
RISC-V®
Security HC meeting
Feb 03, 2022

Only RISC-V Members May Attend

- Non-members are asked to please leave except for Joint Working Groups (JWG).
- Members share IP protection by virtue of their common membership agreement. Non-members being present jeopardizes that protection. Joint working groups (JWG) agree that any IP discussed or worked on is fully open source and unencumbered as per the policy.
- It is easy to become a member. Check out riscv.org/membership
- If you need work done between non-members or or other orgs and RISC-V, please use a joint working group (JWG).
  - used to allow non-members in SIGs but the SIGs purpose has changed.
- Please put your name and company (in parens after your name) as your zoom name. If you are an individual member just use the word "individual" instead of company name.
- Non-member guests may present to the group but should only stay for the presentation. Guests should leave for any follow on discussions.

RISC-V®

Antitrust Policy Notice

RISC-V International meetings involve participation by industry competitors, and it is the intention of RISC-V International to conduct all its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at RISC-V International meetings and in connection with RISC-V International activities are described in the RISC-V International Regulations Article 7 available here: https://riscv.org/regulations/

If you have questions about these matters, please contact your company counsel.

RISC-V®

Collaborative & Welcoming Community

RISC-V is a free and open ISA enabling a new era of processor innovation through open standard collaboration. Born in academia and research, RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and innovation.

We are a transparent, collaborative community where all are welcomed, and all members are encouraged to participate. We are a continuous improvement organization. If you see something that can be improved, please tell us. help@riscv.org

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

https://riscv.org/community/community-code-of-conduct/

RISC-V®

Conventions

- Unless it is a scheduled agenda topic, we don't solve problems or detailed topics in most meetings unless specified in the agenda because we don't often have enough time to do so and it is more efficient to do so offline and/or in email. We identify items and send folks off to do the work and come back with solutions or proposals.
- If some policy, org, extension, etc. can be doing things in a better way, help us make it better. Do not change or not abide by the item unillaterly. Instead let's work together to make it better.
- Please conduct meetings that accommodates the virtual and broad geographical nature of our teams. This includes meeting times, repeating questions before you answer, at appropriate times polling attendees, guide people to interact in a way that has attendees taking turns speaking, …
- Where appropriate and possible, meeting minutes will be added as speaker notes within the slides for the Agenda

Risc-V Security

Agenda

- uArch Side Channel SIG - chair + vice chair announcements
- Configuration schema – discuss signature
- IOPMP TG - charter status & updates
- TG/SIG updates - Blockchain, CFI, Crypto (vector & international), TEE, Trusted Computing, SIRT
- Security Model - status & next steps

RISC-V®

Uarch Side Channel SIG

- Chair:-

Ronan Lashermes
Research Engineer @ Inria-Rennes / SED & LHS

- Vice Chair:-

< still open >

RISC-V

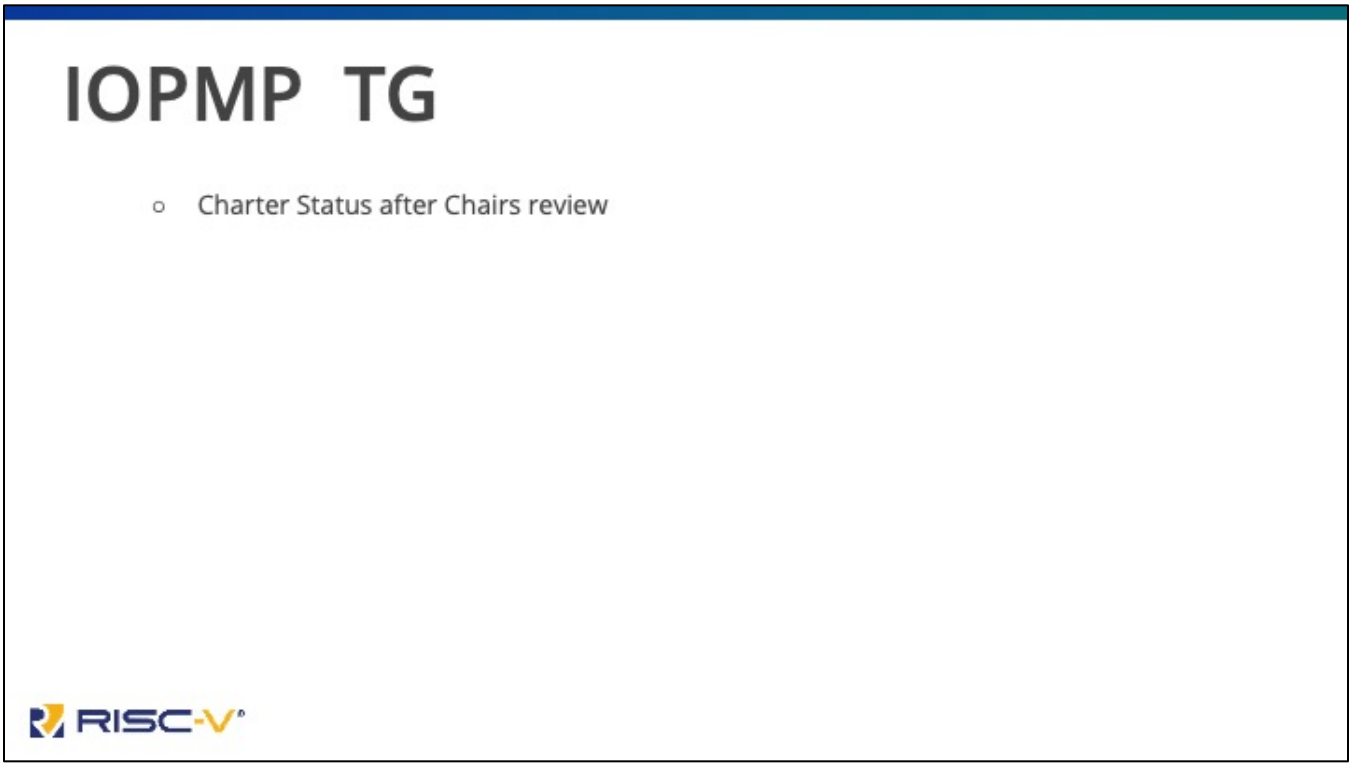
- Ronan is officially chair.
- Looking for a vice-chair.

Configuration Schema

- Plan is to use Cryptographic Message Syntax - RFC 5652
- Covers all options, allows arbitrary signed attributes
- Need recommendations for e2e usage
  - Chapter in Security model ?

RISC-V

- Current proposal is to use PKCS #7 (as defined in RFC 5652 “Cryptographic Message Syntax (CMS) “)
- Need to add recommendations for algo’s/properties/CA’s etc. to Security Model, potentially to Platform Spec where applicable



- Scope discussion: IOPMP stand-alone vs working in conjunction with IOMMU
- Need to come to convergence on scope
- Continue scope discussion on TSC reflector, while also scheduling a meeting to discuss in smaller setting (Stephano action item)

Russian Crypto

- Separate TG proposal, Alexander Kozlov to be acting chair
- Direct Line to UnPriv, Dotted to HC
- Ready to present charter to TSC

Proposed GOST-TG Charter

RISC-V International is committed to helping members succeed in specialized and regional markets where the flexibility of the RISC-V ISA offers a unique advantage in relation to cryptographic algorithm support and performance.

The focus of the GOST-R Crypto Extension TG (GOST-TG) is to investigate, evaluate, and specify ISA extensions for the implementation of Russian defined-symmetric cryptography. The main algorithms in scope are defined in GOST R 34.12-2015 ("Kuznyechik" and "Magma" block ciphers) and GOST R 34.11-2012 ("Streebog" cryptographic hash function). The goal of the extension is to both improve performance and also to reduce the risk of security vulnerabilities such as timing attacks in RISC-V cryptographic stacks. Quantitative analysis (e.g. modes of operation) is primarily based on use cases in IETF, ETSI, and 3GPP/5G security protocols and required platform security features. The TG may propose both stand-alone extensions and ones that work in conjunction with other extensions (such as vector, scalar cryptography, and bit manipulation).

NOTE. The initial algorithm selection rationale is from GOST / TLS 1.2 (https://www.ietf.org/id/draft-smyshlyaev-tls12-gost-suites-10.html) and GOST / TLS 1.3 (https://www.ietf.org/id/draft-smyshlyaev-tls13-gost-suites-05.html) which themselves correspond to ratified standard protocol specifications R 1323565.1.020-2020 and R 1323565.1.030-2020.

--- end charter proposal ---

RISC-V

- Next step: proposal to go to Chairs for approval.

Other Status Updates

- TEE TG – Nick
- Blockchain SIG - Patty
- Trusted Computing SIG - Suresh
- CFI SIG - George
- uArch SIG - Ronan
- Security Model – Suresh / Don ?

RISC-V

- Updates from Blockchain (initial draft whitepaper is out), TC SIG and Security Model.


RISC-V®
Open Action Items

Running list of open AI's

RISC-V®