Open by Design: Why Cramium Open-Source Entire Security Stack

"A secure system must not require secrecy and should not cause any inconvenience if its design falls into the hands of the enemy."

— Auguste Kerckhoffs, 1883

At CrossBar, we believe digital trust isn't built through secrecy — it's earned through transparency, collaboration, and cryptographic verifiability. That's the missions we hold on to day one of building **Cramium product lines**. In a world where self-custody, digital identity, and decentralized value are reshaping ownership, relying on black-box security models has proven not only outdated — but dangerous.

The Close-Source Failures

We've seen the consequences when consumers are forced to "just trust" proprietary systems in the crypto world. In one case, a popular hardware wallet provider introduced a remote recovery feature that revealed the device firmware could be silently updated to access private keys — despite years of assurance that such access wasn't possible. The backlash wasn't just about the feature itself, but about the revelation that the trust model had been broken all along. Without open-source verification, users were left exposed to capabilities they never consented to.

Even deeper in the stack, vulnerabilities have been discovered in closed, undocumented firmware embedded in widely used processors — invisible systems with privileged access to everything on a device. These backdoors, undisclosed and unauditable, have become high-value targets for exploitation, compromising billions of devices before fixes could even be issued. The root cause? A lack of transparency and community oversight.

These failures all point to the same truth: **security that cannot be independently verified is not security at all**.

CrossBar's Open-Source Mission

That's why CrossBar team has embedded this principle and taken the unprecedented step of open-sourcing **Cramium's entire security stack.** We are proud to be among the **first in the world to open source all three layers of secure custody infrastructure**:

- Our **cryptographic software stack** (SDK and MPC protocols)
- Our **portable hardware security module (Cramium PHSM)**
- And even our **secure silicon chip (Cramium Daric SPU)**

This isn't just about code. It's about trust that you don't have to ask for — because it can be **proven.** It's also CrossBar team's strategic engineering commitment to redefine trust architectures for decentralized systems. When securing digital sovereignty, verifiable security must replace blind faith. By inviting scrutiny instead of avoiding it, we're building a security model grounded in **open design, peer review, and zero trust assumptions**.

Cryptography Demands Openness

The cryptographic infrastructure that protects our digital lives doesn't rely on obscurity — it relies on transparent design and rigorous public scrutiny. In cryptography, openness isn't a liability; it's the foundation of trust.

The most widely trusted security technologies in the world are open by default — not because they're simple, but because they've proven secure under the harshest public examination:

- **AES, SHA-2, RSA, ECC** — Globally adopted cryptographic algorithms, all openly published and reviewed by decades of academic and industry research.
- **TLS, HTTPS, WireGuard, Signal** — Open-source protocols that secure the internet, messaging, and VPNs — battle-tested and constantly improved by a global community.
- **NIST Cryptography Standards** — Established through transparent, participatory processes involving researchers, governments, and the public.

This openness is not a weakness — **it's precisely what makes these systems resilient, interoperable, and trustworthy**. When cryptographic tools are closed off behind proprietary software, restricted firmware, or black-box silicon, users are forced into blind trust — a model that's incompatible with the stakes of digital asset custody and decentralized identity.

At **Cramium**, we've taken this principle further than anyone in the secure custody space — not just to the software and protocol layers, but down to the **firmware and silicon** that execute your most sensitive operations. Because **real security starts with full transparency** — and ends with trust you can verify.

MPC Especially Needs Open Source

Multi-Party Computation (MPC) is transforming the way digital assets are secured. By splitting a private key into multiple cryptographic shares distributed across devices or environments, MPC eliminates single points of failure and significantly raises the bar

against theft, loss, and insider threats. But with this power also comes complexity — and with complexity, **transparency becomes critical**.

Unlike traditional single-key models, MPC introduces multiple moving parts: distributed devices, communication protocols, threshold enforcement, and cryptographic coordination logic. Without full visibility into how those pieces work together, you're not securing assets — you're outsourcing trust to another black box.

With a fully open MPC stack, you don't have to guess how the system works — you can verify it yourself line by line:

- **Are key shares ever reconstructed?** Our open SDK and protocols make it provable: key shares are never recombined — not even temporarily.
- **Can a coordinator forge a signature?** The signing flow is fully transparent. Every message, every step, and every cryptographic check is out in the open.
- **Is T-of-N truly enforced?** Threshold logic isn't assumed — it's explicit and auditable in our codebase.
- **What if the coordinator is compromised?** You can self-host, modify, or fully replace the coordinator logic. No vendor lock-in, no hidden risks.
- **What if different parts of the system misbehave?** With our open infrastructure — mobile app, hardware authenticator, and backend — you can simulate and validate end-to-end behavior under any condition.

In short: **MPC must be verifiable to be trustworthy**. If you can't inspect how key shares are handled, how signatures are created, or how devices coordinate — then you're not truly in control. You're just trusting an invisible custodian with a more complicated name.

We've made every layer of our MPC infrastructure open — from the cryptographic math to the secure silicon — because real custody should come with real transparency.

Cramium EMPC SDK – Standardize MPC Engine & Crypto Tooling with Openness

In today's digital custody landscape, developers and wallet providers need more than just functionality — they need full transparency and absolute trust in the software that manages private keys and signing logic. We know that.

That's why Cramium's EMPC SDK is fully open source, line by line, and fully audited by top-tier auditing platform. When software is open and auditable, users and developers gain:

- Complete visibility into how keys are managed, and signatures are created, eliminating the risk of hidden backdoors or unintended behaviors.

- The freedom to customize and extend the software to meet unique security policies, regulatory requirements, or integration needs — without being locked into proprietary platforms.
- Confidence that no secret code can compromise custody — every cryptographic step can be inspected, tested, and verified by independent experts.
- A foundation built on collaboration and continuous improvement, where the community can contribute fixes and innovations, driving security forward together.
- Developers should never have to trust a black-box SDK with key management logic.

With Cramium EMPC, you get more than just code — you get verifiable custody infrastructure that puts control and trust back into your hands.

Cramium PHSM (Portable Hardware Secure Module) – Open Hardware Wallet

Cramium PHSM is a compact, ultra-secure hardware device designed specifically for on-device Multi-Party Computation (MPC), externally owned accounts (EOA) wallets, FIDO2 authentication, crypto payments, decentralized identifiers (DID), and much more. Powered by our custom **Cramium Daric SPU** chip, the PHSM runs fully **open-source firmware** — enabling you to **inspect, audit, and verify** every line of code and cryptographic flow.

As the world's first personal Hardware Security Module with a **native MPC architecture**, Cramium PHSM is purpose-built to deliver **transparent, decentralized custody** with unmatched security and flexibility.

With open-source PHSM, you can:

- **Audit the entire firmware stack** — No black boxes or hidden processes; complete visibility into how your device operates.
- **Verify the MPC signing flow all the way to the user interface** — Ensure your private keys never leave the device or get reconstructed.
- **Customize firmware for your specific needs** — Adapt security policies, threshold rules, or integrations for institutional-grade or retail applications.
- **Integrate seamlessly with multiple wallets and services** — Leverage open protocols for interoperability without vendor lock-in.
- **Validate device behavior under any scenario** — Simulate attacks or failures to ensure robust, predictable responses.

- **Participate in continuous security improvements** — Contribute or review updates from a growing community of developers and researchers.
- **Accelerate innovation in decentralized identity and crypto payments** — Build new features on a trusted, transparent platform.
- **Own your security end-to-end** — From silicon to app, with no hidden components or closed firmware layers.

With Cramium PHSM, you don't just get a hardware wallet — you get **a verifiable, customizable, and community-driven custody platform** that empowers you to take full control of your digital assets and identities.

Cramium Daric SPU - Built from Open-Source Silicon Up for Self-Custody

Most wallets today are powered by off-the-shelf components never meant for crypto custody. Generally-purpose microcontrollers (MCUs) lack physical security. Secure Elements (SEs) lack flexibility and power. Together, they offer a fragile foundation, full of architectural gaps and integration risks.

That's why we built the Cramium Daric SPU — a fully custom, purpose-built, and open secure processor designed specifically for decentralized custody, Multi-Party Computation (MPC), and user-controlled identity. It isn't a repurposed IoT chip or a recycled smartcard controller. It's a new category of silicon: a **Secure Processing Unit (SPU)** that fuses high-performance computing, advanced physical security, and blockchain-native cryptography — and we've open-sourced it for the world to inspect, verify, and build on.

But some may ask: why Aren't Off-the-Shelf Chips Enough? Our answer is that MCUs and SEs can dominate consumer hardware, but they were just not designed for the security needs of self-custody:

- **MCUs are flexible but insecure** — Lacking physical countermeasures, they're vulnerable to side-channel attacks, probing, tampering, and firmware injection.
- **SEs are secure but rigid** — Built for outdated use cases like SIMs and smartcards, they can't handle modern crypto curves (like secp256k1) or logic like MPC.
- **Combining them introduces new risks** — Communication between MCU and SE becomes a weak link, open to interception, spoofing, and supply chain exploits.

Most hardware wallets today are forced into this compromise — a two-chip setup that still exposes the private key to untrusted environments. Attackers know it. And they've exploited it — through supply chain tampering, firmware replacement, key extraction, and

display spoofing. So we believe **true security requires a new approach — from the chip level.**

What We Open Sourced at the Silicon Level

Every layer of Cramium Daric's architecture is transparent. You don't have to wonder or worry what's going on inside. You can inspect it directly. In fact, we've open-sourced the **RTL (Register Transfer Level)** logic of the SPU — the actual circuit-level design of how the chip works.

That means:

- You can **verify security claims independently** — no vendor trust required
- You can **build and simulate your own version** — perfect for high-assurance wallets or research
- You can **audit key paths from screen to silicon** — from user tap to signature emission
- You can **validate the chip's identity and integrity** — using our cryptographic attestation tools

Unlike traditional Secure Elements hidden behind licensing walls and proprietary constraints, Cramium Daric invites the community to inspect, validate, and extend the silicon itself.

Hardware-Rooted Zero Trust

Cramium Daric fuses cryptography, memory, lifecycle control, and user interface into a single secure silicon — establishing a true hardware-rooted Zero Trust foundation with no room for compromise.

- All critical components (crypto engine, memory, display controller) are protected under a **unified physical countermeasure mesh**
- Secure boot, attestation, and firmware signing flows are **enforced on-chip**
- Lifecycle controls and debug lockouts are handled atomically — **no off-chip dependencies**
- Tamper detection triggers automatic key wipes and system lockdowns
- On-chip cryptographic identity (serials, certificates, attestation keys) is embedded at factory — **verifiable by the end user**

This eliminates the MCU-SE handshake problem that plagues conventional wallets and enables an **end-to-end trust chain** from production to signing.

Our Unwavering Commitment towards Open Source

We're not just launching products — we're igniting a movement. One built on radical transparency, community trust, and the belief that real security should never hide behind NDAs or black boxes. At Cramium, open source isn't a marketing slogan — it's a principle.

By open sourcing our **software**, **hardware**, and **custom silicon**, we aim to:

- Lead the shift toward *accountable, community-reviewed security*
- Define the next-generation *MPC standard* with native **T-of-N** and **user-controlled custody**
- Deliver a *vertically integrated security stack* — from cryptographic algorithms to the device, down to the transistor level

As part of this mission, we are proud to be working alongside **Andrew "Bunnie" Huang** — one of the world's foremost hardware security experts. Bunnie is renowned for his work in open hardware, silicon reverse engineering, and supply chain transparency. His groundbreaking projects — from hacking the Xbox to co-authoring *The Hardware Hacker* and launching the secure and open-source laptop Novena — have made him a leading voice in the fight for user freedom and verifiable trust in computing. Together with Bunnie, we are building a platform that welcomes audits, encourages scrutiny, and earns trust — the hard way. You can see Bunnie's work with us in Bunnie's blog.

We invite developers, security researchers, hardware tinkerers, and open-source advocates to join us and form alliance. Whether you're interested in auditing our MPC designs, contributing to the codebase, or pushing the boundaries of what secure hardware can be provided, this is your invitation. Help us challenge the status quo, shape the standards, and build a verifiable future from the silicon up.

About Cramium

Cramium is the crypto security brand of **CrossBar, Inc.**, headquartered in **Santa Clara, California**. Combining cutting-edge silicon engineering with open-source transparency, Cramium delivers a vertically integrated security stack — from custom chips to hardware devices and cryptographic protocols- to help you secure your digital assets with the highest level of protection, without compromising usability. Cramium is committed to making self-custody secure, accessible, and verifiable — by design.