Zero-Knowledge Technology as a Foundation for Digital Sovereignty

Mike McCabe

0xbow · mike@0xbow.io

Abstract. The honeypot doctrine that underwrites contemporary digital infrastructure is no longer defensible against AI-assisted, nation-state-scale offence; data minimisation is therefore migrating from a GDPR principle to a matter of national security. Zero-knowledge proofs are the technology that makes this operationally tractable - prove the property a regulator needs without surrendering the dataset that makes you the next breach. The European Union has already conceded the architectural point: eIDAS 2.0 mandates ZK-enabled identity wallets by end-2026, with public reference implementations (EUDI Wallet, SWIYU). In parallel, the cryptocurrency industry has spent a decade building the experimental ZK frontier on which every nation-state rollout will stand. This workshop frames that landscape and grounds it in working code: in a single in-browser session, participants - including those with no cryptographic or programming background - generate and verify a complete ZK proof of an attribute claim, modelled on the EUDI Wallet's age-over-18 proof, before a short walkthrough of a deployed ZK privacy protocol shows how the primitives compose at production scale.

1 Topic Description

The 2026 Summer School asks whether regulation and innovation are catalysts or antagonists. The honeypot doctrine that underwrites most of today's digital infrastructure is no longer defensible. AI-assisted offence is now baseline, new zero-days are found and exploited faster than defenders can patch, and Q1 2026 alone produced strategic-scale breaches at the FBI's internal surveillance network, the European Commission's cloud, the Dutch Data Protection Authority, and a tier-one Dutch telecom. Centralised data stores have become strategic liabilities. The only durable response is not to collect what cannot be defended - which is to say, data minimisation has become a matter of national security, not merely a GDPR compliance principle.

Europe in particular faces a sovereignty trilemma. Escaping U.S.-headquartered hyperscalers leaves ~90% of EU digital infrastructure exposed to extraterritorial regimes (Schrems II, CLOUD Act, Chat Control). Replacing them with a European hyperscaler (Gaia-X, EuroStack) recreates the same target with worse economics. The third option - minimising the target by proving the property a regulator needs without surrendering the dataset that makes one the next breach - is the only realistic answer, and zero-knowledge proofs are the technology that makes it tractable.

The EU has already conceded the architectural point: eIDAS 2.0 requires member states to offer ZK-enabled wallets by the end of 2026; the EU Digital Identity Wallet's reference implementation ships an ICAO-compatible ZK age-proof library (`av_lib_android_zkp_age_icao`); Switzerland's SWIYU stack uses BBS+ signatures for selective disclosure; France's age-verification mandate is driving real adoption. In parallel, the crypto industry has been the experimental frontier - Zcash, Privacy Pools, Aztec, general-purpose proving systems (Polygon zkEVM, Starknet, RISC Zero, SP1), and ZK identity stacks (Rarimo, Self, Worldcoin) - such that every nation-state that adopts ZK in the coming decade will be standing on infrastructure that crypto built.

This workshop grounds these claims in working code. Participants will run a complete zero-knowledge proof end-to-end in their browser - the same conceptual core as the EUDI Wallet's age-over-18 proof - and walk away with an operational, rather than rhetorical, understanding of what ZK can and cannot do, what it costs, and where the open problems lie.

2 Expected Participants

The workshop is designed for the Summer School's interdisciplinary audience and assumes no cryptographic and no programming background. It will be most directly useful to:

- PhD students and junior researchers in privacy-enhancing technologies, applied cryptography, identity, or law-and-technology who want hands-on grounding in a working ZK system.
- Legal and policy scholars working on eIDAS II, GDPR, AML/CTF, or digital-sovereignty policy who want to see the technology that EU policy is increasingly assuming.
- Social scientists and HCI researchers concerned with usability, surveillance, and the sociotechnical conditions under which privacy-by-default is achievable.

Participants who wish to follow the hands-on segment should bring a laptop with a modern browser; no software installation is required. The notebook runs entirely in-browser (JavaScript-based proving system). Participants without a laptop can pair with a neighbour or follow on the projected screen - the exercise is designed so that observation alone conveys the substance.

3 Activities

The session is part lecture, part guided hands-on, part discussion. Planned structure (90 minutes):

- **0-30 min - Framing.** The honeypot doctrine and its collapse; data minimisation as national security; Europe's sovereignty trilemma; the EU's existing ZK commitments (eIDAS 2.0, EUDI Wallet, SWIYU, France); what a ZK proof is and what it can be applied to.
- **30-70 min - Guided hands-on: build and verify a ZK proof.** Participants run a pre-prepared in-browser notebook that mirrors the conceptual core of the EUDI Wallet age proof: prove possession of an attribute ("I am older than 18") without revealing the underlying value. The walkthrough covers the circuit, witness, proving key, proof, and verification, with participants modifying a witness value to observe what does and does not change. No coding required beyond editing a constant.
- **70-80 min - ZK Proofs in Practice.** A short walkthrough of a deployed ZK system (Privacy Pools v2 on the Sepolia testnet) showing how the same primitives compose into a compliant, regulator-engageable privacy protocol with proof-of-innocence rather than proof-of-guilt.
- **80-90 min - Discussion.** Open exchange seeded by a single question: which of the open problems in ZK for digital sovereignty are technical, which are legal, and which sit between? Targeted at drawing out the legal and policy participants in particular.

A two-page handout summarising ZK proofs, the EU policy receipts, and the open problems will be distributed at the start and used to anchor the closing discussion.

4 Duration

90 minutes, matching the Summer School's standard workshop slot.

5 Support Required

- **Reliable Wi-Fi for participants.** Essential for the hands-on segment. As a fallback, the workshop materials will be available as a single offline-cached page; the speaker will provide a short link distributed at the start of the session.

No specialised hardware, lab infrastructure, software pre-installation, or participant accounts are required. The workshop is self-contained.

6 Speaker

Mike McCabe leads product at 0xbow, the team building privacy and compliance tools including Privacy Pools (`github.com/0xbow-io`) and the Association Set Provider. The workshop is offered from a builder's perspective: the framing arguments are the ones used in industry forums (most recently EthCC and ETHPrague 2026); the hands-on material is original and prepared specifically for an interdisciplinary academic audience. Commercial framing is avoided in favour of the open technical, legal, and policy questions the work has surfaced.

References

1. Buterin, V., Illum, J., Nadler, M., Schär, F., Soleimani, A. *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium.* SSRN (2023).
2. European Commission. *EU Digital Identity Wallet - reference implementation, ZK age-proof library.* github.com/eu-digital-identity-wallet/av-lib-android-zkp-age-icao
3. Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0).