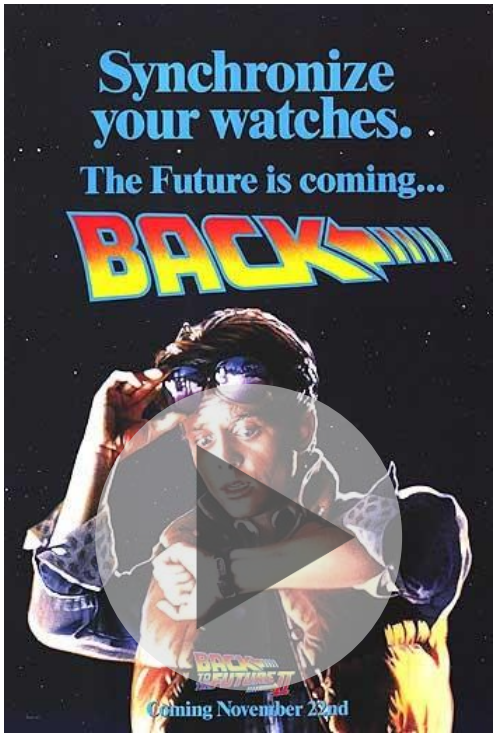
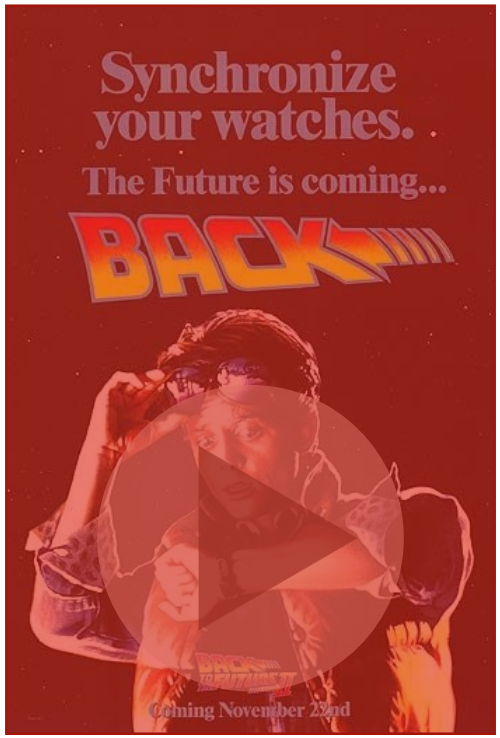
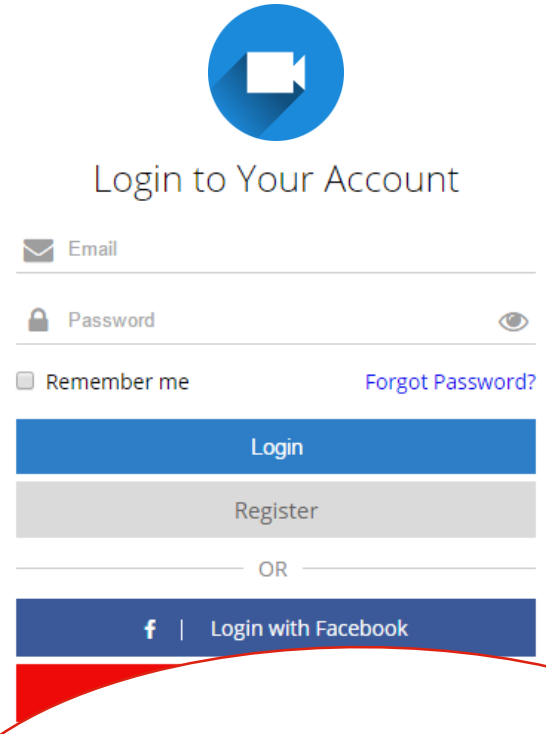
Zero-Knowledge Proofs

An introduction

16.10.2018 · Dimitrij Klesev · R&D


Synchronize
your watches.
The Future is coming...
BACK
Coming November 23rd





IT‘S A TRAP

(icons from icons8)

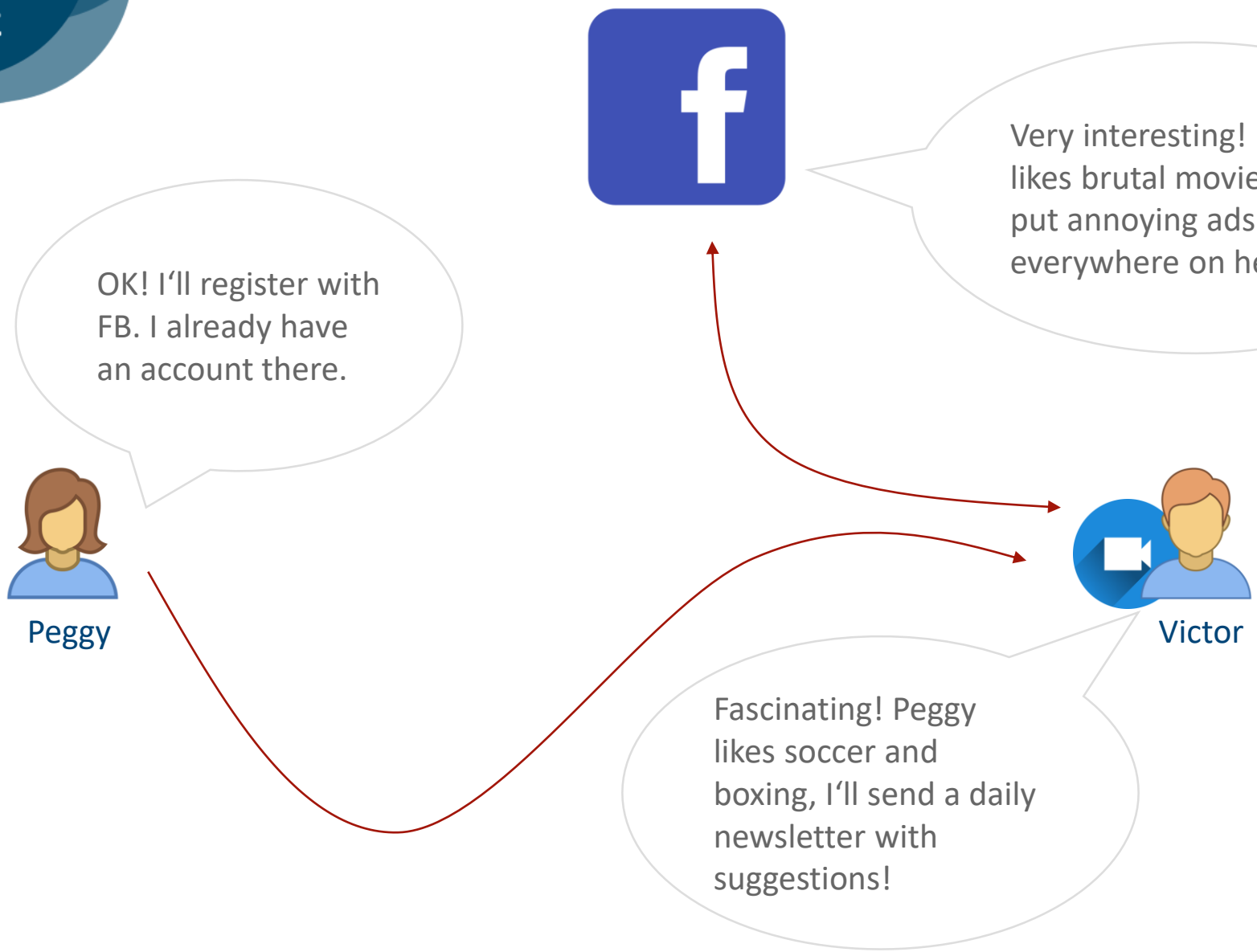
Hey Victor! I would like to see this nice movie! What do I need to do?

Peggy

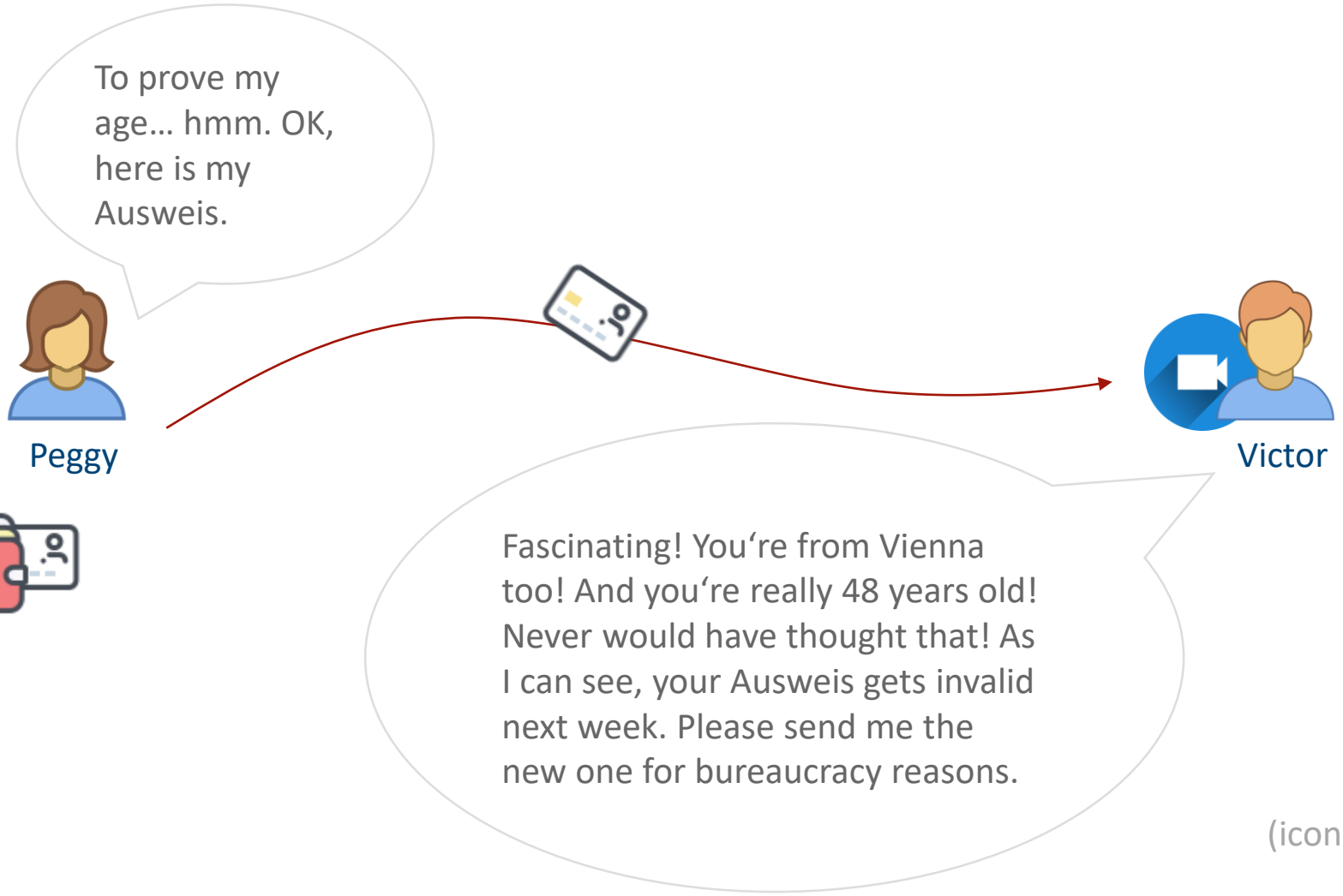
Sure! You just need to have an account and prove that you‘re old enough, as it‘s a really brutal movie!

Victor

(icons from icons8)



(icons from icons8)



(icons from icons8)

Trent

Hey Peggy! I can help you out!

I feel uncomfortable…
I don‘t like everyone taking my data…

Peggy

But.. What can I do?

Victor

(icons from icons8)

$$proof = H^{48+1}(m)$$
$$proof_{sig} = S(proof)$$

Trent

Ok, Peggy! I've signed your age. Here is a proof with my signature.

Hey Trent! Fantastic! Let's agree on a secret value.

Proof with signature

Peggy

Victor

(icons from icons8)

$$proof = H^{48+1}(m)$$
$$proof_{sig} = S(proof)$$

Trent

$$ageDiff = 48 - 18$$
$$enc = H^{ageDiff+1}(m)$$

Peggy

Proof with signature and the „encrypted“ age value

Victor

(icons from icons8)

Trent

My **verification value** seems to be what Trent has **signed!** You seem to be 18 years old!

Peggy

Victor

$$validated = H^{18}(enc) = H^{18}\left(H^{30+1}(m)\right) = H^{48+1}(m)$$

$$proof_{sig} == validated$$

Victor calculates his verification value based on the „encrypted“ age

(icons from icons8)

$$proof = H^{48+1}(m)$$
$$proof_{sig} = S(proof)$$

Trent

Peggy

$$ageDiff = 48 - 18$$
$$enc = H^{ageDiff+1}(m)$$

Victor

$$validated = H^{18}(enc) = H^{18}\left(H^{30+1}(m)\right) = H^{48+1}(m)$$
$$proof_{sig} == validated$$

(icons from icons8)

Thank You!

Sources

[1]: Free Classic Images

Url: https://freeclassicimages.com/images/BACK-TO-THE-FUTURE-II--TEASER--movie-poster.jpg

[2]: Wikimedia Commons

Url: https://commons.wikimedia.org/wiki/File:Otakuthon_2014-_Admiral_Ackbar_Cropped.jpg

[3]: Zero-knowledge Proof: Proving age with hash chains

Url: https://asecuritysite.com/encryption/age

[4]: Icons8

Url: https://icons8.de

[Dimitrij Klesev] · [R&D]

dimitrij.klesev@nic.at T +43 662 4669 -742