Firmware, the Last Frontier: Open System Firmware (OSF)

Gundrala “Devender” Goud/Director/Microsoft
Ron Minnich / Google
What is this UEFI FW (BIOS)?
Current Challenges ‘System Firmware’ and Why Open?

▪ ‘Closed’ System Firmware **could have impacts to** rapid prototyping of new or derivative products development (NDA, IP, etc.)
▪ Variance in boot flows of different Silicon vendors’, causing inefficiencies in System Firmware development and maintenance.
▪ Various System Firmware implementations exist, but **not one single implementation** addresses the needs of different CSP use models.
▪ System Firmware current **development models not able** to keep pace with ‘High Octane’ Innovation by multiple Cloud HW vendors.

**Truly Open ‘Solution’ = open HW+ open FW**
Convergence of Different System Firmware(s) → Open System Firmware (OSF)

Collaborative Community development model

Infrastructure, Tools & Eco-system support
<table>
<thead>
<tr>
<th>Workstream name</th>
<th>Owner (Companies)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEI</td>
<td>Intel</td>
</tr>
<tr>
<td>Intel FSP binary</td>
<td>Intel</td>
</tr>
<tr>
<td>AGESA RC binary</td>
<td>AMD</td>
</tr>
<tr>
<td>ARM Boot code binary</td>
<td></td>
</tr>
<tr>
<td>Power Host boot</td>
<td></td>
</tr>
<tr>
<td>Core Boot</td>
<td>9 Elements</td>
</tr>
<tr>
<td>Silicon Interface Firmware Module</td>
<td>Intel</td>
</tr>
<tr>
<td>Linux Boot</td>
<td>Google, FB, Two Sigma, Horizon</td>
</tr>
<tr>
<td>Open EDK II DXE core</td>
<td>MSFT, Intel</td>
</tr>
<tr>
<td>HW platform modules</td>
<td>HW supplier</td>
</tr>
<tr>
<td>Boot loader support</td>
<td>OS vendor(s)</td>
</tr>
<tr>
<td>Build tools</td>
<td>Two Sigma</td>
</tr>
<tr>
<td>Automated test support</td>
<td>Horizon, Google</td>
</tr>
<tr>
<td>Telemetry/Diags</td>
<td></td>
</tr>
<tr>
<td>FW variables standardization</td>
<td>Intel, MSFT</td>
</tr>
<tr>
<td>Bug tracking and GitHub source code control</td>
<td>Google, 9 Elements, OCP/Rajeev</td>
</tr>
<tr>
<td>HW requirements to comply to OSF boot</td>
<td>Two Sigma, MSFT</td>
</tr>
<tr>
<td>Security coding guidelines</td>
<td></td>
</tr>
</tbody>
</table>
OSF- Open EDKII Workstream

Gundrala Devender Goud/Director/Microsoft
Contributor(s): Vincent Zimmer/Sr.PE/Intel
Mallik Bulusu/Director/Microsoft
Background and UEFI FW progression....

- **Pre-year 2000**: Legacy BIOS

- **Year 2000**: Intel invented EFI & sample implementation under free BSD

- **Year 2004**: tianocore.org, open source EFI community launched

- **Year 2005**: Unified EFI (UEFI) Industry forum

- **Year 2017**: ~240 Major MNCs shipping UEFI platforms in IOT, mobile, Client and Server segments. Supports Microsoft Client/Server OS and different flavors of Linux OS.

- **Industry successfully transitioned from Legacy BIOS to UEFI FW**

- **Lot of maturity/stability and tech equity built into current UEFI FW**

Let's leverage UEFI learnings to Open System Firmware initiative.
Current State of UEFI FW implementation ...

Open EDKII workstream is expected to address current gaps and be cloud ready

Current Gaps:

- Not truly ‘Open’ - Commercial products with EDKII core based UEFI FW solutions still shipping with proprietary content
- Silicon/Chipset modules are not open
- Not Optimized for ‘Cloud’ Use Models
Open EDK II workstream plans and progress

Open EDK II workstream goals:
- Make complete tree open
- Support multi-silicon architectures and multi-OS.
- Standardize the HW ROT interfaces in SEC/PEI modules
- Support new ‘Silicon Interface Firmware module interfaces’ to open EDKII DXE core
- Simply Setup and make it OOB configurable
- Optimize the solution for Performance, Reliability, Serviceability, Scalability and Deployability.
- **Deliver initial open EDKII based tree to support Mt.Olympus HW - done**

Let’s together accelerate OSF development
Call for Action(s)

- Please attend weekly OCP/OSF calls
- Encourage each of you to bring-in your challenges, innovative ideas to OSF
- Contribute to workstreams->Great opportunity to showcase your passion in open system firmware development
- Identify additional workstreams, own them and drive solution
Questions?