Challenges in open, self-sovereign identity

Tom Marble

FOSSY 2023
July 13-16
Portland, Oregon

Challenges in open, self-sovereign identity

01 What is self-sovereign identity?

02 Current Problems and Approaches

03 Tech is not sufficient

04 How can open source help?

What is self-sovereign identity?

Christopher Allen's
Ten Principles of Self-Sovereign Identity

Existence. Users must have an independent existence.
Control. Users must control their identities.
Access. Users must have access to their own data.
Transparency. Systems and algorithms must be transparent.
Persistence. Identities must be long-lived.
Portability. Information and services about identity must be transportable.
Interoperability. Identities should be as widely usable as possible.
Consent. Users must agree to the use of their identity.
Minimalization. Disclosure of claims must be minimized.
Protection. The rights of users must be protected.

The Path to Self-Sovereign Identity
http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

My goals for SSI

Outcome: asking the right questions!

Basics

Share messages and files securely (combat deep fakes)
Authenticate with third party services
- non correlation (prevent merging)
- with *multiple personas*
Opt-in, discoverable identity (white pages, pub keyservers)
User friendly and intuititive (does the right thing)
Self hosted or delegated (does not require third party)

Thought experiment...

Open every email in a container
Open every web page in incognito mode
Access via VPN/Tor

Not Government ID
Not Corporate ID

Secondary Concerns

Out of scope for the immediate context...

Application transparency, auditing (FOSS)
Signing software releases
Verifiable credentials
Micropayments
Selective disclosure: User decides what data to share (think "app permissions")
Legal Electronic Signatures (getting beyond Docusign)
SPAM - filter on authenticated sender, white/black lists, payment/work

Reproducible builds
https://reproducible-builds.org/

Verifiable credentials
https://en.wikipedia.org/wiki/Verifiable_credentials

Current Problems

email is identity (forgot password)
- human meaningful, but not secure, nor decentralized
- can easily be spoofed
X.509 weaknesses, MiTM, Certificate Transparency
DID (often) on chain, asymmentric ownership/control, DID resolution under specified (DIDweb)
Managing passwords is hard: so we delegate to big companies (or password managers)
- surveillance capitalism - "Real Names" policies – DNT is advisory

How monopoly enshittified Amazon
https://pluralistic.net/2022/11/28/enshittification
Adversarial Interoperability
https://www.eff.org/deeplinks/2019/10/adversarial-interoperability
Director's Decision on DID 1.0 Proposed Recommendation Formal Objections
https://www.w3.org/2022/06/DIDRecommendationDecision.html
DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust
https://dl.acm.org/doi/fullHtml/10.1145/3446983.3446992

Current Approaches: SQRL

Secure Quick Reliable Login
A highly secure, comprehensive, easy-to-use replacement for usernames, passwords, reminders, one-time-code authenticators . . . and everything else.

https://www.grc.com/sqrl/sqrl.htm

Current Approaches: FIDO2

https://fidoalliance.org/specifications/

W3C WebAuthn
WebAuthn defines a standard web API that is being built into browsers and platforms to enable support for FIDO Authentication.

CTAP2
Allows the use of external authenticators (FIDO Security Keys, mobile devices) for authentication on FIDO2-enabled browsers and operating systems over USB, NFC, or BLE for a passwordless, second-factor or multi-factor authentication experience.

CTAP1
The new name for FIDO U2F, CTAP1 allows the use of existing FIDO U2F devices (such as FIDO Security Keys) for authentication on FIDO2-enabled browsers and operating systems over USB, NFC, or BLE for a second-factor experience..

Current Approaches: Passkeys

Passkeys are designed to eliminate the usability shortcomings of classic FIDO credentials or single-device credentials. They achieve this with a simple trick: they allow the FIDO credential to roam across multiple devices.

Passkeys
https://fidoalliance.org/passkeys/

Introducing passwordless authentication on GitHub.com
https://github.blog/2023-07-12-introducing-passwordless-authentication-on-github-com/

Challenge: Zooko’s Triangle

Zooko's triangle is a trilemma of three properties that some people consider desirable for names of participants in a network protocol:

Human-meaningful: Meaningful and memorable (low-entropy) names are provided to the users.
Secure: The amount of damage a malicious entity can inflict on the system should be as low as possible.
Decentralized: Names correctly resolve to their respective entities without the use of a central authority or service.

Zooko's triangle
https://en.wikipedia.org/wiki/Zooko%27s_triangle
Linked Local Names: An Overview
https://github.com/christianlundkvist/rebooting-the-web-of-trust/blob/master/topics-and-advance-readings/linked-local-names.md
Petname Systems
https://spritelyproject.org/news/petname-systems.html

Approaches: European Digital Identity

OBJECTIVES OF THE EUDI WALLET
- Secure and trusted identification to access online services
- Mobility and digital driving license
- Health
- Education/Diploma
- Digital Finance

The EUDI Wallet shall ensure full control of the user over their data held within their individual EUDI Wallet by integrating security and privacy by design. Therefore, the core functions of the EUDI Wallet such as identification, authentication, signature, seal and attributes sharing shall not occur without the consent of the user.

The EUDI Wallet shall enable the user to share only the information they intend to share.

European Digital Identity Architecture and Reference Framework – Outline
https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

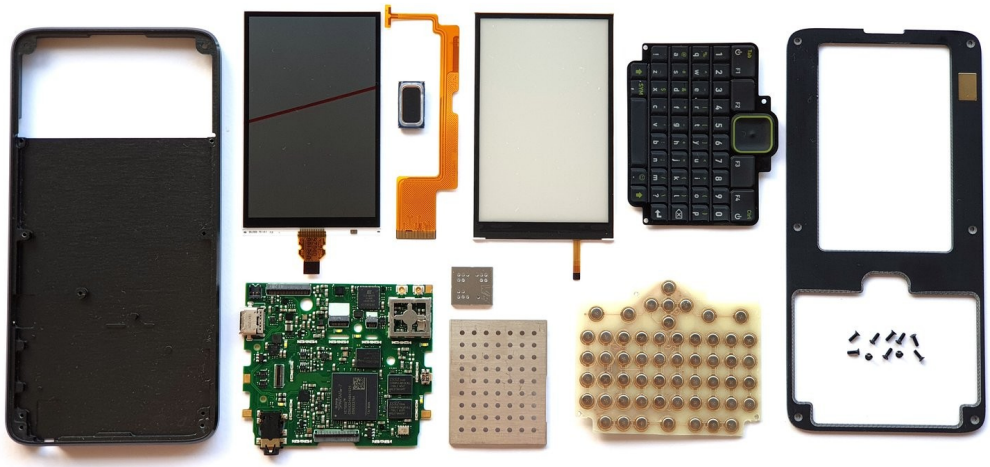
Tech is not sufficient

Awareness How can we get people to care about privacy, security, FOSS, etc. (software facts like nutrition facts)?

Competition We are competing against proprietary solutions and governments (e.g. identity bound to smartphone, biometrics, etc.)

Leaking correlation "Self Sufficiency Theatre" -- Pamela Dingle, Director of Identity Standards at Microsoft
It's hard to not leak correlation like email, birthdate, phone, SSN

What is Hide My Email?
https://support.apple.com/en-us/HT210425



Could open hardware help?

Betrusted

Betrusted is more than just an app, and more than just a gadget – it is a co-designed hardware + software solution that provides safe defaults for everyday users. It's also open source, empowering advanced users to analyze, extend and explore this secure mobile computer.

Betrusted
https://betrusted.io/
Precursor
https://precursor.dev/
FIDO2 mode
https://github.com/betrusted-io/betrusted-wiki/wiki/The-Vault-App
Linux Conf Australia: Betrusted: Better Security Through Physical Partitioning
https://lca2020.linux.org.au/schedule/presentation/37 (may be down)

References and Events

Christopher Allen: The Origins of Self-Sovereign Identity
https://hackmd.io/PwR3qsUaQ2iMmrcdUFX3VQ

M41LZ in Tails: securing e-mail – the complexity we're trying to avoid!
https://info9.net/presentations/mailz-in-tails/

Athenticate
https://authenticatecon.com/

Internet Identity Workshop
https://internetidentityworkshop.com/

Rebooting the Web of Trust
https://www.weboftrust.info/

Summary and Q/A

Getting to a better web of trust with open, self-sovereign idenity

FOSS Software

We can continue to build on the shoulders of giants and work with standards groups like W3C

User Education

Help users gain awareness to privacy, security, FOSS and best practices

Open Hardware

Betrusted and similar hardware could provide secure storage for private key material

Collaboration

We can work together in the community

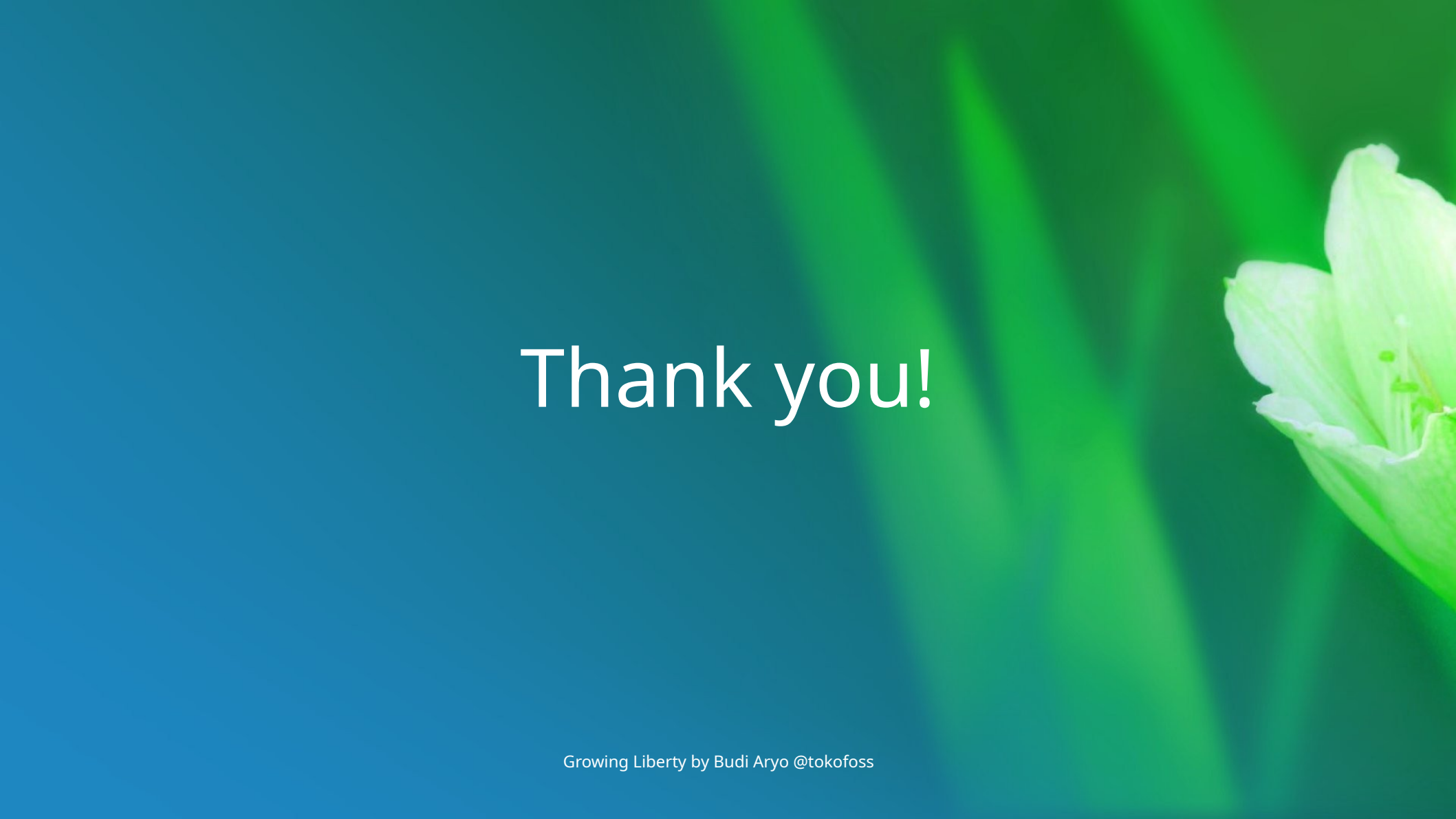
User Experience (UX)

Getting the UX right for security is essential

Q/A

What do YOU think?

Slides will be available at
https://tmarble.info9.net and **tmarble@info9.net**


Thank you!