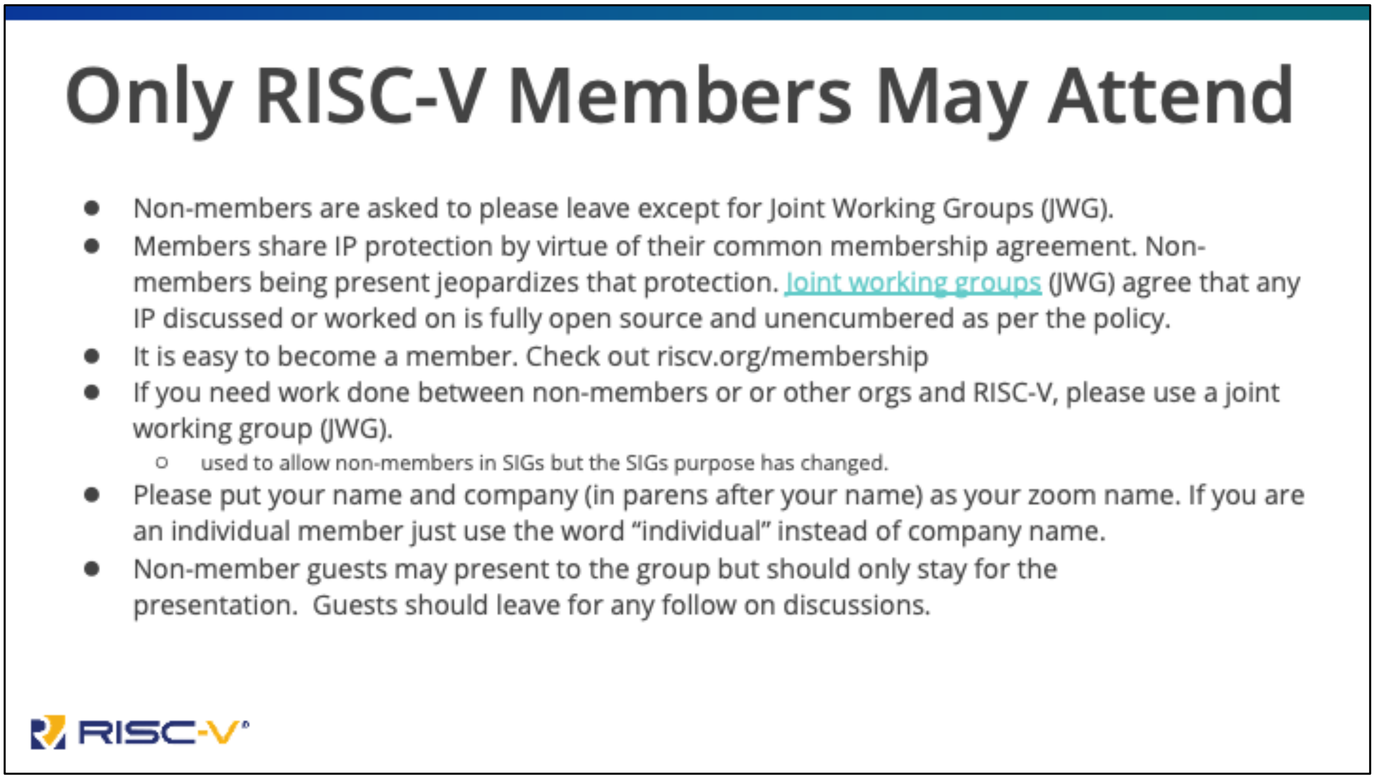
RISC-V®

Security HC meeting

September 1st, 2022



Only RISC-V Members May Attend

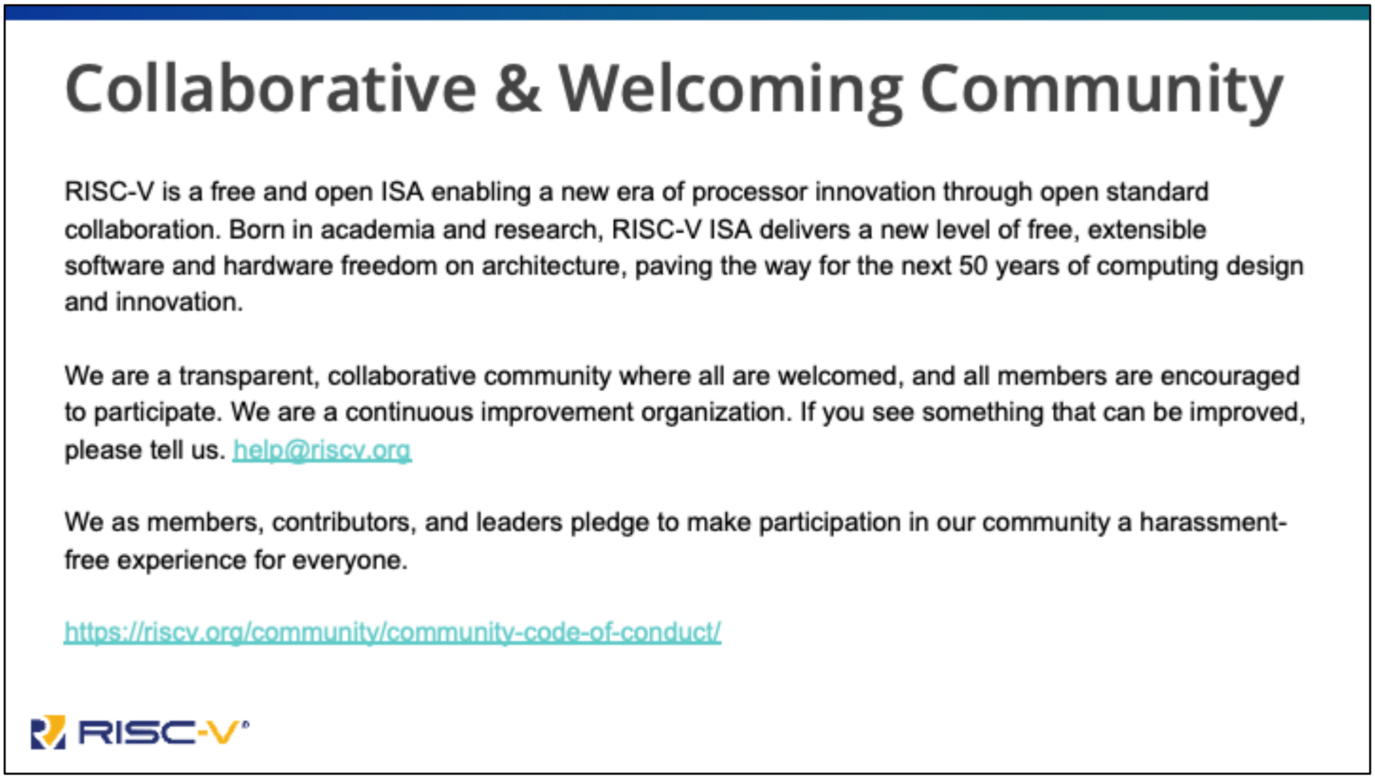
- Non-members are asked to please leave except for Joint Working Groups (JWG).
- Members share IP protection by virtue of their common membership agreement. Non-members being present jeopardizes that protection. Joint working groups (JWG) agree that any IP discussed or worked on is fully open source 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.

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.



Collaborative & Welcoming Community

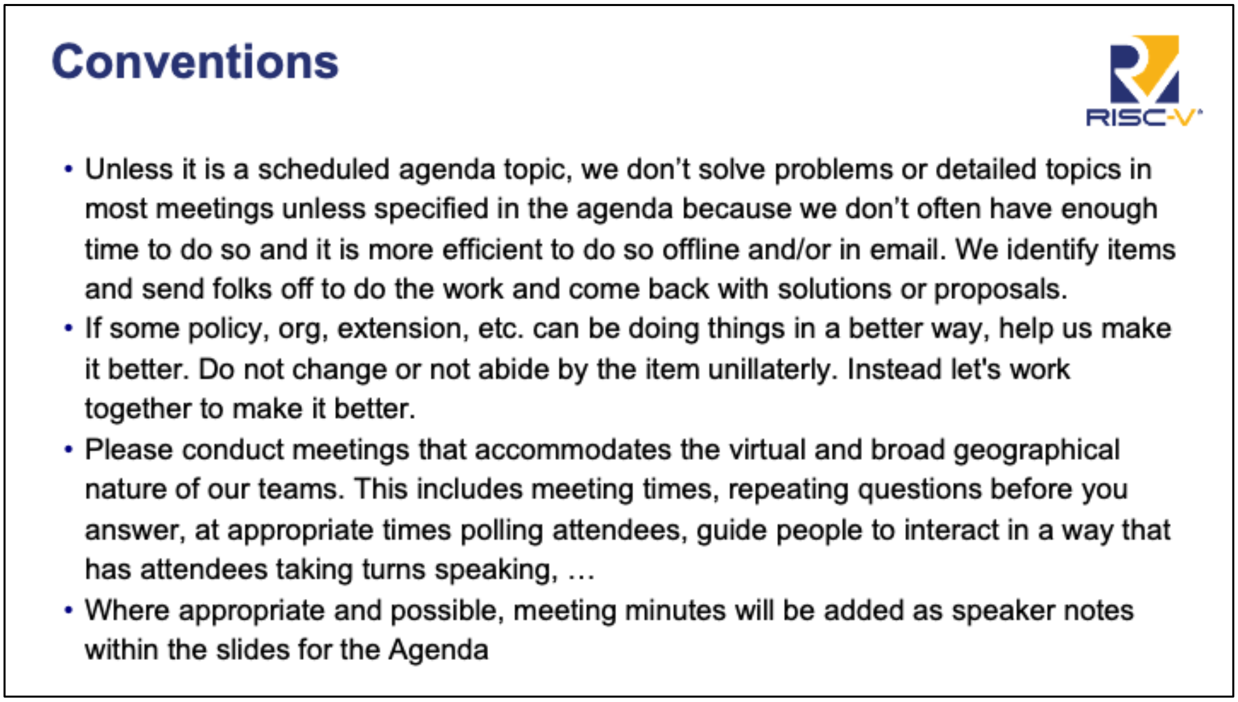
RISC-V is a free and open ISA enabling a new era of processor innovation through open standard collaboration. Born in academia and research, RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and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

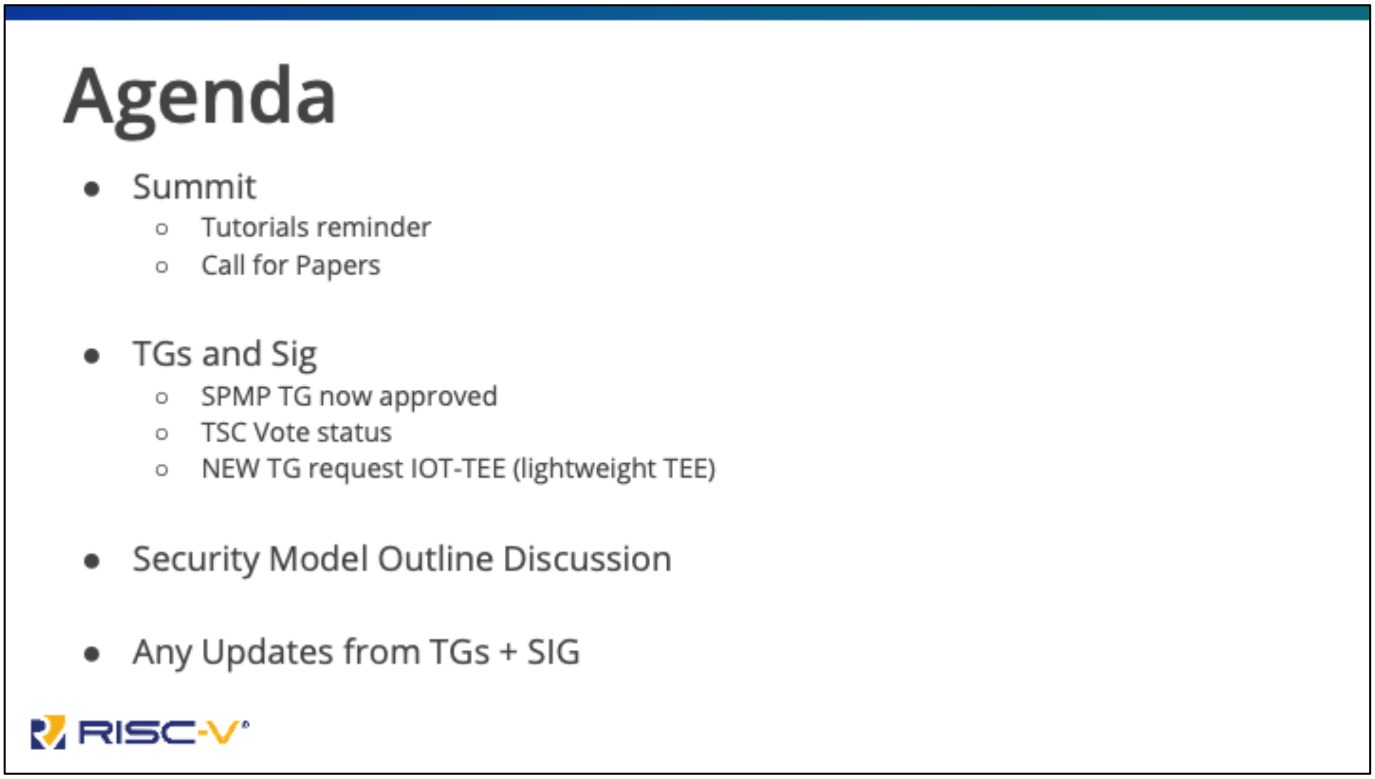


Conventions

- 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

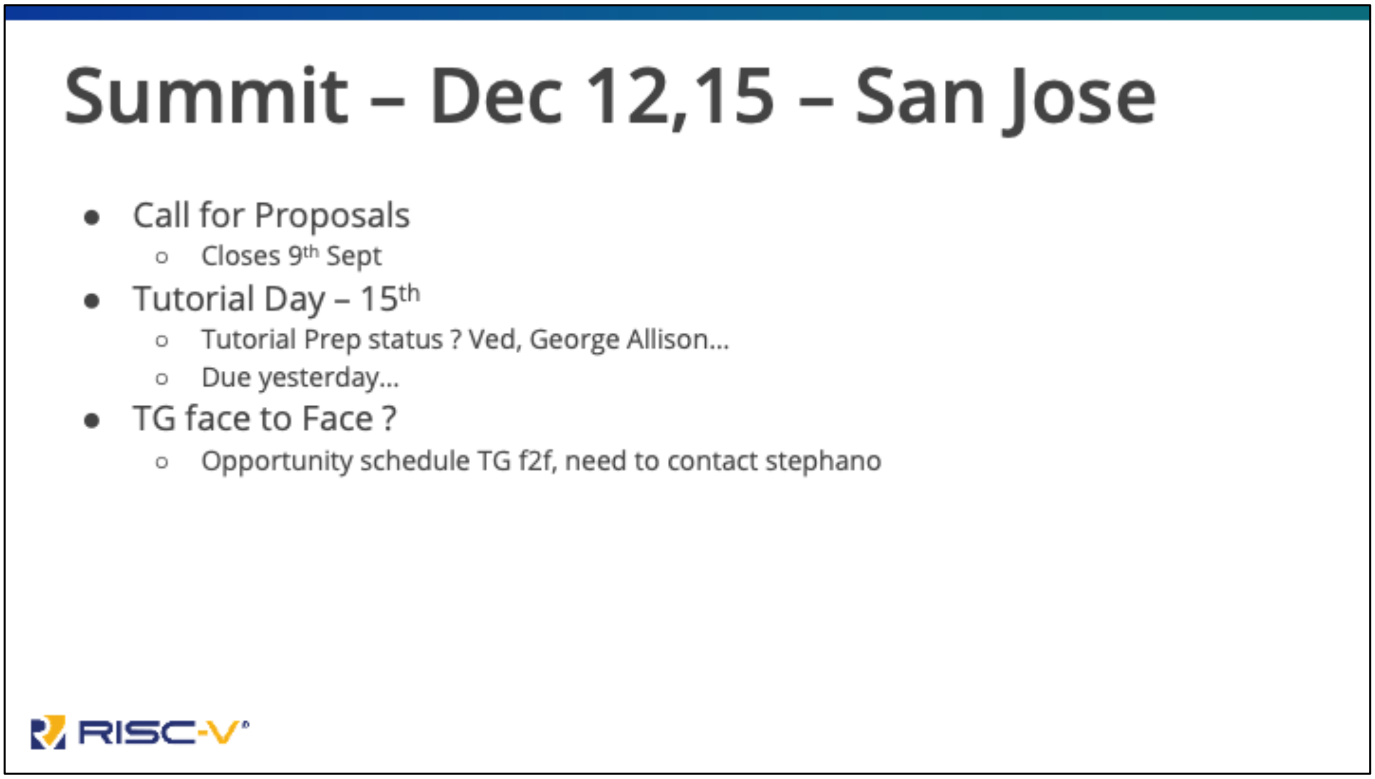
Risc-V Security

RISC-V



Agenda

- Summit
  - Tutorials reminder
  - Call for Papers
- TGs and Sig
  - SPMP TG now approved
  - TSC Vote status
  - NEW TG request IOT-TEE (lightweight TEE)
- Security Model Outline Discussion
- Any Updates from TGs + SIG

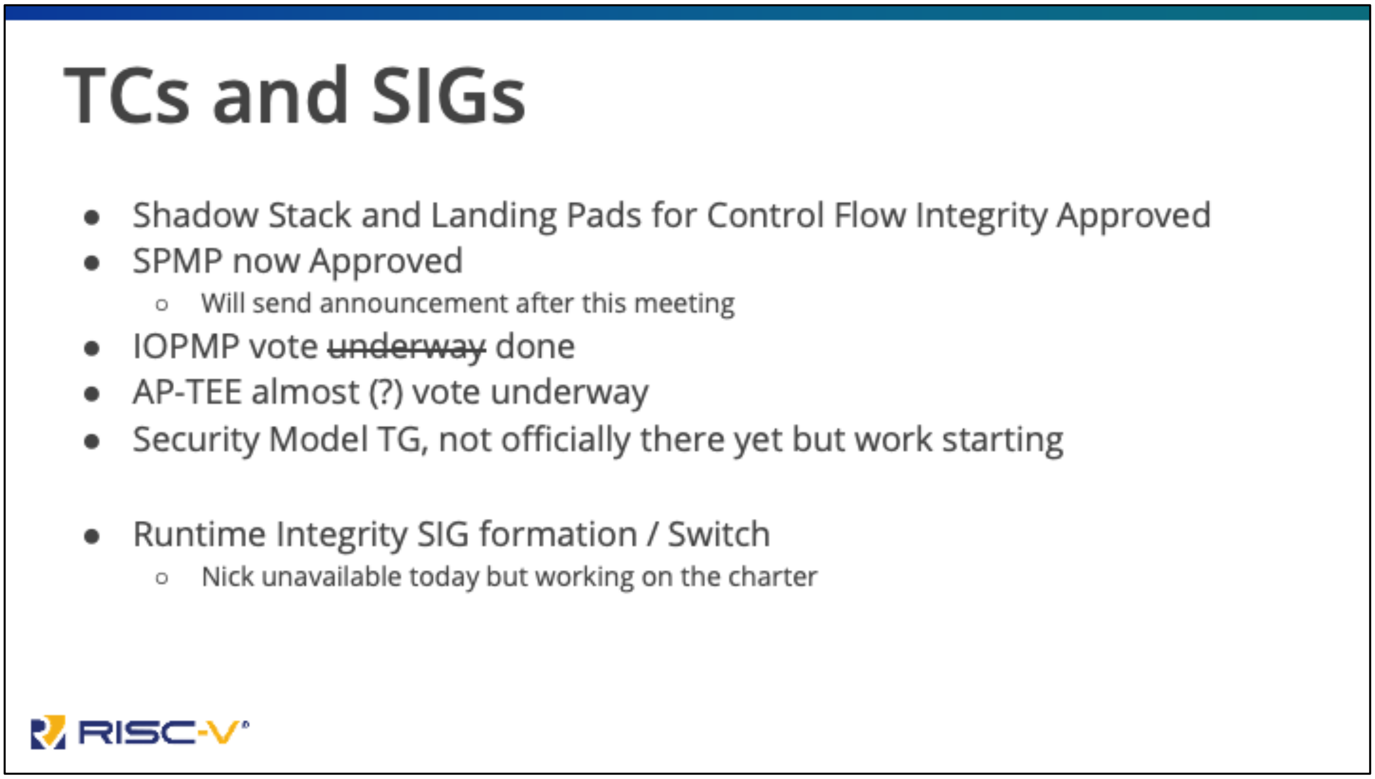


Summit – Dec 12,15 – San Jose

- Call for Proposals
  - Closes 9th Sept
- Tutorial Day – 15th
  - Tutorial Prep status ? Ved, George Allison…
  - Due yesterday…
- TG face to Face ?
  - Opportunity schedule TG f2f, need to contact stephano

Summit:

- Your are allowed to submit multiple proposals for talks.
- Tutorial: we have speakers. Need to submit outline ASAP, material not due until later
- Meeting room for Security F2F – Manuel to contact Stephano (done)

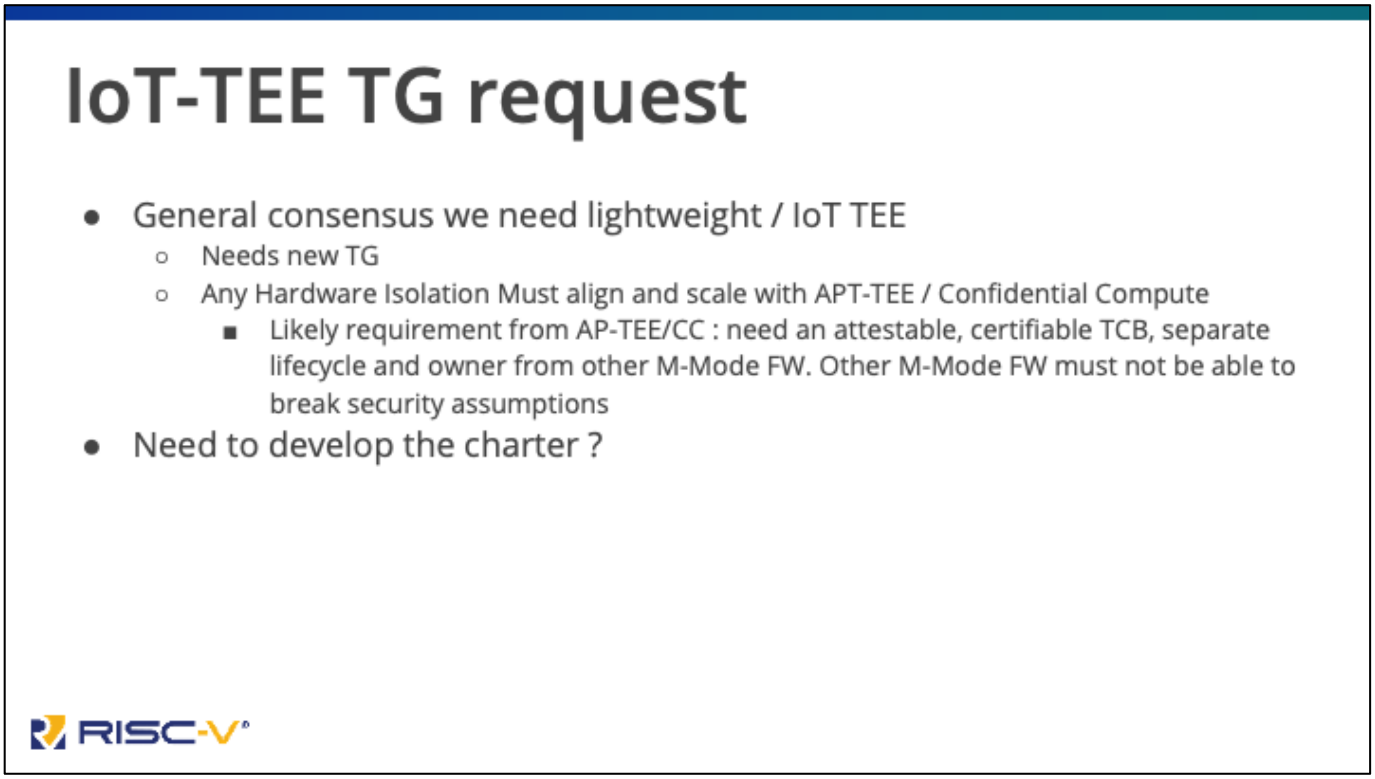


TCs and SIGs

- Shadow Stack and Landing Pads for Control Flow Integrity Approved
- SPMP now Approved
  - Will send announcement after this meeting
- IOPMP vote ~~underway~~ done
- AP-TEE almost (?) vote underway
- Security Model TG, not officially there yet but work starting

- Runtime Integrity SIG formation / Switch
  - Nick unavailable today but working on the charter

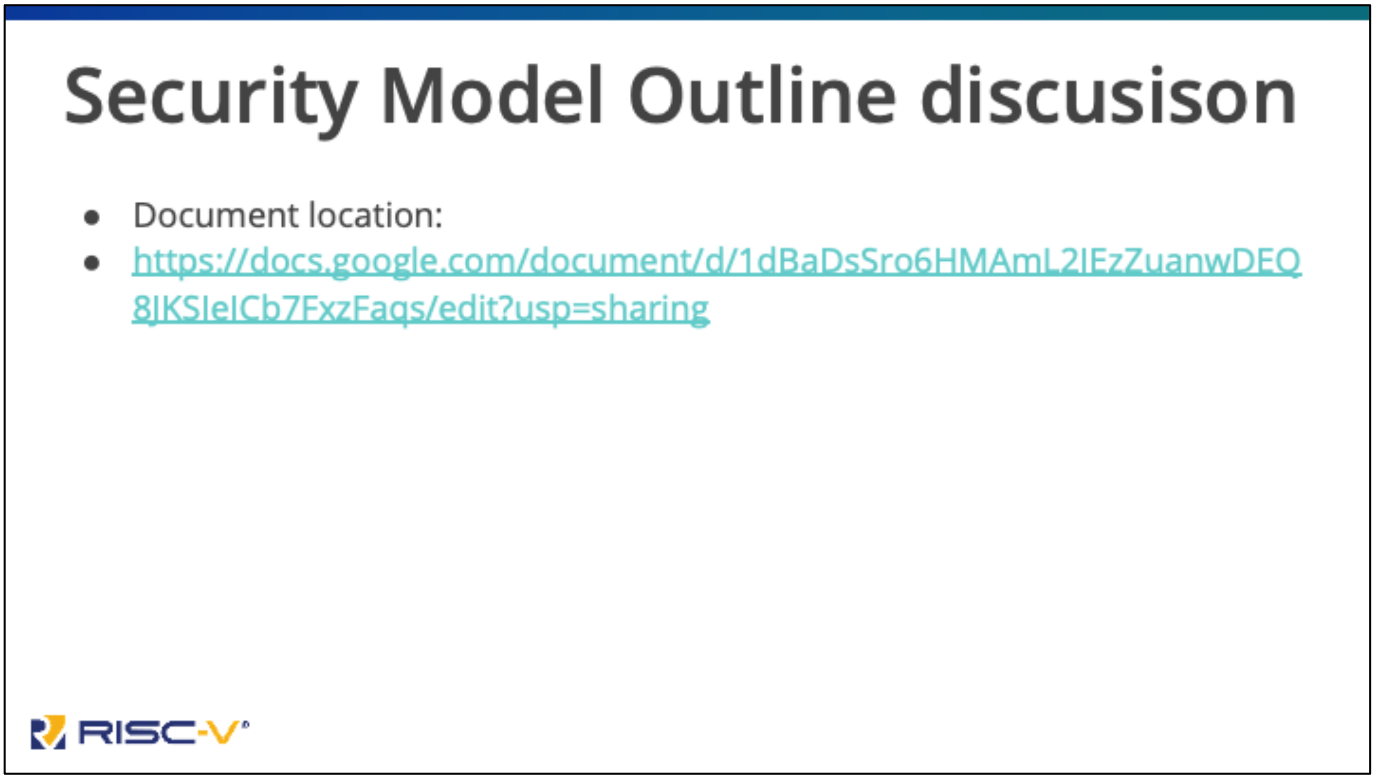
- Currently TSC approved TGs:
  - Shadow Stack & Landing Pads
  - IOPMP
  - SPMP
- Vote in-process at TSC:
  - AP-TEE – vote end date is Sept 5
  - Security Model: currently on-hold due to discussion around Architecture Overview
- Runtime Integrity SIG: Nick to finalize charter soon



IoT-TEE TG request

- General consensus we need lightweight / IoT TEE
  - Needs new TG
  - Any Hardware Isolation Must align and scale with APT-TEE / Confidential Compute
    - Likely requirement from AP-TEE/CC : need an attestable, certifiable TCB, separate lifecycle and owner from other M-Mode FW. Other M-Mode FW must not be able to break security assumptions
- Need to develop the charter ?

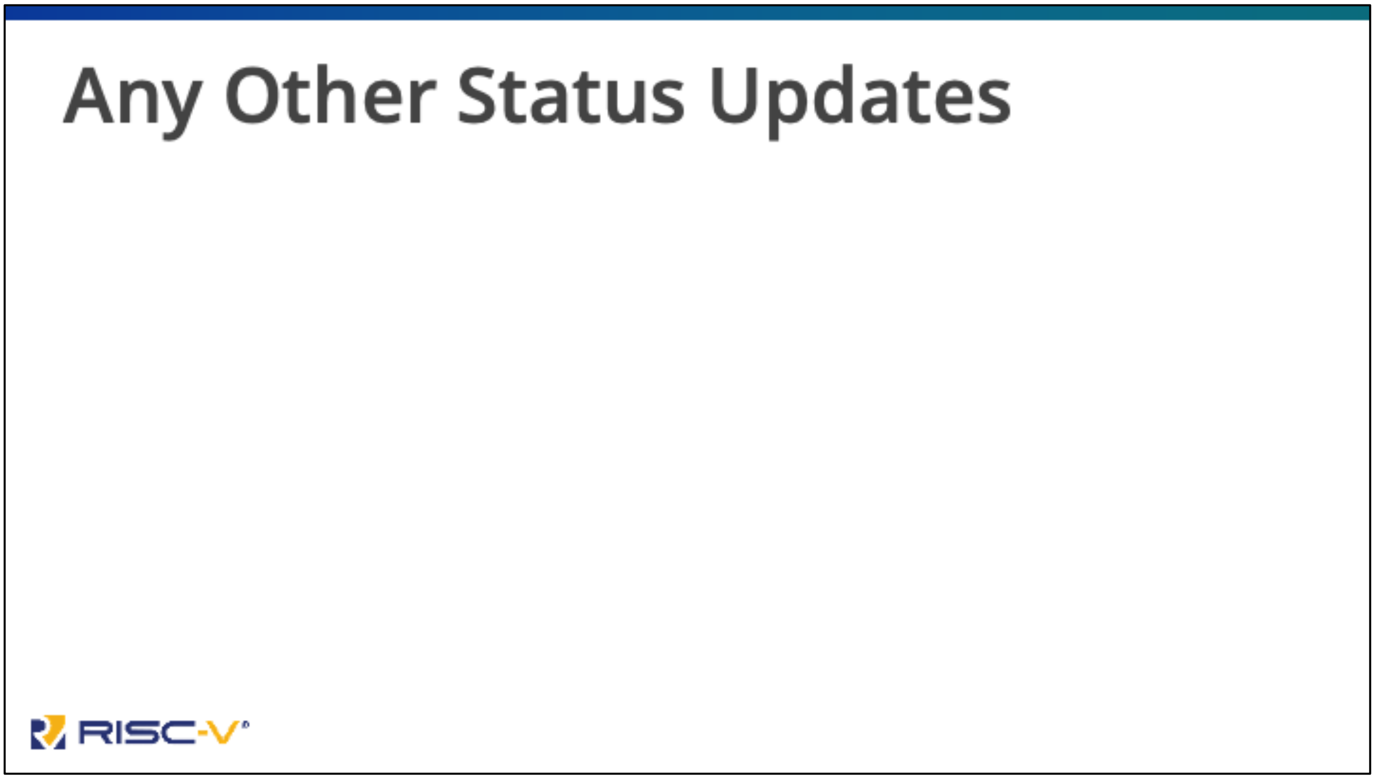
- Call for potential volunteers to lead TG
  - holding off while having ongoing discussion in Trusted Computing SIG
  - Dingji willing to step in and drive
- Looking for single model that potentially fits all solutions
  - Convergence required for all use cases => have discussion in Trusted Computing SIG



Security Model Outline discusison

- Document location:
- https://docs.google.com/document/d/1dBaDsSro6HMAmL2IEzZuanwDEQ8JKSIeICb7FxzFaqs/edit?usp=sharing

- Looking for inputs on outline within the next next coupe of weeks
- May not be able to cover all topics in 1st version of document due to large number; ay need to prioritize



Any Other Status Updates

- Did not get to this topic.

RISC-V®

Open Action Items

Running list of open AI’s