

UEFI advanced concepts

Overview

- Memory protection mechanisms in UEFI
- Boot Service and Runtime Services hands-on
- UEFI Authenticated Variables
- Virtualization in firmware and its use cases
- System Management Mode deep dive
- SMI Transfer Monitor design and practical use cases
- ACPI in UEFI
- SecurityPkg and CryptoPkg use cases

Audience

People with very good knowledge of Linux, C and Python. Good knowledge of computer systems architecture is required. Preferred audience after accomplishing 3mdeb UEFI fundamentals training or similar.

Materials

All training materials presentations and source code will be available for customer internal usage..



Duration

5 days

40 hours (8h/day)

50% lectures

50% hands-on workshop

Language

English.