tillitis

Michael “MC” Cardell Widerkrantz

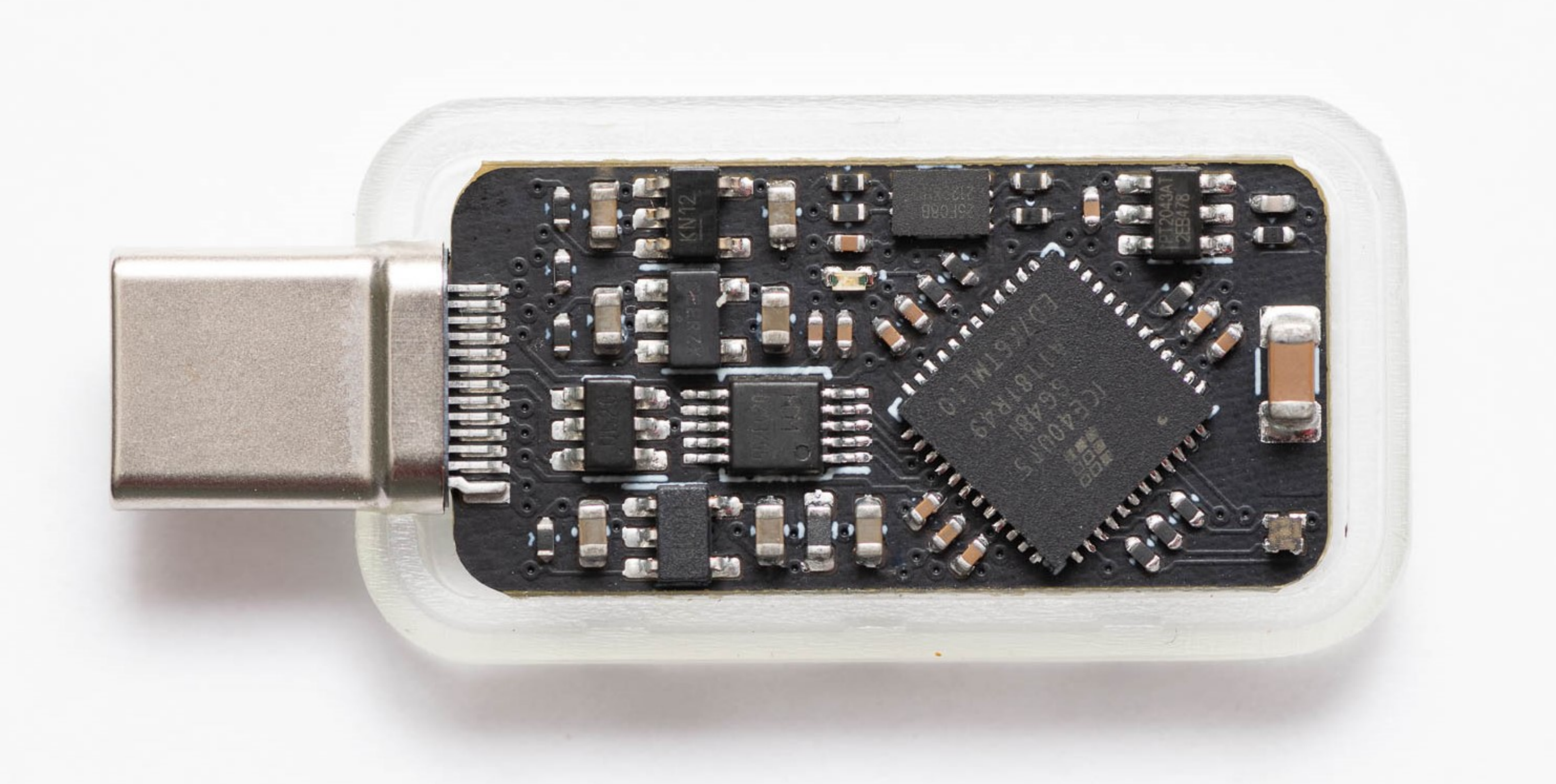
Tillitis AB https://tillitis.se/

MC

Origin

- Sister company to Mullvad VPN.
- Trustworthy Computing Research team at Mullvad.

We have built a computer!



The TKey computer

- Has a Unique Device Secret (UDS) in hardware.
- Runs small programs.
- Uses measured boot to produce unique identities for every program.
- Talks with your computer/mobile phone (client).
- Everything under open licenses.

What?

- Authentication.
- Identification.
- HSM-like applications.
- Generate secure (and maybe signed) random numbers.
- Encryption.
- Other things… It's a general computer!

Advantages

- You can use TKey for many things.
- Function defined by uploaded program.
- The client computer decides function of the TKey.
- No need for a new TKey for new functionality.
- Organisations can customize TKey.
- No risk for persistent threats.
- Hardware security guarantees.

How to use?

- Insert TKey into the client.
- The client uploads a small program to TKey.
- The TKey firmware receives the program, measures it, and derives a new unique identity (Compund Device Identifier).
- Firmware starts the TKey program.
- The client program and the TKey program talk to each other.

Advantages of measured boot and CDI

- Compound identity can be used as a private key.
- Private keys are not stored persistently on the TKey.
- Unlimitied number of private keys.
- Private keys don't leak between uploaded programs.

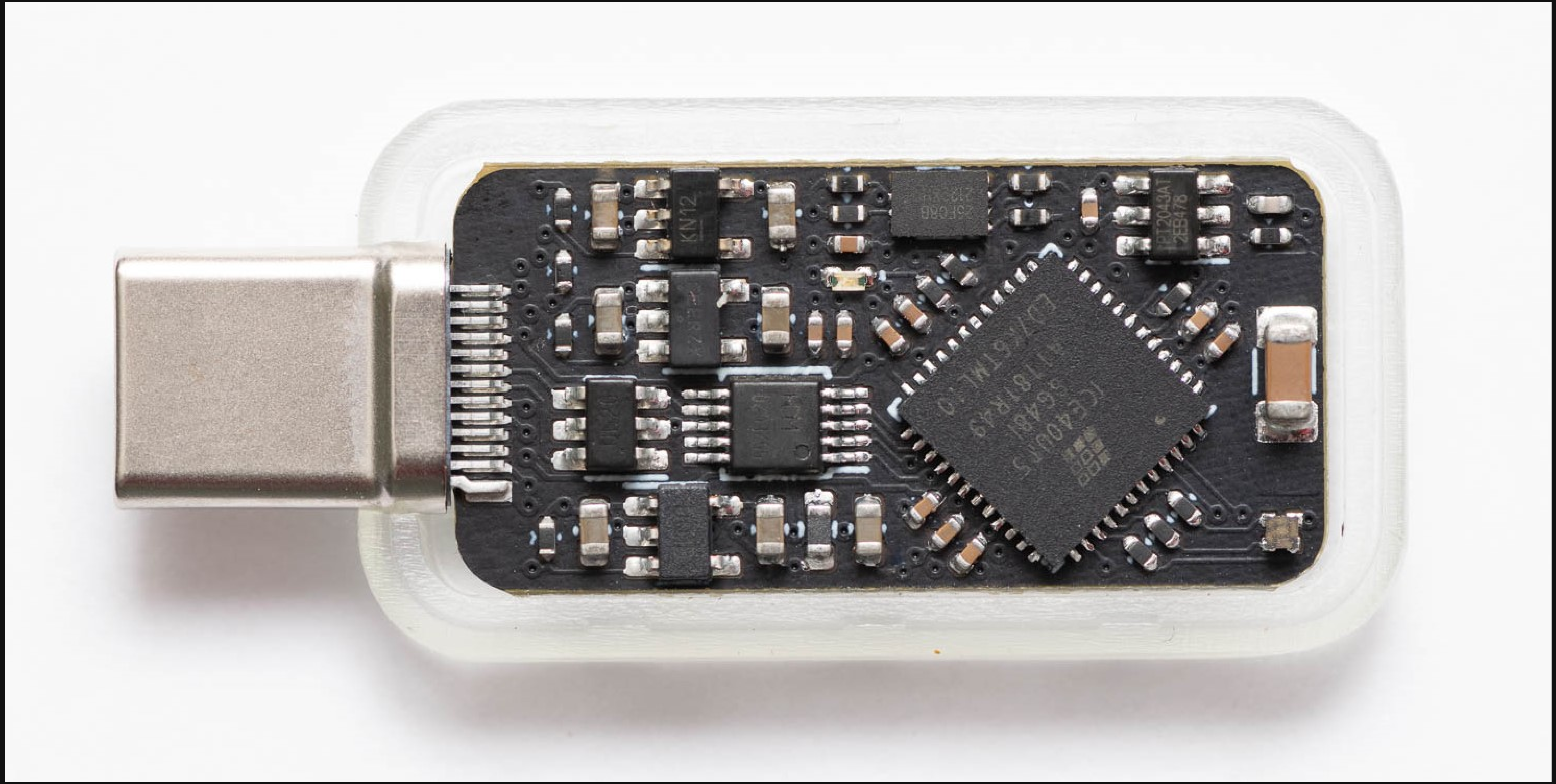
Compound Device Identity?

CDI is a mix of:

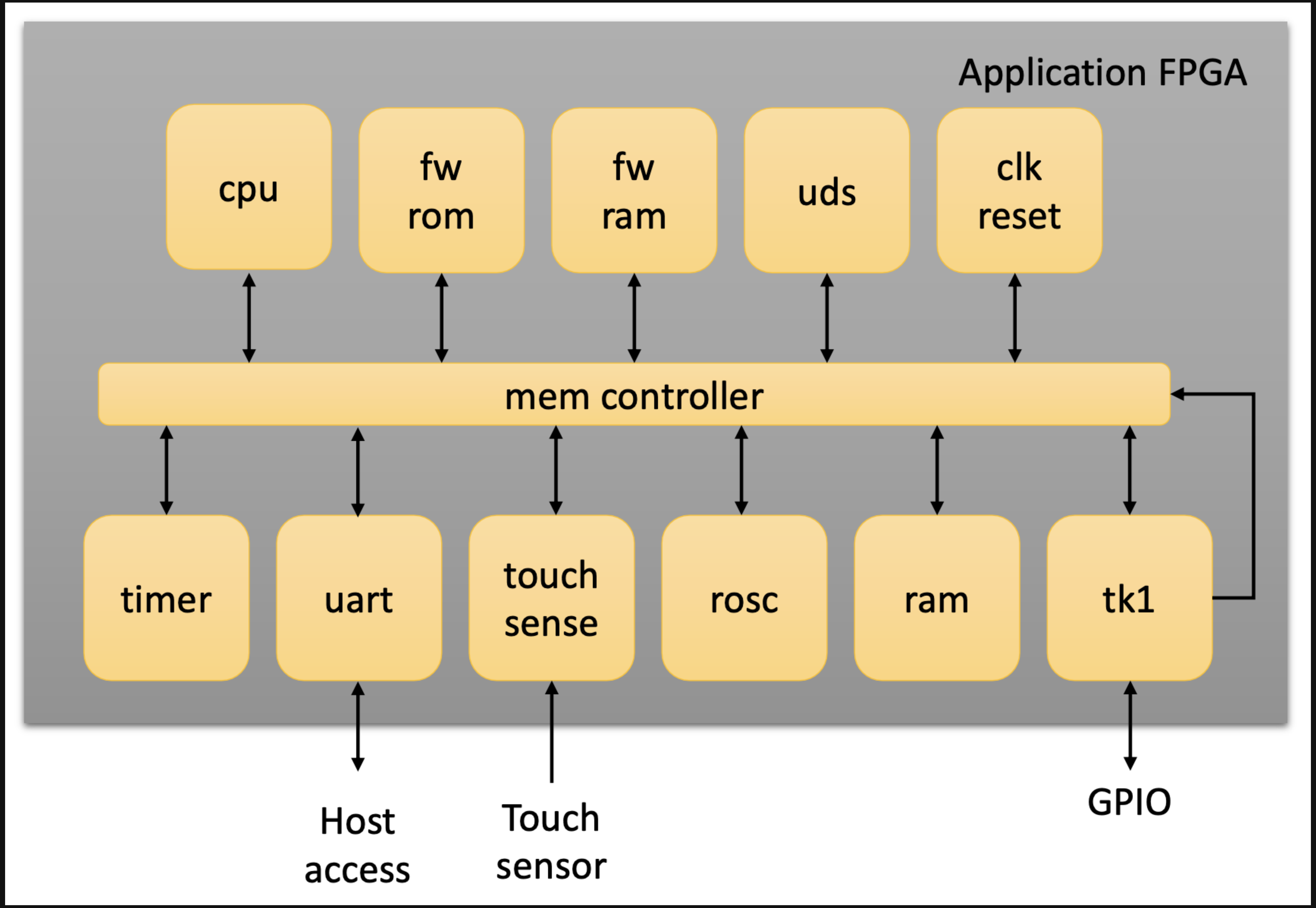
- Unique Device Secret (UDS) in hardware.
- Optional User Supplied Secret (USS).
- Digest of TKey program is mixed in to the identity.

```
identity = blake2s(UDS, blake2s(program), USS)
```

Hardware



In the FPGA


Application FPGA
cpu
fw rom
fw ram
uds
clk reset
mem controller
timer
uart
touch sense
rosc
ram
tk1
Host access
Touch sensor
GPIO

Specs

- 32 bit RISC-V (RV32IC_Zmmul) @ 18 MHz.
- 128 kiB RAM.
- Hardware cores memory mapped.
- Execution monitor.
- Hardware-assisted ASLR and RAM scrambling.
- Support in compiler framework LLVM-15.

Our software

- Emulator: qemu (use the "tk1" branch).
- Firmware/boot loader.
- Client programs.
- TKey programs.

Some client programs

- Written in Go.
- `tkey-runapp`: Load and run a raw binary.
- `tkey-sign`: sign data.
- `tkey-ssh-agent`: An SSH Agent.

SSH Agent

- OpenSSH compatible agent in Go.
- Runs on client computer.
- Runs the TKey `signer` program for signing operations.
- Packaged for Ubuntu, Debian, and Homebrew for macOS (Windows support ongoing).

SSH Agent 2

- Login to other computers.
- Sign Git commits.
- …other SSH operations.

Client SDK

Go modules:

- `tk1`: Module to detect and talk to TKey and load a program.
- `tk1sign`: Module to talk to the TKey program `signer`.

First TKey program

```
        li a0, 0xff000024 # LED MMIO
        li a1, 0x1
loop:
        sw a1, 0(a0)
        addi a1, a1, 1

        li a2, 0
        li a3, 100000
delay:
        addi a2, a2, 1
        blt a2, a3, delay
        j loop
```

TKey programs

- `signer`: An Ed25519 signing oracle.
- `rng_stream`: A random number generator.
- And some debug programs.

TKey SDK

- clang/llvm-15 for RV32IC_Zmmul.
- `libcrt`: C runtime.
- `libcommon`: Common convenience functions.
- `libmonocypher`: cryptographic library.
- `tk1_mem.h`: Header file with all memory mapped hardware functions.
- `blake2s()`: A single 'system call' (well...) provided by firmware.

Verificiation

- You can verify the TKey.
- We run a program on all TKeys before delivery.
- We sign this program's public key and the firmware hash it computes.
- We publish these signatures.
- You can yourself run the same program and see that it has the same identity and firmware.

Summary

- A new RISC-V computer.
- USB stick form factor.
- No persistent state.
- Uses measured boot to create unique program identities.
- Client & TKey SDK.
- Custom SSH Agent in Go.
- Open licences.

The End

- Michael “MC” Cardell Widerkrantz, **mc@tillitis.se**
- General inquiries, **hello@tillitis.se**
- #tillitis @ irc.oftc.org, #tillitis:matrix.org

https://tillitis.se/