LinuxCon Europe

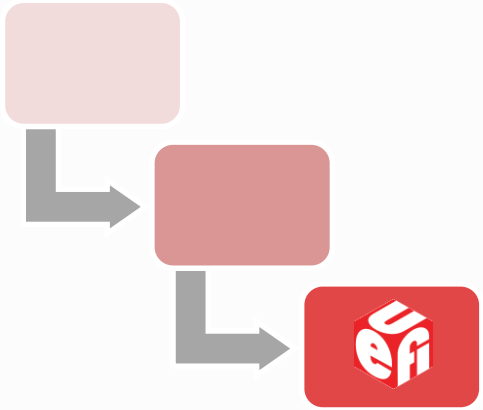
UEFI Mini-Summit

7 October 2015

Session 2 – What Linux Developers Need to Know About Recent UEFI Spec Advances

Jeff Bobzin, Insyde Software Corp.

Agenda



- **Overview - The UEFI Process**
- Some UEFI 2.5 Spec Highlights
  - System Firmware Versions Published
  - Security Profile Management at the Data Center
  - System Prep Applications
- Progress To Date
- Call to Action

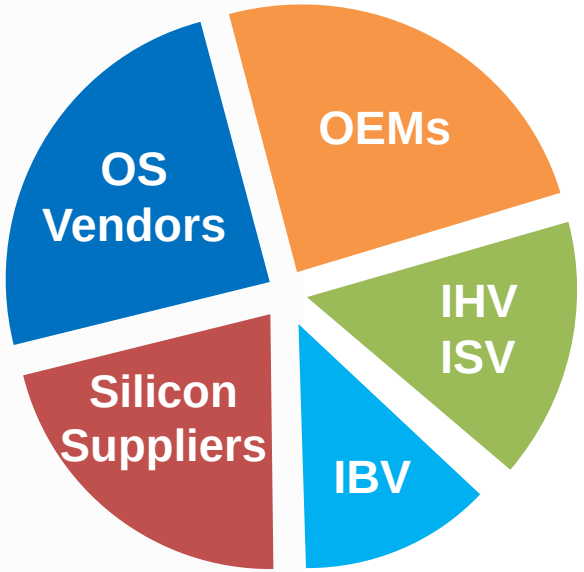
UEFI Content Builds From Wide Industry Participation

The UEFI Committee Agenda is Driven by Community Input

Cloud Operators

User Community

Enterprise

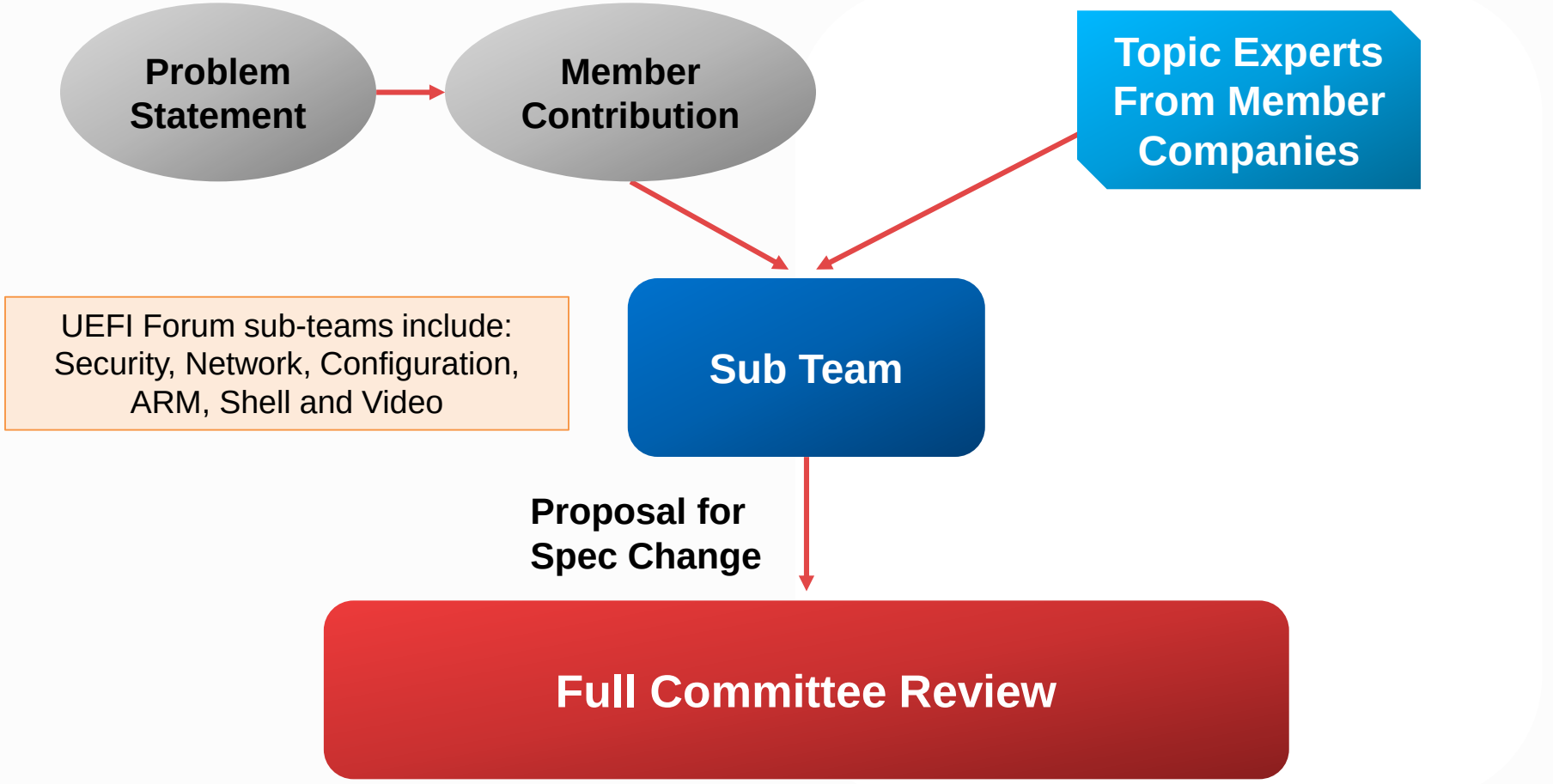


UEFI SPECS

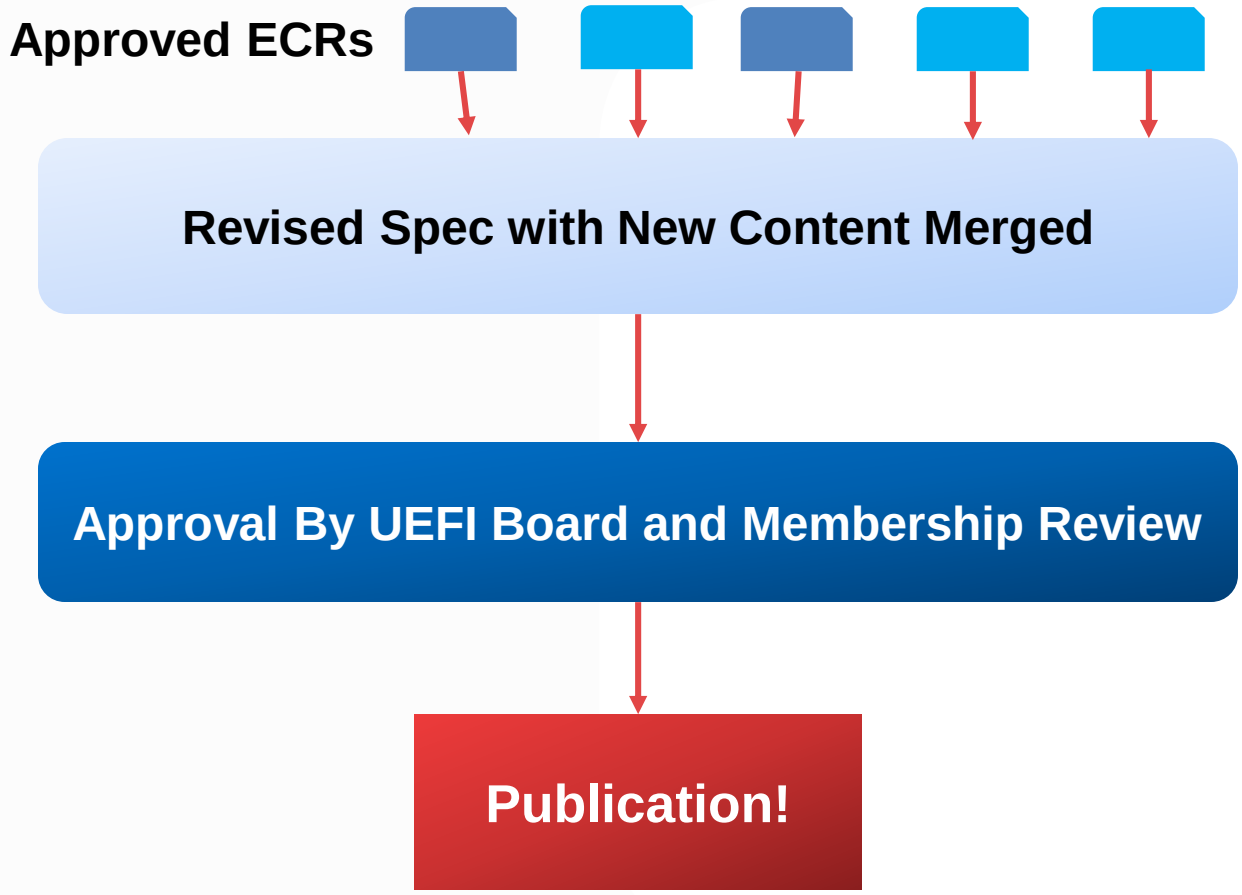
Some Messages UEFI Heard From The Ecosystem

1. PXE Boot too slow and unreliable
2. Field provisioning of Secure Boot security keys was awkward
3. Manual matching of firmware updates was too hard
4. UEFI did not support ISV needs for pre-OS tools like disk encryption

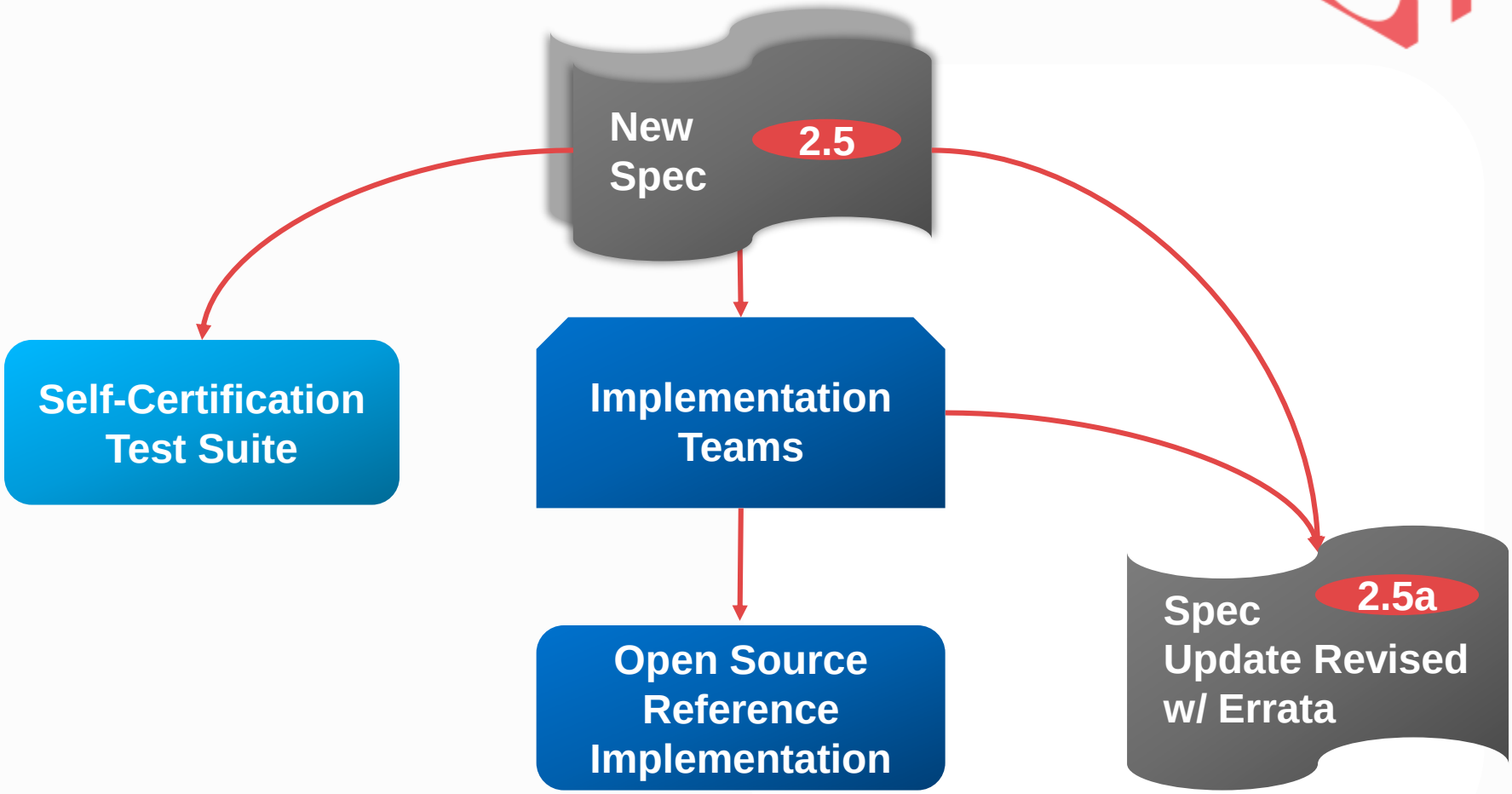
UEFI ‘ECR’ Process



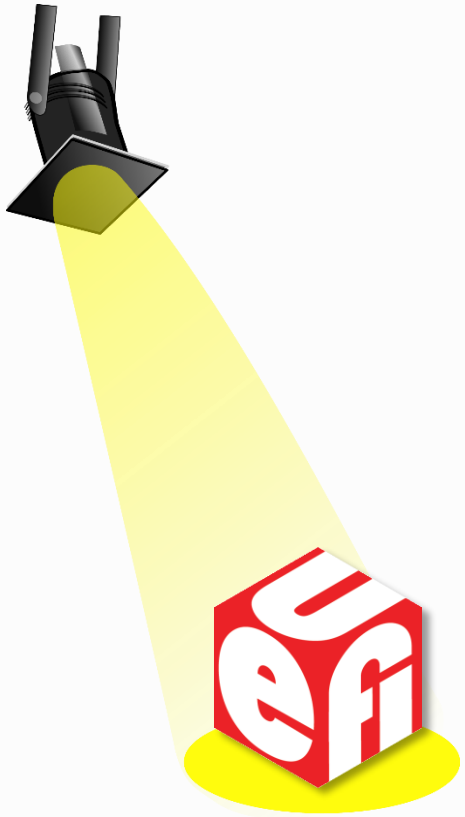
Spec Approval Process



After Publication



Agenda



- Overview - The UEFI Process
- **Some UEFI 2.5 Spec Highlights**
  - System Firmware Versions Published
  - Security Profile Management at the Data Center
  - System Prep Applications
- Progress To Date
- Call to Action

Deeper Review Of 3 Important New Elements

1. [New] Section 22.3, EFI System Resource Table
2. [New] Section 30.3.x Audit Mode and Deployed Mode
3. [New] Section 3.1.7 System Prep Applications

In Upcoming Session:

4. [New] Section 23.7.1 Boot from URL

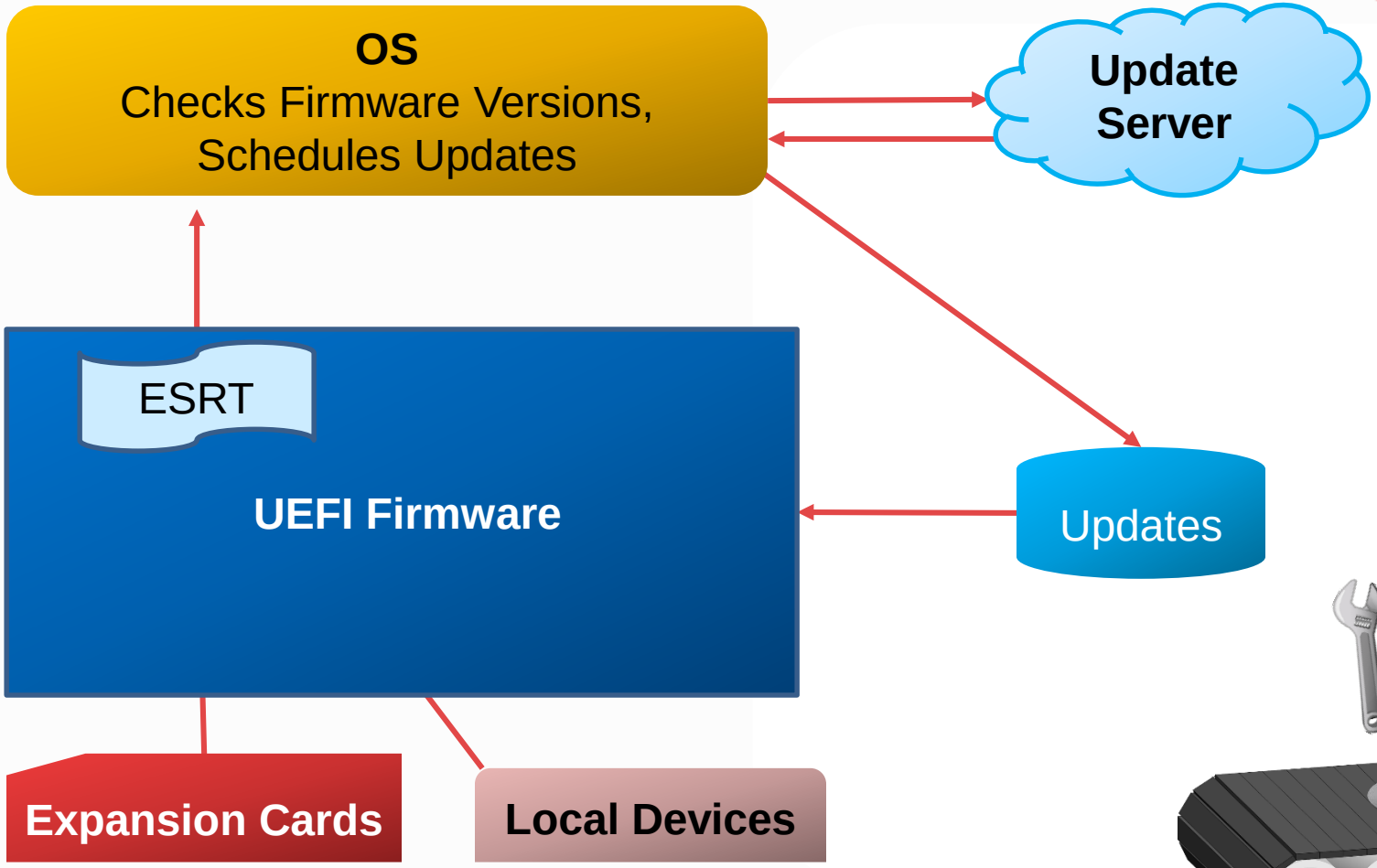
Agenda

- Overview - The UEFI Process
- **Some UEFI 2.5 Spec Highlights**
  - **System Firmware Versions Published**
  - Security Profile Management at the Data Center
  - System Prep Applications
- Progress To Date
- Call to Action

Enable System To Advertise Updatable Firmware

- UEFI 2.5 has added ESRT table
  - List of Firmware Elements
  - Identified by GUID and Version
  - Status of last update
- Expansion Boards are added to ESRT by platform and updated by Firmware Management Protocol

ESRT Allows Automation



Advantages Of ESRT-based Firmware Management

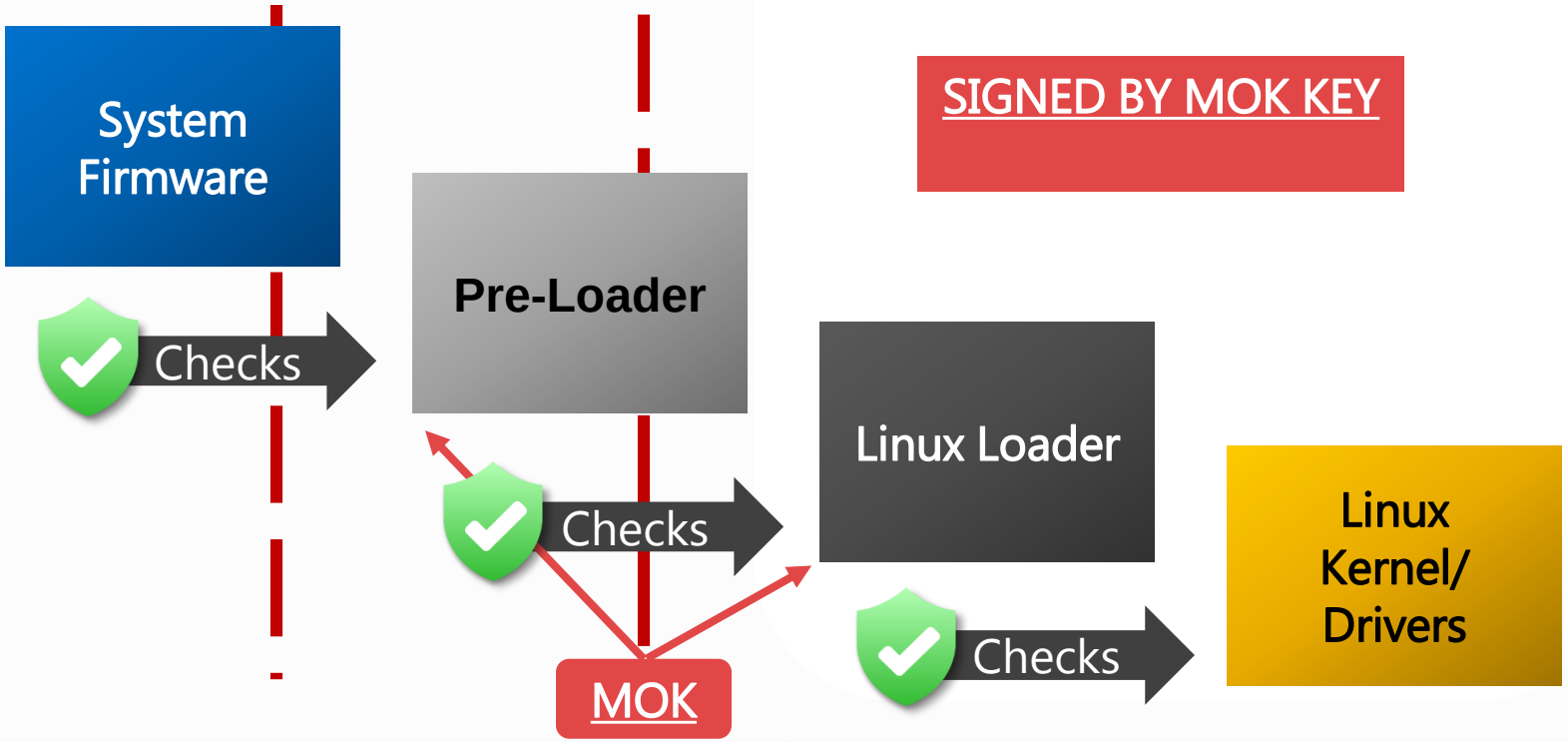
1. Move away from older proprietary schemes which require user learning for each platform or expansion board / vendor
2. OS able to easily confirm that correct (latest) versions are installed
3. Increased update participation will help to more quickly close any security flaws

Agenda

- Overview - The UEFI Process
- Some UEFI 2.5 Spec Highlights
  - System Firmware Versions Published
  - **Security Profile Management at the Data Center**
  - System Prep Applications
- Progress To Date
- Call to Action

Security Profile Management

- Secure Boot and its database of signing keys can protect every boot step



Provisioning Local Signing

- Some sites use local signing. Until UEFI 2.5, local key provisioning was a manual process with non-std. menus
- Hands on steps added greatly to the workload of setting up new server
- UEFI 2.5 adds new ‘Audit’ and ‘Deployed’ modes (these modes are security enforcement states)

Using Audit and Deployed Modes

- **Audit Mode**
  - OS can update security signing key lists and test the revised boot chain
  - Unbootable state is avoided
- **Deployed Mode**
  - Entered with OS is satisfied with key list
  - Most Secure Mode

Agenda

- Overview - The UEFI Process
- Some UEFI 2.5 Spec Highlights
  - System Firmware Versions Published
  - Security Profile Management at the Data Center
  - **System Prep Applications**
- Progress To Date
- Call to Action

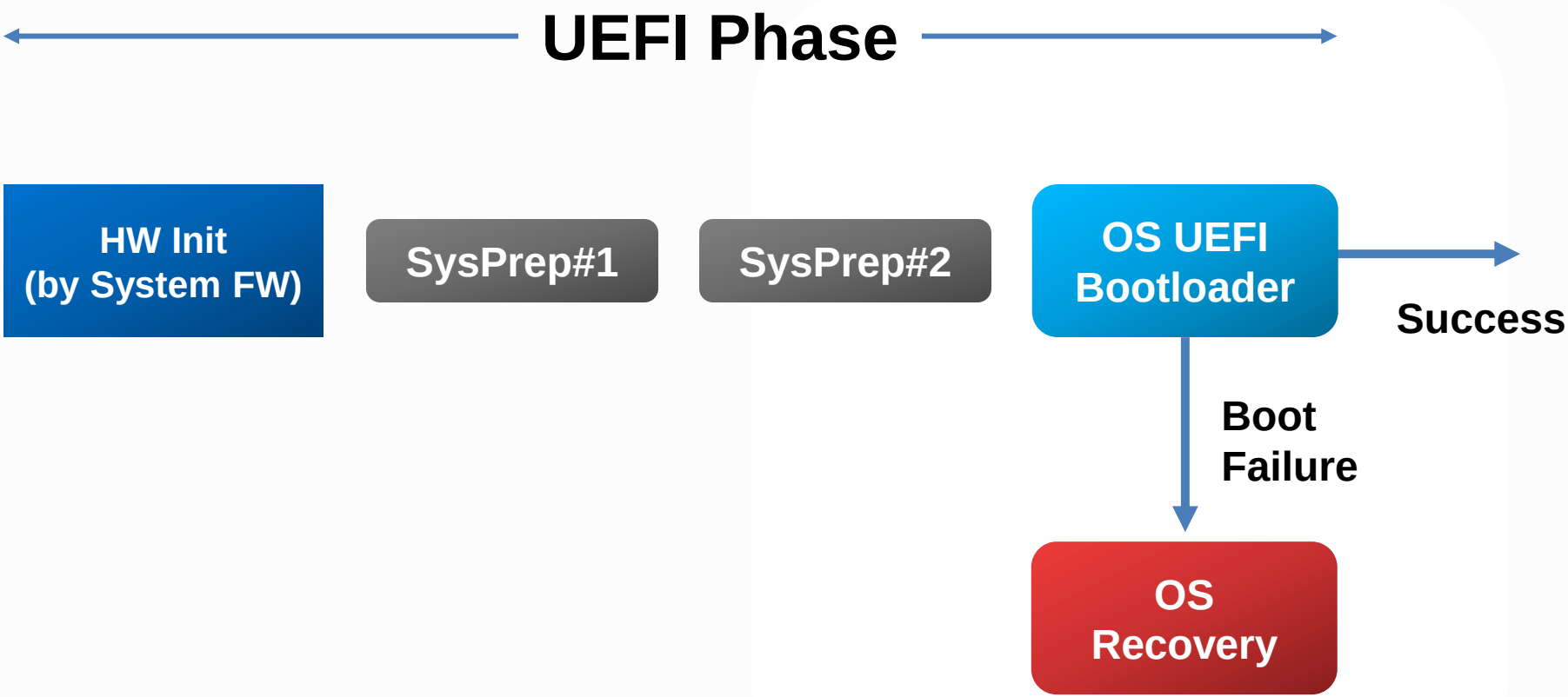
System Prep Applications

Problems we are solving:

1. Enable ISV Software that needs to run before OS to unlock encrypted disk (client and server)
2. Enable Firmware Version monitor/update when multiple OS are supported (enterprise/data center)
3. Pre-OS provisioning due to changing work-loads (data center)

- Why change was needed - Avoid war with OS over BootOrder – “OS always fights to be first”

Boot Timeline



Sys Resources Available

- System Prep can use same system resources as OS bootloader
  - Screen, Kbd, etc.
  - Network

- If a required device is not normally initialized by fast boot a new API is provided to request device be made operational for the App to use

Agenda

- Overview - The UEFI Process
- Some UEFI 2.5 Spec Highlights
  - System Firmware Versions Published
  - Security Profile Management at the Data Center
  - System Prep Applications
- **Progress To Date**
- Call to Action

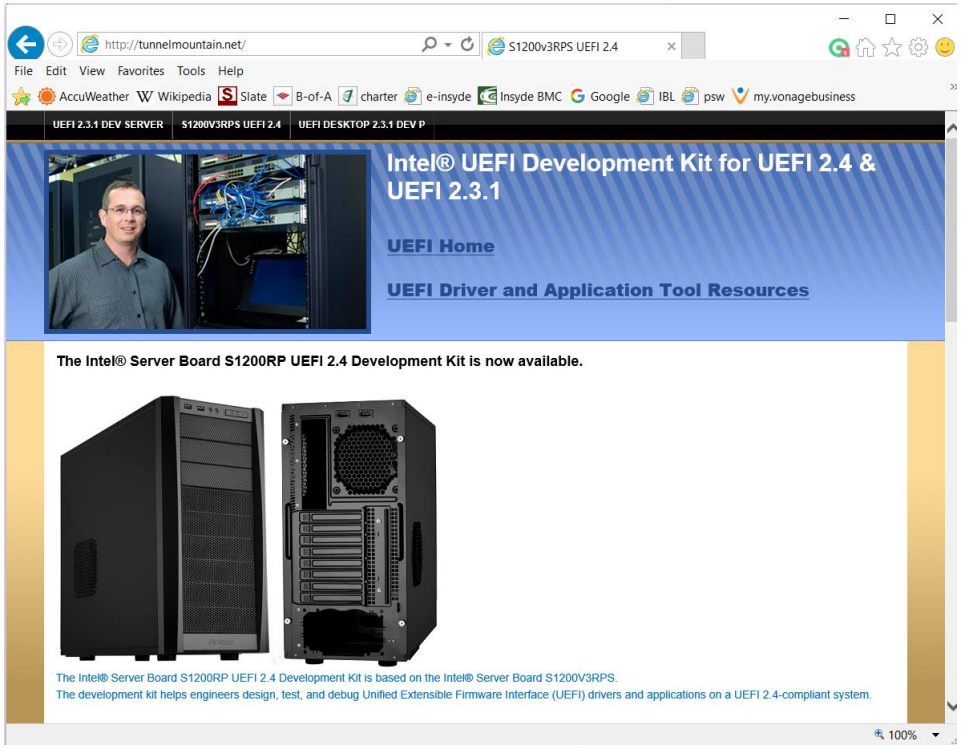
UEFI 2.5 Partial Feature List Implementation Status

UEFI 2.5 Item	Open Source Sys Firmware	OS Support
Boot from http *(details session 4)*	In final test	Ready to engage with OS teams
Boot from https	Scheduled	Currently in review/plan
ESRT Firmware Table	In final test, early versions shipping	Linux* & Windows have support, distribution path from OEM needs work
Security Profile Audit Mode	To be Scheduled	Time to review/plan
System Prep Applications	In final test	Ready to engage

* https://github.com/vathpela/linux-esrt

Development System

Purchase at www.tunnelmountain.net
($1399)



Note: UEFI 2.5 binary is not yet posted, still in test

Agenda

- Overview - The UEFI Process
- Some UEFI 2.5 Spec Highlights
  - System Firmware Versions Published
  - Security Profile Management at the Data Center
  - System Prep Applications
- Progress To Date
- **Call to Action**

We have heard from our user community, especially data center operators, about the improvements they need to streamline their operations. UEFI firmware is a good foundation for solutions, but only a foundation.

Requires:

- Cooperative and interactive development effort from IBVs, OEMs, distros, IHVs and...
- Feedback from the original requestors.

Let's figure out how to work together!

Interested In Joining?

www.uefi.org/membership

UEFI FW/OS Forum:
uefi.org/FWOSForum
A free public forum focused on firmware and O/S integration

USRT Security Issue Reporting:
uefi.org/security
A safe reporting site to inform the UEFI of any security issue or vulnerability based on firmware