Leveraging Passkeys in Regulated Markets

Rolf Lindemann

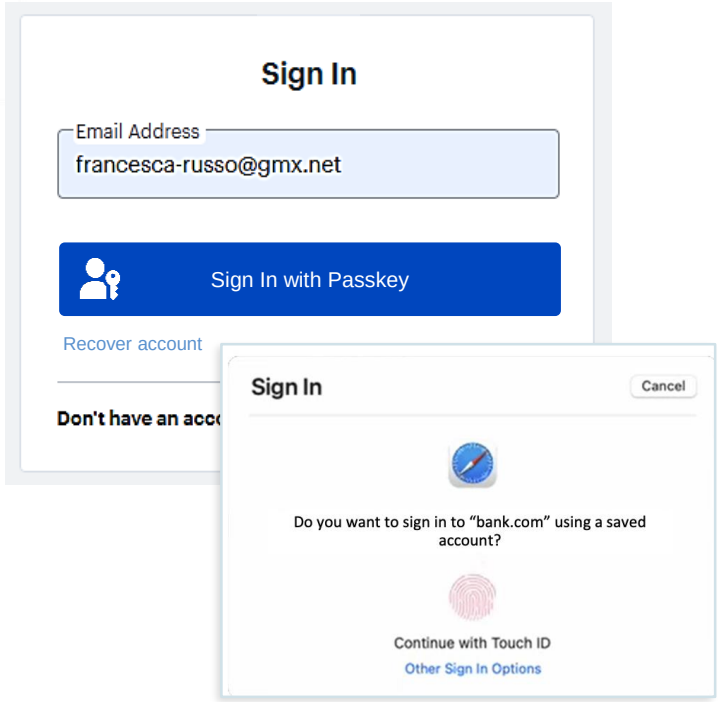
VP Products

Nok Nok

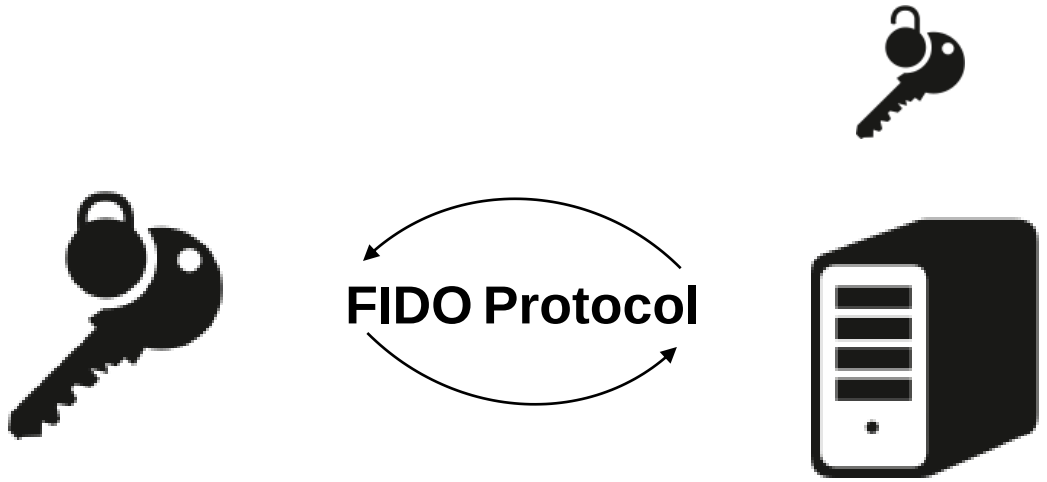
Passkeys surface the realities of believed truths…

FIDO Passkeys

1st Factor



2nd Factor



User Authenticates

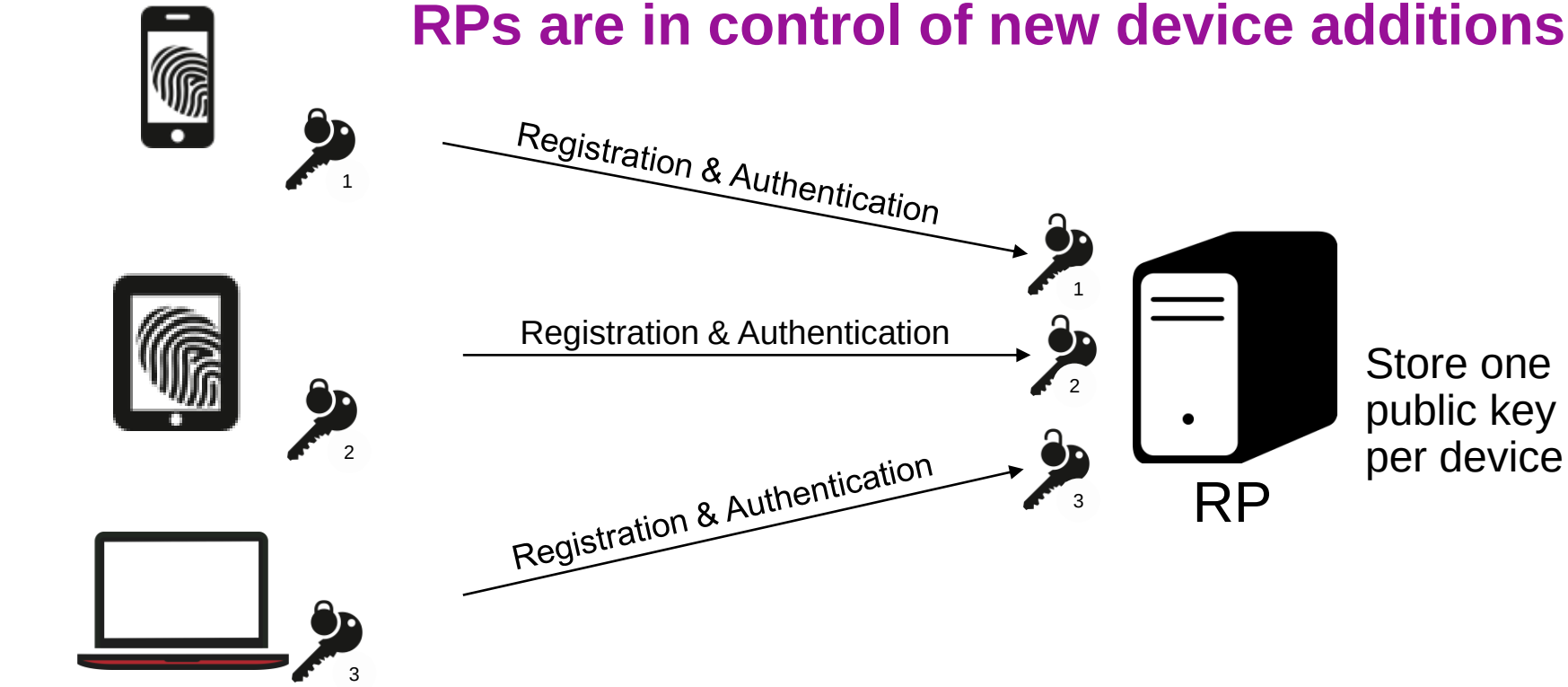
Key is Unlocked on User’s Device

Key is Validated

FIDO: Simple Phishing-Resistant MFA

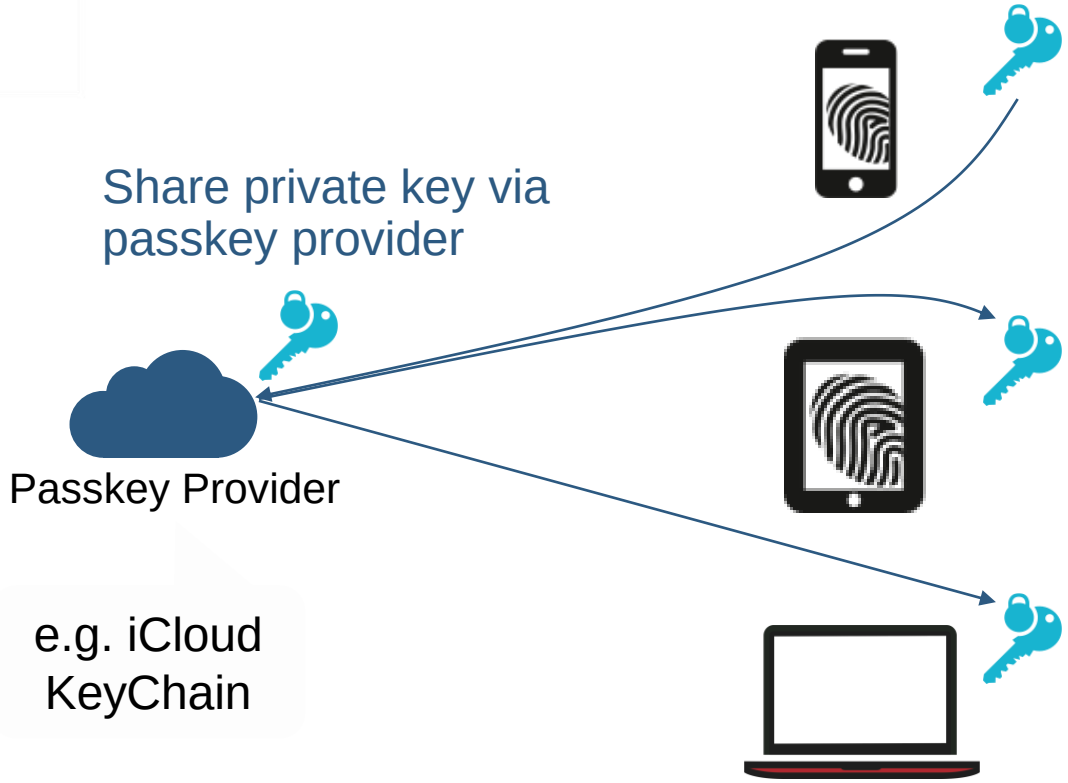
Device-Bound Credentials

RPs are in control of new device additions

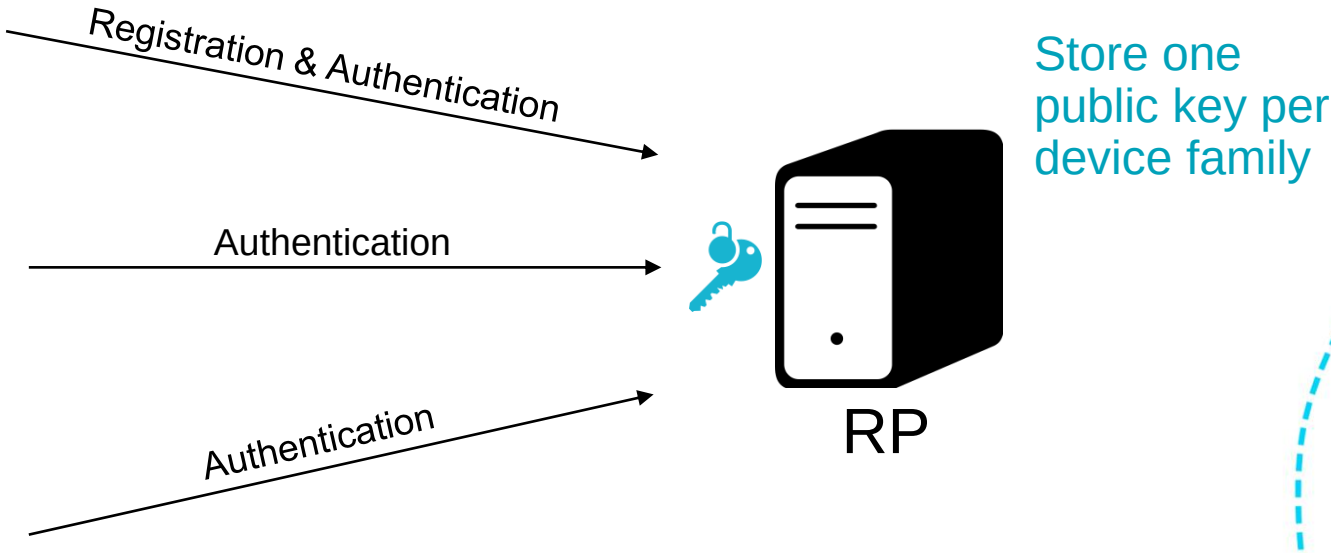


Private Key cannot leave device
Stored in (TEE/SE)

Synced Passkeys



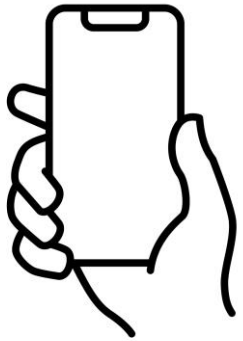
How are regulated entities impacted?



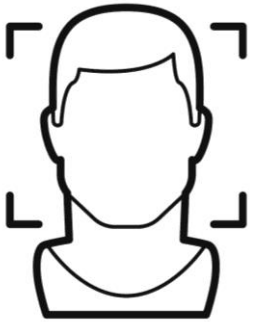
Regulatory Requirements

Authentication “Factors” or “Elements”

Knowledge Factor



Possession Factor

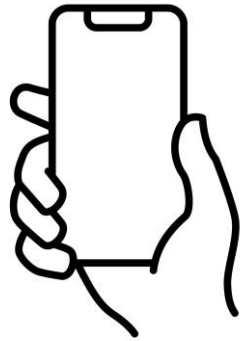


Inherence Factor

Authentication “Factors” or “Elements”

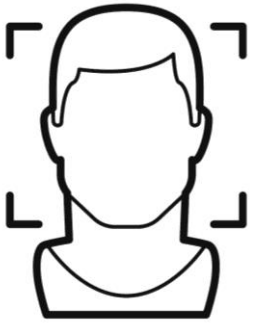
Knowledge Factor

Password



Possession Factor

OTP Token/Phone



Inherence Factor

Fingerprint, Face

Regulatory Authentication Requirements

PSD2 RTS Article 4

"…authentication shall be based on **two or more elements** which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code."

SP 800 63 v4 (IPD), sec 4.2

At AAL 2: "Proof of possession and control of **two distinct authentication factors** is required through secure authentication protocols"

Regulatory Authentication Requirements

PSD2 RTS Article 4

"…authentication shall be based on **two or more elements** which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code."

PSD2 RTS (6)

"…security features for the elements of strong customer authentication categorised as knowledge ***(something only the user knows)*** […] ensure that those ***elements are independent****, so that the breach of one does not compromise the reliability of the others […]"*

SP 800 63 v4 (IPD), sec 4.2

At AAL 2: "Proof of possession and control of **two distinct authentication factors** is required through secure authentication protocols"

SP 800 63 v4 (IPD), sec 5.1.1

"A Memorized Secret authenticator—commonly referred to as a password or, if numeric, a PIN — is a secret value intended to be ***chosen and memorized by the user****. […] A memorized secret is something you know."*

But in Practice…

- In 62% of the cases, the password is written down, so a “Look-Up Secret”
- Only in 30% of the cases, the password is a “knowledge factor”
- … and I don’t even know most of my passwords…

Source: https://www.passwordmanager.com/password-manager-trust-survey/

Yet still ...

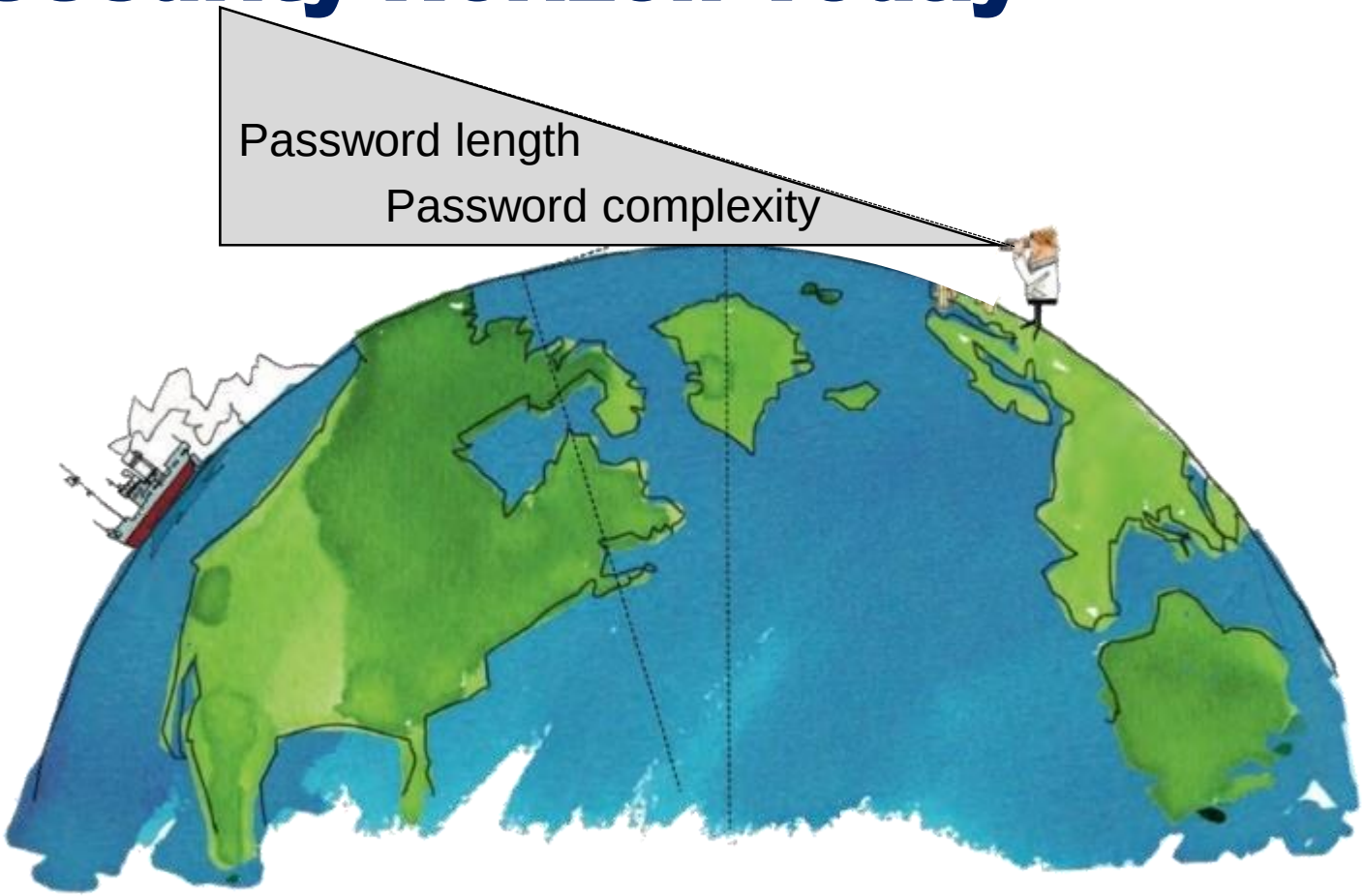
Using password managers reduces risk.

Identity Theft Rate:

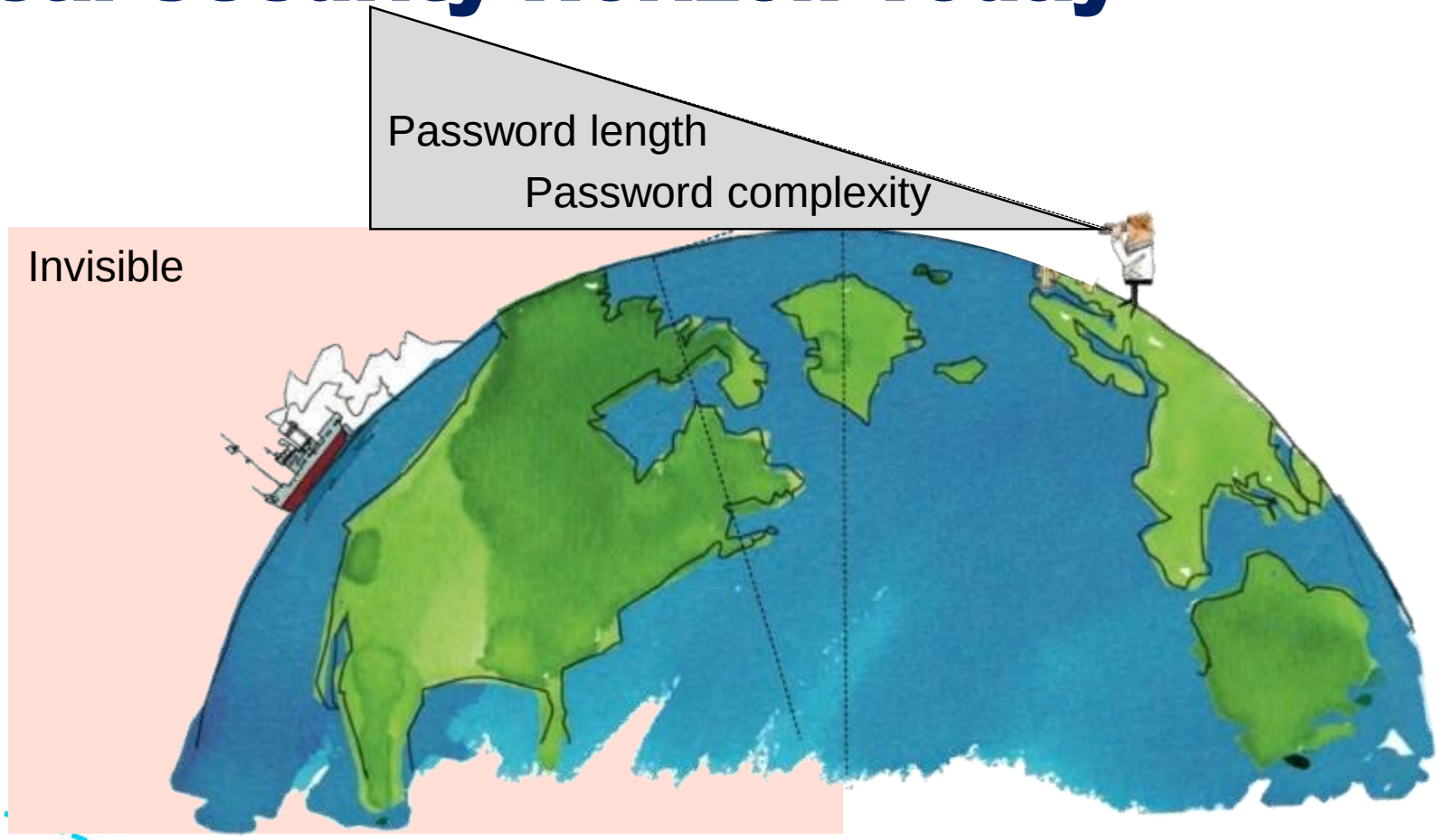
- No Password Manager: 35%
- Password Manager (used correctly): 12%

Source: https://www.passwordmanager.com/password-manager-trust-survey/

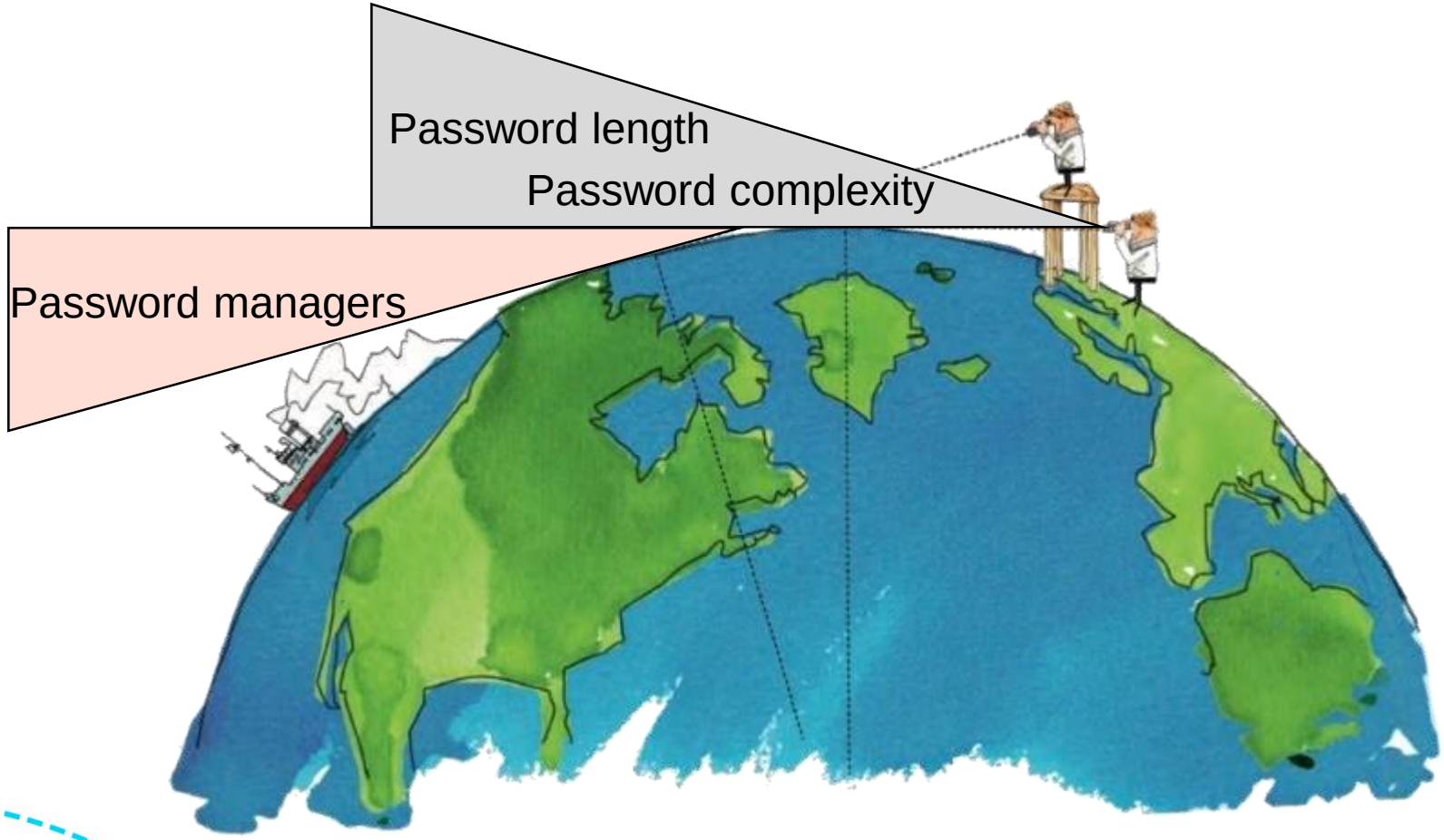
Typical Security Horizon Today



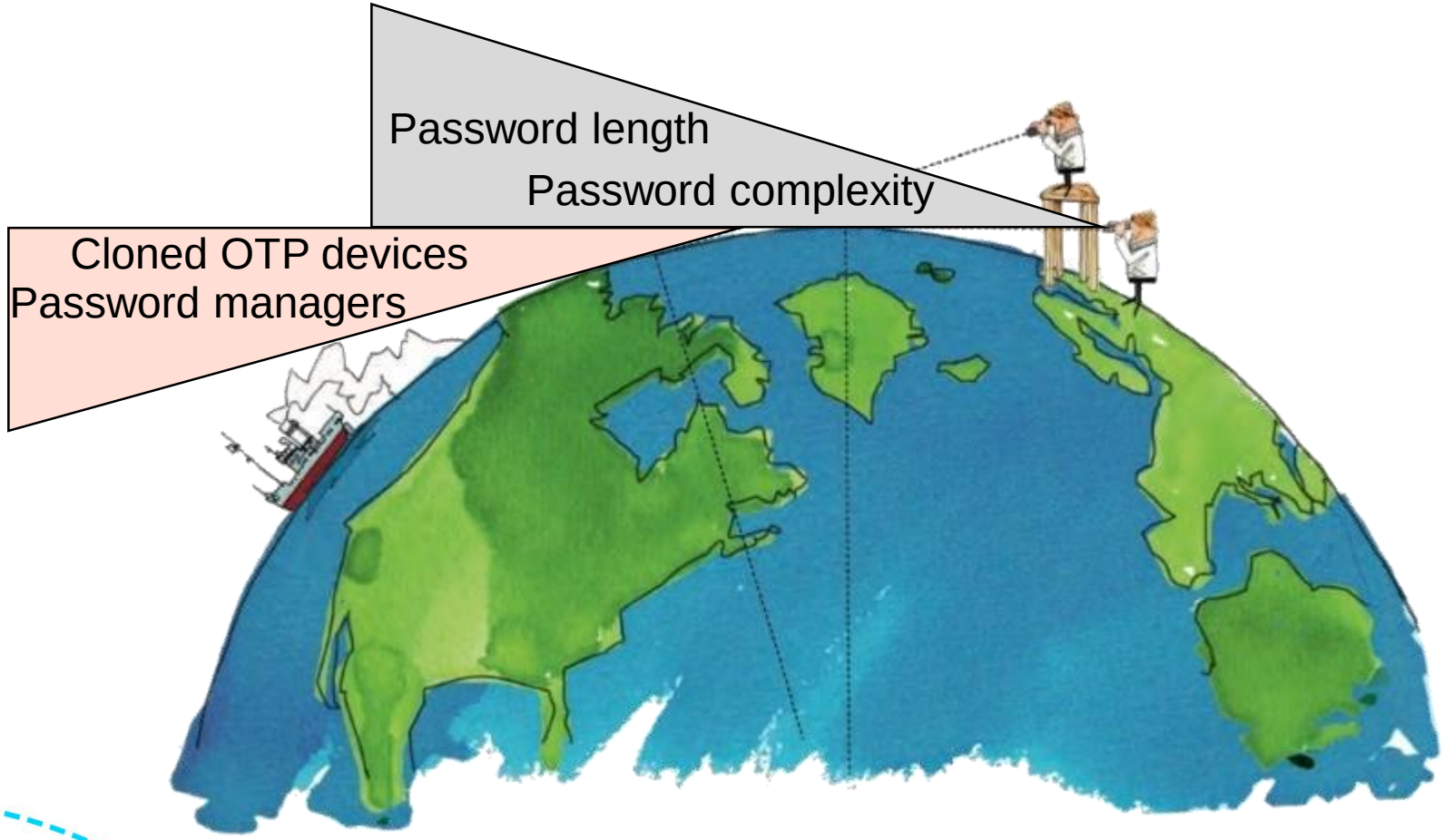
Typical Security Horizon Today



What is Overlooked



What is Overlooked



Summary #1:

The Reality: We cannot rely on passwords being a "Knowledge Factor" and independent from any "Possession Factor"

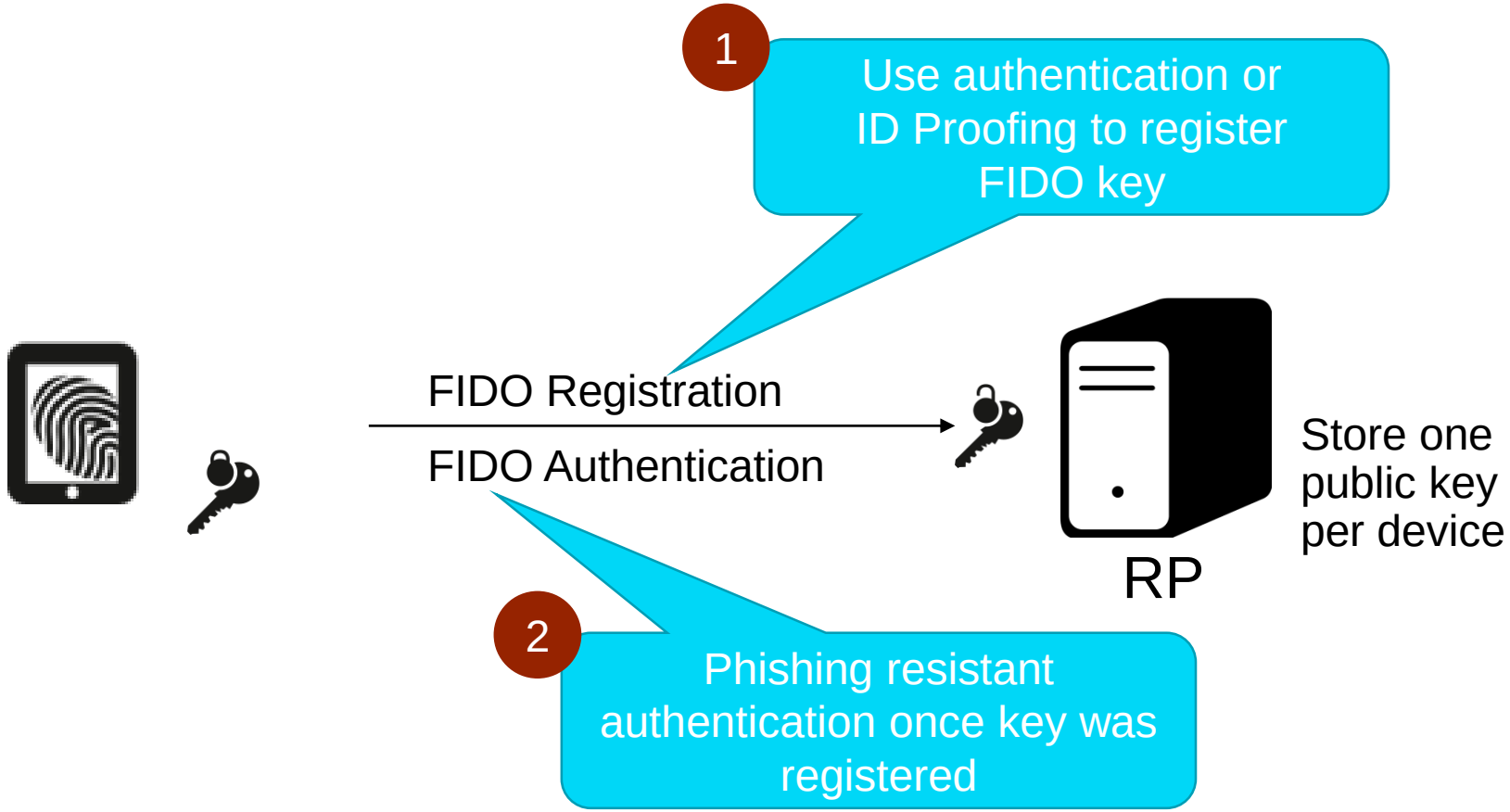
- **Stored passwords** = possession factor
- **SMS OTP** = possession factor

2X possession factor on same device

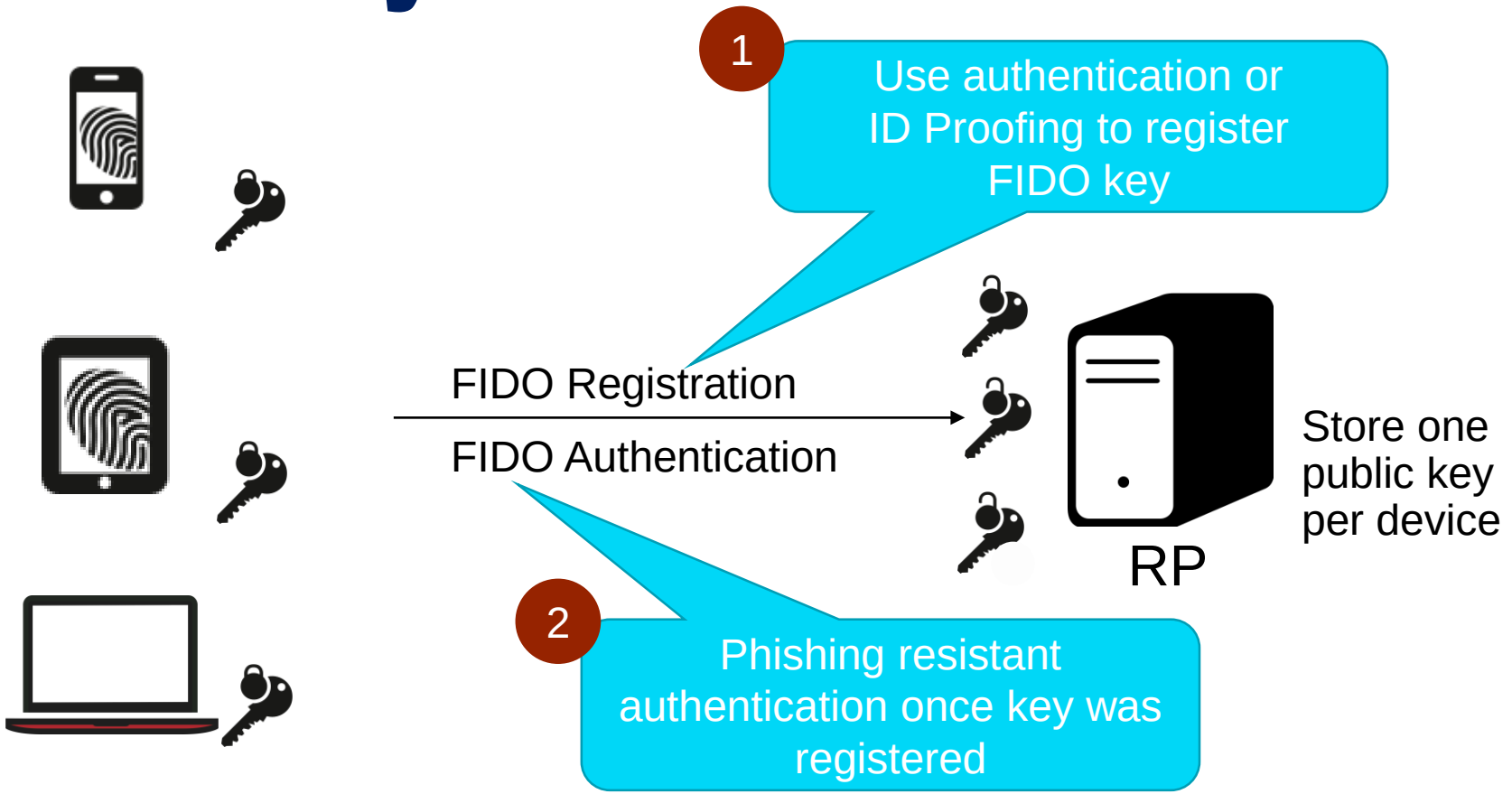
Eating from the Tree of Knowledge

Passkeys in Regulated Markets

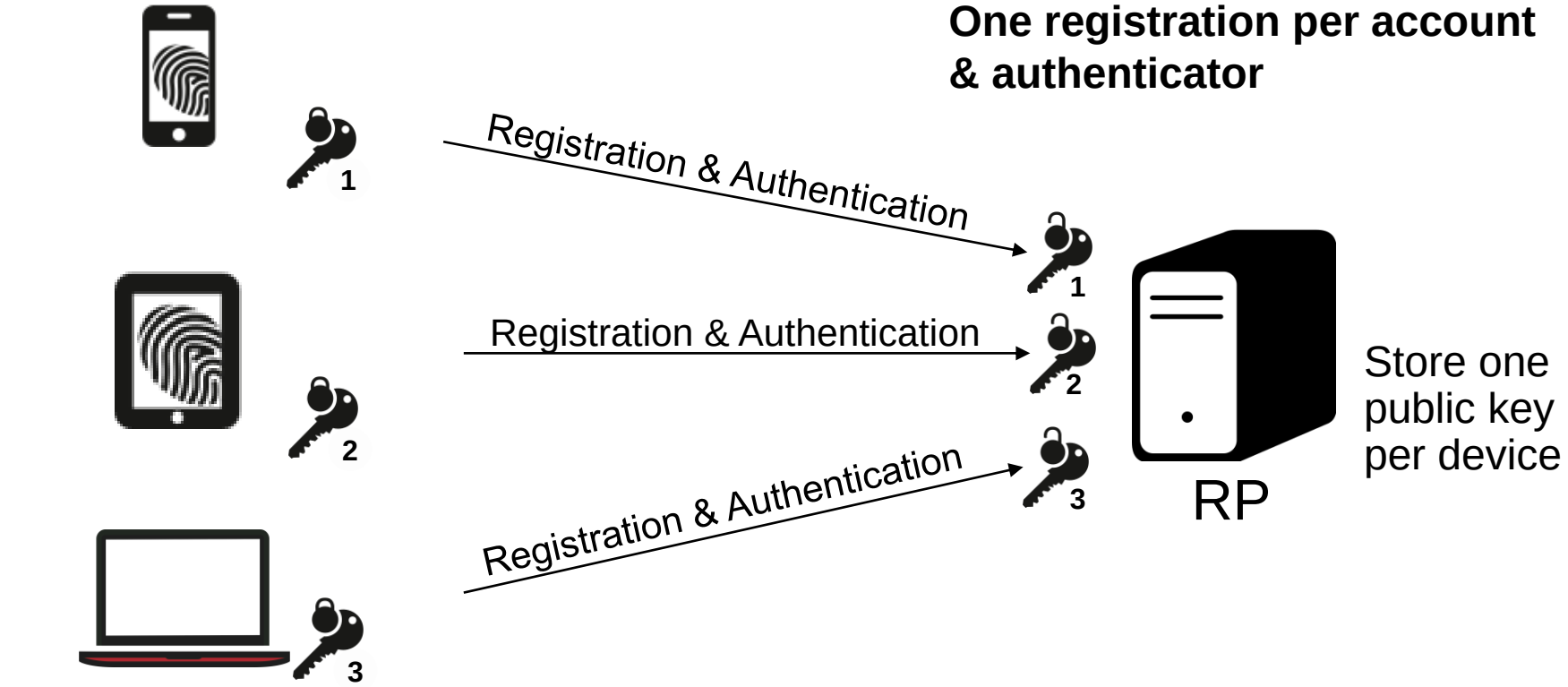
The Basics of FIDO Authentication



Device-Bound Passkeys



Device-Bound Passkeys

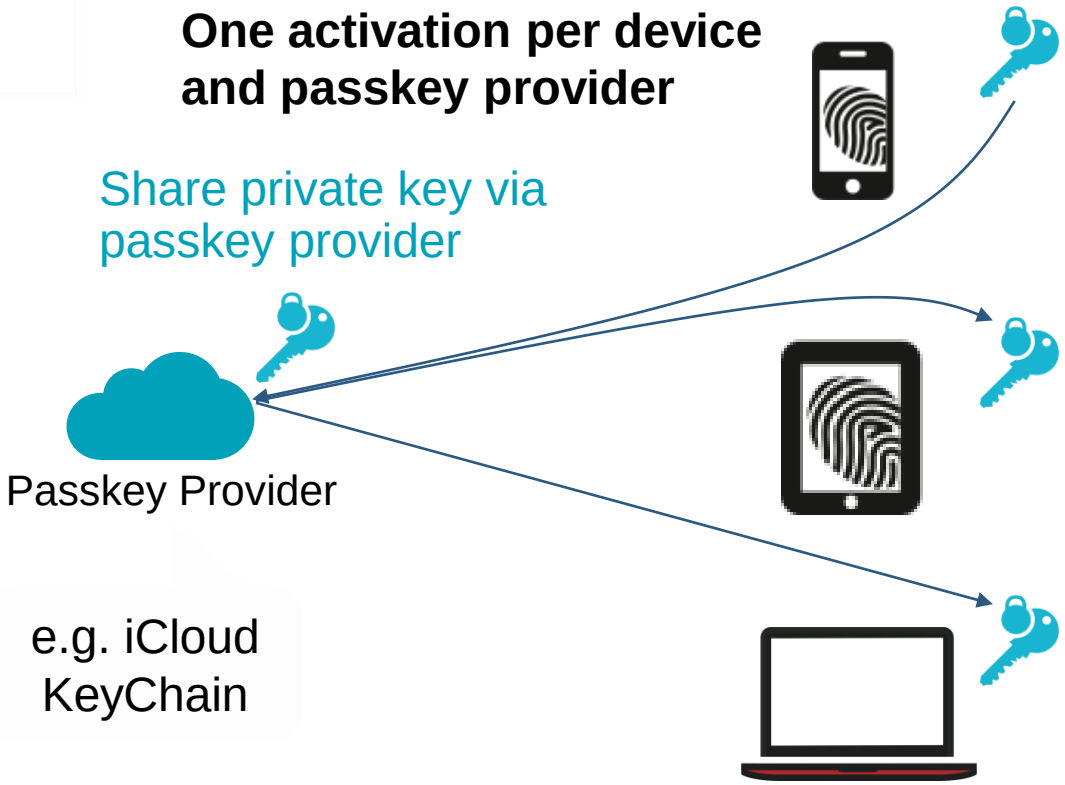


Private Key cannot leave device
Stored in (TEE/SE)

Synced Passkeys

One activation per device and passkey provider

Share private key via passkey provider



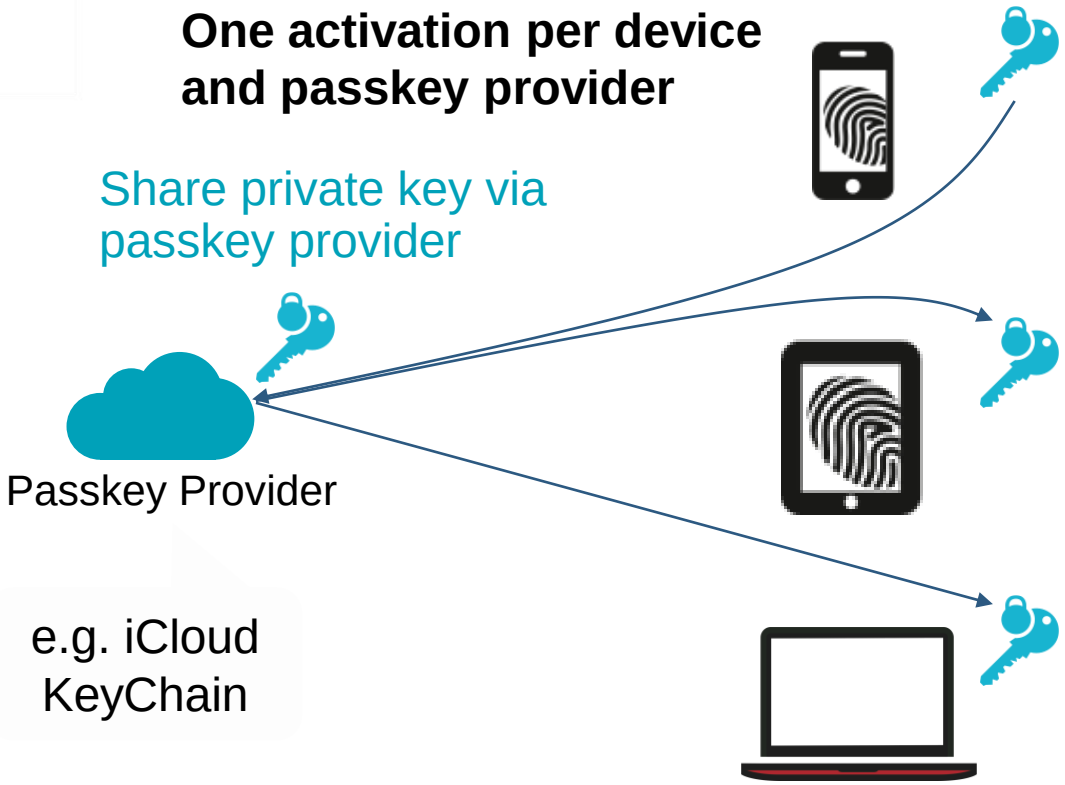
Store one public key per passkey provider

e.g. iCloud KeyChain

Synced Passkeys

One activation per device and passkey provider

Share private key via passkey provider



Store one public key per passkey provider

e.g. iCloud KeyChain

Challenge: Adding new devices handled by passkey provider – not relying party

What does that mean?

Advantages

- Reduced complexity for the relying party
- Only one action per user per device – not one per device and relying party

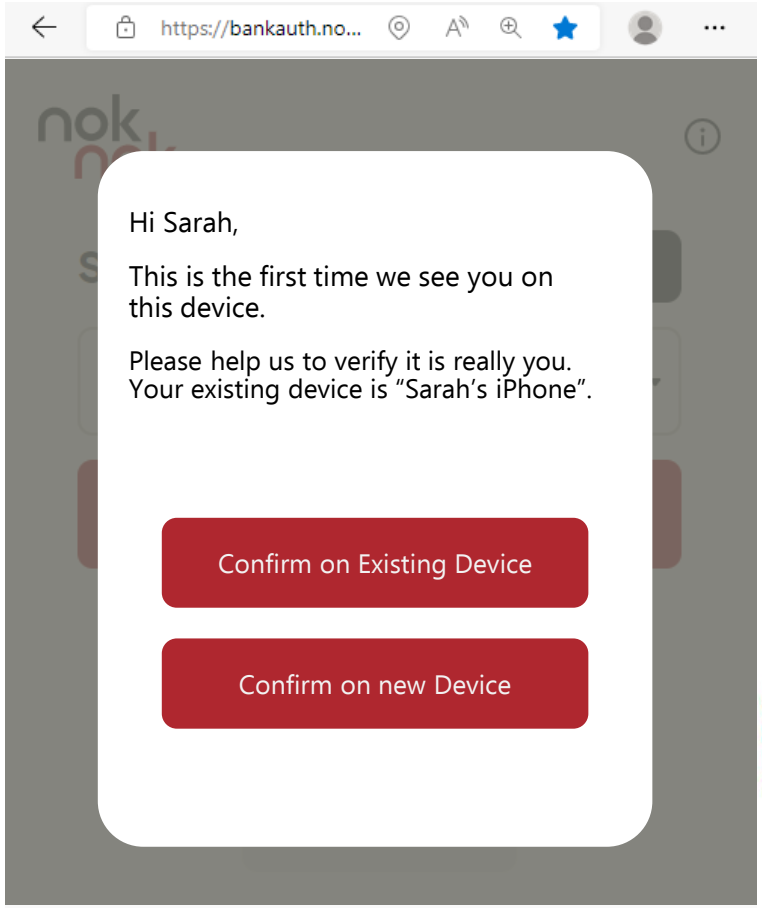
Challenges

- Regulated entities are responsible for handling device additions
- Regulated entities need to enforce security when adding new device

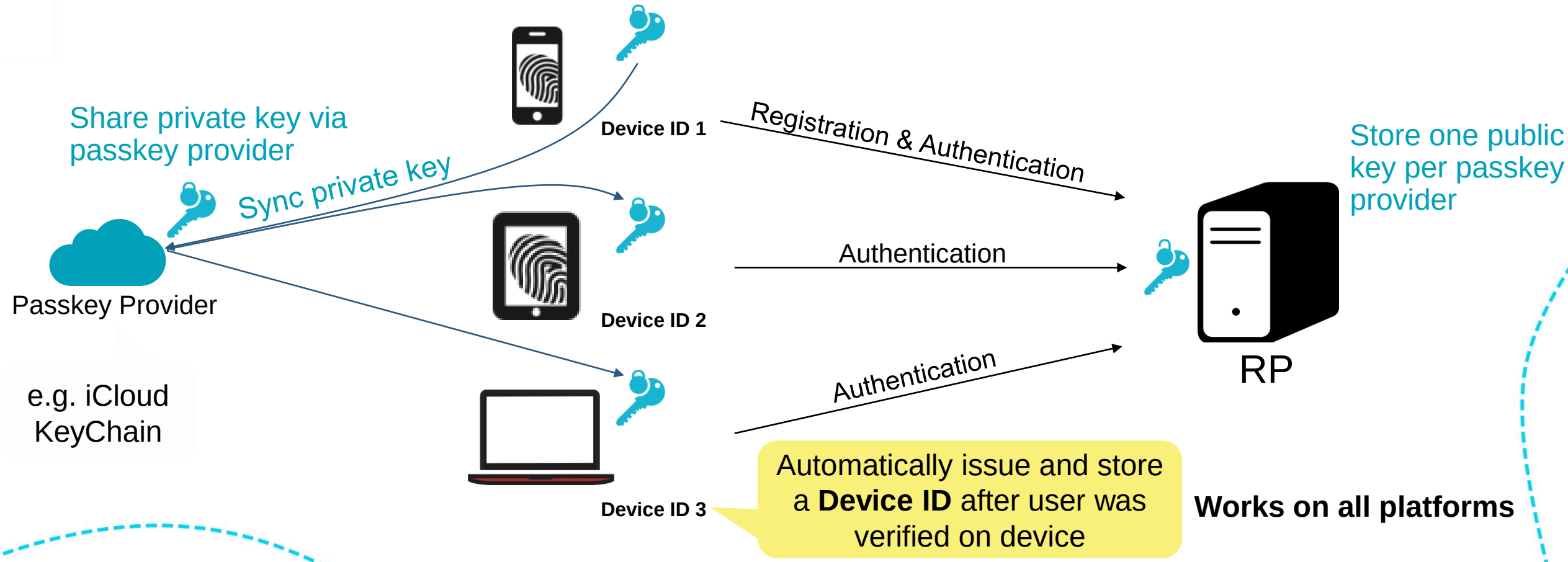
Meeting Regulatory Requirements with Passkeys

Adding New Devices

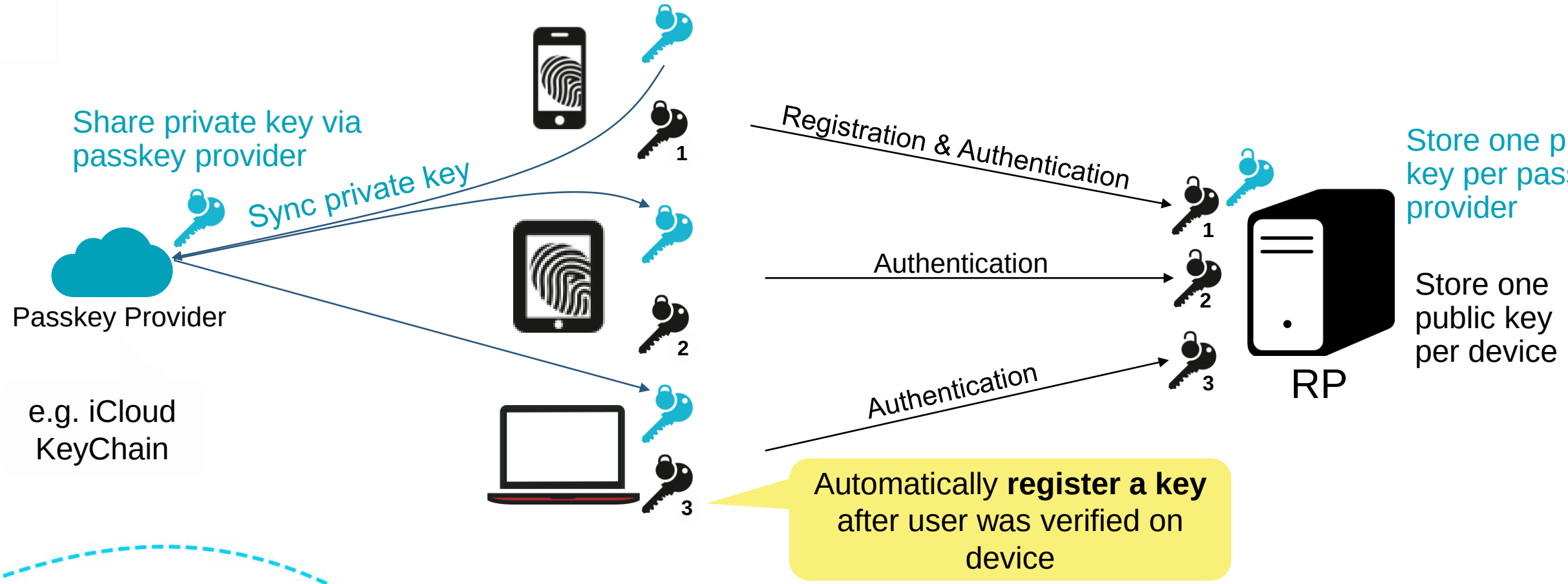
- Exercise passkey on new device plus
  - Send SMS-OTP or
  - Out-of-Band using existing device (e.g., scan QR) or
  - FIDO Cross-Device (CTAP hybrid) or
  - Remote ID Proofing (e.g., Selfie+Picture ID)



Adding Device Binding to Passkeys (1)



Adding Device Binding to Passkeys (2)



Summary

- **Passkeys provide better security than passwords!**
  - Even if you change nothing else, you will improve your security!
- Passkeys make it easier for users to use multiple devices
- Synced passkeys can be augmented to implement strong device binding as required for regulated markets

No need to wait!

THANK YOU!

rolf@noknok.com