OpenSSL CONFERENCE

OpenDaiY

Move fast and make things · Justin Corlett, Cryptsoft

§ PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

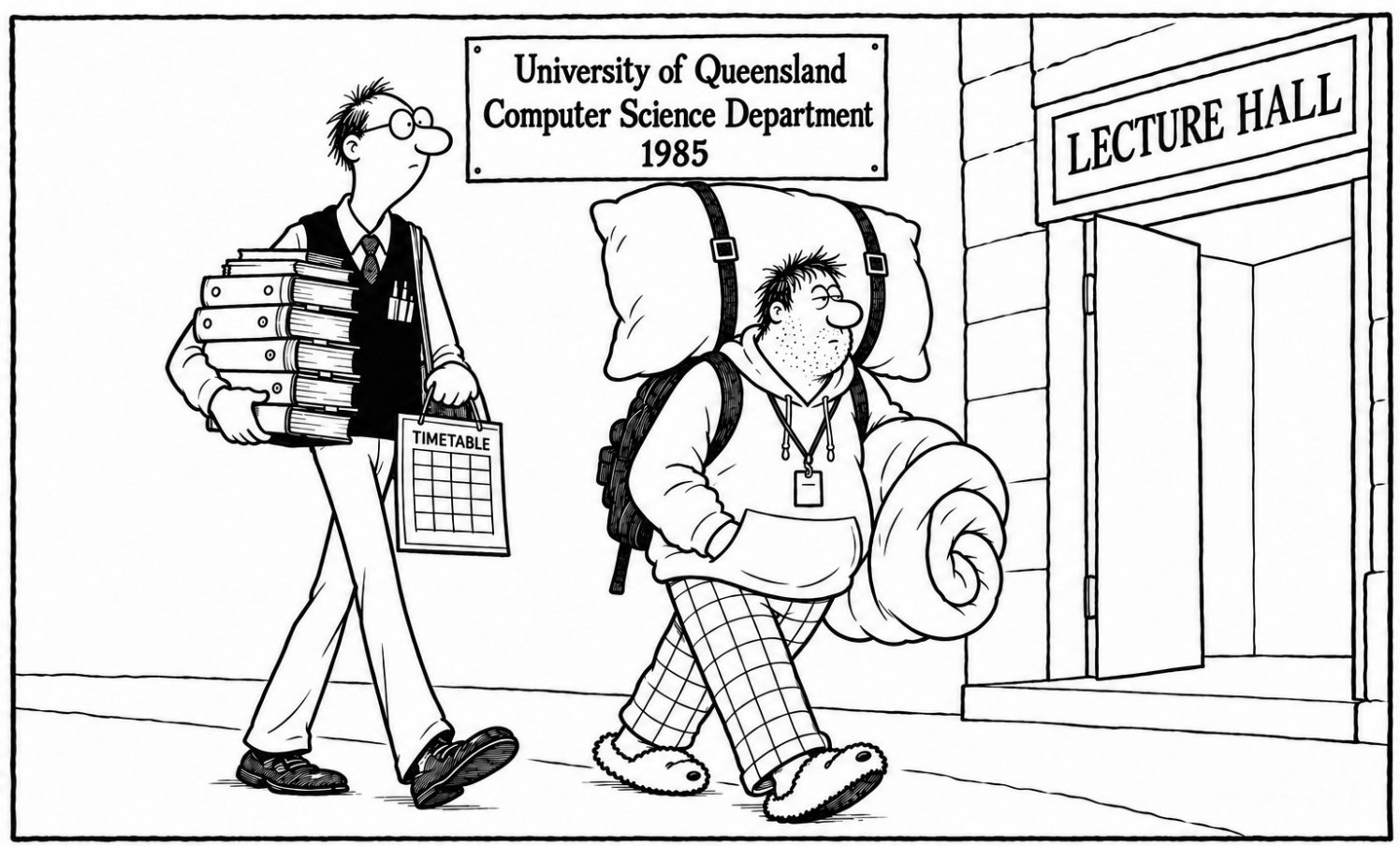
13.10.2026

Is OpenDaiY the saviour of security?

- By the end of this talk it will be in your vocabulary, and you will have your answer.

1985. Two very different students

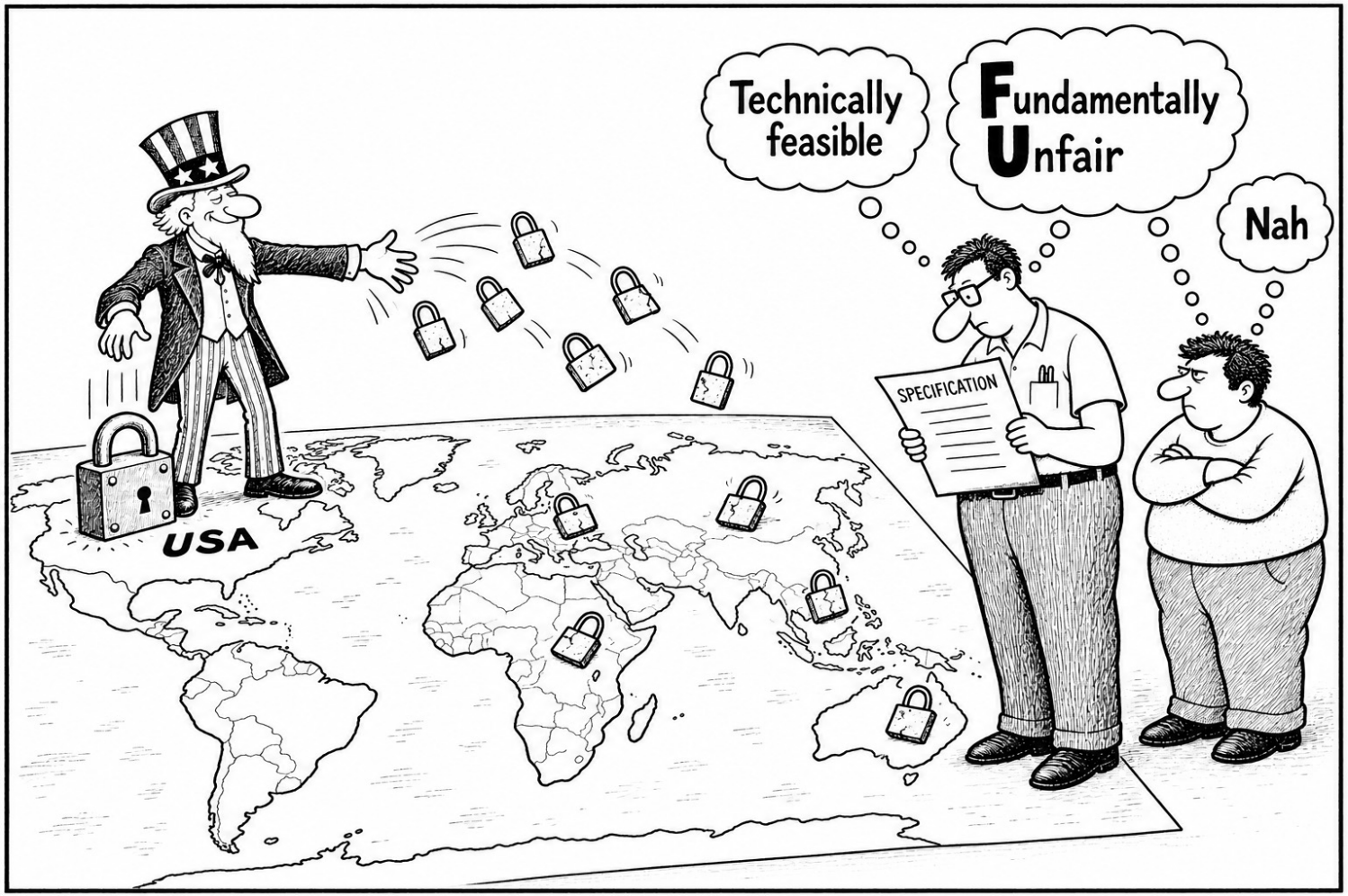
OpenSSL CONFERENCE



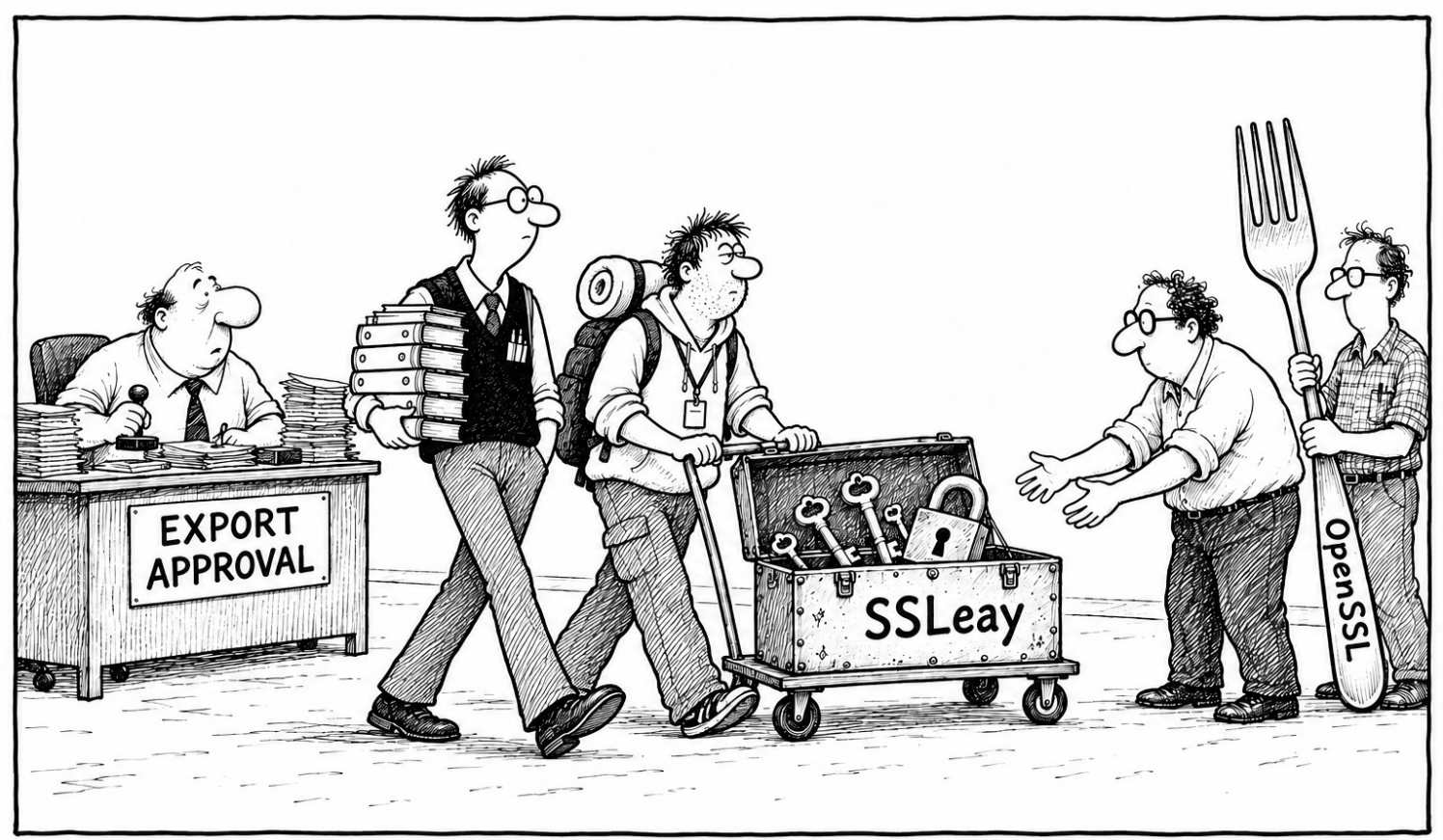
They were both prepared for the 9 a.m. lecture.

The birth of SSLeay

OpenSSL CONFERENCE



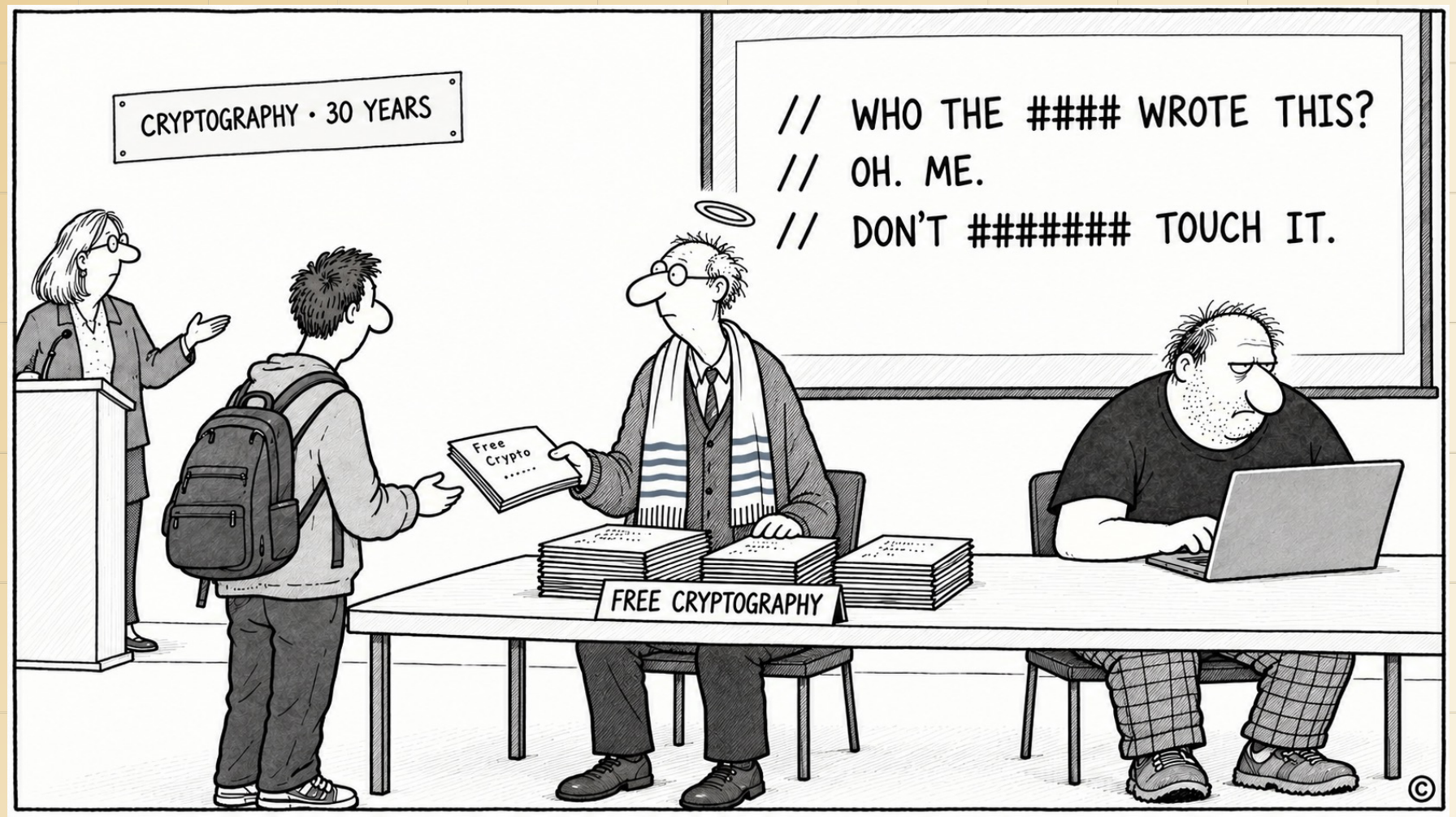
The birth of SSLeay



"Export approval? Yeah, yeah, yeah, NAH!"

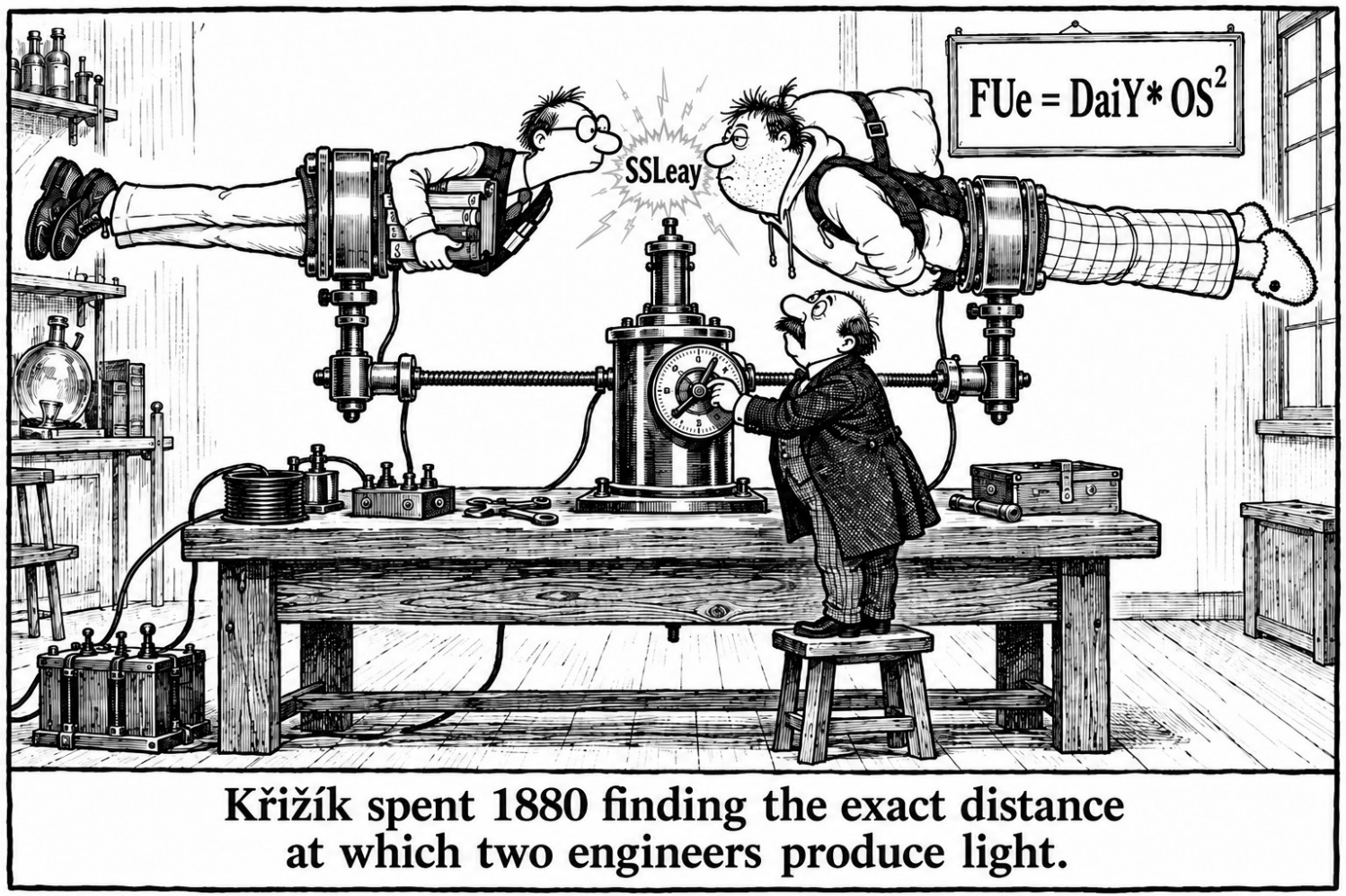
The mothers of internet security

OpenSSL CONFERENCE



Two rods, a gap, and a spark

OpenSSL CONFERENCE



OpenSSL CONFERENCE

01 The message

A business model, not a company. Three punches, three doors.

Three punches

One. Demand open models

Anyone can read it, test it, fork it, design it and make it.

The only way to keep a customer is to deserve them.

Performance beats profit. Innovation beats inertia. Features beat flatulence.

Two. Zero trust applies to the word open

Open source and open standards have been counterfeited for years.

Every vendor claims PKCS#11 support; almost none mean the same thing.

Trust, but verify. Actually, skip the trust.

Three. The walls have come down

The ability to make stuff arrived, faster than any closed model can rebuild.

Do it yourself, with AI filling the skills that stopped you.

Move fast and make things. Patent pending. Apache 2.0, so the patent licence is included.

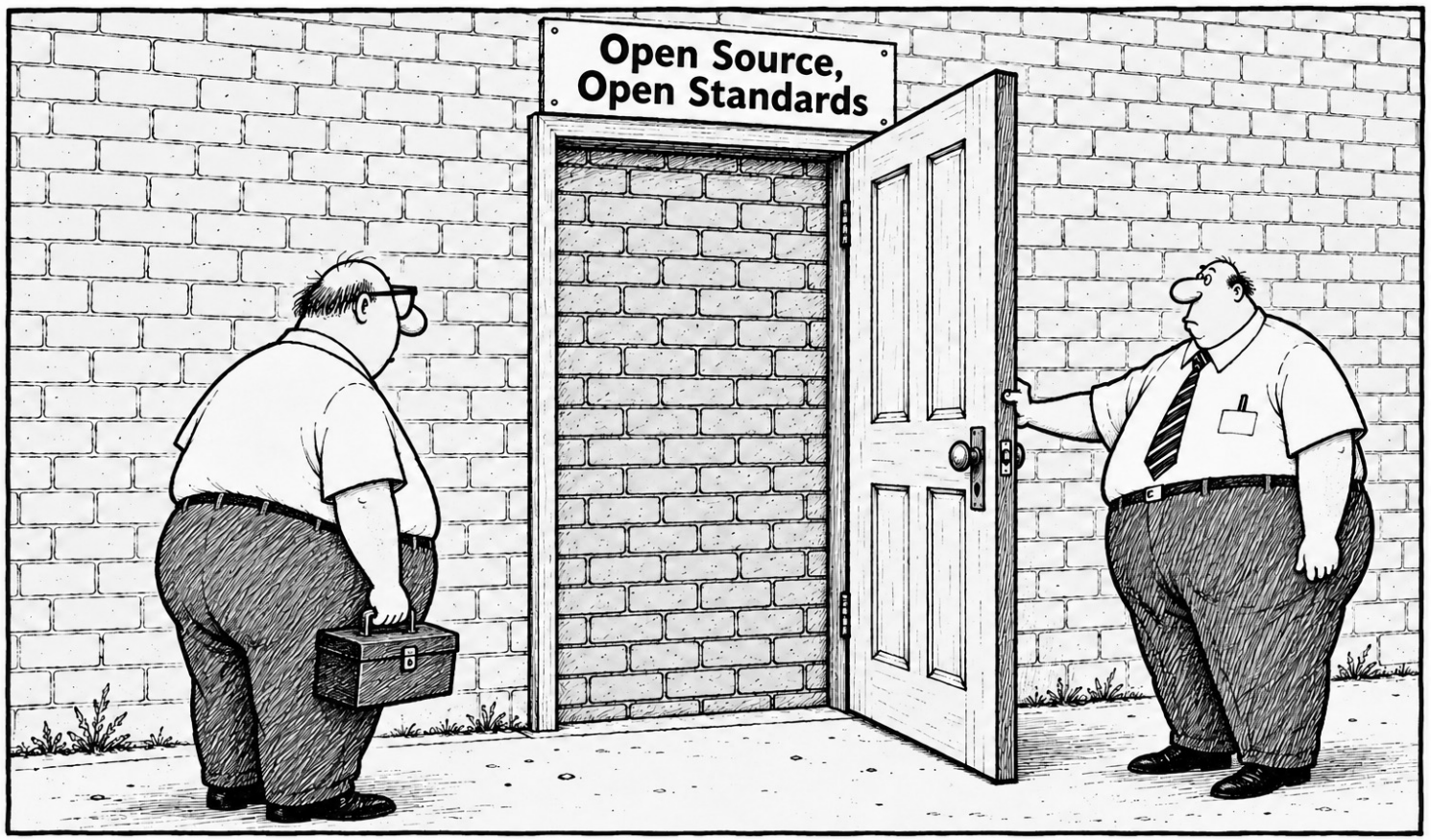
OpenSSL CONFERENCE

02 Door one: open source

Free is door one. The most valuable part of open source is its community.

Naturally, open refers to the door

OpenSSL CONFERENCE



Naturally, ‘open’ refers to the door.

How does an open source community get built?

OpenSSL CONFERENCE

Way one: it forms by itself

Two blokes in Brisbane give away some code.

Unplanned growth has its own risks: by 2014 OpenSSL ran on one paid developer.

Heartbleed. The answer was structure: funded maintainers, review rules, a Foundation and a Corporation in 2024.

Way two: build the ecosystem first

A standard and an interoperability programme every year.

Servers and clients proving themselves in public; an installed base in real products.

Then open the technology so everyone can reach it. Both ways work.

The third way never works

Throw the code over the wall and do nothing.

No support, no community, some PR.

A difference? Not really.

OpenSSL CONFERENCE

Not all open source is the same

Zero trust applies to the word open. Read the ladder from the bottom rung up.

- **Top rung, stewarded community:** rules in public, a way in for outsiders, a name behind it.
- **Cryptsoft, until today:** halfway. Licence the source, read it, fork it, be supported. Still not open source.
- **Source available:** the eyes that paid. Ten licensees fix the same bug ten times. A transparent cage.
- **Bottom rung, gives then takes back:** open source rights with so many strings it is no longer open source. Llama: past 700 million users, ask Meta.

Source available, then the fork

Terraform, Aug 2023

Goes source available.

Forked within weeks. OpenTofu now lives at the Linux Foundation.

Elasticsearch, 2021

OpenSearch within months.

Elastic added an open source licence back in 2024.

Redis, Mar 2024

Forked as Valkey almost immediately.

Back under an open source licence by May 2025.

The pattern

Open to build the community. Close to cash it in. The community forks.

The community was the asset all along.

Open source today: KMIP Tiny SDKs

Not the vendor you cannot leave. The one you do not need to ask.

13.10.2026

- Cryptsoft's KMIP Tiny SDKs provide a lightweight implementation of the KMIP protocol suitable for embedded and resource-constrained environments.
- Designed for IoT devices, embedded systems, and applications where a full KMIP SDK may not be appropriate, the KMIP Tiny SDKs provide essential KMIP operations with a minimal footprint.
- **Seven languages:** JavaScript, C, Go, Ruby, Python, Perl and Delphi.
- **Already conformant:** tested against the standard and interop proven.
- **Open source, not source available:** Apache 2.0, the proven path OpenSSL has taken.
- **Early access this week:** public later this month. Come to the Cryptsoft booth.

OpenSSL CONFERENCE

03 Door two: open standards

The same word, open, counterfeited a second way. Two stories, two more announcements.

OpenSSL
CONFERENCE

How a captured standard survives

Non-interoperability is a business model.

13.10.2026

- PKCS#11 parked in 2004. Vendor-defined mechanisms, proprietary header files, magic attributes. The words stayed open. The interface quietly closed.
- **Regulated herding:** examiners benchmark every bank against its peers, so nobody is punished for buying what everyone else bought.
- **Buyers cannot see under the label:** ask a vendor and they say they are excellent. The market runs on reputation instead of inspection.
- **The brand is the only witness:** the only one telling you that they are conformant.

Out of the building, and still not adopted

Tim's Mother Teresa moment

PKCS#11 carried out of RSA and into OASIS.

A technical committee anyone can join and everyone can watch.

A standard, handed to everybody.

Standardised PKCS#11 is available. Today.

Vendor sludge pulled out, extension by extension.

ML-KEM and ML-DSA in the standard itself.

They are just PKCS#11.

Available is not adopted

Applications keep calling the proprietary paths.

Nobody wants to be first to rewrite.

The lock changed shape. It did not go away.

PKCS#11 interop: no lies, no veils

Bring your implementation, run the suite, publish what passes.

13.10.2026

- Run the way KMIP has run it for well over a decade. Verifiable interop.
- **Customers, demand it:** pure, standardised PKCS#11 conformance in the RFP. No vendor-defined mechanisms on the critical path. You hold the pen.
- **Vendors, come and prove it:** bring your device, run the tests, show your work. The standard kills your moat, not your product.
- **The empty chair is a disclosure:** everyone can see who turned up, and who did not.

cloudhsm.com: conformant, you are on the shelf

Registered in 2012

Before the name got famous.

That tells you how long we have been waiting to do this.

One entry requirement

Pass the interop tests.

Conformant, you are on the shelf. Not conformant, you are not.

Being open is how vendors win

For the first time in twenty years.

The only way to keep a customer is to deserve them.

Performance beats profit

On that shelf, the only thing that sells a device is passing the test.

OpenSSL CONFERENCE

KMIP: open standard, closed on-ramp

Told partly against ourselves.

13.10.2026

- We built the community and ran the interop. We trusted the industry to seed the client market; a lot of it pushed proprietary protocols instead.
- **First step, the KMIP Tiny SDKs:** seven languages, already conformant and interop tested. The conformance comes with the code.
- **Under consideration, the full KMIP client SDKs:** C, C++, C#, Java and Python, under the same Apache 2.0 licence.
- **Free to use, supported when you need it:** if you need a name on a support contract, that name is Cryptsoft.

Post-quantum is a once-in-a-generation exit

OpenSSL CONFERENCE

Every key, every certificate, every HSM

The NIST algorithms are standardised; the deprecation dates are in writing.

If you have to re-key anyway, the cost of leaving just fell to almost nothing.

For the first time in twenty years, everyone gets to choose again.

Choose well

A vendor who is actually innovating.

Committed to pure PKCS#11 and conformant KMIP, proven at the interop table.

One who trusts their product enough not to lock you in.

FUD minus the D

This industry has run on fear, uncertainty and doubt forever.

Testable, post-quantum PKCS#11 and conformant KMIP just removed the doubt.

Every engineer in this room knows what is left.

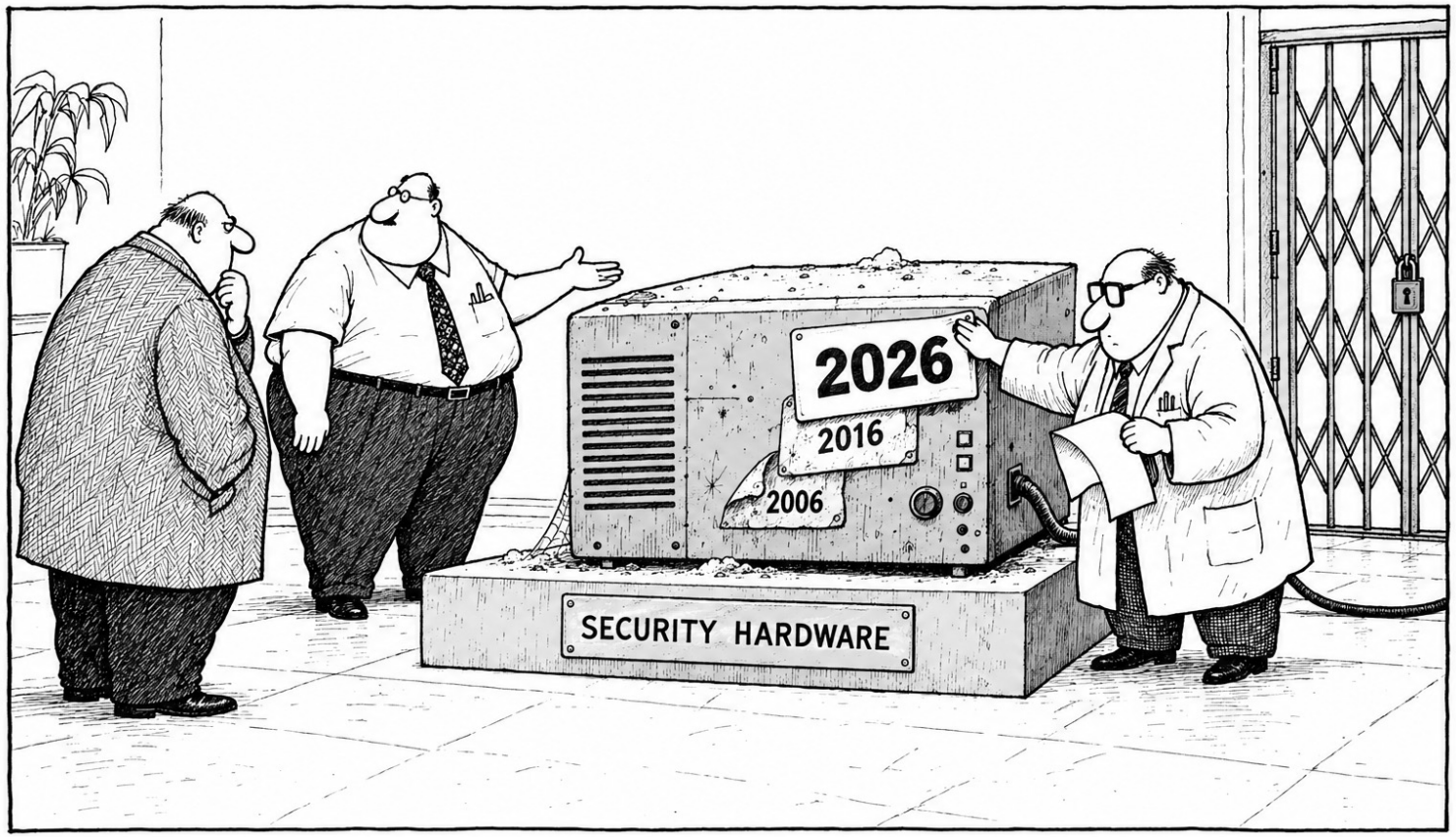
OpenSSL CONFERENCE

04 Door three, welded shut

Open to do it yourself. First, what it cost to have the door shut.

Room for one more sticker

OpenSSL CONFERENCE



"R&D says there's room for one more sticker."

We used to be a hardware company

2007. The need existed. The path did not.

- **We set out to build an HSM.** To build it we needed an authentication device.
- **No vendor would supply one.** Not on the embedded platform we had chosen. Nobody was interested.
- **So we built a token.** Which meant learning hardware engineering, losing Tim's button, and learning capacitance touch instead.
- **Then the last wall: a million units.** A global sales team, or external investment.
- **Game over.** We were ahead of everybody, and we did not launch.

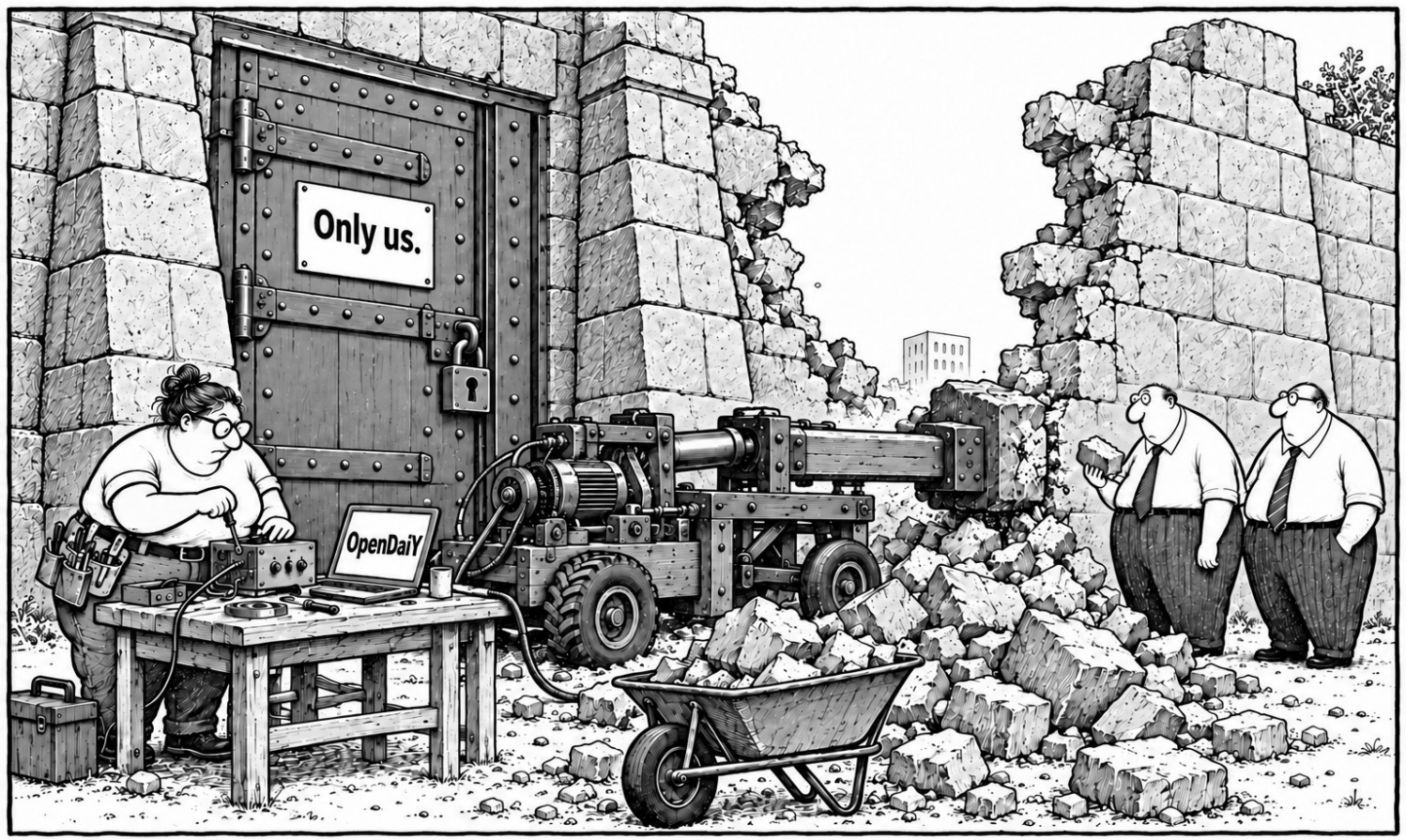
OpenSSL CONFERENCE

05 Door three, kicked open

How a dozen people attack a market this size.

We said they couldn't come in

OpenSSL CONFERENCE



"We said they couldn't come in."

The method

OpenSSL CONFERENCE

- **1. Find the empty layer.** The incumbents' moat is almost never where you think: certification, the channel, the brand.
- **2. Build it on open standards.** So nobody is locked in, including us.
- **3. Prototype with AI and cheap hardware.** Working on the bench in weeks, not years.
- **4. Open the building blocks.** So adoption does not wait for a purchase order.
- **5. Say out loud what you are not.** Not certified. Not a secure element. A prototype. Every time.

Markets with no open door

Smart cards

USD 15 bn, 8 bn cards a year.

jcpico: a post-quantum signature in under a minute against 6+ on a certified card. Not a secure element.

Source: Grand View Research, 2024.

Security keys

Authentication USD 1.5 to 3 bn; 5 bn passkeys in use.

csfido: hybrid ECDSA plus ML-DSA in unmodified browsers. Not certified.

Source: QYResearch, Vantage.

HSMs

USD 1.2 bn (2023) to 2.3 bn (2028). Certification is the moat.

CATE, the Cryptsoft Air-gapped Trust Enclosure: a prototype.

Source: MarketsandMarkets.

Authorisation

Palo Alto paid about USD 25 bn for CyberArk.

Approvals and the PQC Pager: post-quantum signed, even with no internet.

Source: SEC 8-K.

The rest of the pattern

- **Entropy:** hardware RNG USD 3.8 to 7.7 bn. Nobody can size the quantum slice honestly. Every FIPS 140-3 module needs validated entropy: qrngBridge.
- **IoT security:** USD 6 to 46 bn, a factor of seven between analysts. A mood, not a measurement. Every device needs keys: the KMIP Tiny SDKs.
- **The pieces underneath:** TLS 1.3 with post-quantum key exchange in 98 KB; ML-DSA in 7 to 26 KB; a FIDO2 toolkit; SSH and a shell on a Pico.
- **Key management:** USD 2.4 bn. A console that manages other vendors' key servers.
- **Tape:** USD 8.5 bn. A controller that makes a tape library robot carry cartridges full of keys.
- **The calendar:** FIPS 140-2 historical 21 Sep 2026. CNSA 2.0 from 1 Jan 2027. EU CRA in full Dec 2027.
- All of it at the Cryptsoft booth.

OpenSSL CONFERENCE

06 Naming it

The whole revolution is one letter.

OpenSSL
CONFERENCE

Open source. Open standards. Open to DaiY

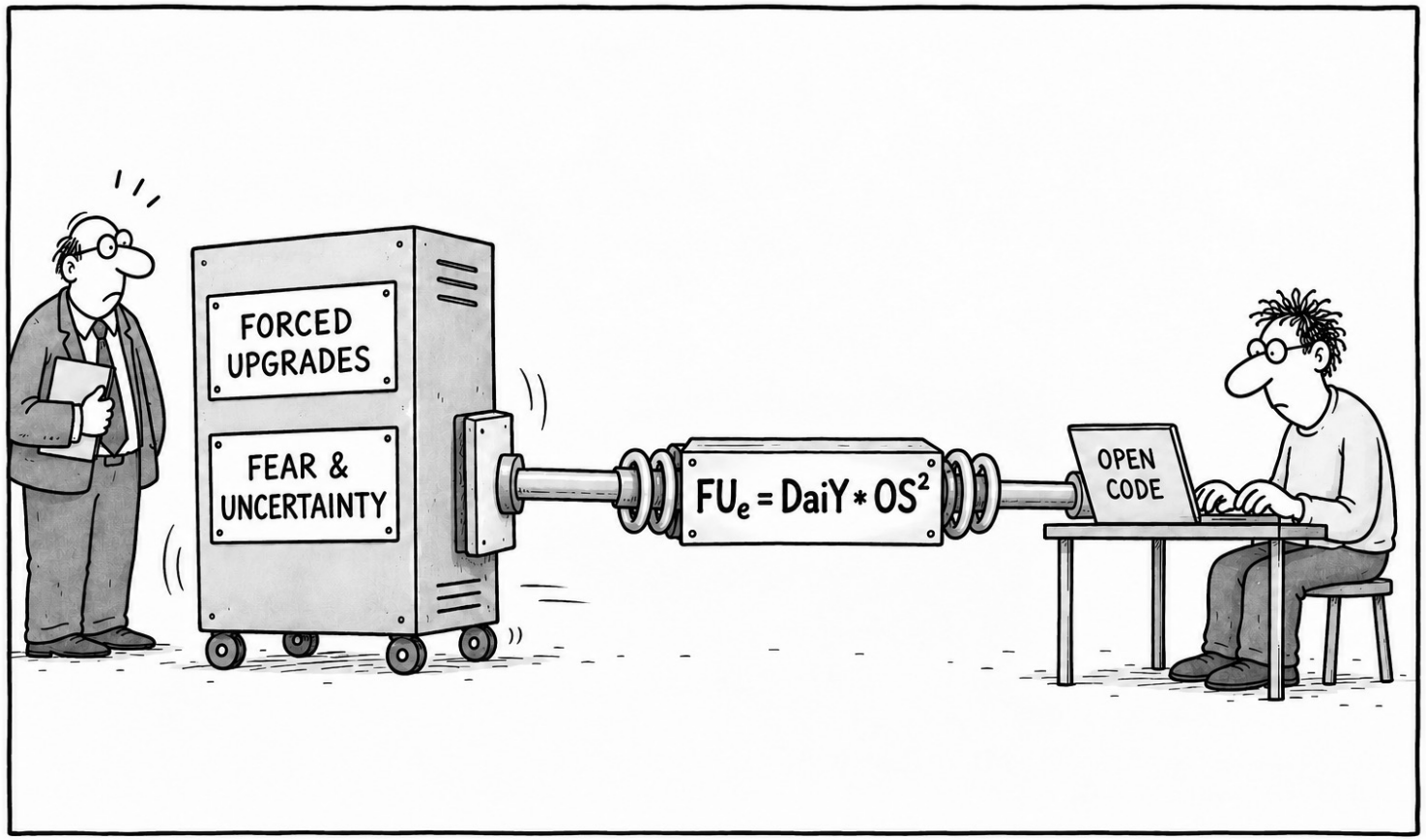
Stack the three and you get the word. DIY was the novelty. This is the Křižík Effect, arriving in hardware.

13.10.2026

- **Open to DaiY:** do it, with AI, yourself. Open manufacturing, open design, AI where your missing skills used to be. The new one.
- **Open standards:** KMIP and PKCS#11, interfaces nobody owns and everybody can implement. Thirty years in the making.
- **Open source:** code anyone can read, fix and fork, with a community around it. Thirty years in the making.

No alternative

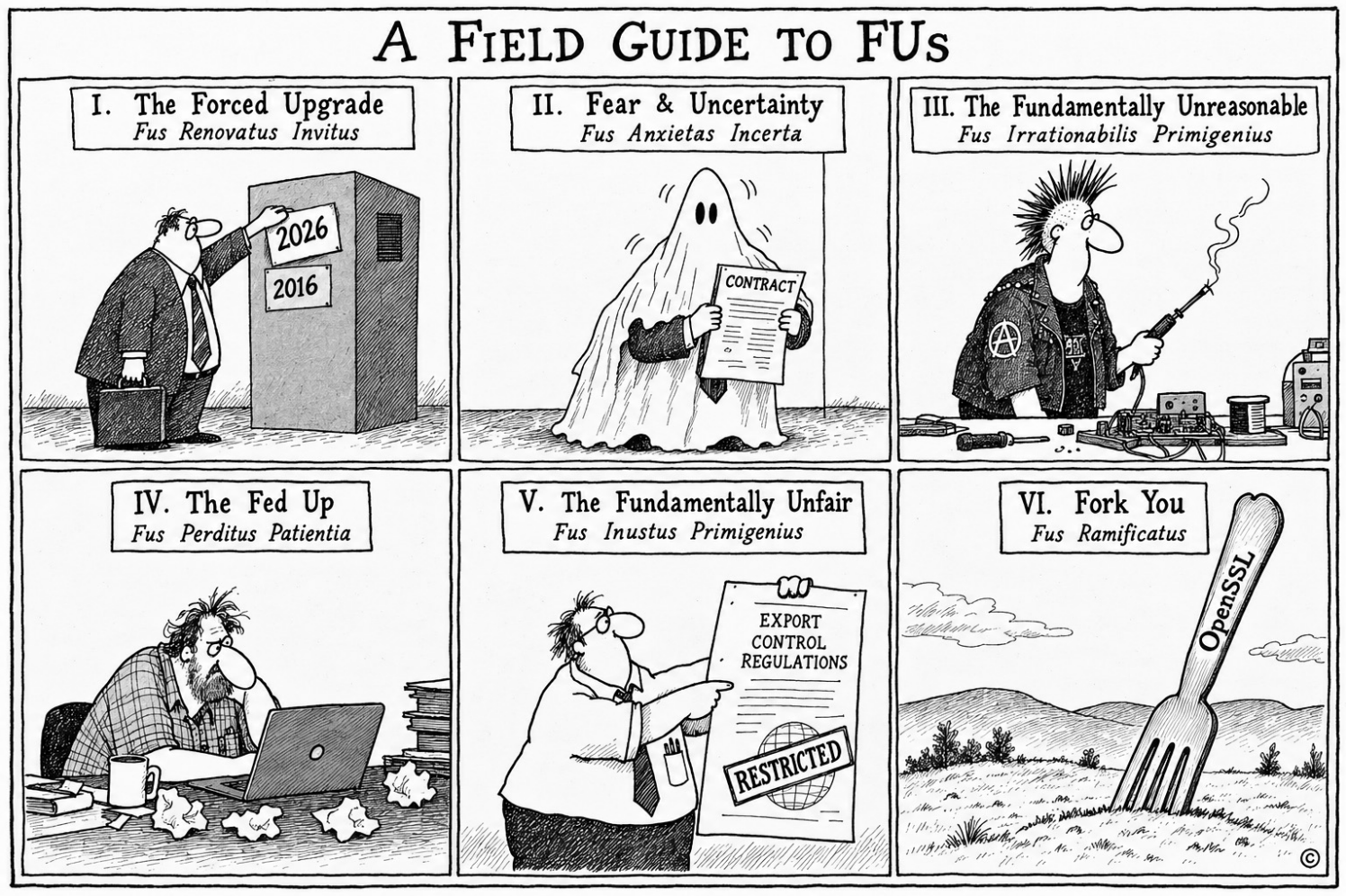
OpenSSL CONFERENCE



"We told them they had no alternative."

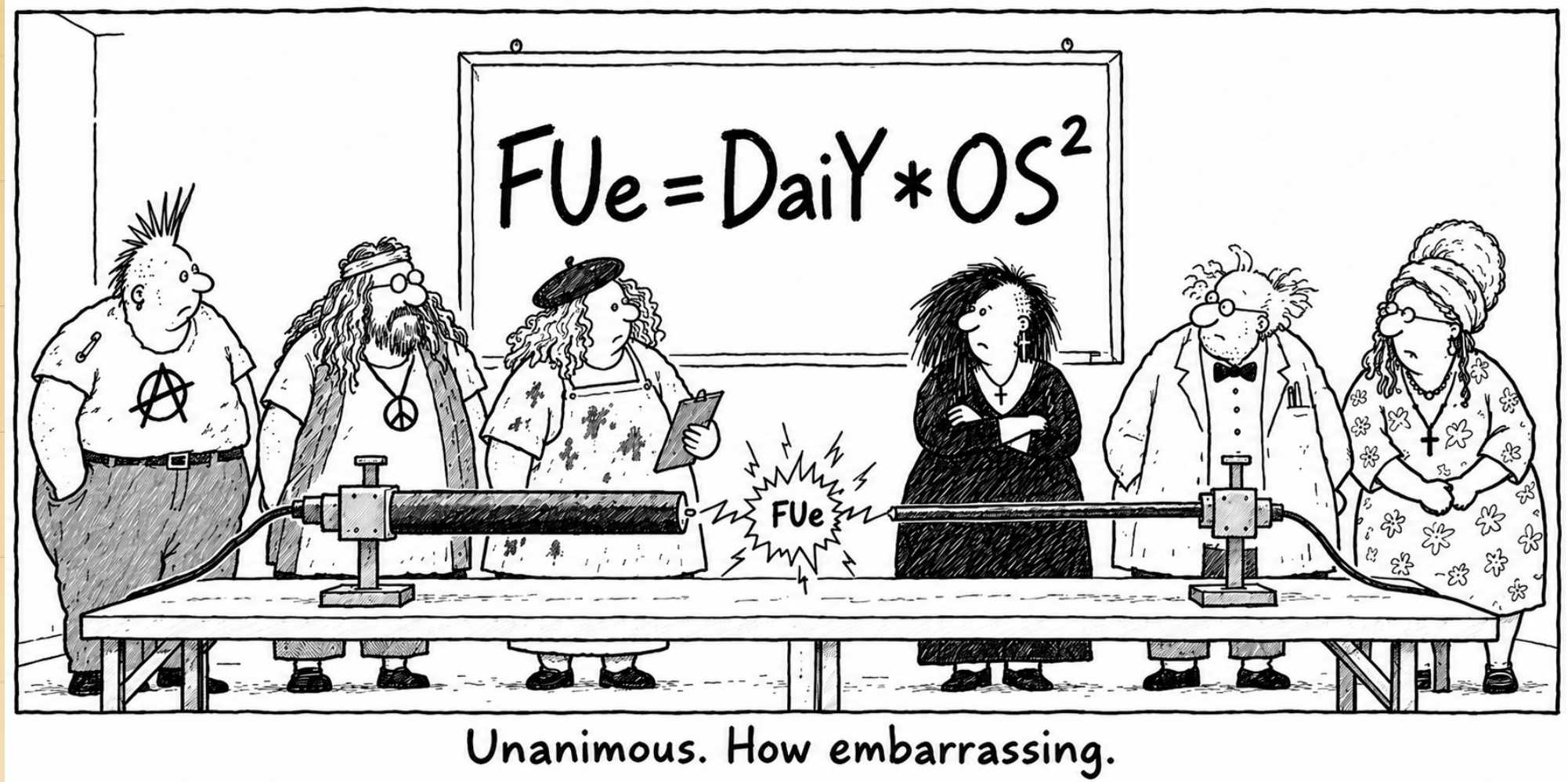
Know your FUs

OpenSSL CONFERENCE



$FU_e = DaiY \cdot OS^2$

OpenSSL CONFERENCE



OpenSSL CONFERENCE

07 The cogs

Not our products. The pieces inside them.

Take the cogs

We built the pieces. You build the things.

13.10.2026

- Our device needed about five cogs that did not exist. We took an existing open source TLS stack, found where the teeth were missing, and machined them: hybrid post-quantum support and validation. The improvements go back into the open.
- **The mini TLS stack:** hybrid post-quantum, mutually authenticated, into a Pico-2-class token. Take it.
- **Take all five:** rearrange them into something we would never think of.
- **AI makes you fast. Testing makes you right:** move fast and make things, then test them.

One more wall, this one incoming

Cyber Resilience Act

Obligations on the manufacturer: secure by default, a bill of materials, vulnerability handling, a CE mark.

Reporting live since 11 Sep: 24 hours for an exploited vulnerability.

Full application December 2027.

Product Liability Directive

Software is a product in law.

Strict liability for the harm a defect causes, components included.

A no-warranty disclaimer no longer protects you.

The direction of travel

Open source outside a commercial activity sits outside both laws.

Do not pre-declare what you are before you have to.

Inspectable building blocks stop being a philosophy and become a defence.

No. You are.

It just finally got out of your way.

- Somebody has to jump the gap, and somebody has to keep it lit. Do both.

OpenSSL
CONFERENCE

$FU_e = DaiY \cdot OS^2$

Early access at the Cryptsoft booth · KMIP Tiny SDKs · PKCS#11 interop · cloudhsm.com

§ PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

13.10.2026