OpenAlt 2026

https://scrutiny.cloud

Open, transparent, end-user verifiable and LLM-ready security testing framework

Funded by the European Union

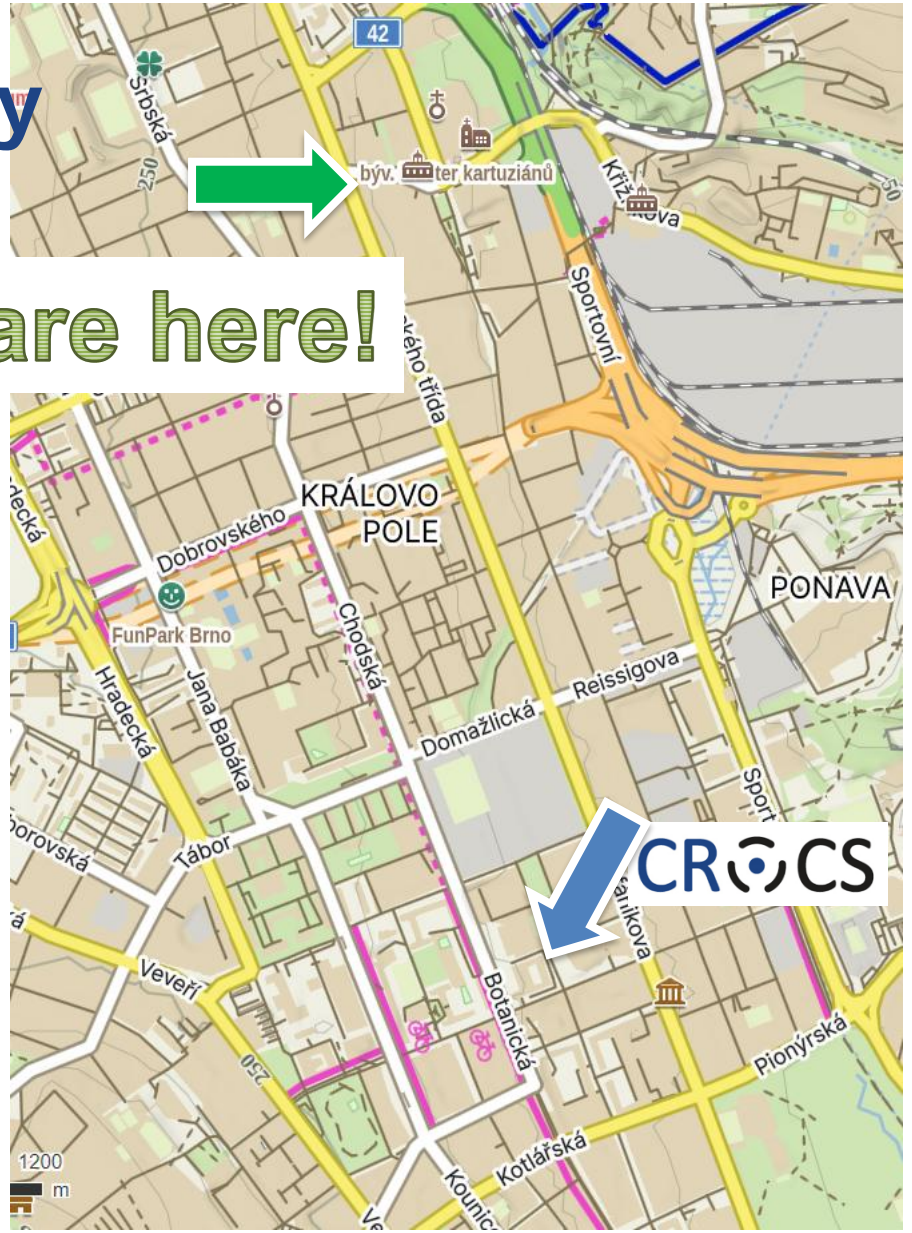
CAT
CYBERSECURITY CERTIFICATION AND ASSESSMENT TOOLS

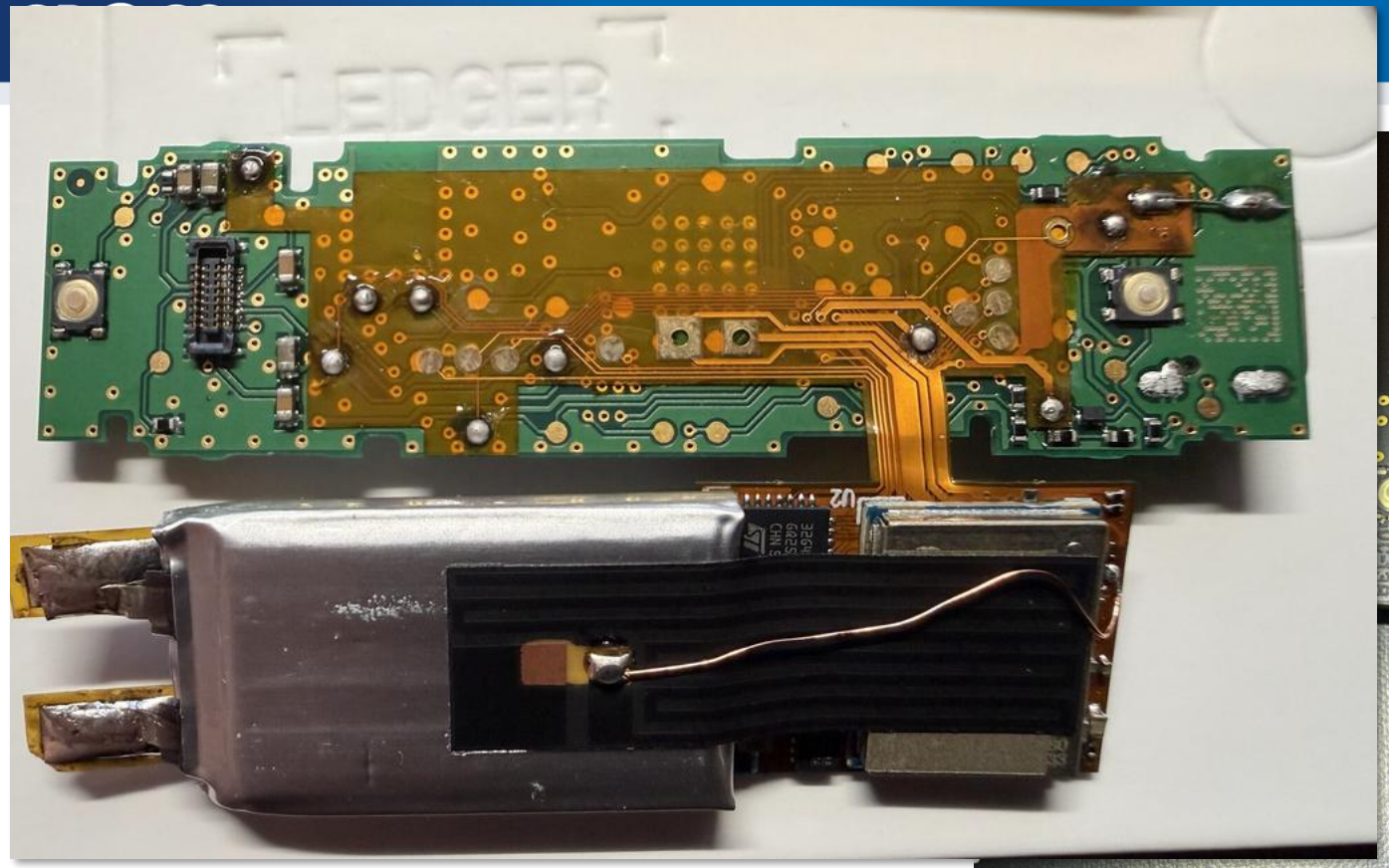
Ali Al-Sorehi, Petr Svenda

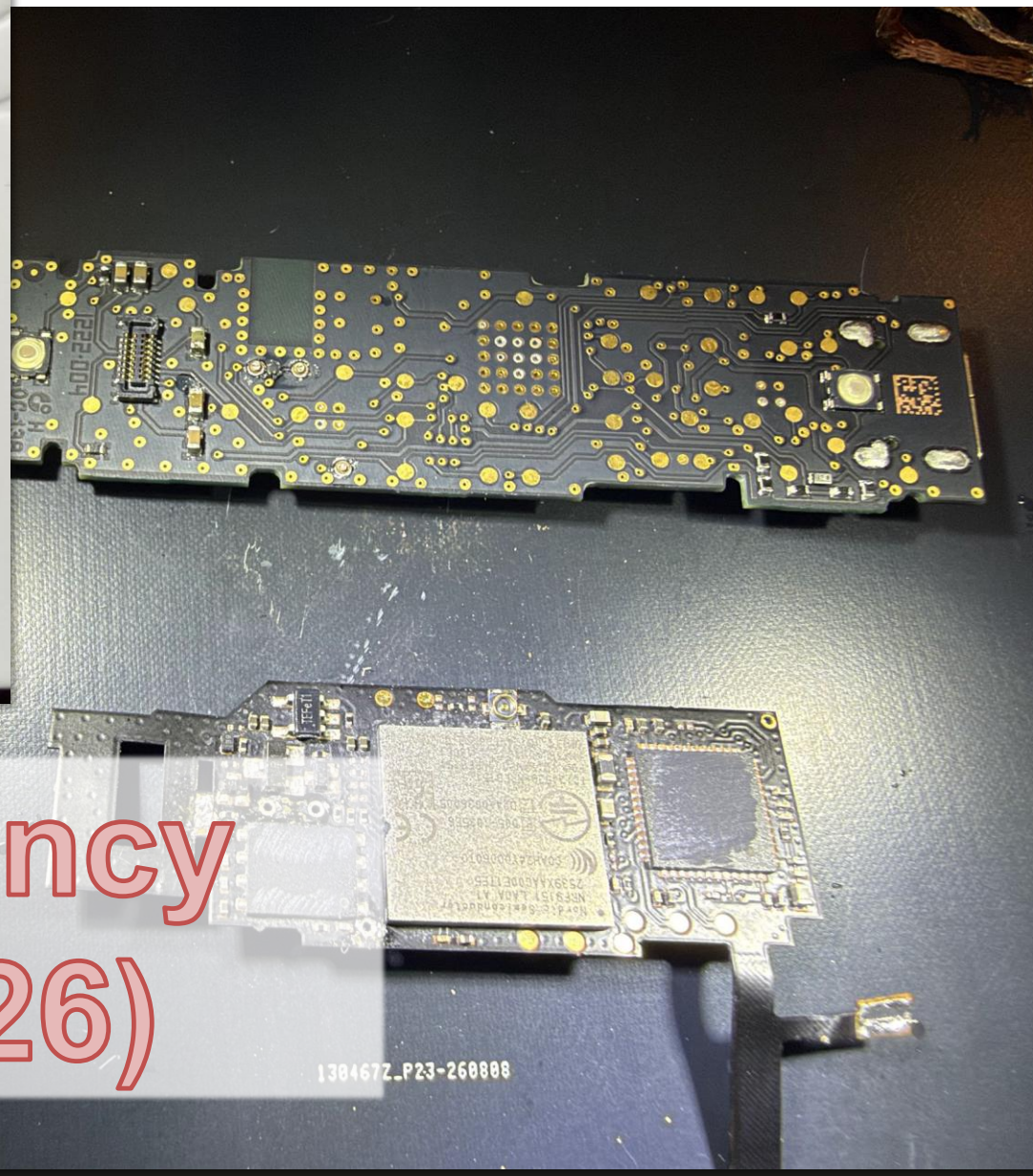
CROCS
Centre for Research on Cryptography and Security

CRoCS laboratory, Masaryk University



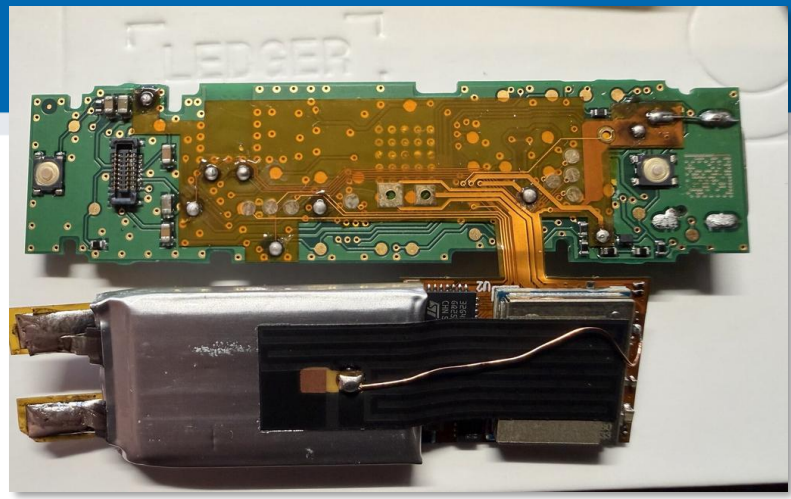






Ledger cryptocurrency wallet implant (2026)

Cryptocurrency wallet implants (2026)



- Hardware crypto wallets with a secure element
  – Ledger: ST33 secure element, Trezor Safe: Infineon OPTIGA Trust M…
- Huge, technically skilled hobbyist community
- Secure element is CC-certified (the device as a whole often not)
- People want to know whether the device is genuine, what the secure element actually protects, and what the firmware does…
- Teardowns and side-channel results exist, but they are scattered across Reddit, YouTube and conference talks, and (some) vendors push back against critical findings

Security product ecosystem is (largely) closed

- Vendors, evaluation labs, certification bodies
  - Raised the security baseline a lot (Common Criteria, FIPS 140, EUCC)
  - But detailed evaluation reports stay private: you get a certificate, not supporting evidence
- Public data exists, but is hard to find and use
  - sec-certs.org: CC and FIPS 140 certificates parsed, searchable, linked to CVEs
  - Authoritative answers about certificates, not about your actual device



End users are expected to just “trust the label”



- Certified != secure

THE OPEN-SOURCE HOBBYIST HAS A HARD TIME :)



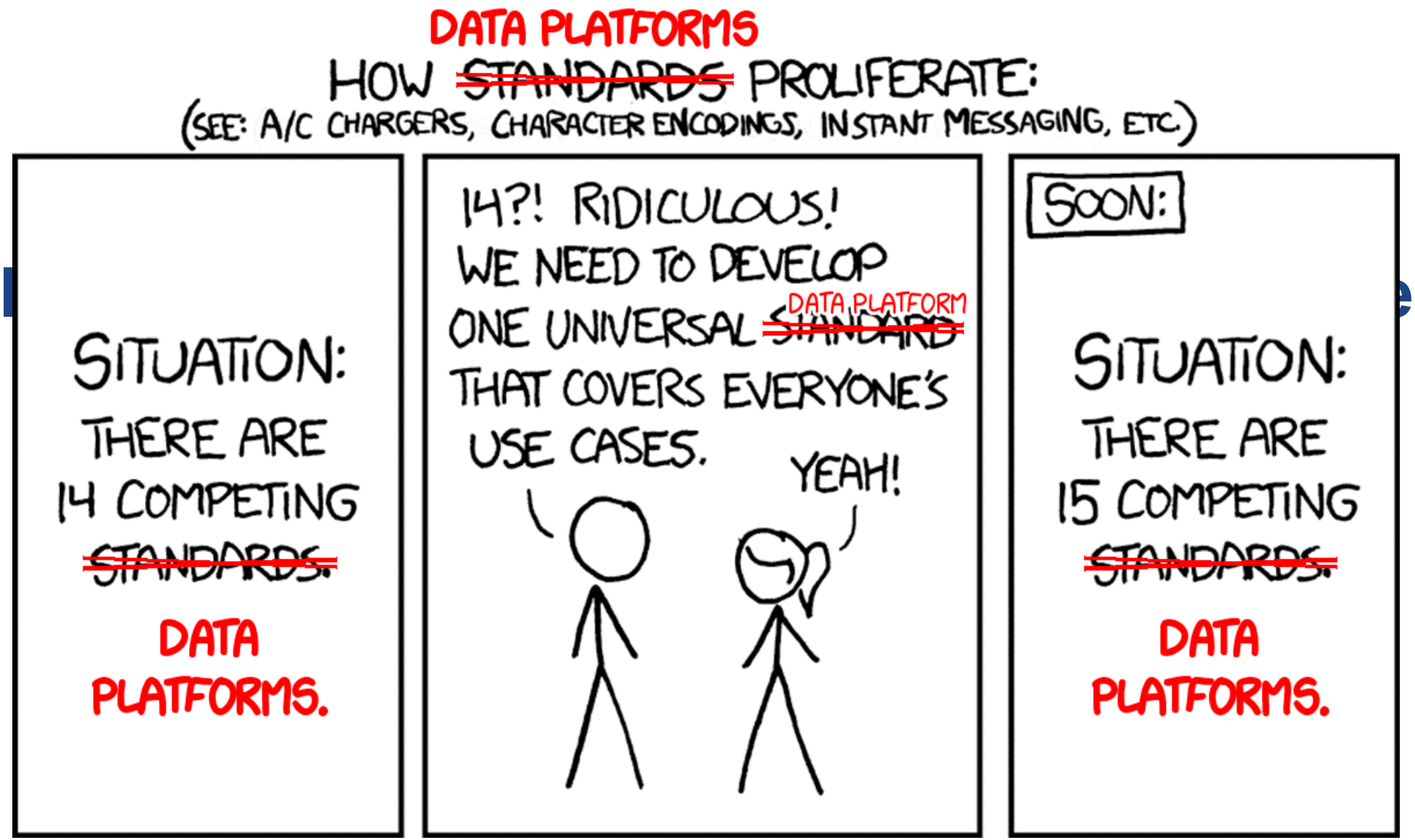
YET WANTS TO VERIFY OWN DEVICES
…AND WANT HELP OTHERS WITH OWN ANALYSIS

PROBLEM 1: DISCOVERABILITY

Hobbyists can help, but results are scattered

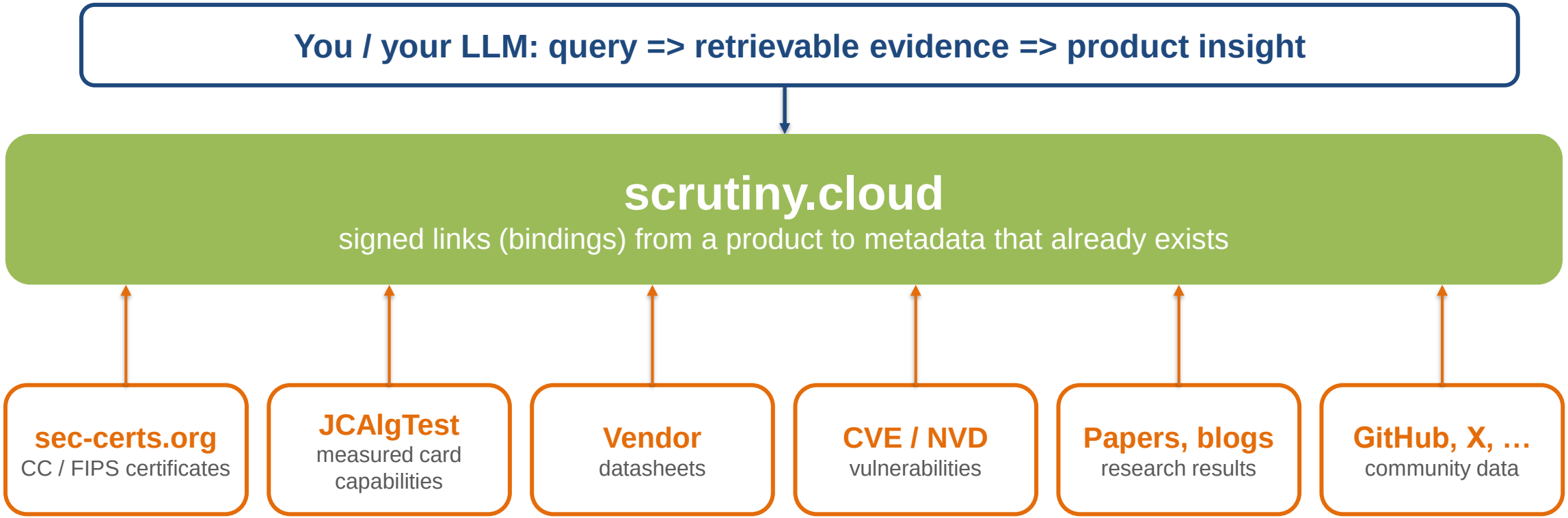
- Hobbyists already analyze a lot
  - Algorithm support, performance, teardowns…
- Results end up everywhere
  - X/Twitter, Mastodon, blogs, GitHub, forums, papers, talks
- Poor discoverability
  - Blog post about your card? Nobody will find it
  - No link between product, evidence and author





https://xkcd.com/927/

scrutiny.cloud: discovery layer on top of existing



Not the N+1 place to store data (see xkcd #927 “Standards”) → data stays where it is

PRODUCTS
(ProductEvent)

BINDINGS
(BindingEvent)

METADATA
(MetadataEvent)

Infineon M7794A12
BSI-DSZ-CC-0814-2012
CC EAL4+

CSV information

Status	archived
Valid from	26.07.2012
Valid until	01.09.2019
Scheme	DE
Manufacturer	Infineon Technologies AG
Category	ICs, Smart Cards and Smart Card-Related Devices and Systems
Security level	
Protection profiles	SECURITY IC V1.0, PRISKPT
Maintenance updates	Certification report

Binding

Binding

Binding

Binding

RSA keypairs
Distribution of primes P and Q

ECDSA signature
Dependency of sig time on private key

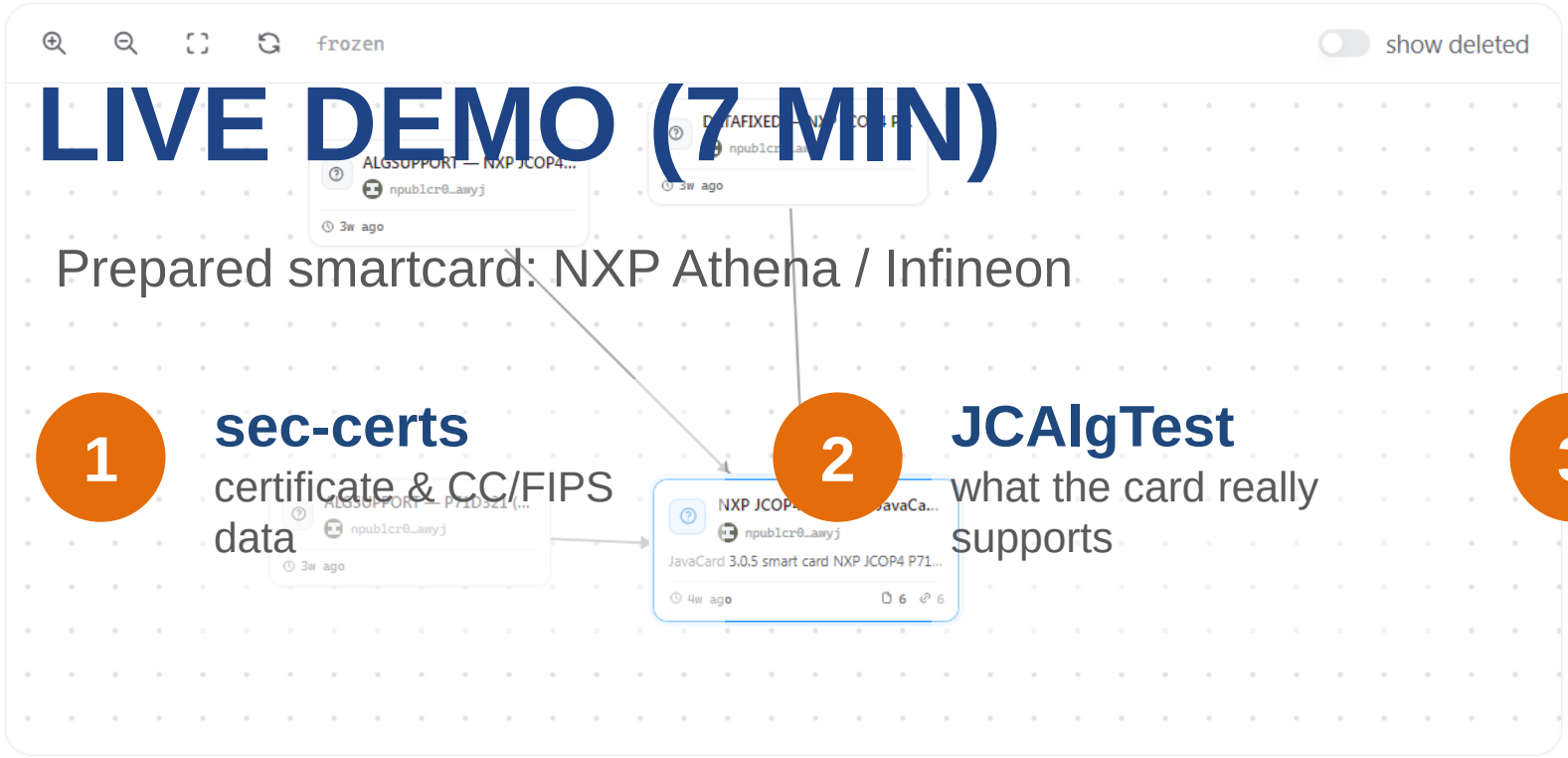
CVE-2017-15361
Vulnerability in keygen (ROCA)

ChatGPT summary
Prompt: Vulnerabilities in jTOP SLE78

Data stays where it already is, scrutiny.cloud binds it to the product

LIVE DEMO (7 MIN)

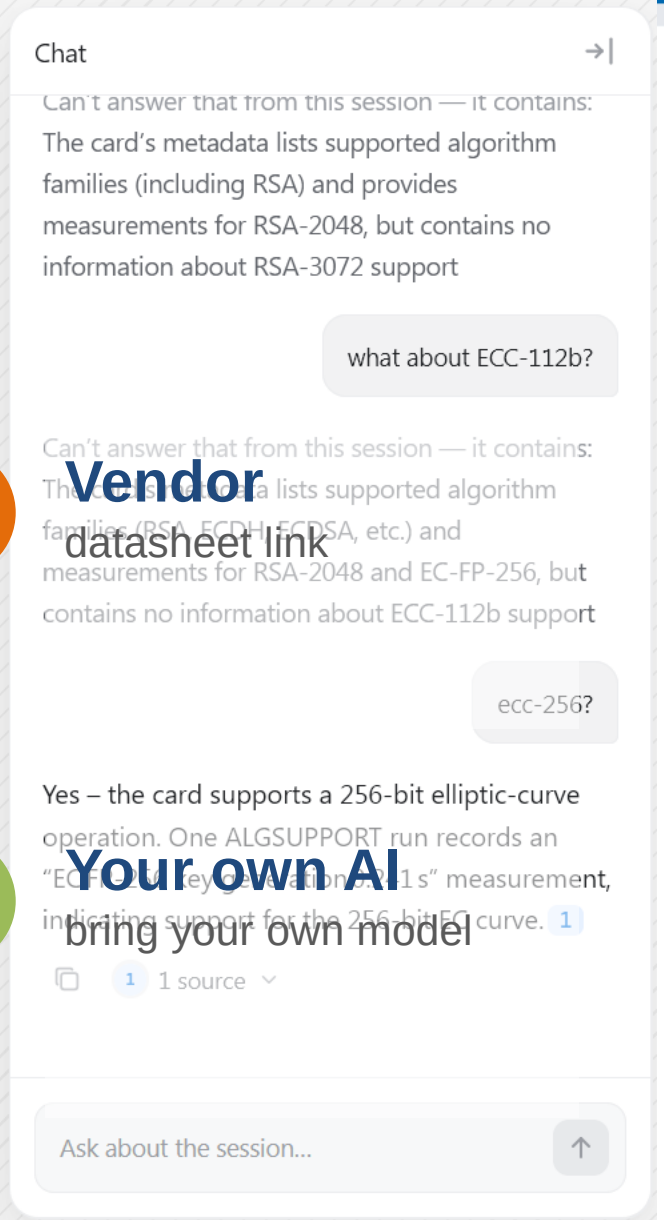
Prepared smartcard: NXP Athena / Infineon



1. **sec-certs** — certificate & CC/FIPS data
2. **JCAlgTest** — what the card really supports
3. **Vendor** — datasheet link
4. **Diff** — claimed vs. measured
5. **AI** — interprets all the evidence
6. **Your own AI** — bring your own model

```
NXP JCOP4 P71D321 – JavaCard 3.0.5 smart card (JCAlgTest profile c075).
Card identity: ATR 3b 8a 80 01 50 56 4a 43 4f 50 34 53 49 44 71; chip-line key 4790-d321; snapshot 2026-10-05.

- ATR 3b 8a 80 01 50 56 4a 43 4f 50 34 53 49 44 71 (continuous lowercase hex 3b8a800150564a434f503453494471).
- CPLC fabricator 4790 (NXP Semiconductors), ICType d321, OS ID 4700 → chip-line key 4790-d321.
- Declared JavaCard support version: 3.0.5 (exact, from the card's ALGSUPPORT runs) → cohort buckets jcver-lte:3.0.5, jcver-lte:3.1 of the frozen cut points 3.0.4 / 3.0.5 / 3.1.
```



PROBLEM 2: CENSORSHIP OF DATA

Home › Mobile Security



Apple Sues Corellium Over Security Research Tool

By Eduard Kovacs on August 16, 2019

LinkedIn Tweet Recommend 0 RSS

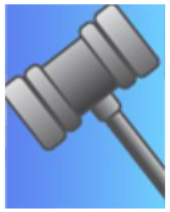
Apple has filed a copyright infringement lawsuit against Fl
company Corellium for creating "perfect replicas" of iOS t
res

German Software Company Threatens Security Researcher With Lawsuit

By: Fahmida Y. Rashid | April 29, 2011

ened legal action against a security researcher for privately reporting a critical
nt "Acidgen," an independent security researcher, a letter threatening a lawsui
security vulnerability he discovered in the vendor's music application, Dark Re

Security Researchers Sued For Exposing Internet Filtering Company's Sale Of Censorship Software To Blacklisted Country



Legal Issues

from the *'you're-making-us-look-bad'-said-company-caught-looking-bad* dept

Fri, Jul 29th 2016 3:51am — Tim Cushing

Nothing says "Please ~~stop~~ *keep* talking about the bad stuff we do
defamation lawsuit. Citizen Lab, which has reported on a great r
that are less than discriminating in their selection of customers (
been served with a lawsuit by a purveyor of internet censorship s

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS

MUST READ: WFH and burnout: How to be a better boss to remote workers

Lawsuits threaten infosec research — just when we need it most

Security researchers and reporters have something in common: both hold the powerful accountable. But doing painted a target on their backs — and looming threats of legal action and lawsuits have many concerned.

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDI

MUST READ: WFH and burnout: How to be a be

Security firm Keeper sues news reporter over vulnerability story

The vulnerability was fixed, but Keeper now demands that the allegedly defamatory article is pulled offline.



is permissionless distributed protocol by design

- Anyone can publish after generating keypair
  - no barrier to entry (=> permissionless)
- Signed events replicated over many independent relays
  - no gatekeeper, no single point takedown (=> censorship resistance)
- Permissionless => spam & trust problem
  - How do you know whom to believe?

In Nostr, everything is signed

You bring a curated trust list: only evidence from trusted signers is fetched/shown

PRODUCTS
(ProductEvent)

BINDINGS
(BindingEvent)

METADATA
(MetadataEvent)

Infineon M7794A12
BSI-DSZ-CC-0814-2012
CC EAL4+

CSV information

Status	archived
Valid from	26.07.2012
Valid until	01.09.2019
Scheme	DE
Manufacturer	Infineon Technologies AG
Category	ICs, Smart Cards and Smart Card-Related Devices and Systems
Security level	AVA_VAN.5, EAL4+, ATE_DPT.2, ALC_DVS.2
Protection profiles	• SECURITY_IC_V1.0, PKISKPP
Maintenance updates	Infineon smartcard IC (Security Controller) M7794 A12 with optional RSA2048/4096 v1.02.013, EC v1.02.013 and Toolbox v1.02.013 (15.03.2013) Certification report

Binding

Binding

Binding

Binding

RSA keypairs
Distribution of primes P and Q

ECDSA signature
Dependency of sig time on private key

CVE-2017-15361
Vulnerability in keygen (ROCA)

ChatGPT summary
Prompt: Vulnerabilities in jTOP SLE78

The current state od scrutiny.cloud

- Protocol specs., threat model: https://github.com/crocs-muni/scrutiny-fabric/
- Protocol implementation: https://github.com/crocs-muni/scrutiny-fabric-tools
- Initial batch of datasets published:
  - All Common Criteria and FIP140 certified devices (12000+ products) + extracted information (cryptography, security claims, references, CVEs…)
  - JCAlgTest datasets (100+ smartcards, algorithm support, performance bench)
  - Soon:
    - Cryptocurrency wallets (18+ devices), Self Encryption Drives (40+ devices)
    - RSABias and ECTester databases (30+ hw/sw cryptographic libraries)
    - Bitcoin CoinJoin transactions (4 designs, 10+ years of data)…
- LLM-powered evidence browser https://lens.scrutiny.cloud

scrutiny.cloud summary

- Permissionless sharing
- Discover evidence posted by others
- Define your own trust scope (keys)
- Process the data (manually / llm)

https://lens.scrutiny.cloud

💡 Try it! (Bring Your Own LLM, endpoint + API key)

- Help us – try it, feedback, add own data 🙏