Speranza: Usable, privacy-friendly software signing

Kelsey Merrill (Jane Street*)
Zachary Newman (Independent**)
Santiago Torres-Arias (Purdue)
Karen Sollins (MIT)

Lady Jane Wilde, pen name Speranza

work completed while at MIT* and Chainguard**

Motivation

Software supply chain attacks are a problem

People are bad at managing keys

Open-source maintainers care about privacy

Software signing!

Sigstore!
(Newman et al 22)

Speranza!

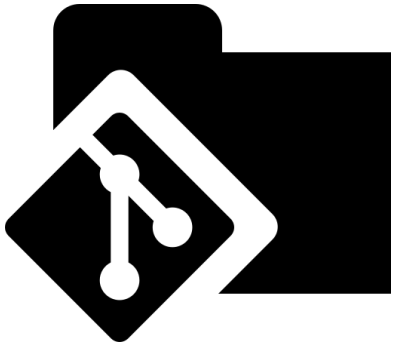
Replace maintainer identities with commitments to get maintainer privacy while keeping certificate-based signing authenticity and usability guarantees

Design Goals

Maintainers

Usability
& Privacy

Software
Repositories



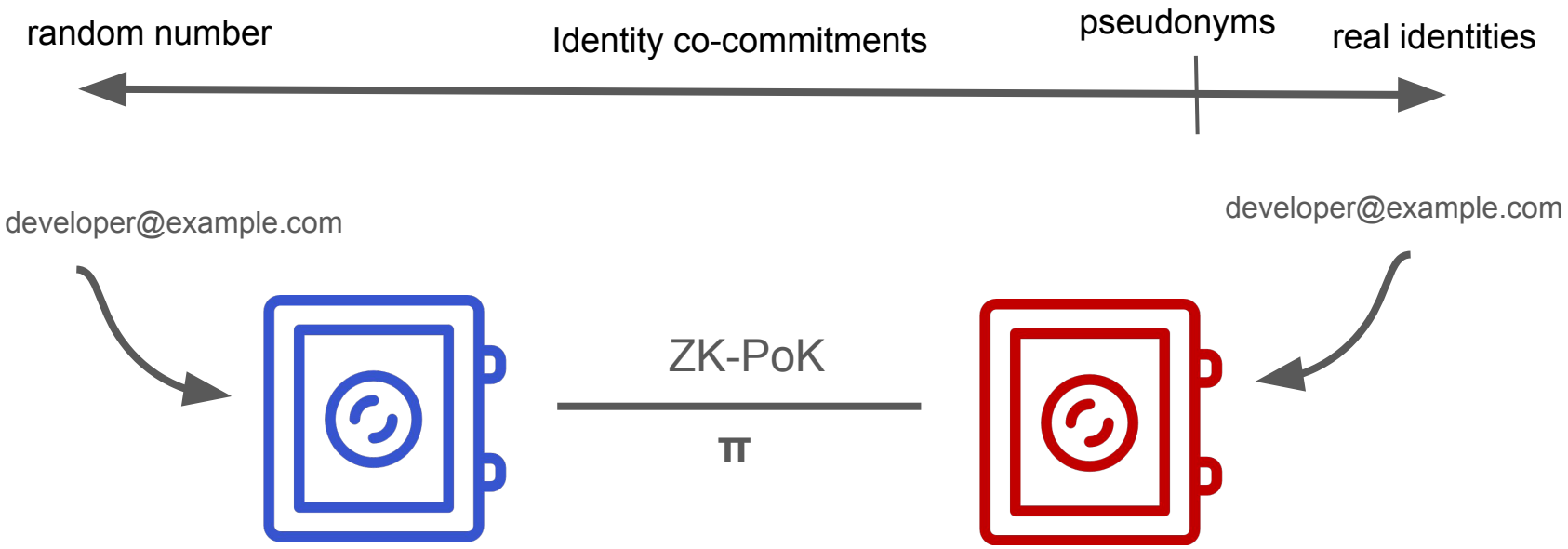
Deployability

Users

Software
Authenticity

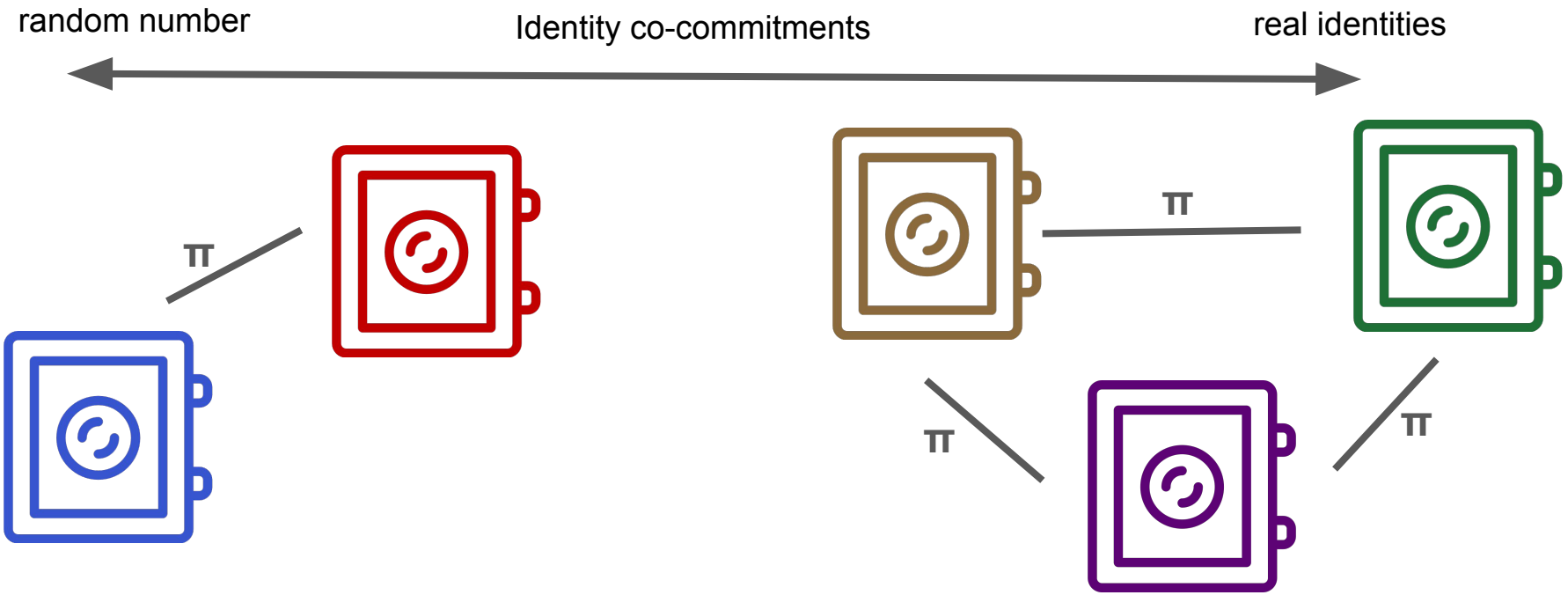
Identity Co-Commitments

"Selectively linkable pseudonyms"

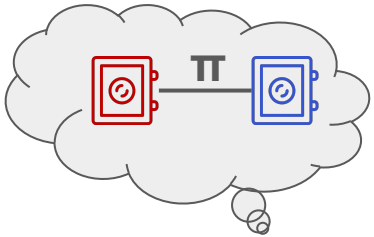


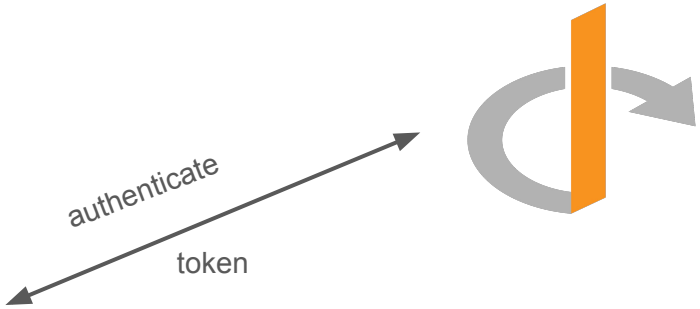
Identity Co-Commitments

"Selectively linkable pseudonyms"

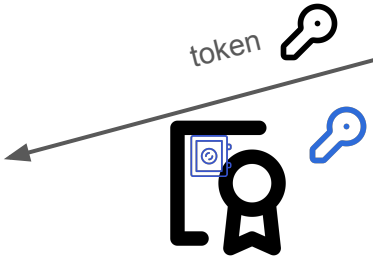


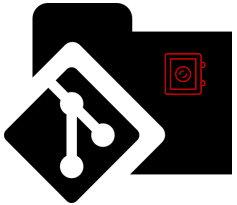
Speranza Protocol

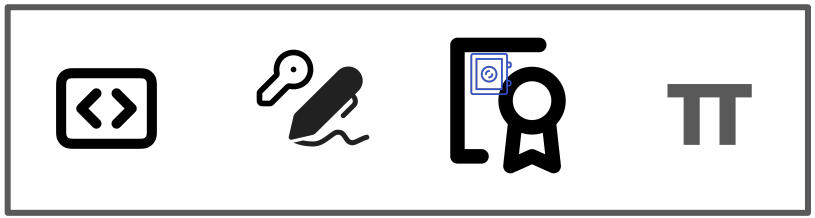




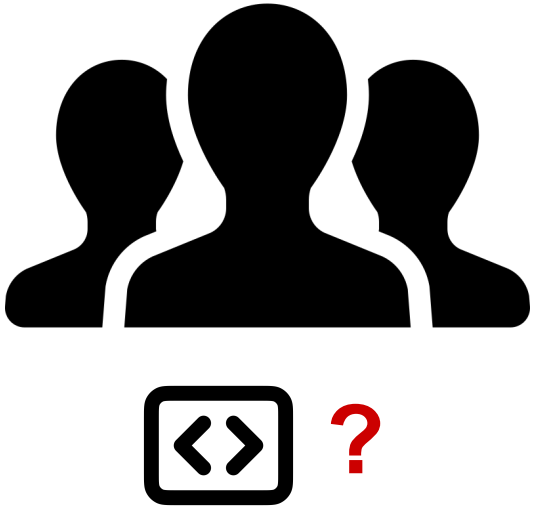
CA







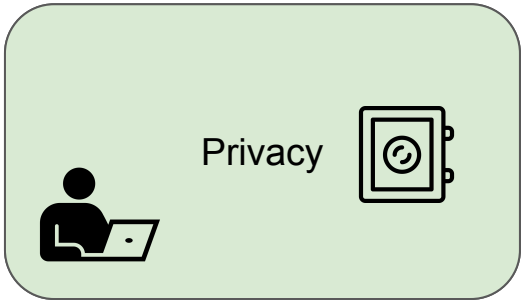
Speranza Protocol

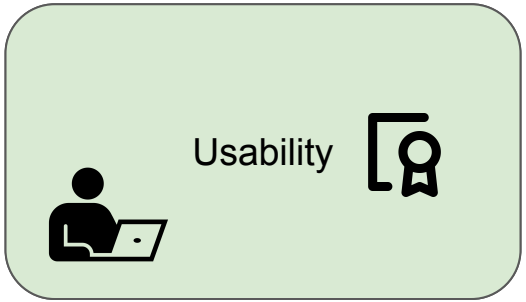


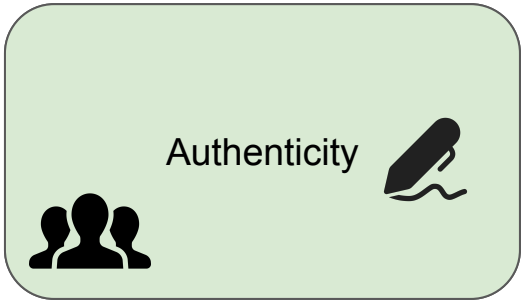
1. Valid signature
2. Valid certificate
3. Valid zk-proof

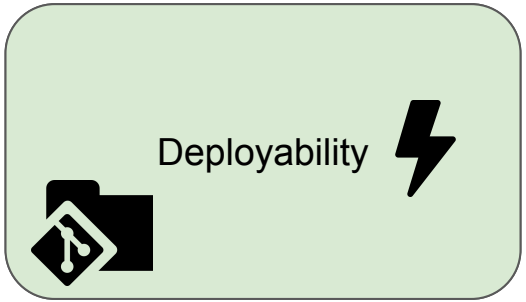
Evaluation: Speranza End-to-End

Meeting Our Goals









More details in the paper

- Formal definitions and arguments
- Publishing authority and delegation
- Further benchmarks and evaluation
- Alternatives considered

Thank you!