# Keylime Remote Attestation PoC - Summary Slide

## Overview of Key Achievements:

- ■ Full PoC with Rust Agent and Python Verifier on Ubuntu 22.04
- ■ Integration with TPM 2.0, Secure Boot, and IMA
- ■ Fixed UUID and TPM NV Index for reproducibility
- ■ Verified compliance with NIST SP800-155 and SP800-193
- ■ Aligned with Zero Trust architecture and BIOS security trends

## Strategic Recommendations for BIOS Vendors:

- → Embed Keylime modules in firmware validation workflows
- → Standardize PCR/IMA exposure interfaces in BIOS
- → Collaborate on UUID/NV Index standardization via JEITA/TCG
- → Promote reproducible attestation as a Secure Boot enhancement

Prepared by: Akihiro Hosoya, Remote Attestation Security Architect