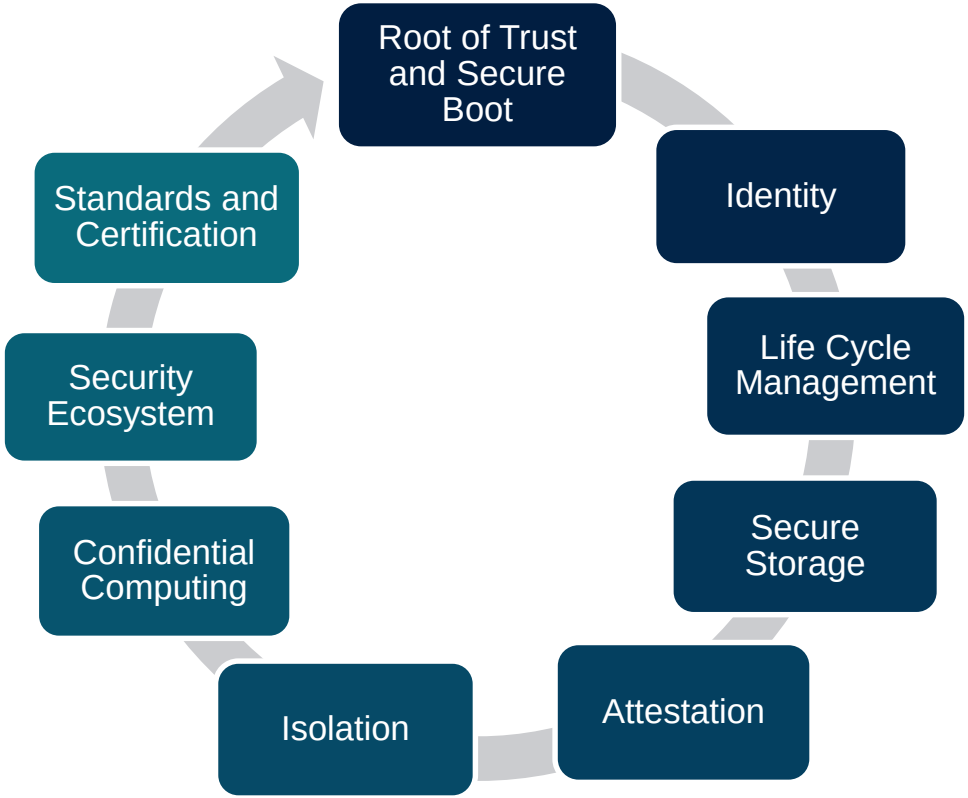
RISC-V Security

EU Summit 2023

Intrinsic Security

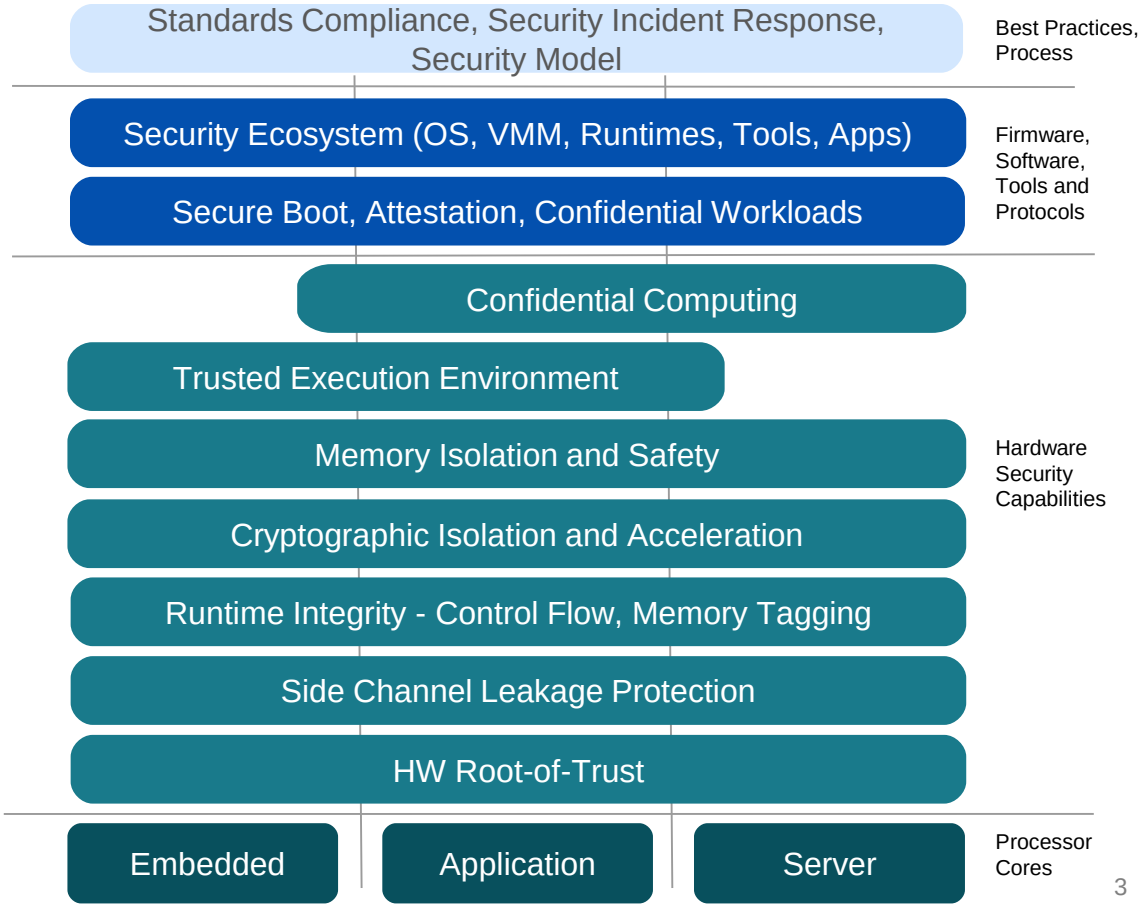
- Security as a basic feature of HW, SW Firmware
- Support security through entire lifecycle
- Published Guidelines matched to usage profiles



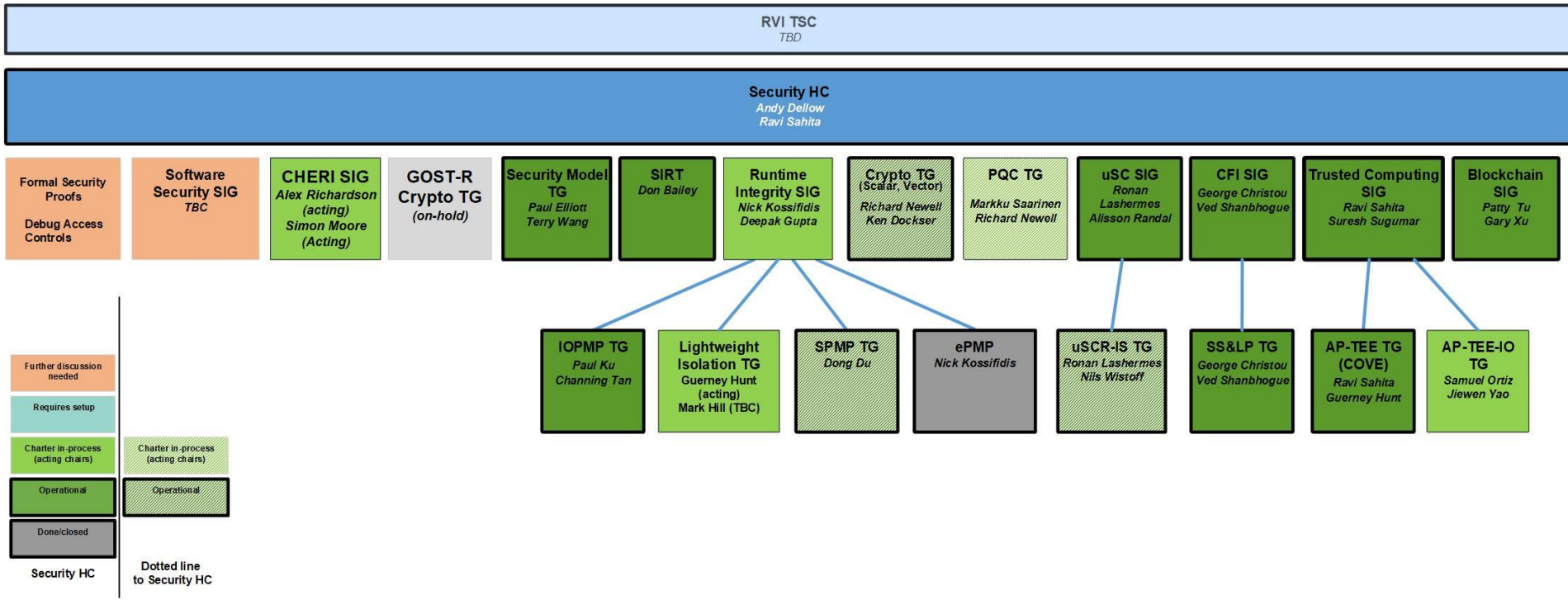
Security and RISC-V

RISC-V's open and clean-slate design presents a unique opportunity to ingrain security for the next generation of compute infrastructure.

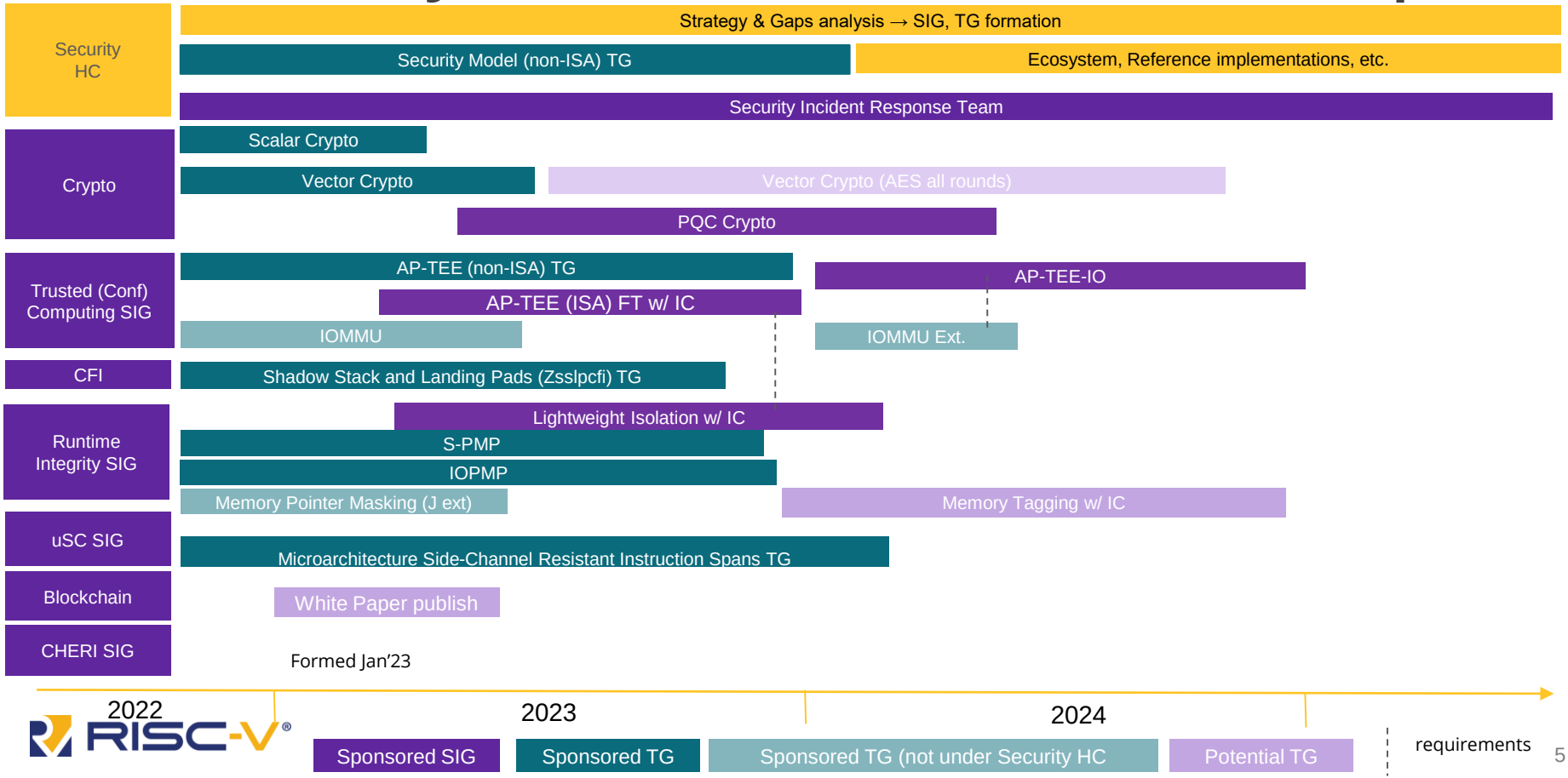
- Foundational Security and Cryptography
- Application & System Hardening against bugs/ exploits
- Trusted Execution & Confidential Computing
- Security Lifecycle



Security HC - Organization

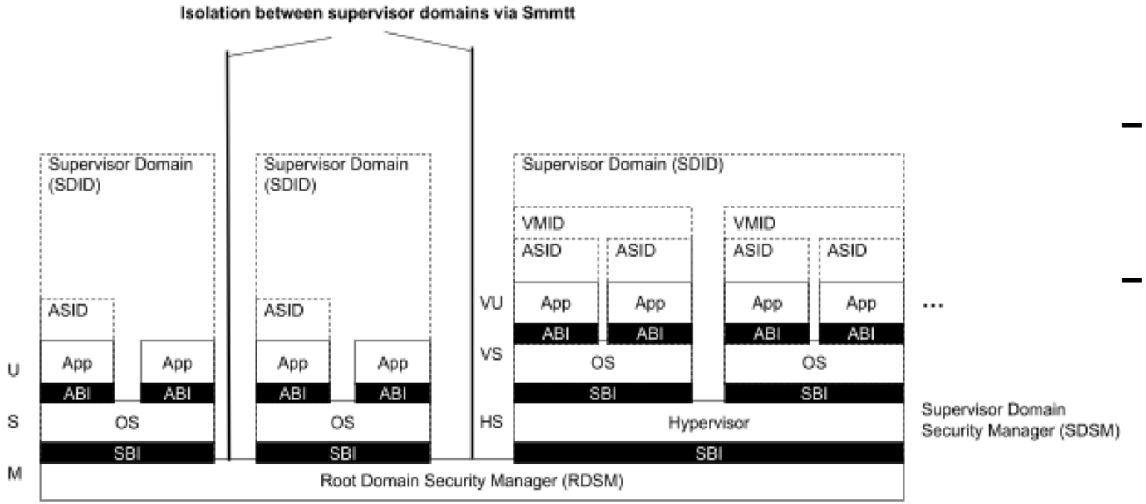


Security HC - Active Items & Roadmap



Trusted Computing

- AP-TEE TG
  - Interim release of Confidential VM Extension ABI
  - Open source TEE security manager
  - RFC Patches for Linux etc
  - SmMTT - Memory Tracking Table
  - AP-TEE IO TG spun up to manage trusted I/O devices



- Supervisor Domain is a set of physical Address regions isolated from other SDID
- Memory Tracking Table structure enforces access by SDID, under control of Root Domain Security Manager

Trusted Computing

- Embedded Isolation – LightWeight TEE
  - Collecting usecases and requirements
  - Direction is to deprivilege to S-Mode
    - (nearly) All CSR have S mode equivalent
    - RTOS etc can be run below m-mode
    - Small TCB security monitor at m-mode only
  - Looking at performance, interrupts, call-gates, ePMP/MTT usage

Crypto

- Scalar Crypto Complete
- Vector Crypto at or near Freeze
  - Inc AES and SHA2
  - Two additional instructions under consideration for fast track
- Post Quantum TG being set up
  - Dilithium and Kyber
- Full Round AES under consideration
  - SCA resistant implementations
  - Key management by privilege level

Runtime Integrity etc.

- Analysing TCB reduction, Various Exploit Reduction Mechanisms
- SiFive Donated Aspects of WorldGuard, under analysis

- IOPMP – progressing well
- CFI – SSLP progressing well
- uSCR-IS microarchitectural side channel resistant instruction spans progressing well

RISC-V Security 5 year horizon

- Platform Security Model outlining RISC-V security capacities and system's integration
- Tools and Software support for RISC-V security capabilities
- Protection against side-channel information leakage at the hardware level
- Robustness capabilities to prevent malicious manipulation of e.g., code execution flows
- Cryptography support for small to large devices, including Post-Quantum Crypto
- Memory isolation and Trusted Execution Environments to securely separate applications from each other across all workloads
- Support for Confidential Compute models to enhance application and data privacy
- Blockchain technology on RISC-V based systems