Technical Report for Tim Lewis (Insyde Software CTO)

Subject: Successful PoC of Remote Attestation Using Keylime with TPM, Secure Boot, and IMA on Insyde BIOS Platform
Author: Akihiro Hosoya
Date: August 2025

1. Executive Summary

This report summarizes the successful implementation of a Remote Attestation Proof of Concept (PoC) using Keylime on an Insyde BIOS platform with TPM 2.0, Secure Boot, and IMA. This is the first known fully reproducible implementation in the world that integrates Rust-based and Python-based components of Keylime, proving the viability of a scalable and standards-compliant remote attestation system in real-world PC OEM environments.

2. PoC Environment

- Platform: Intel Arrow Lake (vPro SKU)
- BIOS: InsydeH2O with Secure Boot enabled
- TPM: dTPM 2.0 (STMicroelectronics)
- OS: Ubuntu 22.04 LTS
- Kernel: 5.15.0-112-generic
- Keylime Components:
- - Python-based Verifier, Registrar, and Tenant
- - Rust-based Agent (latest stable build)
- Security Features:
- - Secure Boot: Enabled
- - IMA: Enabled
- - UUID: Fixed to 11111111-1111-1111-1111-111111111111
- - TPM NV Index: Defined as 0x1500016

3. Key Achievements

- Successfully launched Rust-based Keylime Agent and Python-based Verifier/Registrar on Ubuntu with TPM 2.0.
- Validated the End-to-End Remote Attestation flow, including PCR quote verification, TPM key bootstrapping, and policy-based validation.
- Achieved full consistency in UUID and NV Index across all components for reproducibility.
- Verified compatibility of Insyde BIOS with Secure Boot + TPM + IMA integration.
- Established a reusable PoC configuration package including keylime.conf, ima-policy, logs, and configuration diagrams.

4. Business & Strategic Impact

- OEM Differentiation: Demonstrates the ability to ship laptops with built-in Remote Attestation functionality.
- Security Assurance: Enables compliance with NIST SP800-155 and SP800-193.
- Customer Value: Assures platform integrity and boot chain verification in Zero Trust environments.

- Market Leadership: First OEM-level reproducible PoC with open-source Keylime + Rust Agent.

5. Next Steps / Proposal to Insyde

- Offer support to Insyde in integrating Keylime-based Remote Attestation modules into BIOS development/testing workflows.
- Collaborate on creating a standard BIOS interface layer to expose PCRs, boot measurements, and IMA logs more efficiently.
- Co-author a JEITA or TCG proposal on UUID/NV Index standardization for reproducible attestation.
- Present this work at future TCG or security-focused technical summits.

6. Attachments

- PoC Configuration Diagram (PDF): Visual layout of all components, UUID/NV Index settings, and data flow.
- Full Configuration Package: keylime.conf, ima-policy, logs, scripts, UUID/NV Index definitions.
- Presentation Slide (PDF): Summary of architecture, achievements, and recommendations for BIOS vendors.

Thank you for your continued leadership in BIOS innovation.

Akihiro Hosoya
Remote Attestation Security Architect
Email: [your email]
LinkedIn: [your LinkedIn]