EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

FACULTY OF
SCIENCE
Communication Networks

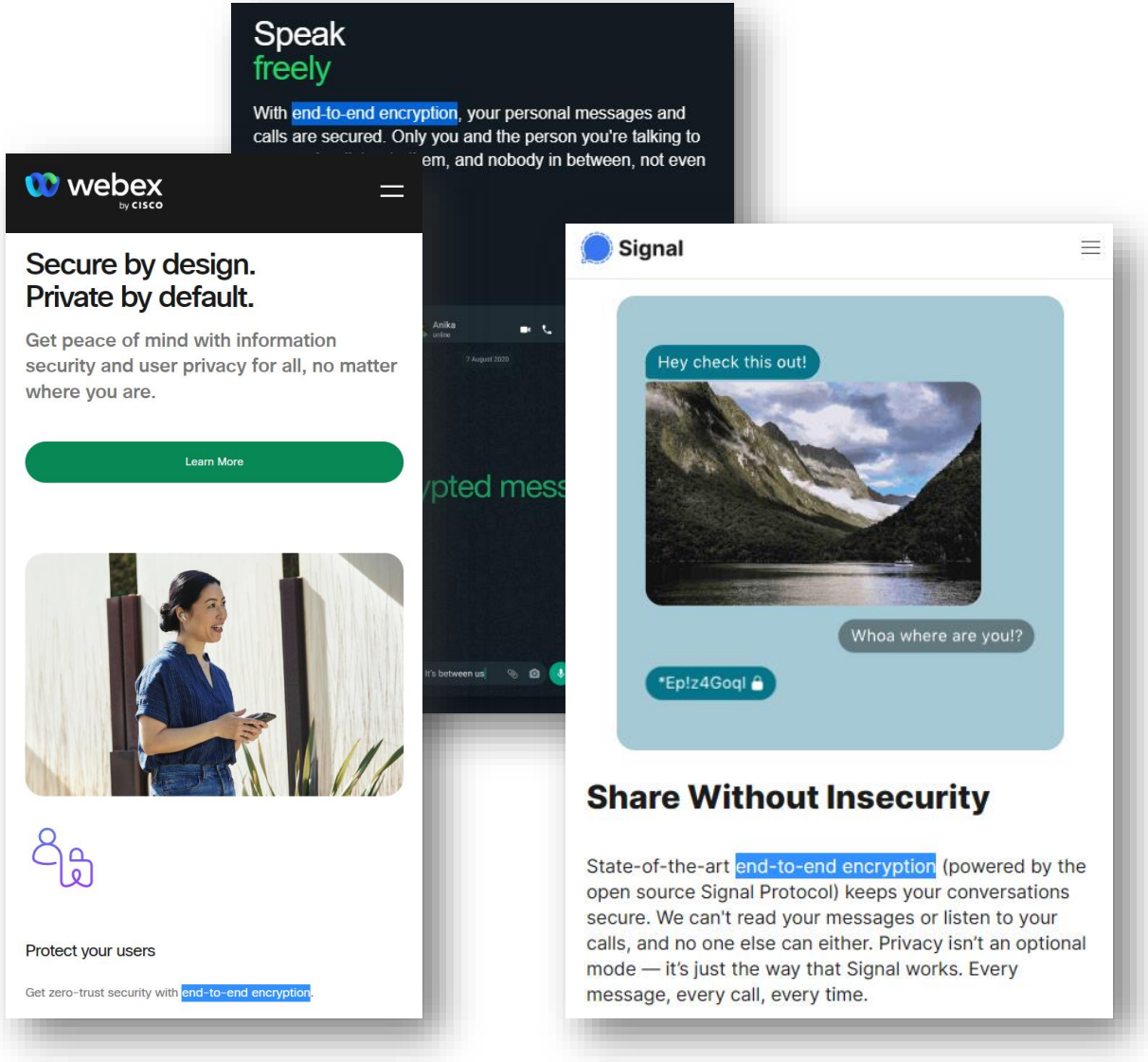
OIDC² - A Simple End-to-End User Authentication Method for the Internet

by Jonas Primbs, Chair of Communication Networks, University of Tübingen, Germany

http://kn.inf.uni-tuebingen.de

What is “Secure” Communication?

- Instant messenger and video conference services promote their systems with “end-to-end encryption”
- End-to-end encryption = secure communication?
- **No!** We cannot know to who we are communicating end-to-end encrypted!
- We also need end-to-end **authentication**!



Even in Video Calls?

- **YES!**
  - Deep fakes

Source: Tagesspiegel

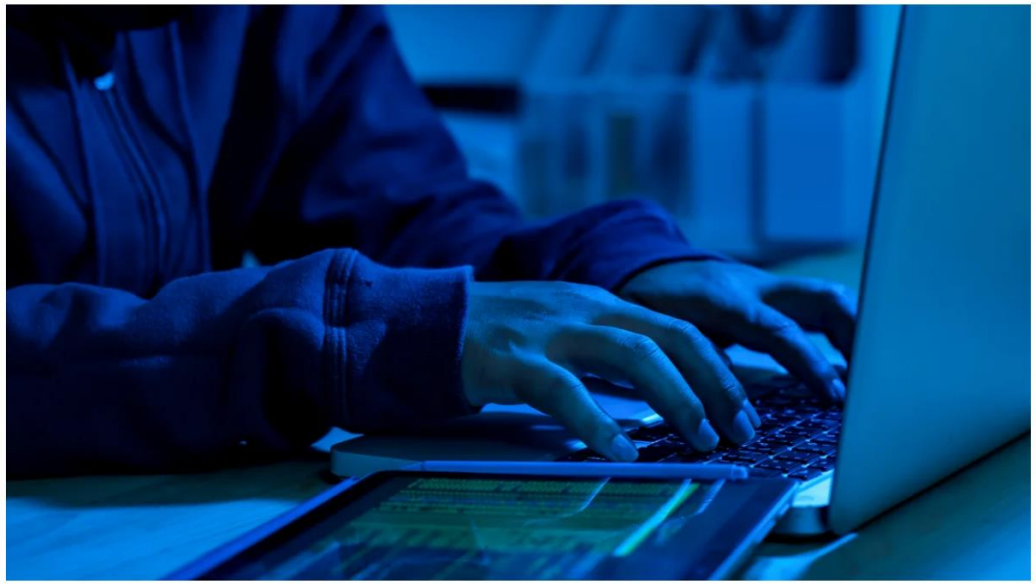
CNN World Watch Audio Live TV Log In

World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

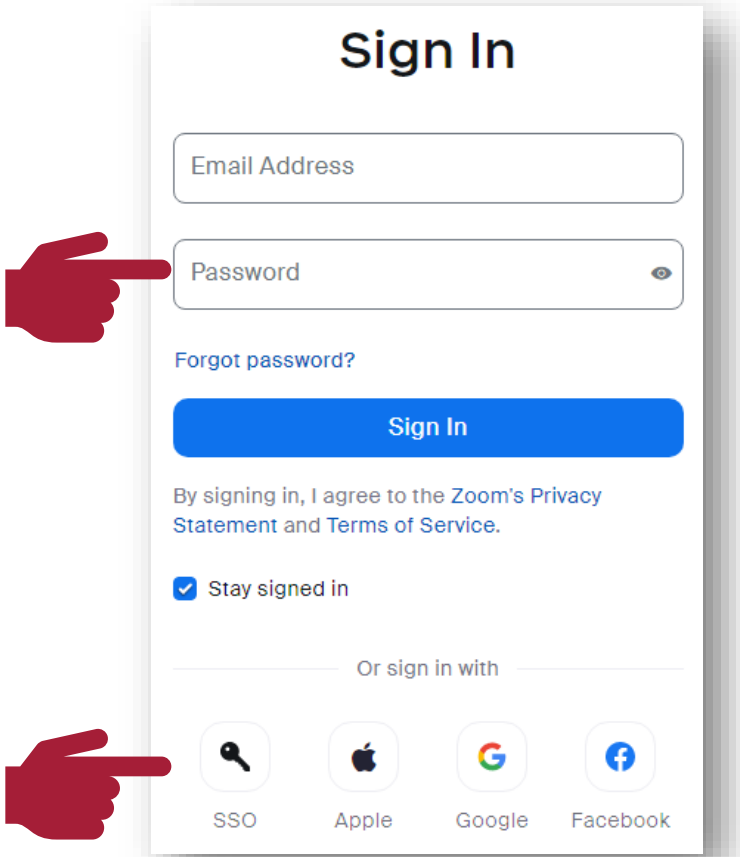


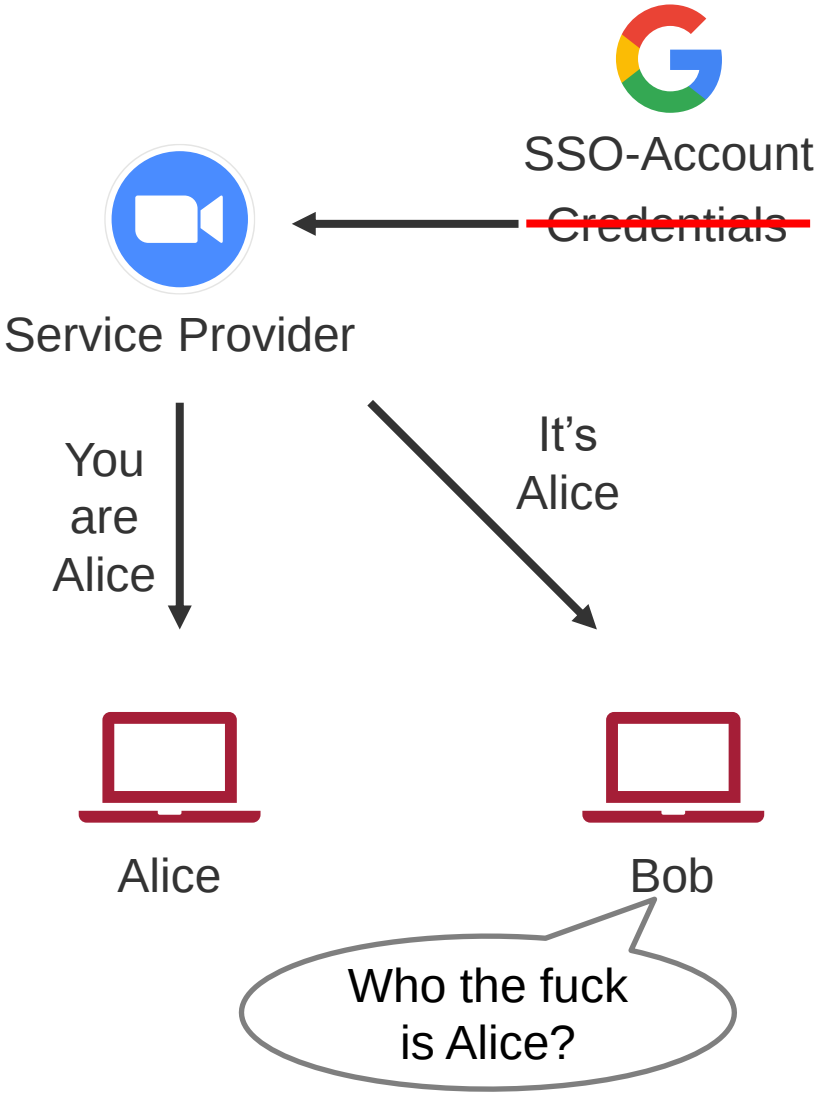
Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

Source: CNN

State of the Art Authentication

- **Trust in Service Provider is required**
  - May or may not verify user's real-world identity
- **What about Single Sign-On (SSO) Solutions?**
  - Same problem!

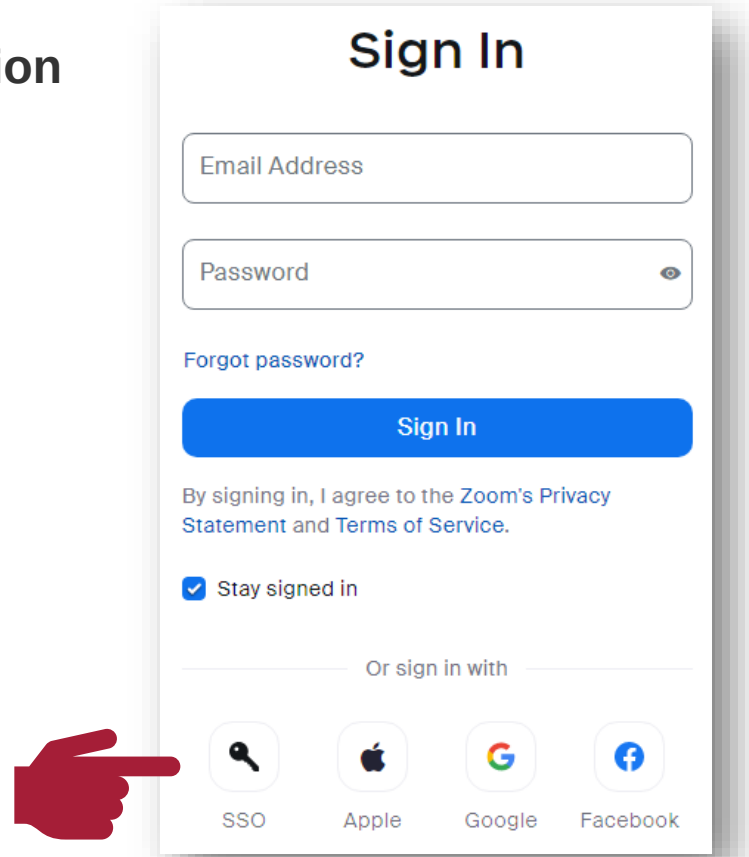


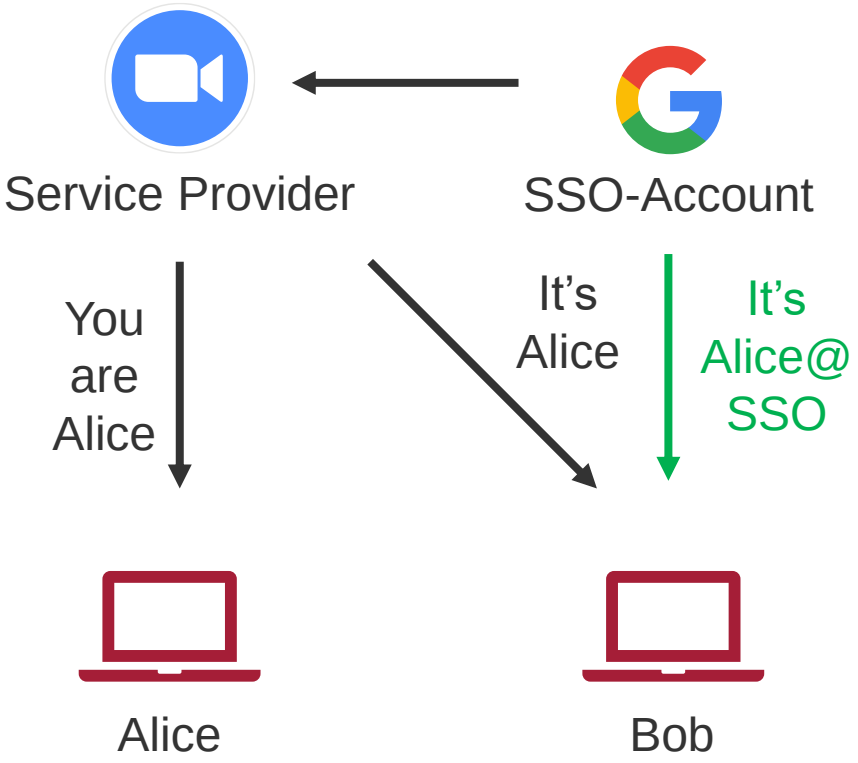


Introduction: OIDC²

- **With OIDC², the SSO Identity Provider (IdP) certifies the account**

- **OIDC² = Open Identity Certification with OpenID Connect**





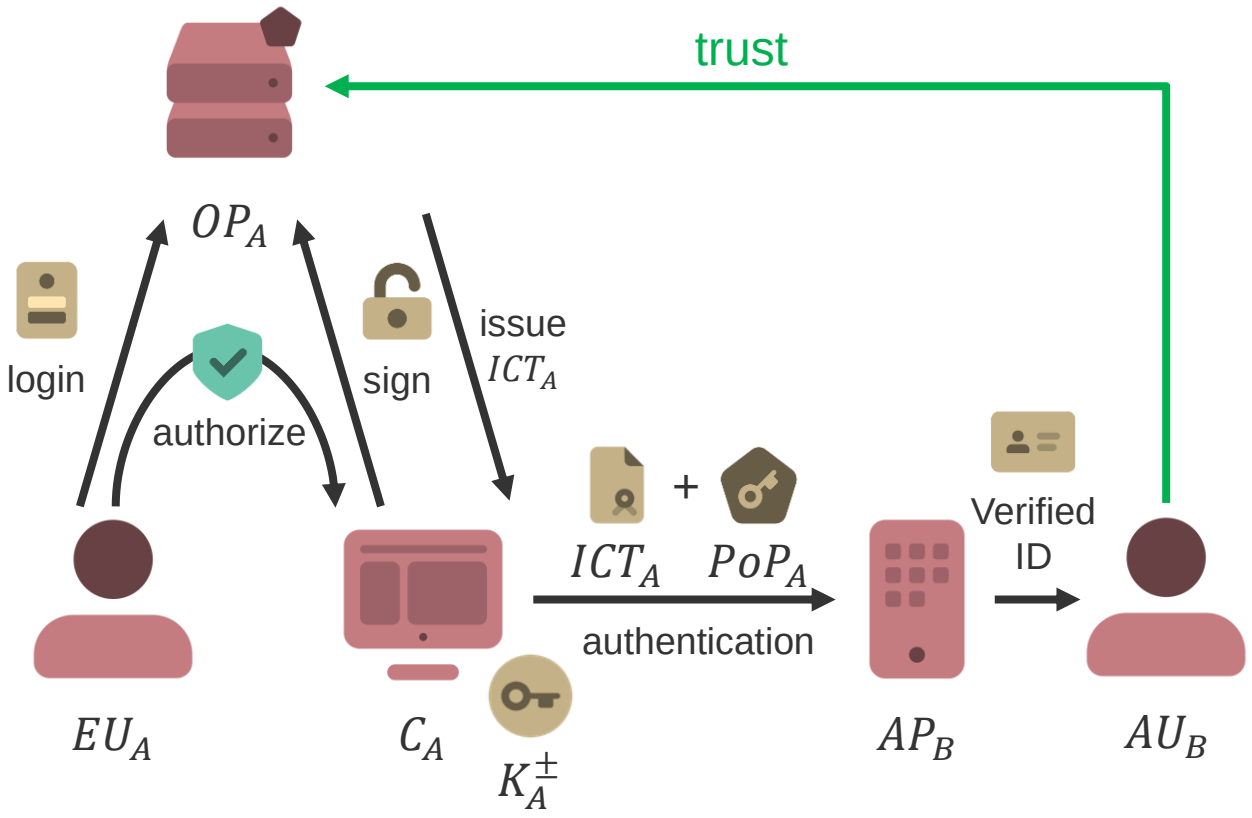
Introduction: OIDC²

Entities

- End User EU_A (Alice)
- Client C_A (Alice's client)
- OpenID Provider OP_A (Alice's IdP)
- Authenticating User AU_B (Bob)
- Authenticating Party AP_B (Bob's client)

Overview

1. Alice logs in to her SSO account
2. Alice authorizes her client for E2EA
3. Her client signs a challenge with private key K_A^-
4. Her IdP issues Identity Certification Token ICT_A
5. Her client sends ICT_A and a Proof of Possession PoP_A to Bob's client
6. Bob's client verifies this authentication and provides the verified identity claims to Bob
   - **Bob must trust Alice's IdP!**



IdP Classification

- Problem: IdPs certify possession of an **account**
  - But: the IdP may **not verify identity claims**
- Classification:
  - **Authoritative OpenID Provider**
    - Verifies login credentials
    - Protects accounts
    - Is an authority for some credentials
    - Examples:
      - Governments for real-world identities
      - Social media platforms for profiles
  - **Verifying OpenID Providers**
    - Verifies login credentials **+ real-world identity**
    - Protects accounts
    - Examples: Banks, Insurances
      - New: X, Facebook, Instagram, LinkedIn

© Dan Kitwood / Getty Images

Source: Top Indian News

Applications

Email

- S/MIME and PGP are rarely used [1]
  - ~2.5% emails are signed with S/MIME
  - ~0.3% emails are signed with PGP
  - Problem: Usability
- We developed a web app which generates or uses a PGP key, certifies it with an OIDC account and sends signed + encrypted emails via Gmail
  - No need for manual PGP key generation, installation, and exchange
  - Instead: Trust in OpenID Provider required

Instant Messaging

- Signal, WhatsApp, Threema, etc. implement E2E encryption and promote this as “secure”
- E2E authentication is optional:
  - By default, users rely on service provider to verify phone numbers etc.
  - Users can verify integrity of chats via QR Codes or security codes
    - But who has ever used it?
- We developed an extension to the Matrix IM protocol where a user certifies its key pair with OIDC²
  - No need for manual QR or security code exchange and verification
  - Instead: Trust in OpenID Provider required

Applications

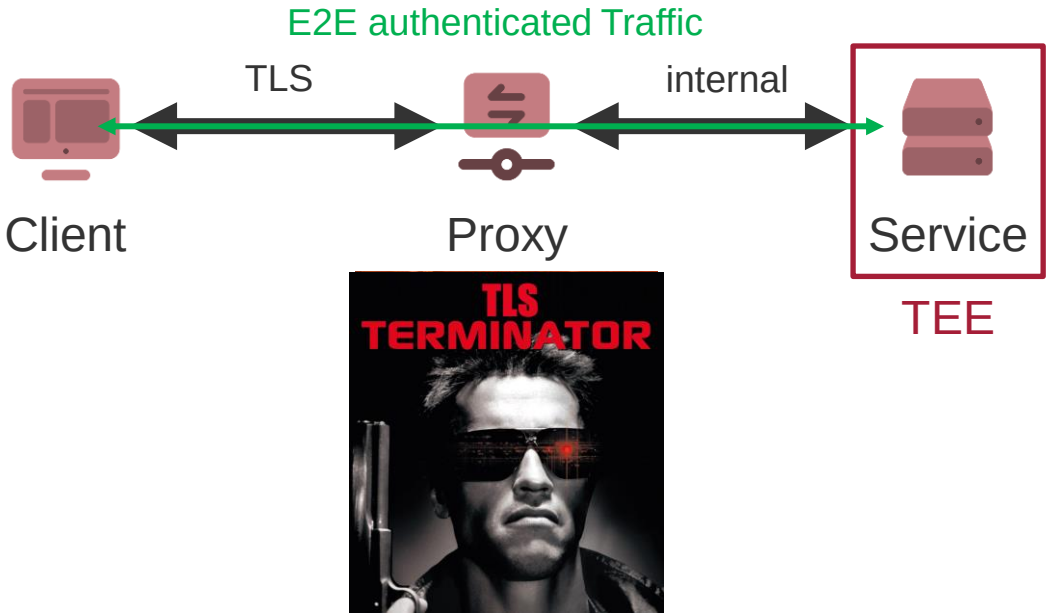
Video Conferences

- Webex, Zoom, etc. implement E2EE and promote this as “secure”
- Real E2EA possible in Webex but requires X.509 certificate

- We implemented OIDC² in a WebRTC-based video conferencing application
  - Automatic identity verification
  - Users must only login to a trusted OpenID Provider

Service Authentication

- Cloud Providers control the TLS-terminating (reverse) proxy / load balancer
- **Idea**: Authenticate E2E from your client to a service inside a secure enclave (TEE)



EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Thank you!

- Contact & follow me on
  - LinkedIn: https://www.linkedin.com/in/jonasprimbs/
  - X: https://twitter.com/JonasPrimbs
  - Email: jonas.primbs@uni-tuebingen.de

- Full paper: https://doi.org/10.1109/ojcoms.2024.3376193

- Questions, feedback, and application suggestions welcome!