Technology Innovation Institute

seL4 SUMMIT

seL4 SUMMIT
SYDNEY 2024

Exploring an seL4-based Trusted Execution Environment in a RISC-V Platform

Everton de Matos

Introduction

- With the **exponential growth of connected devices** and the constant threat of cyber-attacks, there's never been a more crucial time to **ensure that our computational environments are trustworthy**

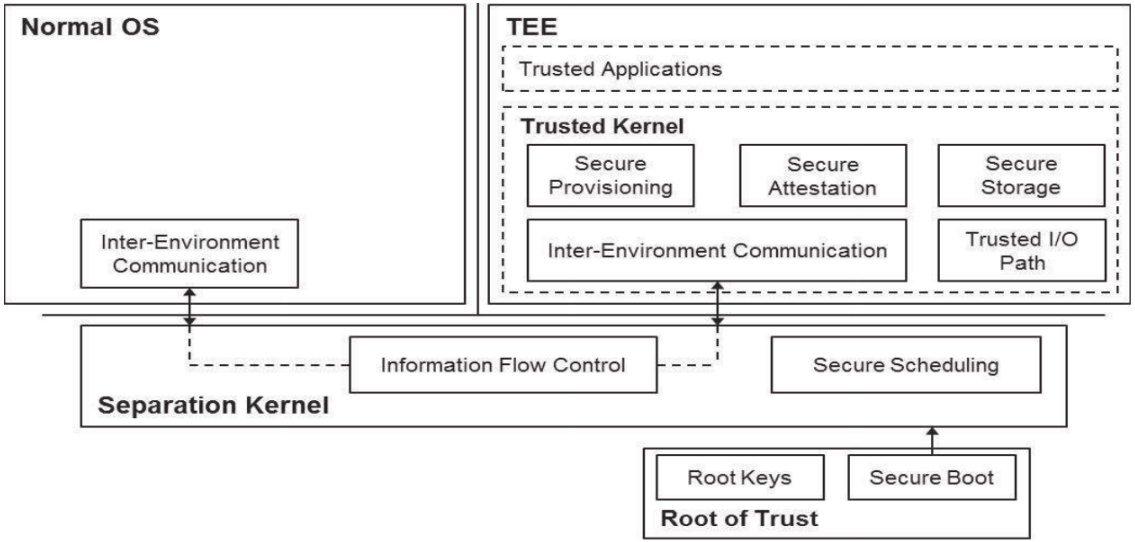
- While hardware security mechanisms and traditional software barriers have their roles, there are **gaps that need to be addressed** to ensure absolute trust in our digital environments

- The necessity for **robust security** solutions is more pronounced than ever. **TEEs** stand as **one of the possible solutions** to meet intricate security needs

- In this landscape, **seL4** presents itself as a strong candidate to anchor a **secure operating system within a TEE**, offering a robust foundation to build trusted digital environments

Trusted Execution Environments

- **Trusted Execution Environments (TEEs)** provide a **secure execution environment** for sensitive applications and data, ensuring that they are protected from attacks and unauthorized access
- TEEs are typically implemented as a separate execution environment within a system, with their own hardware and software resources that are **isolated from the rest of the system**



[1] Sabt, Mohamed, Mohammed Achemlal, and Abdelmadjid Bouabdallah. "Trusted execution environment: what it is, and what it is not." 2015 IEEE Trustcom/BigDataSE/Ispa. Vol. 1. IEEE, 2015.

Trusted Execution Environments – Use cases

- **Secure Storage**
  - Sensitive data can be stored safely, isolated from the main operating system
- **Secure Execution of Code**
  - Code can be executed in a protected and isolated environment, ensuring the integrity of the operations
- **Cryptographic Operations**
  - Encryption, decryption, and digital signing
- **Remote Attestation**
  - Remote verification of software's integrity and authenticity
- **Secure Multi-party Computation**
  - Parties can jointly compute a function over their inputs while keeping these inputs private

seL4 TEE – Related Work

- TEEVseL4: Trusted Execution Environment for Virtualized seL4-based Systems [2]

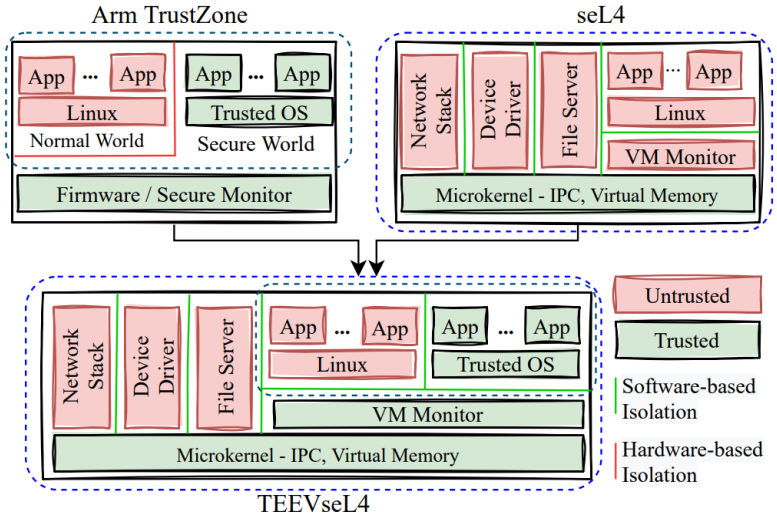


Fig. 1: The TEEVseL4 system architecture, leveraging microkernel (seL4) and Arm TrustZone-compatible software solutions, provides a trustworthy virtualization system with a TrustZone-compatible TEE for secure isolation of security-critical functions.

- MicroTEE: Designing TEE OS Based on the Microkernel Architecture [3]

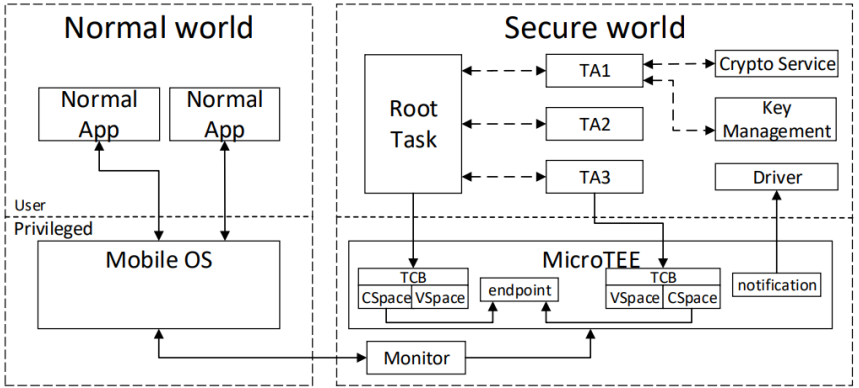


Fig. 2. The Architecture of MicroTEE

[2] Blazevic, B., Peter, M., Hamad, M., & Steinhorst, S.. "TEEVseL4: Trusted Execution Environment for Virtualized seL4-based Systems." 2023 IEEE RTCSA 23.
[3] Ji, D., Zhang, Q., Zhao, S., Shi, Z., & Guan, Y. (2019, August). Microtee: designing tee os based on the microkernel architecture. In 2019 18th IEEE TrustCom (pp. 26-33).

TEE on RISC-V

- **HEX-Five Multizone** [4]
  - Provides hardware-enforced, software-defined separation of multiple security domains, thus enabling isolation in separate "zones"
- **Penglai** [5]
  - Enclave framework, providing a mechanism to run trusted applications in an isolated environment
  - Designed to leverage the hardware isolation features provided by the RISC-V architecture, such as PMP
- **Keystone** [6]
  - Provides customizable TEEs
  - Provided example scenarios:
    - seL4 being used in S mode inside an enclave
    - seL4 being used in M mode as Security Monitor

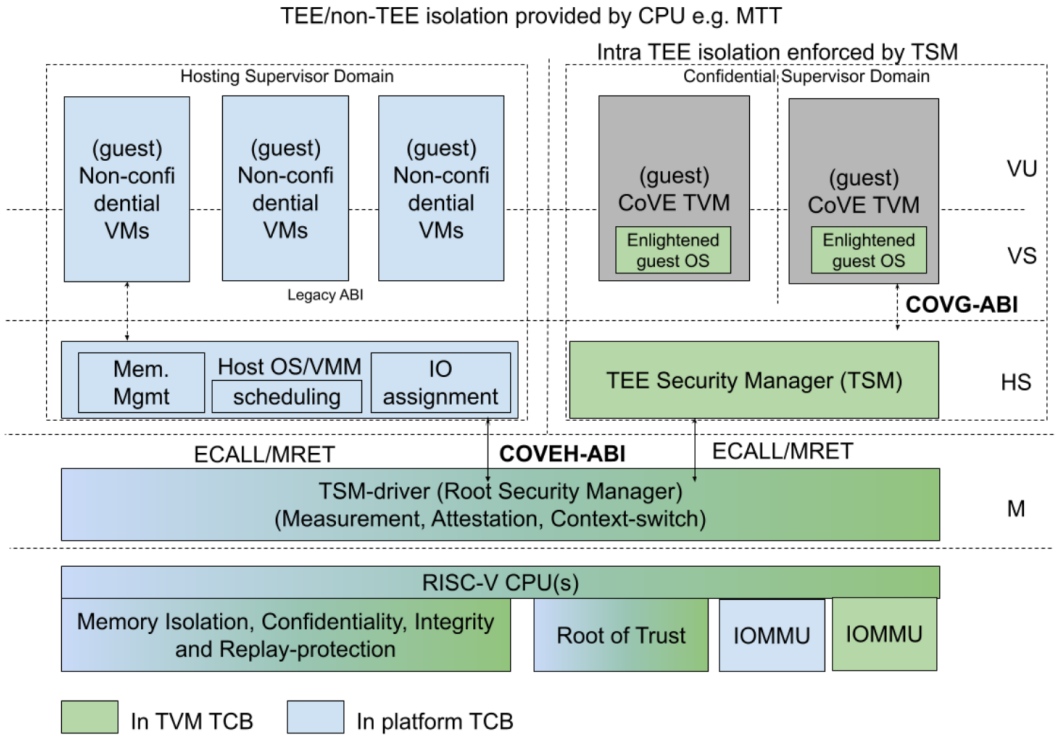
[4] HEX-Five. https://hex-five.com/multizone-security-tee-riscv/
[5] Feng, E., Lu, X., Du, D., Yang, B., Jiang, X., Xia, Y., ... & Chen, H. (2021). Scalable Memory Protection in the {PENGLAI} Enclave. In 15th USENIX OSDI (pp. 275-294).
[6] Lee, D., Kohlbrenner, D., Shinde, S., Asanović, K., & Song, D. (2020, April). Keystone: An open framework for architecting trusted execution environments. In 15th EuroSys (pp. 1-16).

TEE on RISC-V

RISC-V Application-Processor TEE (AP-TEE) Task Group Specifications

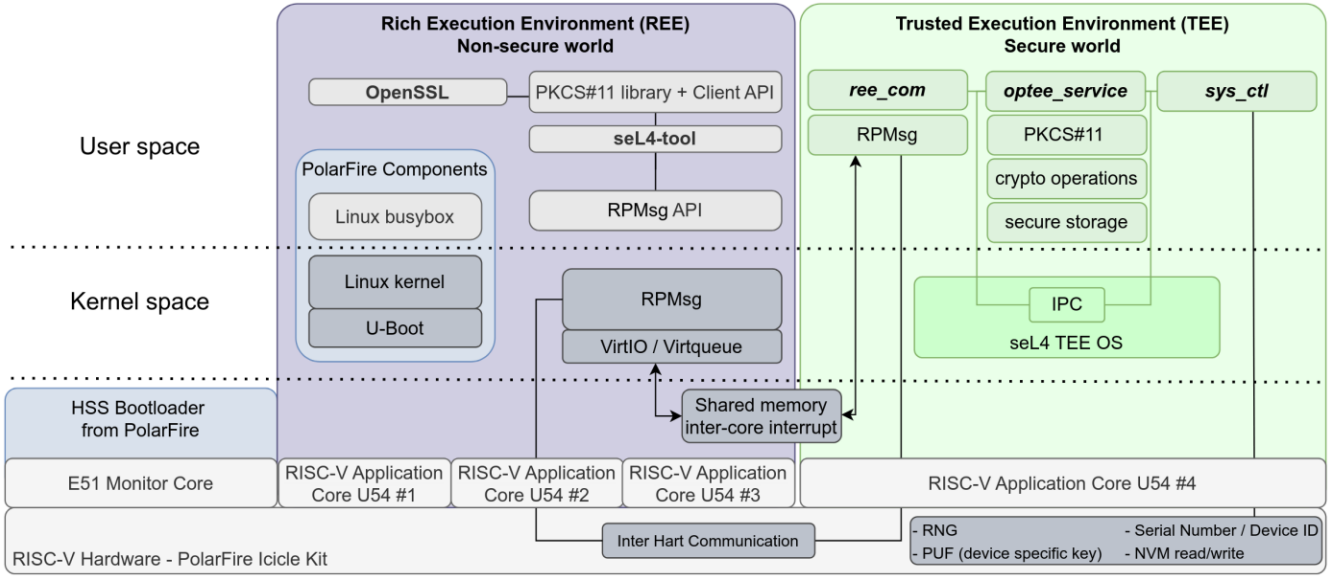
https://github.com/riscv-non-isa/riscv-ap-tee

- This specification describes the **CoVE architecture** which enables a new class of hardware-attested trusted execution environment called **TEE Virtual Machines** (**TVMs**)
- TEE Security Manager (**TSM**) acts as the trusted intermediary between TEE and non-TEE workloads
- The responsibility of the TSM is to enforce the security objectives accorded to TEE workloads (**TVMs**) assigned to that supervisor domain



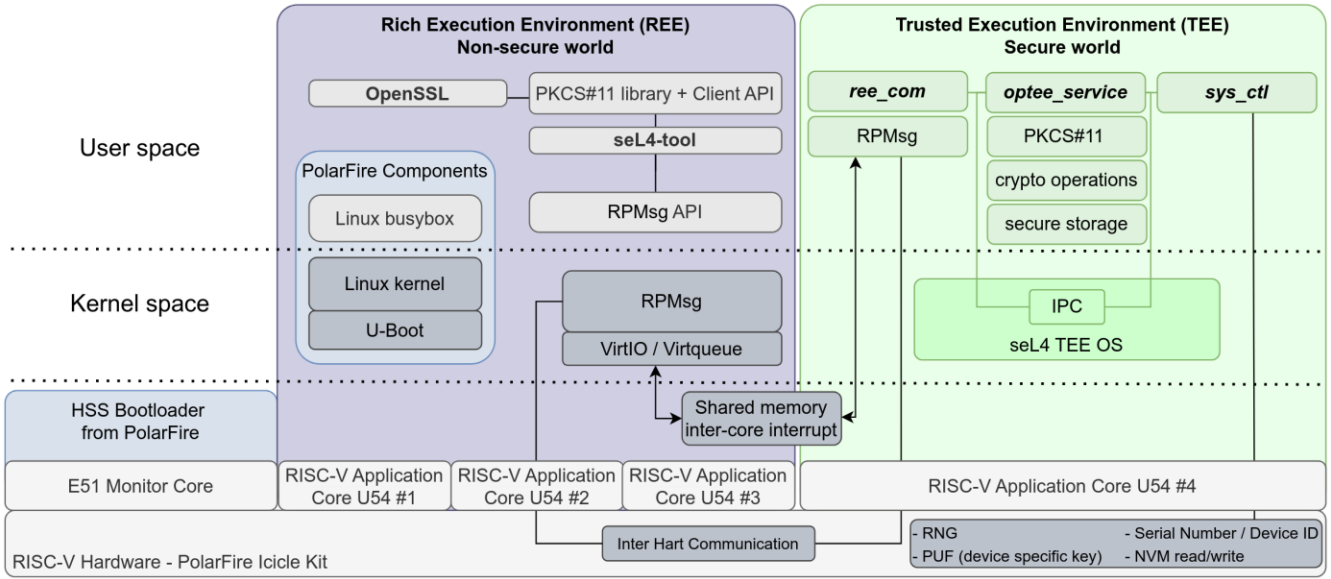
seL4 TEE on RISC-V – Our approach

- **PolarFire SoC FPGA Icicle Kit**
  - 4x U54 Application cores
    - RV64GC
  - 1x E51 Monitor core
    - RV64IMAC
- AMP – PMP configuration
  - 3x U54 – Linux
  - 1x U54 – seL4
- HSS Bootloader
  - E51 Monitor Core



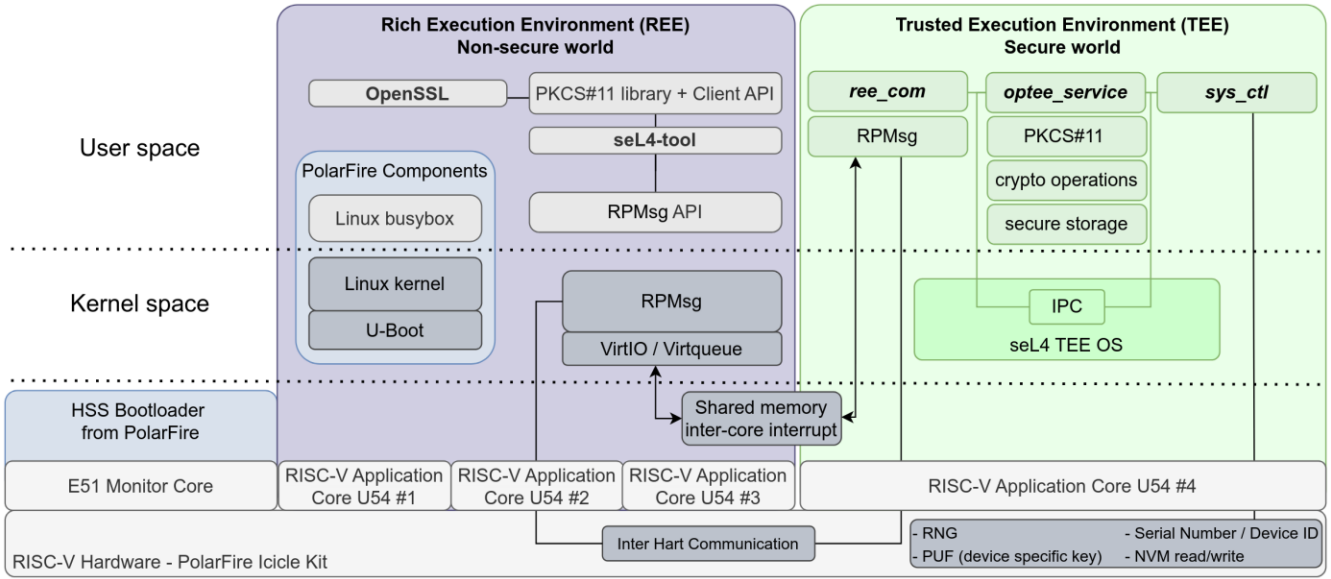
seL4 TEE on RISC-V – Our approach

- **CAmkES applications:**
  - ***ree_com:*** IPC for communication from/to other CAmkES components
  - ***optee_service:*** Following the GlobalPlatform TEE specifications: Crypto / sNVM / PKCS#11
  - ***sys_ctl:*** Uses Polarfire system controller services. Support for device ID read, sNVM read/write



seL4 TEE on RISC-V – Our approach

- **seL4-tool**
  - Test tool for seL4 TEE - used for initial demonstration and testing seL4 TEE services
  - TEE services: (i) random number from seL4 TEE, (ii) Write/Read sNVM, (iii) Generate keys
  - Uses the *seL4_TTY_rpmsg* (TEE) driver for communicating between Linux (REE) and seL4 (TEE)



seL4 TEE on RISC-V – Evaluation

- **Evaluation Overview**
  - **REE Performance:** Assess the performance overhead of the Linux REE when operating the seL4-based TEE
  - **TEE Services:** Evaluate the performance of TEE services facilitated by the seL4 TEE.
- **System Configuration**
  - **Platform:** PolarFire SoC FPGA (MPFS250T-FCVG484EES)
    - SiFive E51 Monitor core (1 x RV64IMAC)
    - Four SiFive U54 Application cores (4 x RV64GC)
    - 2 GB of LPDDR4 x32 memory
    - 1 Gb SPI flash and 8 GB eMMC flash
- **Software**
  - **REE:** Linux kernel version: 5.12.19
  - **TEE:** seL4 version: 12.1.0-dev

seL4 TEE on RISC-V – Evaluation

- **REE Performance**
- **Defined scenarios**
  - **Scenario A**: Linux 3x Cores & seL4 TEE 1x Core
  - **Scenario B**: Linux 3x Cores & 1x idle Core
  - **Scenario C**: Linux 4x Cores, no seL4 TEE.
- **Performance Metrics**
  - CPU and memory usage measured using the *top* command
  - Disk I/O tested with *dd* command for write/read speeds
  - Network throughput measured using *iperf3*
- **Load Simulation**
  - *awk* scripts for CPU and memory load
  - Network and disk loads to simulate real-world usage

seL4 TEE on RISC-V – Evaluation

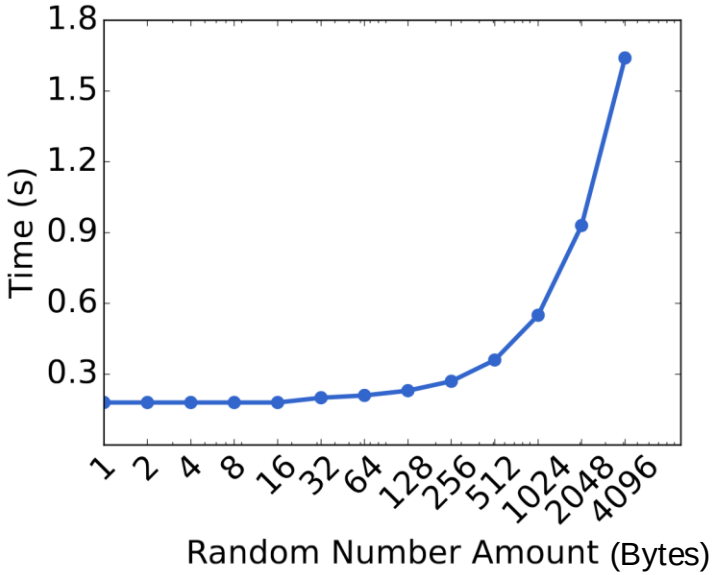
- **REE Performance**

Table: Performance Test Results of Linux REE

Metric	Scenario A	Scenario B	Scenario C
Average CPU Usage (%)	32.81	32.67	26.33
Peak CPU Usage (%)	36	36	28
Available Memory (MB)	429.15	792.37	792.37
Average Memory Usage (MB)	169.15	176.91	174.70
Peak Memory Usage (MB)	237.34	245.13	242.84
Disk Write Speed (MB/s)	60.63	60.62	60.66
Disk Read Speed (MB/s)	66.48	66.56	66.57
Network Throughput (Mbps)	138.2	144.45	168.87
Scenario Descriptions:			
Scenario A - Linux 3x Cores & seL4 TEE 1x Core			
Scenario B - Linux 3x Cores & 1x idle Core			
Scenario C - Linux 4x Cores			

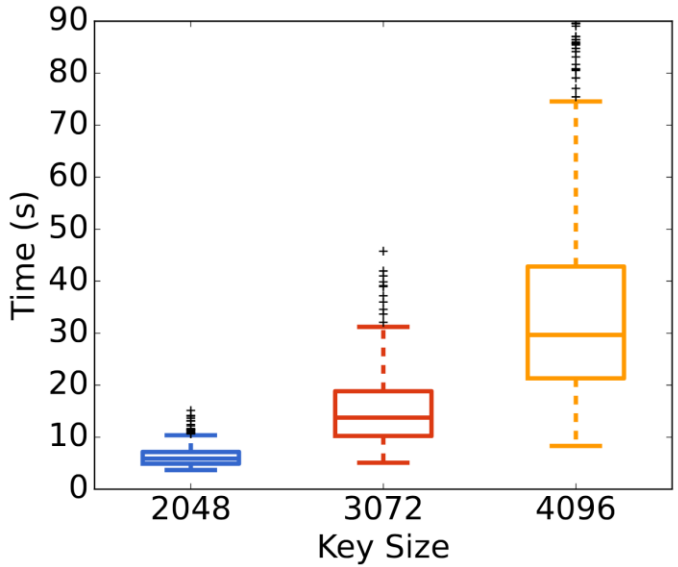
seL4 TEE on RISC-V – Evaluation

- **TEE Services**
- **Random Number Generation (RNG)**
  - Efficiency and latency of generating cryptographically secure random numbers

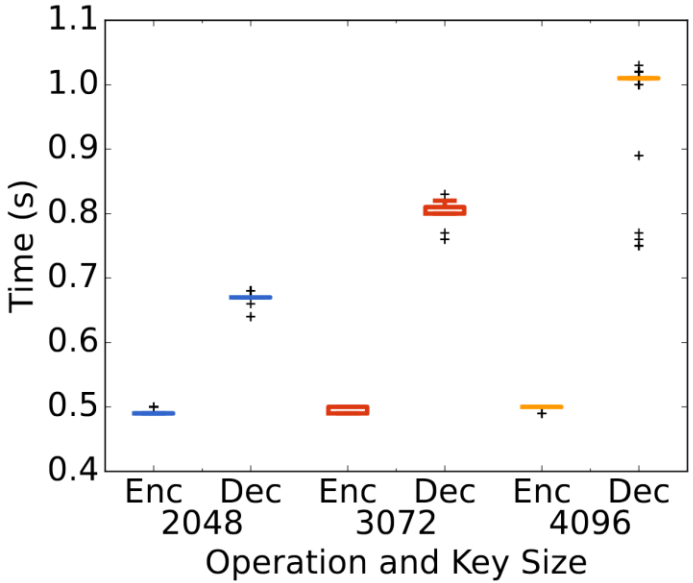


seL4 TEE on RISC-V – Evaluation

- **TEE Services**
- **Key Pair Generation**
  - Time efficiency and performance in generating RSA key pairs



- **Encryption and Decryption**
  - Assess the efficiency of using generated keys for secure data encryption and decryption



seL4 TEE on RISC-V – Evaluation

- **TEE Services**

Metric	Key Generation (s)			Signing (s)			Encryption (s)			Decryption (s)		
	2048-bit	3072-bit	4096-bit	2048-bit	3072-bit	4096-bit	2048-bit	3072-bit	4096-bit	2048-bit	3072-bit	4096-bit
Mean	6.31	15.21	34.68	0.464	0.603	0.796	0.491	0.497	0.500	0.671	0.806	1.007
Median	5.89	13.77	29.66	0.45	0.59	0.79	0.49	0.50	0.50	0.67	0.81	1.01
Std Dev	1.88	6.79	18.13	0.040	0.042	0.031	0.003	0.005	0.001	0.003	0.006	0.029
Minimum	3.68	5.09	8.32	0.44	0.57	0.73	0.49	0.49	0.49	0.64	0.76	0.75
Maximum	15.14	45.77	89.61	0.60	0.81	1.08	0.50	0.50	0.50	0.68	0.83	1.03
25th Percentile	4.92	10.24	21.33	0.45	0.58	0.79	0.49	0.49	0.50	0.67	0.80	1.01
75th Percentile	7.16	18.84	42.81	0.45	0.59	0.80	0.49	0.50	0.50	0.67	0.81	1.01
IQR	2.25	8.61	21.49	0.00	0.01	0.01	0.00	0.01	0.00	0.00	0.01	0.00

Find out more

- **Publications:**

  - De Matos, E., Lunardi, W. T., Ukkonen, J., & Salminen, T. (2024, May). An seL4-based Trusted Execution Environment on RISC-V. In 2024 International Wireless Communications and Mobile Computing (IWCMC) (pp. 712-717). IEEE. https://doi.org/10.1109/IWCMC61514.2024.10592332
  - Submitted: De Matos, E., Lawton, G., & Lennon, C. "An Analysis of seL4 for Enhanced System Isolation and Security on Embedded Devices." In IEEE Access.

- **Source code:**
  - https://github.com/tiiuae/tee_manifest

Technology Innovation Institute

Thank you!

seL4 SUMMIT
SYDNEY 2024

Exploring an seL4-based Trusted Execution Environment in a RISC-V Platform

Everton de Matos