



# Security HC Meeting

August 17, 2023

# Agenda

- PQC TG status –
  - Markku to fwd the autogenerated email. Andy to send the call
- Svadu extension fast track ratification.
  - Hardware updating of PTE A/D bits  
Ravi has reviewed, Guernsey will also review and comment.
- Work Group Status
  - A few corrections - Smmmtt is dotted line
  - App tee IO and IOPMP to present their plans at next chairs meeting
  - Lightweight iso TG – guernsey and mark to meet to discuss next steps end of august
  - Crypto – Vector TG will remain active to push last two instructions as fast track
  - High Assurance Crypto TG - Richard will define candidate quals ready for call for candidates
  - Security Model – slow progress due to holidays since restructuring of the doc.

- Discussion topics Status

- Andy to ask nick to start a gap analysis and strategy doc, linking back to SIG charter goals.
- Idea is to agree on gaps and optimal solutions, to avoid multiple solutions diluting effort
  - Alisson, Ravi, Gurney, Andy all agreed to assist
- Debug – low security attendance to the DTPM meeting, but agreement that dtpm should own the solution. Security team tol define the security issues gap and requirements to the debug. Nvidia already has most of that in their slides.
- Andy to align with the DTPM chair.

# Working groups Status

RVI TSC  
TBD

Security HC  
Andy Dellow  
Ravi Sahita

Formal Security  
Proofs  
  
Debug Access  
Controls

Software  
Security SIG  
TBC

**CHERI SIG**  
Alex Richardson  
(acting)  
Simon Moore  
(Acting)

**GOST-R  
Crypto TG**  
(on-hold)

**Security Model  
TG**  
Paul Elliott  
Terry Wang

**SIRT**  
Don Bailey

**Runtime  
Integrity SIG**  
Nick Kossifidis  
Deepak Gupta

**Crypto TG  
(Scalar, Vector)**  
Richard Newell  
Ken Dookser

**PQC TG**  
Markku Saarinen  
Richard Newell

**uSC SIG**  
Ronan  
Lashermes  
Alisson Randal

**CFI SIG**  
George Christou  
Ved Shanbhogue

**Trusted Computing  
SIG**  
Ravi Sahita  
Suresh Sugumar

**Blockchain  
SIG**  
Patty Tu  
Gary Xu

**IOPMP TG**  
Paul Ku  
Channing Tan

**Lightweight  
Isolation TG**  
Guernsey Hunt  
(acting)  
Mark Hill (TBC)

**SPMP TG**  
Dong Du

**ePMP**  
Nick Kossifidis

**uSCR-IS TG**  
Ronan Lashermes  
Nils Wistoff

**SS&LP TG**  
George Christou  
Ved Shanbhogue

**AP-TEE TG  
(CoVE)**  
Ravi Sahita  
Guernsey Hunt

**AP-TEE-IO  
TG**  
Samuel Ortiz  
Jiewen Yao

**SmMTT TG**  
Ravi Sahita  
Krste Asanovic

Further discussion  
needed

Requires setup

Charter in-process  
(acting chairs)

Operational

Done/closed

Security HC

Charter in-process  
(acting chairs)

Operational

Dotted line  
to Security HC

# Discussion Status

- RTI SIG
  - HFI
  - Pallette Memory
  - Memory Tagging, Pointer Masking
  - Interactions with lightweight Isolation TG
- Debug
  - Proposals being discussed, but we need gap analysis, Charter 1<sup>st</sup>