EUROSMART

The Voice of the Digital Security Industry

Soft IP Taskforce

Introduction for JIWG

Soft-IP Taskforce Description (1/2)

The Soft-IP taskforce addresses the challenges of ***evaluating the security of "Soft Intellectual Property (IP) core" hardware components, also called soft macros****. Soft-IP cores play an important role in chip development with reusable building blocks for specific functions, like a processor, crypto engine, or a complete security subsystem. To make a chip, Soft-IPs must be synthetized to a gate-level netlist which is then mapped to the specific silicon process technology, resulting in a hard macro.*

Security evaluation and certification of chips is a proven approach to provide trust to end-users about product security claims. As security evaluation and certification of hard macros and PL macros is now being defined by JHAS and supported by new protection profiles like PP-0117, this task force aims to address soft macros. ***To extend the benefits of Soft-IP cores from development efficiency to certification efficiency, security evaluation should start on the Soft-IP level and facilitate re-use of Soft-IP evaluation results for chip certification.***

(continued next slide)

Soft-IP Taskforce Description (2/2)

(continued from previous slide)

The Soft-IP taskforce prepares for this by performing a gap analysis and scope definition for evaluation of Soft-IP cores. The work builds on the methodologies that are in use for Secure Element (Smartcard chips) and the 3S in SoC. We identify the similarities and differences in the evaluation processes, the risks inherent to the Soft-IP supplier/consumer relationship and create a gap analysis of differences with the current evaluation processes.

The taskforce will provide recommendations to the Eurosmart board for next steps, such as creating a new working group to develop a methodology for evaluating Soft-IP Cores and for using the results of such evaluation for the certification of silicon products.

Taskforce Organization and Members

- The work is organized as a Eurosmart Taskforce, reporting to the Eurosmart board
  - Not yet an ISCI working group or ITSC activity, that would be a next step

- Good representation of various stakeholders
  - Soft-IP developers/vendors
  - Soft-IP users/integrators
  - Evaluation labs and certification schemes

- Parties involved and contributing, in alphabetical order:
  - Applus+, BSI, Eurosmart, G+D, Idemia, Infineon, NXP, Qualcomm, SGS, ST, Synopsys (chairing the taskforce), Thales, Tiempo Secure, TrustCB, Trustsec, T-Systems, Winbond, Wisekey

Work Plan and Outlook

- The taskforce started October 2021 and normally meets every other week
- Sessions target a specific topic, introduced and presented by a taskforce member and discussed by the group
- Topics identified and discussed
    - Soft-IP scope, and definitions of terminology
    - Lifecycle aspects
    - PP0117 3S-in-SoC learnings
    - Review of CC Soft-IP certification case (ARM processor IP)
    - Review of methodologies in use for Secure Element and 3S in SoC PP
    - Review of new ISO-CC Composite evaluation
    - Review of SESIP approach to composite evaluation
- Planned results and output
    - Consolidating results of the sessions – report / white paper incl. gap analysis with current methodologies
    - Recommendations for next steps
- Expected taskforce completion date: August/September 2022

Thank You