

New phone who dis?

User verification using X.509 certificates

Richard van der Hoff, Element Crypto team

We need better trust anchors



The Boss created this DM.



The Boss invited Alice



The Boss

Hi Alice! I'm locked out of my account. Can you send me the password for the main server?

21:39



Alice joined the room

We need better trust anchors

Three questions for Alice

- **Identity** of the sender
- **Authenticity** of the sender
- **Integrity** of the communication channel

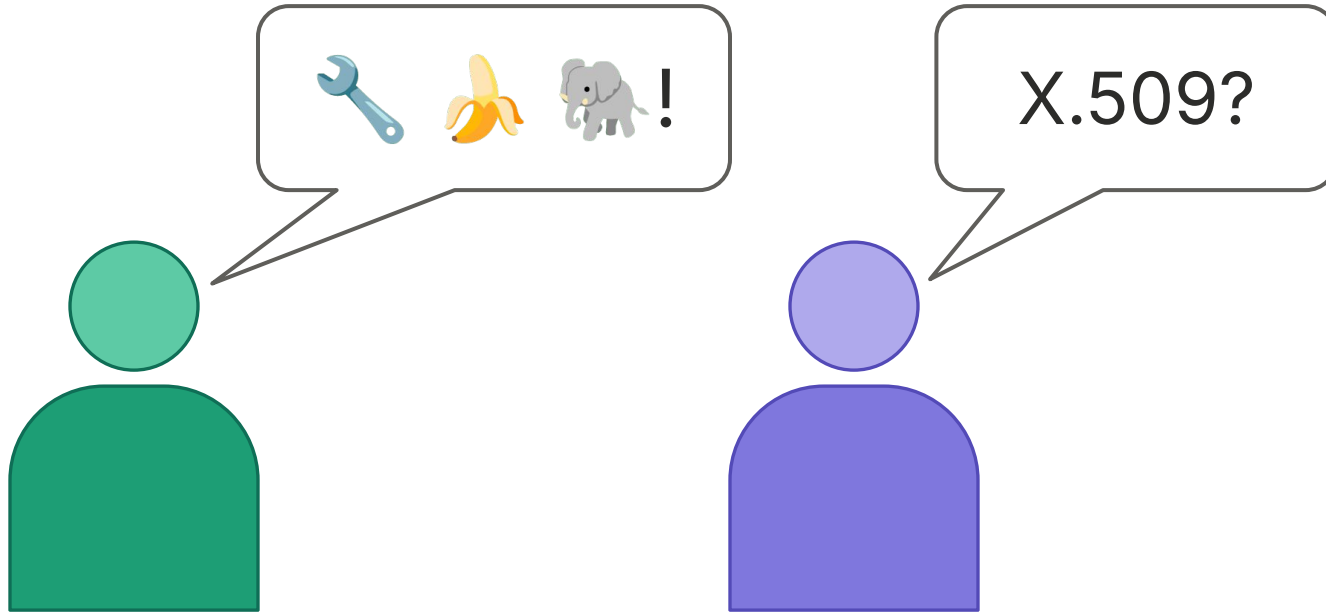
We need better trust anchors



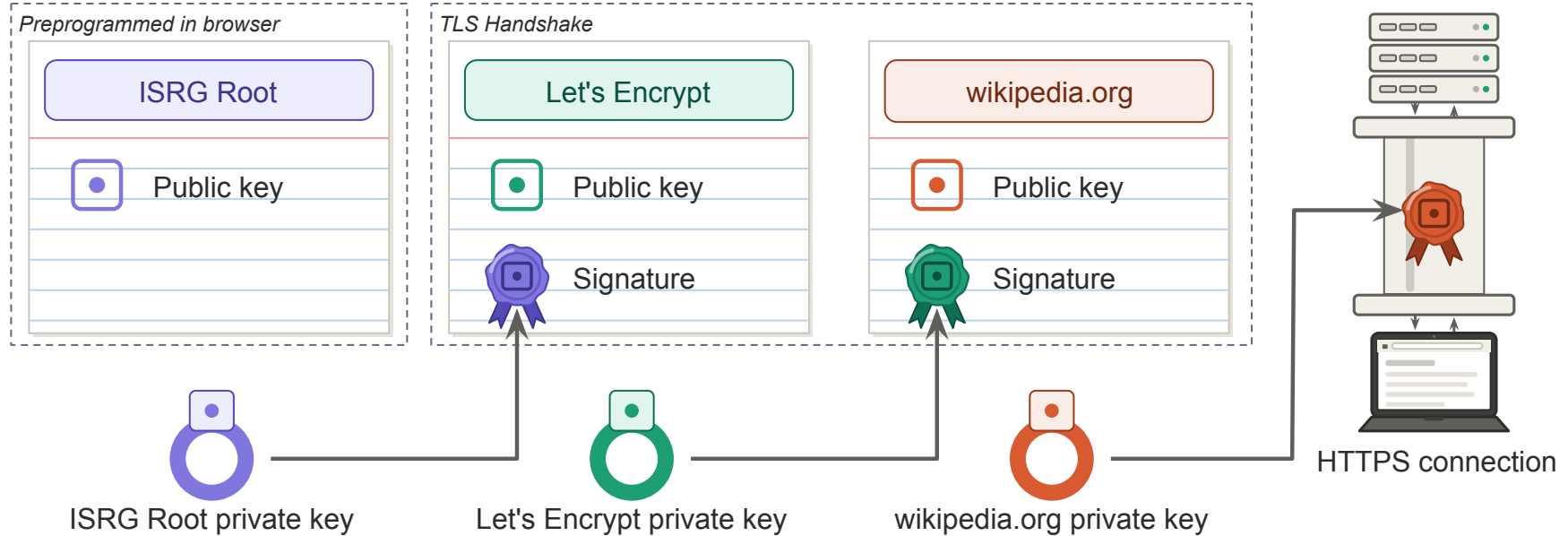
The Boss's (@g:xps9320.sw1v.org) digital identity was reset. [Learn more](#)

Dismiss

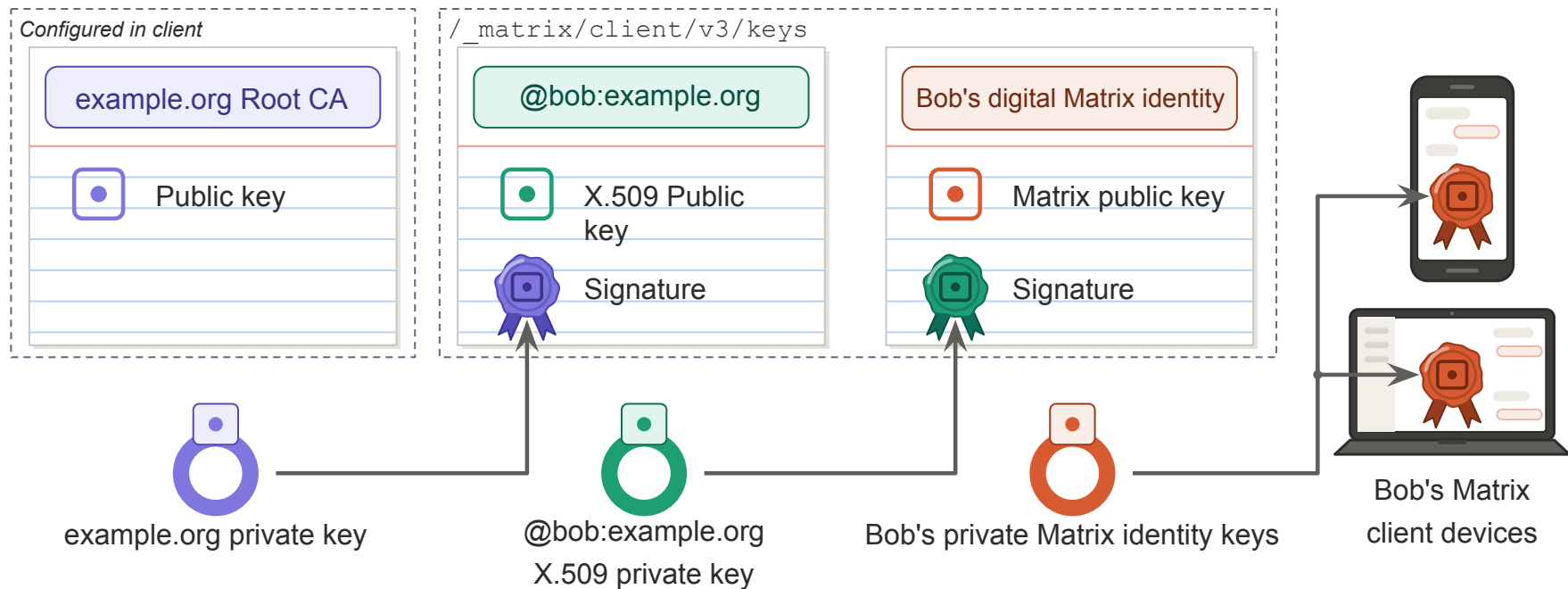
User verification



X.509 signing example



X.509 signing in Matrix



Demo time!

Takeaways

- If this matches your usecase, come and talk to us!
- If this *doesn't* match your usecase, don't panic!
- Support for multiple trust roots

In future: trust root attribution?



The Boss



Verified by ACME.org

Hi Alice! I'm locked out of my account. Can you send me the password for the main server?

Thank you!

@richvdh:sw1v.org
<https://mastodon.me.uk/@richvdh>