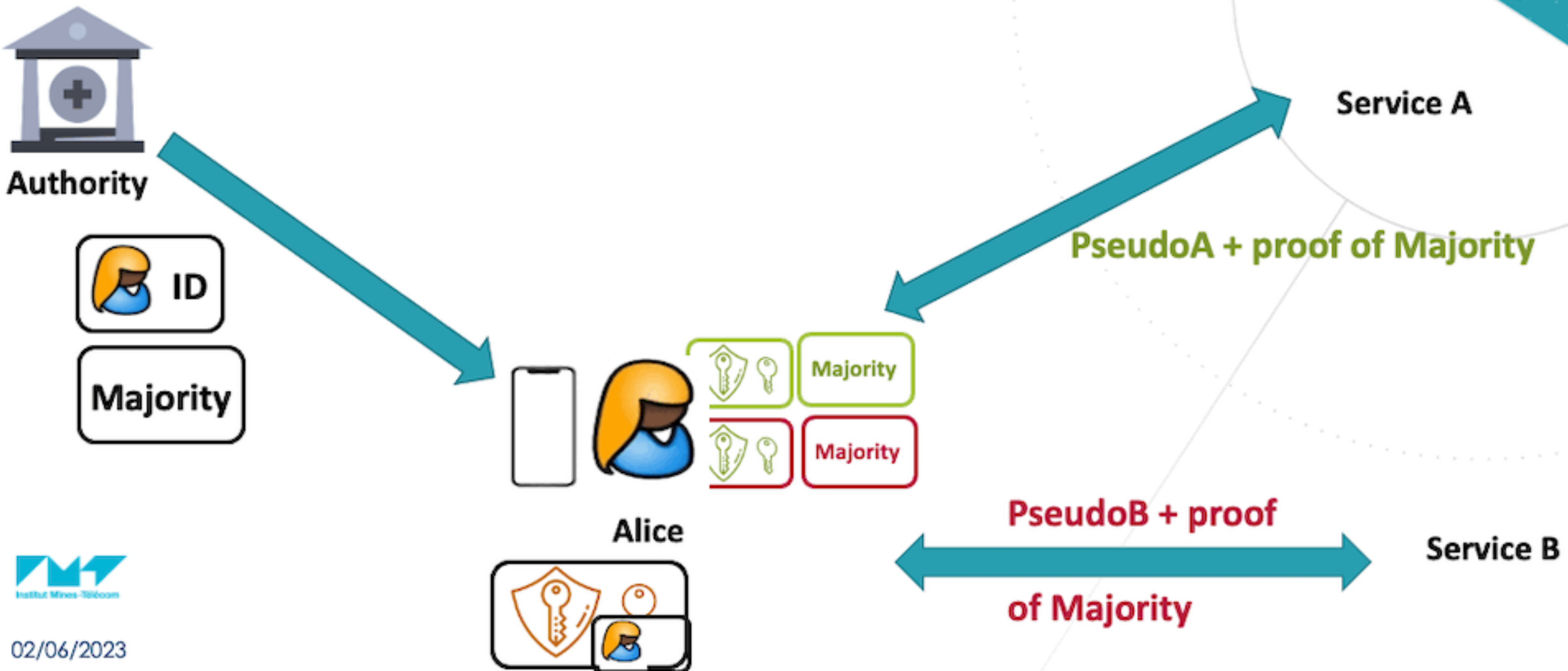
PseudoB + proof of Majority

Service B

WHAT IS THE PIMA APPROACH ABOUT?

Technical privacy properties:

Pseudonymity: Service A does not know that PseudoA is Alice

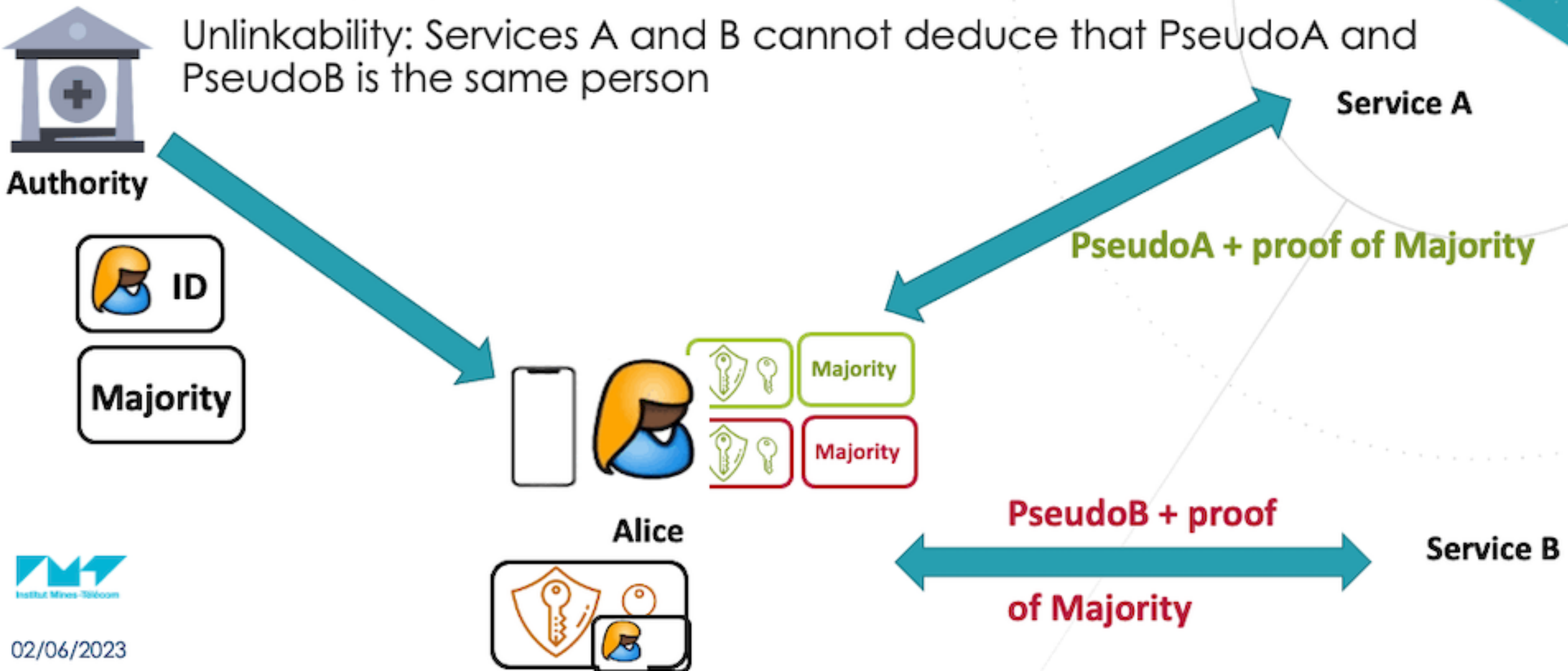


WHAT IS THE PIMA APPROACH ABOUT?

Technical privacy properties:

Pseudonymity: Service A does not know that PseudoA is Alice

Unlinkability: Services A and B cannot deduce that PseudoA and PseudoB is the same person



CONCLUSION

Next steps: adoption of eIDAS2 during summer 2023; an EU digital wallet expected for 2026-2027

A lot of research until then still needed to develop a wallet that respects EU cybersecurity regulations and standards, and GDPR

A strict framework also needed to avoid excessive traceability of users

Further information

PRIMA

Description: http://www-public.imtbs-tsp.eu/~lauren_m/PROJECT/PIMA.html

Source code: https://github.com/soumasmoudi/malleable_unlinkable_sig

S. Masmoudi, M. Laurent, N. Kaaniche. PIMA: A privacy-preserving identity management system based on an unlinkable MAlleable signature. JNCA, Elsevier, 2022

VP-IP chair

http://cvpip.wp.mines-telecom.fr/

@CVPIP

Chair VALUES AND POLICIES OF PERSONAL INFORMATION
Data, identities and trust in the digital age