presented by

The UEFI Forum

UEFI 2025 Developers Conference and Plugfest / Open Source Firmware Conference

October 7 – 10, 2023

Sunnyvale, CA

presented by

The UEFI Forum

State of the UEFI: A Standardized Approach to Firmware

Presented by Mark Doran

UEFI Forum President

Introduction

Mark Doran, UEFI Forum President

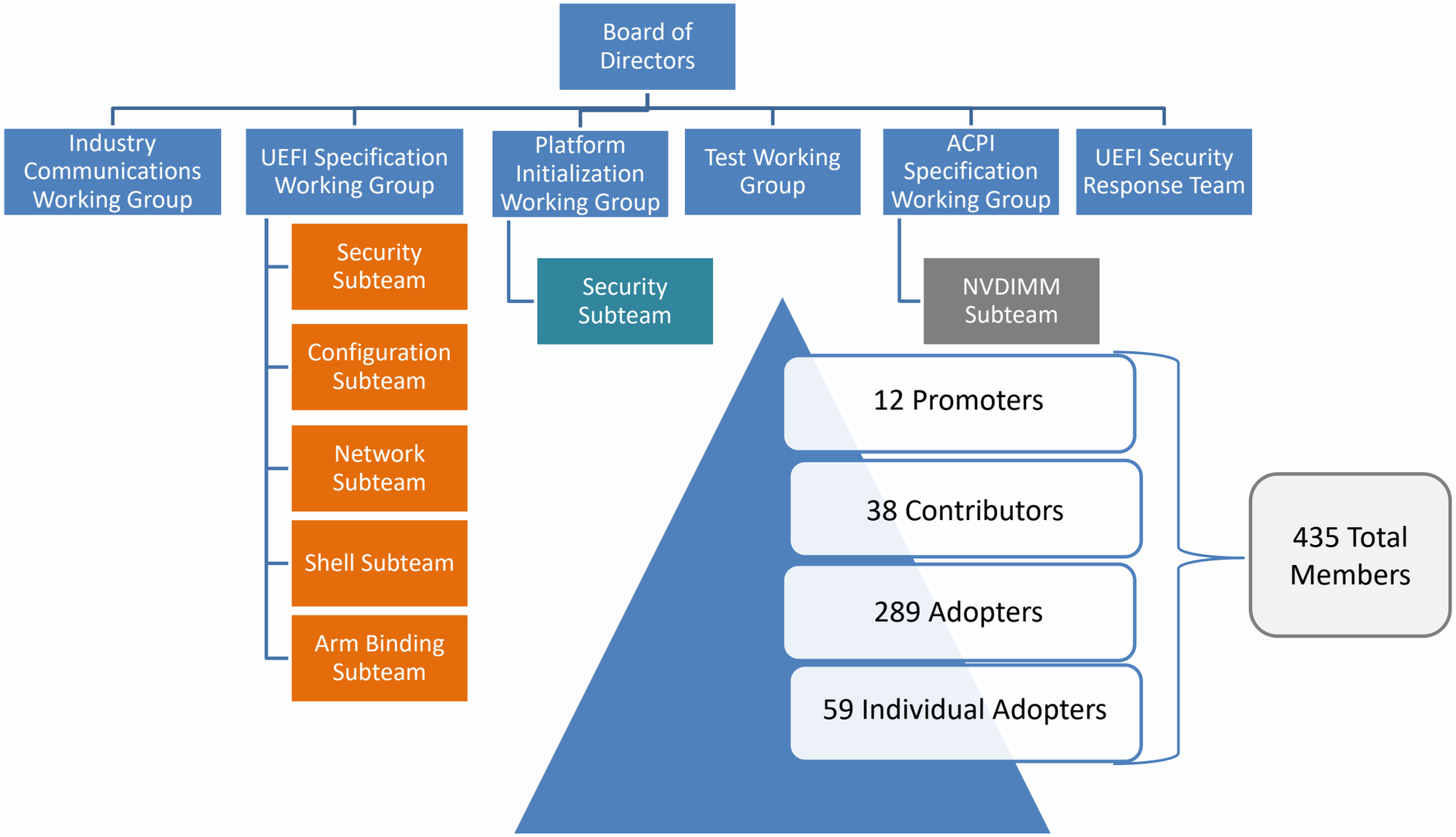
Mark Doran is President of the UEFI Forum and an Intel Fellow. Mark graduated from University College London, University of London. He joined the UEFI Forum in 2005.

Agenda

- About The UEFI Forum
- Specifications Update
- UEFI Security & Open Source
- UEFI DevCon Event Overview
- Questions

The UEFI Forum

UEFI Forum Overview



UEFI Forum Mission / Purpose

The UEFI Forum champions firmware innovation through industry collaboration and the advocacy of a standardized interface that simplifies and secures platform initialization and firmware bootstrap operations.

The UEFI Forum maintains the following main specifications:

UEFI Specification

Defines a new model for the interface between personal-computer operating systems and platform firmware. The interface consists of data tables that contain platform-related information, plus boot and runtime service calls that are available to the operating system and its loader. Together, these provide a standard environment for booting an operating system and running pre-boot applications.

ACPI Specification

Provides standardized, flexible mechanisms for device discovery, operating system configuration and power management (OSPM), thermal management and RAS (reliability, availability and supportability) features. The ACPI standard improves system power distribution and conservation through its communications with the system firmware, operating systems and peripheral devices

PI Specification

Describes the boot execution phases to encompass UEFI supported protocols and services. While UEFI primarily focuses on the interface between firmware and the operating system, PI focuses on interfaces between low-level firmware components.

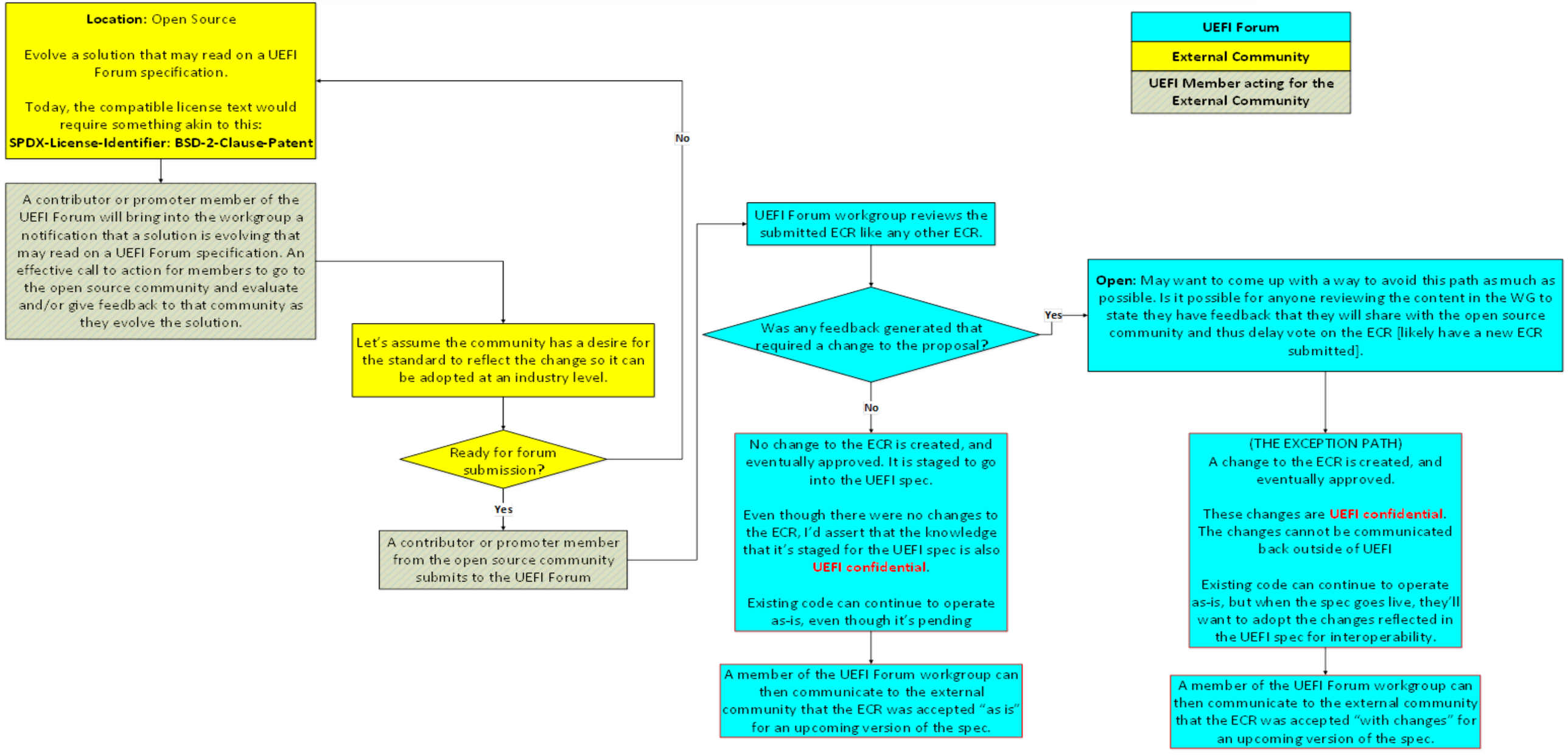
UEFI Forum & TianoCore / EDK2

- The **UEFI Forum's** role is about defining specifications for interface, meaning how do bits of firmware and or operating systems
- **TianoCore** is a community supporting open source implementation of UEFI, with most of their focus on EDK2.
- **EDK2** is an open source implementation of the UEFI specifications, including UEFI, ACPI and PI
  - The UEFI Forum does not govern or endorse EDK2, but it is the preeminent solution / implementation of the UEFI specifications

Working Group Process / Open Source

- Enable “Code-First” approach
- Encourage open source contributions
  - Increase in open source contributions in reference implementations
  - Improve open source process

Code-First Approach



Latest Specifications & Recent Updates

v2.11 v2.2 v1.9 v2.7 v1.1 v6.6 < Current Versions

- **ACPI Specification v. 6.6 (Updated May 2025)**
  - Updates for RISC-V architecture support for multiple APICs and memory attributes
  - Enhancements for CPPC and SRAT for resource priority and hot-plug memory description
  - Modifications to General Purpose Event handling in S0 idle
- **UEFI Specification v. 2.11 (Updated Dec. 2024)**
  - Updates to memory management and allocation (i.e. new memory attribute for hot plug and Arm memory allocation mandates)
  - Enhancements to protocols, algorithms and boot management
  - Corrections to EFI_KMS_PROTOCOL, new crypto algorithms and support for Proxy Host URI in HTTP Boot
  - Improvements to error handling and documentation updates (i.e. CPER definitions and Arm processor error information)
- **UEFI PI Specification v. 1.9 (Updated Dec. 2024)**
  - Expands algorithm options by providing enhanced security with additional cryptographic algorithms for signed Firmware Volume (FV) and signed sections extending beyond the previous RSA2048_SHA256
  - Adds Random Number Generator (RNG) PEIM-to-PEIM Interface (PPI) to serve as an entropy source for seeding cryptographic services
  - Includes new protocol for Multiple SPI Regions with varying block erase sizes, enhancing flexibility and functionality
  - Adds support for LoongArch architecture

UEFI Testing Updates

- UEFI SCT (Self-Certification Test) measures conformance to the UEFI 2.7 specification
  - Arm is leading the efforts to update the testing to the current UEFI 2.11 specification
  - RISC V and LoongArch support have recently been added; test support for these architectures are needed
    - **Community Support Needed:** Join the UEFI Test Work Group (UTWG) to support the development of these tests
- FWTS (Firmware Test Suite) measures conformance to the ACPI specification and how if your platform firmware can support Linux
  - Canonical is supporting testing updates

UEFI Security

- As broad architecture support continues, security will continue to be a concentrated effort for the Forum and the community. We have developed the following sub-teams to support security concerns:
  - UEFI Security Sub-Team (USST) is the security infrastructure design group, which produces design guides around the safe composition of PI based components
  - SBOM Sub-Team (USBT) are building guidelines to Software Bill of Materials as it relates to firmware
  - UEFI Security Response Sub-Team (USRT) are dedicated to aiding members of the supply chain to respond to vulnerabilities in a timely manner and communicating with stakeholders to improve to state of the art in firmware
- One of the live issues are what it means to have firmware behave well in a post-quantum world for security and robustness

Collaborate or Join the UEFI Forum

- If you want to become a UEFI Forum member or need next steps as a current member…
  - **New Members:** Visit the UEFI Forum website to learn more about the membership opportunities: https://uefi.org/join
  - **Current Members:** Join a working group and support future development of the specifications: https://uefi.org/workinggroups

UEFI 2025 DevCon and Plugfest: Event Overview

Thursday, October 11

UEFI DevCon 2025 Session Highlights – **Open to OSFV Attendees**

Time	Session Title	Presenters
10:15 – 10:45 am	Next Frontiers in Firmware Standardization: OCP OPF efforts and their effect on UEFI	Felix Polyudov (AMI)
10:45 – 11:15 am	Web-Scale UEFI Configuration Management: The Cloudflare Way	Nnamdi Ajah (Cloudflare)
11:15 – 11:45 am	Virtualization for UEFI DXE Driver Testing and Deployment Validation	Aaron Rossetto (Cirrus Logic)
11:45 am – 12:15 pm	Signed and Dangerous: BYOVD Attacks on Secure Boot	Alex Matrosov (Binarly) & Fabio Pagani (Binarly)
12:15 – 12:45 pm	Pantina: UEFI in Rust	Michael Kubacki (Microsoft)
12:45 – 1:15 pm	Secure and Scalable Firmware Updates via Capsules	Mohamad Saleh (Insyde) & Sean Loe (Insyde)
1:15 – 2:15 pm	Lunch	

Testing from 9:30 am – 6:00 pm

Friday, October 12

UEFI DevCon 2025 Session Highlights – **Members-Only**

Time	Session Title	Presenters
9:00 – 9:30 am	Repeatable Supply Chain Security Failures in Firmware Key Management	Alex Matrosov (Binarly) & Fabio Pagani (Binarly)
9:30 am – 10:00 am	Trusted Execution Environment Protection for Firmware Integrity	Kun Qin (Microsoft) & Chris Fernald (Microsoft)
10:00 – 10:30 am	Advancing Firmware Compliance in the Arm Ecosystem	Samer El-Haj-Mahmoud (Arm) & G Edhaya Chandran (Arm)
10:30 – 11:00 am	Redfish UEFI and EDK2 Implementation	Abner Chang (AMD) & Igor Kulchytskyy (AMI)
11:00 – 11:30 am	Secure Boot Ecosystem	Sochi Ogbuanya (Microsoft) & Doug Flick (Microsoft)
11:30 am – 12:00 pm	Evolving ACPI Standards for Arm Systems: Advancements in Specification and Implementation	Samer El-Haj-Mahmoud (Arm) & Jose Marino (Arm)
12:00 – 1:00 pm	Lunch	
1:00 – 1:30 pm	Arm System Firmware Architecture	Dong Wei (Arm)
1:30 – 2:00 pm	Enablement of Secure Boot with GRUB Under UEFI for Linux	Sumeet Pawnikar (Cisco)
2:00 – 2:30 pm	Integrate Arm SystemReady Band –UEFI and ACPI Compliance for Better Quality and Faster Debug	Sunny Wang (Arm)

Testing from 9:00 am – 2:30 pm

Made Possible by our Gold Sponsors...

Questions?