tillitis

A transparent HSM using transparency technology

Fredrik Strömberg

Amagicom Group

Mullvad VPN AB

VPN
Browser

Tillitis AB

TKey
HSM (WIP)

Glasklar Teknik AB

Sigsum
System Transparency
Debian Snapshot service

Karlstad Internet Privacy Lab AB

Maybenot framework

Where we came from, and where we're going

tillitis

March 2009

The **Mullvad VPN** service launches.

June 2019

The **System Transparency** project was revealed.

October 2021

The **Sigsum** project launches.

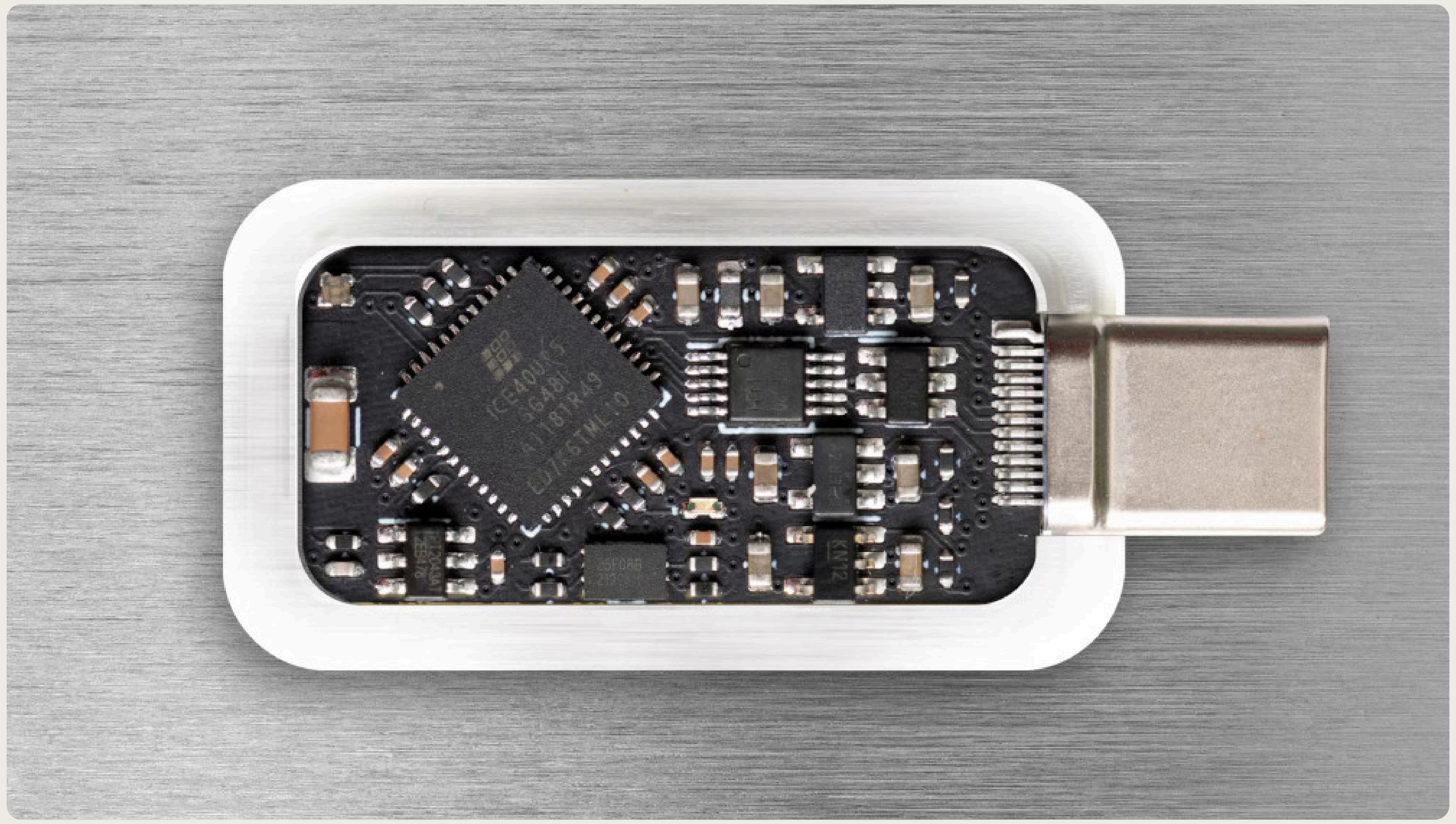
September 2022

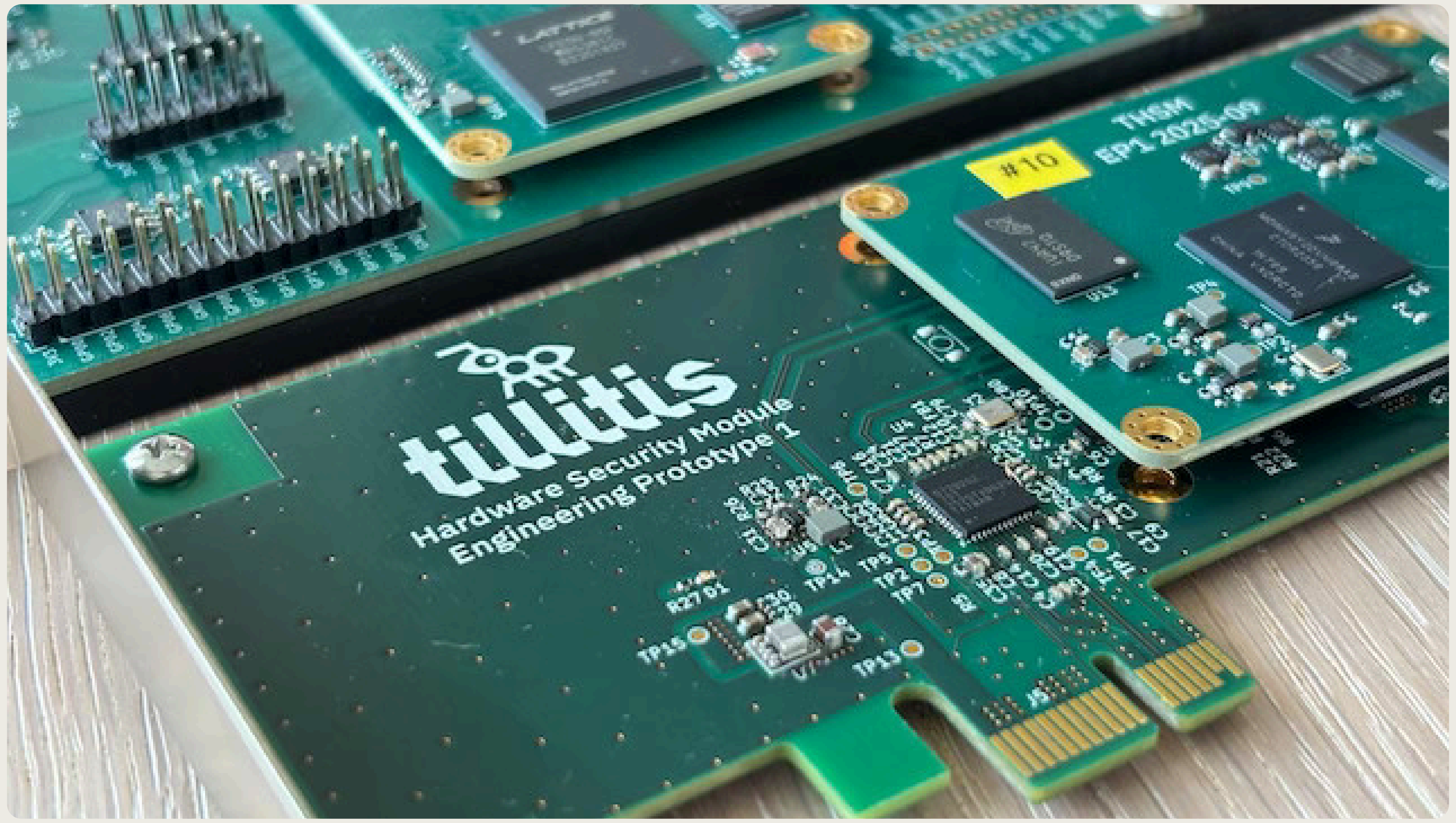
Tillitis was founded and the **TKey** was announced.

September 2025

We announce the existence of the **Tillitis** HSM project.

Tillitis hardware





Tillitis TKey

For individuals and end-point devices.

Tillitis HSM (work-in-progress)

For organizations and servers.

What is a Hardware Security Module?

Cryptographic keys

Creation and management of cryptographic key material.

Cryptographic operations

Performs operations like encryption and digital signing using the securely stored key material.

Tamper resistance

Often comes with some kind of tamper response system, which erases cryptographic keys if physical tampering is detected.

The HSM market today

Oligopoly

The industry is dominated by a small number of companies.

Black boxes

Mostly closed-source, proprietary systems.

Unverifiable

Impractical to inspect and verify.

tillitis

Our design philosophy

Hardware defenses

Hardware sets the rules for software.

Cryptographic defenses

Provides a security margin measured in computational complexity and Joules.

Restricted state space

Stop weird machines! Context-free or regular!

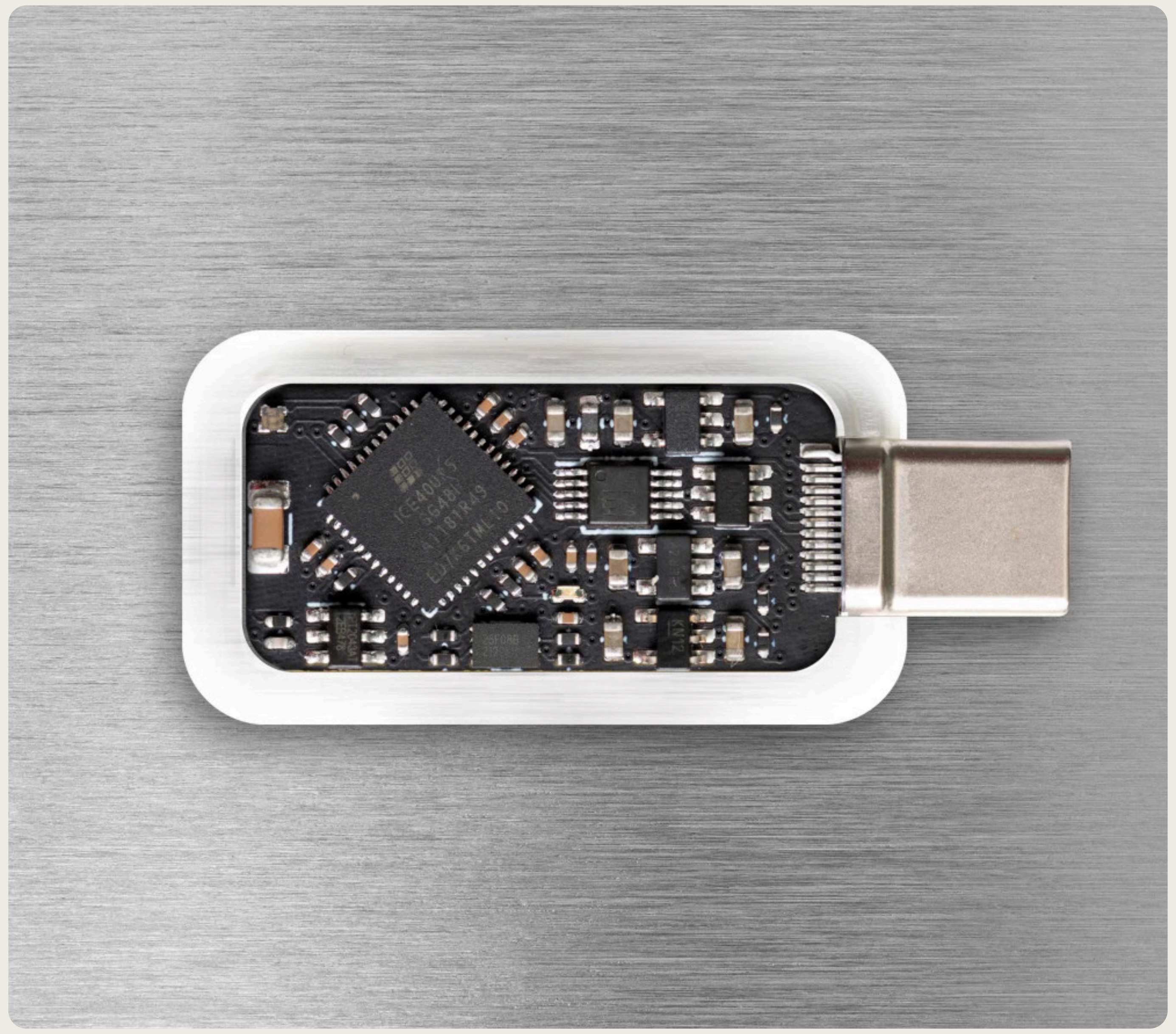
Distributed trust assumptions

Multi-signature schemes, multiple branch instructions, cores running in lock-step.

Available & understandable...

specification, implementation, supply chain.

Tillitis HSM builds upon



TKey

FPGA-based, measured boot, security token.

USB armory

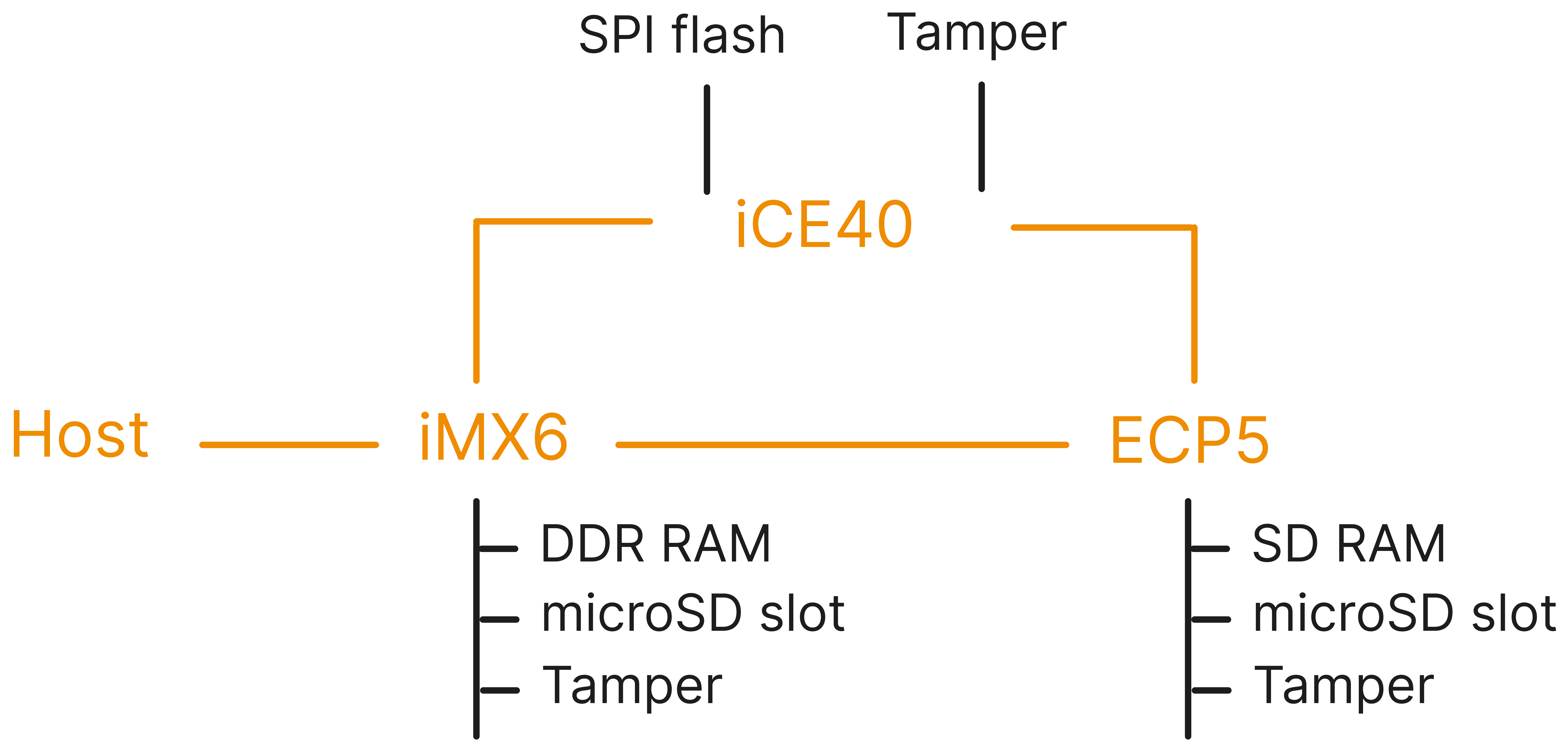
An open-source compact secure computer, running a Go unikernel.

CrypTech HSM

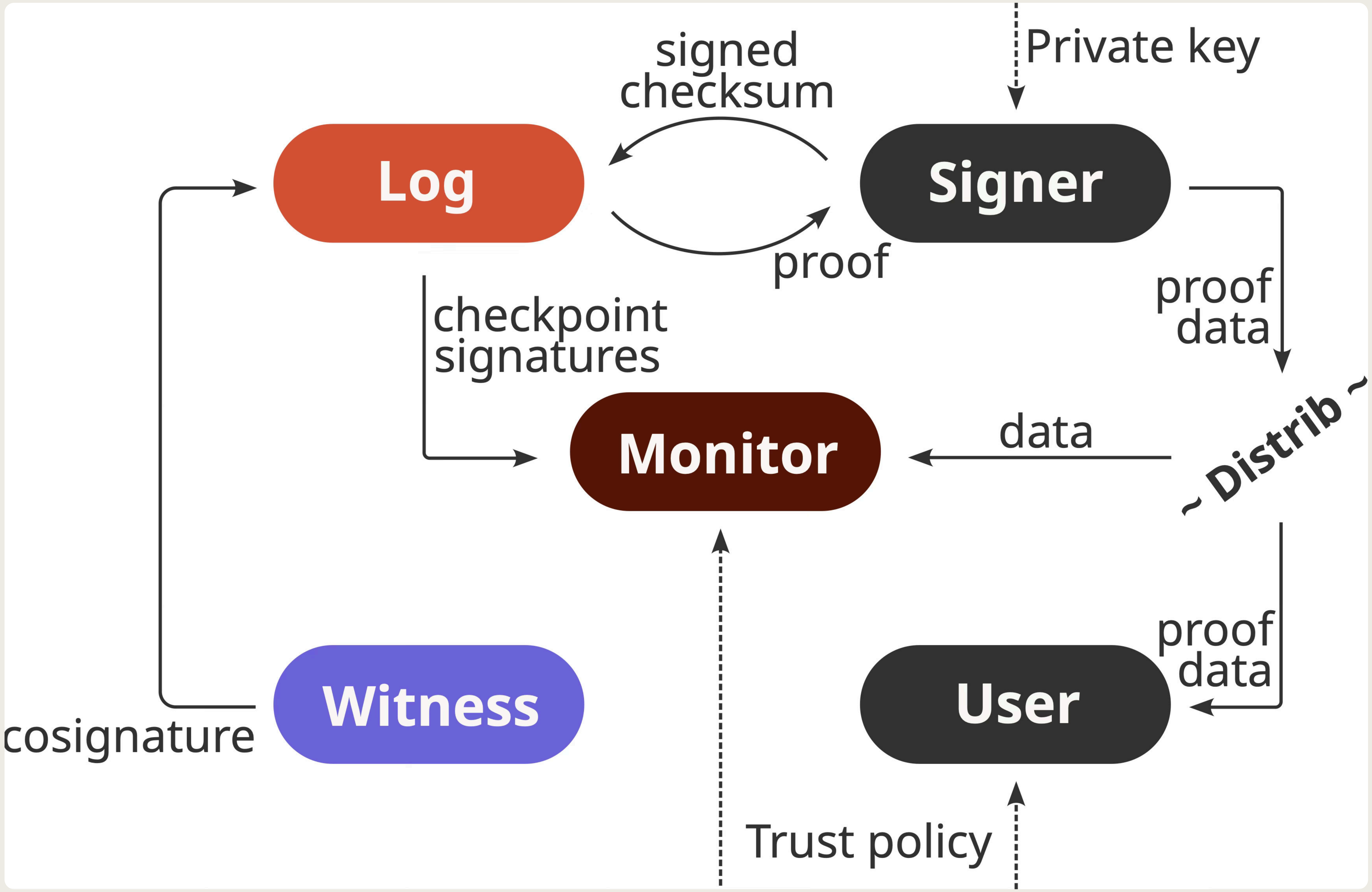
Open-source hardware cryptographic engine.

Design overview

tillitis



Sigsum (a transparency log design with distributed trust)



Future plans

Integrate transparency technology

Continue to develop functionality that supports different use cases related to our **Sigsum** and **System Transparency** projects.

Research & education

Use our open-source hardware projects for your research and education purposes!

Open-source silicon

Design and manufacture our own open-source silicon, using open tooling, on Global Foundries 180mcu process.

Thank you for listening!

hello@tillitis.se