presented by

Advancing Firmware Compliance Testing in the Arm Ecosystem

UEFI 2025 Developers Conference & Plugfest

Oct 10th, 2025

G Edhaya Chandran (Arm),
Samer El-Haj-Mahmoud (Arm)

Meet the Presenters

G Edhaya Chandran

Staff Engineer, Arm Ltd.

G Edhaya Chandran is a Staff Engineer at Arm Architecture and Technology Group (ATG). He contributes to the Arm System Standards specializing in firmware and represents Arm in the UEFI, ACPI, DMTF and other industry standards forums. He is the Arm maintainer of TianoCore edk2-test (UEFI-SCT) and chairs the UEFI Tests Working Group (UTWG) activities. He also contributes code to the TianoCore edk2 and FWTS and has an expertise in the Arm Architectural Compliance Suite (ACS), primary tool used in the Arm SystemReady compliance program

Meet the Presenters

Samer El-Haj-Mahmoud

Distinguished Engineer and System Architect, Arm Ltd.

Samer El-Haj-Mahmoud is a Distinguished Engineer and System Architect at Arm Architecture and Technology Group (ATG). He has 25 years of experience specializing in server system architecture, firmware, remote management, and industry standards. His current work focuses on Arm system architecture for servers and PCs. Samer has a long history of contribution to industry standards and related open-source projects, including the UEFI Forum, DMTF, OCP, CXL, UCIe, OpenBMC, TianoCore, and the Arm System Architecture Advisory Council (SystemArchAC).

Agenda

- Arm Firmware Compliance: Our initiatives. What is covered? What is tested?
- The tools
- UEFI-SCT improvements
  - UEFI Spec coverage
  - Trusted Platform Module (TPM), UEFI SecureBoot
- Firmware Test Suite(FWTS) improvements
  - ACPI spec coverage
  - Arm Secure Monitor Call Calling Convention (SMCCC)
  - Arm Power State Coordination Interface (PSCI)
- UEFI Test Work Group(UTWG) Community driven efforts

Arm Firmware Compliance: What is Tested?

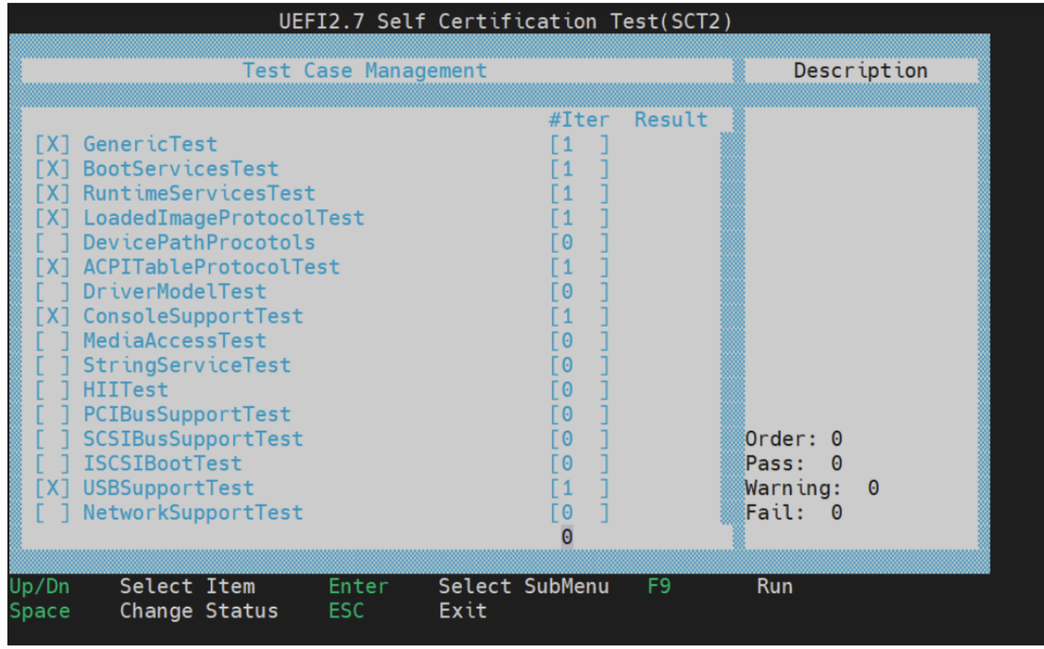
- Arm has been advancing the tests for firmware compliance as part of Arm SystemReady compliance program and Arm ACS (Architecture Compliance Suites)
  - Chairing the UEFI Test Work Group (UTWG),
  - Maintainer-ship of EDK2-test
  - Code contributions to Firmware Test Suite (FWTS).
- The compliance suites test the interfaces for UEFI (including Secure Boot), ACPI, SMBIOS, TPM TCG protocols, and Arm firmware interfaces
- The requirements for these interfaces feature in the Arm Base Boot Requirements (BBR) and Arm Base Boot Security Requirements (BBSR) specifications.
- This presentation will focus on the recent advancements done in the coverage and the future roadmap

Device Tree

Trusted Firmware - A

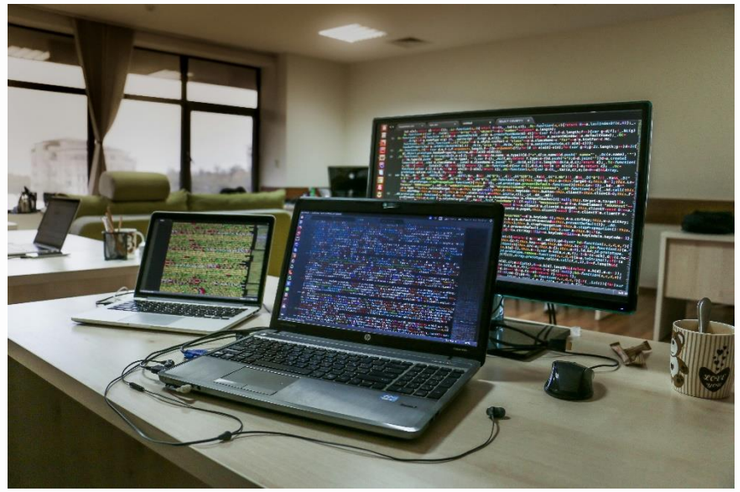
The Tools: EDK2-Test and UEFI-SCT

- EDK2-Test : test infrastructure for EDK2-based firmware.
  - Part of TianoCore - open-source reference implementation of UEFI.
- EDK2-Test includes various sub-projects and components
  - UEFI Self-Certification Test (SCT) - implementations conformance to UEFI specifications.
- UEFI-SCT is a
  - Cross-platform firmware test environment
  - Test harness for executing built-in UEFI spec compliance tests.
  - Scope for integrating user-defined tests.
  - Built and run as an UEFI Shell App
- Latest version of EDK2-test :
- https://github.com/tianocore/edk2-test/releases/tag/edk2-test-stable202509



The Tools: FWTS

- **FWTS** : **Firmware Test Suite**
- Open-source, Linux-based tool, developed and maintained by Canonical
- Performs sanity checks to validate system firmware implementations, including
  - BIOS/UEFI
  - ACPI tables
  - CPU configuration
  - PCI/PCIe setup
  - Power management
  - Security features (e.g., TPM2)
  - And other firmware interfaces (SMCCC, PSCI etc)



- The latest UEFI Test Work Group (UTWG) verified version is here: https://fwts.ubuntu.com/release/fwts-V25.01.00.tar.gz

UEFI-SCT and FWTS in Arm SystemReady

- UEFI-SCT and FWTS are leveraged, customized and automated to run within the Arm SystemReady ACS
- Collectively called: BBR-ACS.
- UEFI-SCT is customized with additional tests which perform **Arm specific** checks and assertions, and this suite is run with specific sequence files.
- A **sequence file** is a configuration to the UEFI-SCT and represents the selection of tests to be run

Sequence file	Link	Documentation
SBBR.seq	https://github.com/ARM-software/bbr-acs/blob/main/sbbr/config/SBBR.seq	https://github.com/ARM-software/bbr-acs/blob/main/docs/SBBR_recipe_testlist.md
BBSR.seq	https://github.com/ARM-software/bbr-acs/blob/main/bbsr/config/BBSR.seq	https://github.com/ARM-software/bbr-acs/blob/main/docs/BBSR_recipe_testlist.md
EBBR.seq	https://github.com/ARM-software/bbr-acs/blob/main/ebbr/config/EBBR.seq	https://github.com/ARM-software/bbr-acs/blob/main/docs/EBBR_recipe_testlist.md

UEFI-SCT and FWTS in Arm SystemReady

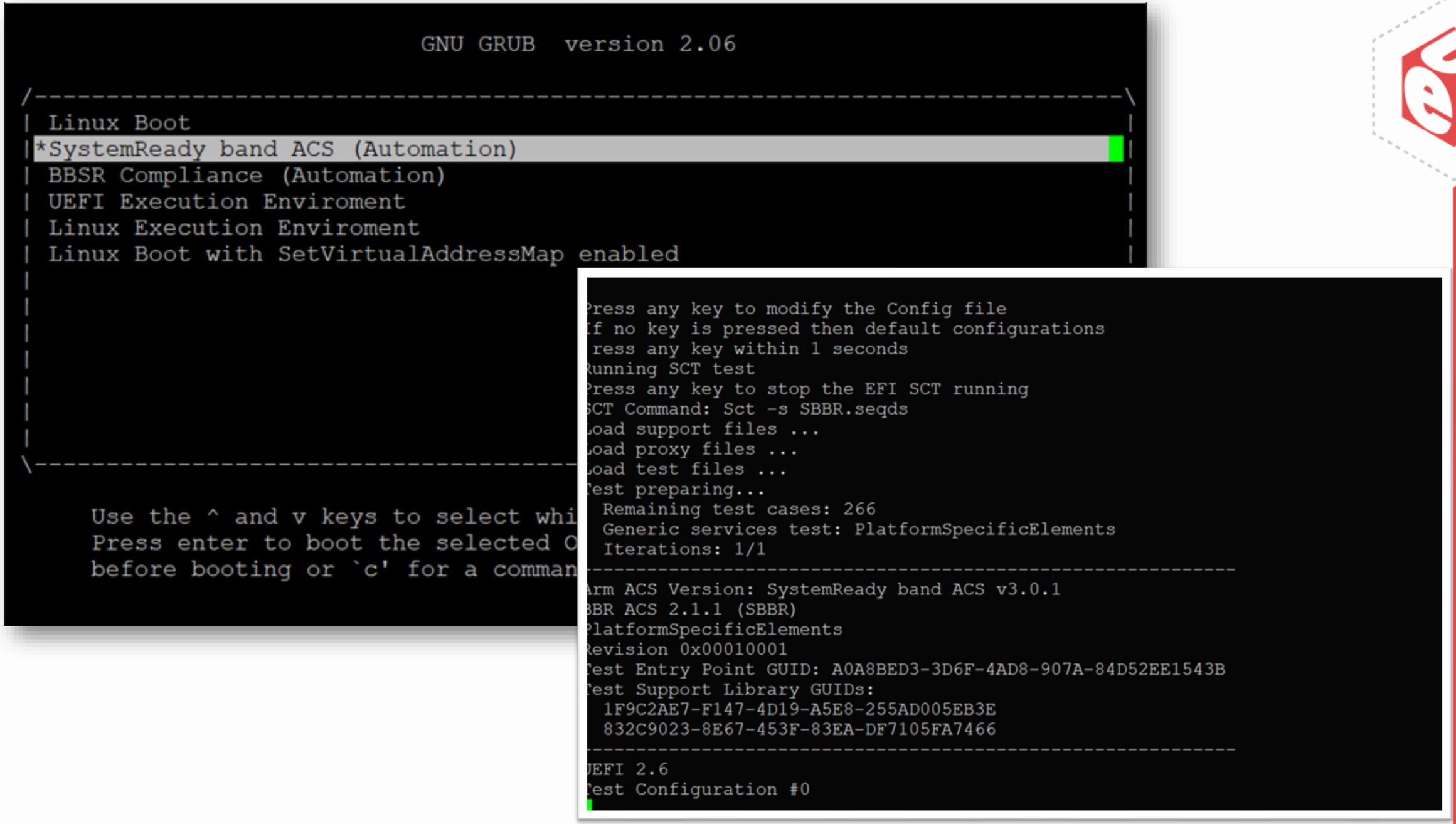
FWTS is customized in the Arm Base Boot Requirements (BBR) ACS is run with the **--sbbr** and **--ebbr** switches which select specific set of suites to be run

SBBR run:

```
sudo fwts  -r stdout -q --uefi-set-var-multiple=1 --uefi-get-mn-count-multiple=1 --sbbr esrt uefibootpath aest cedt slit srat hmat pcct pdtt bgrt bert einj erst hest sdei nfit iort mpam ibft ras2
```

EBBR run:

```
sudo fwts --ebbr
```


GNU GRUB version 2.06
Linux Boot
*SystemReady band ACS (Automation)
BBSR Compliance (Automation)
UEFI Execution Enviroment
Linux Execution Enviroment
Linux Boot with SetVirtualAddressMap enabled
Use the ^ and v keys to select whi
Press enter to boot the selected O
before booting or `c' for a comman
ress any key to modify the Config file
f no key is pressed then default configurations
ress any key within 1 seconds
unning SCT test
ress any key to stop the EFI SCT running
CT Command: Sct -s SBBR.seqds
oad support files ...
oad proxy files ...
oad test files ...
est preparing...
Remaining test cases: 266
Generic services test: PlatformSpecificElements
Iterations: 1/1
rm ACS Version: SystemReady band ACS v3.0.1
BR ACS 2.1.1 (SBBR)
PlatformSpecificElements
evision 0x00010001
est Entry Point GUID: A0A8BED3-3D6F-4AD8-907A-84D52EE1543B
est Support Library GUIDs:
1F9C2AE7-F147-4D19-A5E8-255AD005EB3E
832C9023-8E67-453F-83EA-DF7105FA7466
EFI 2.6
est Configuration #0

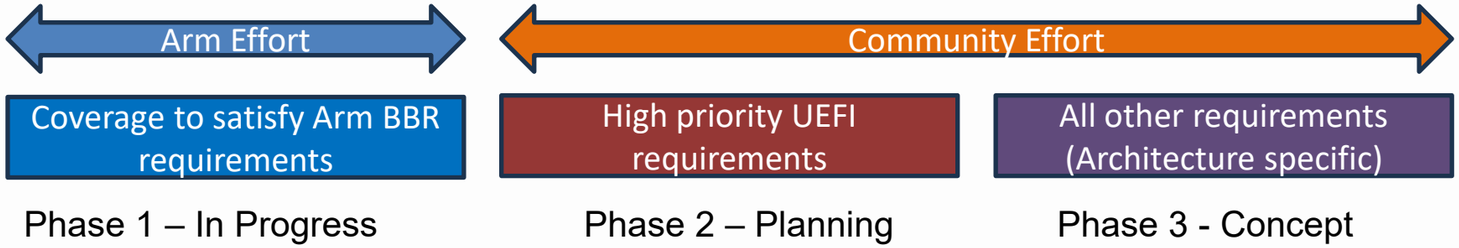
UEFI-SCT Improvements

Test Coverage for UEFI v2.7B to v2.11

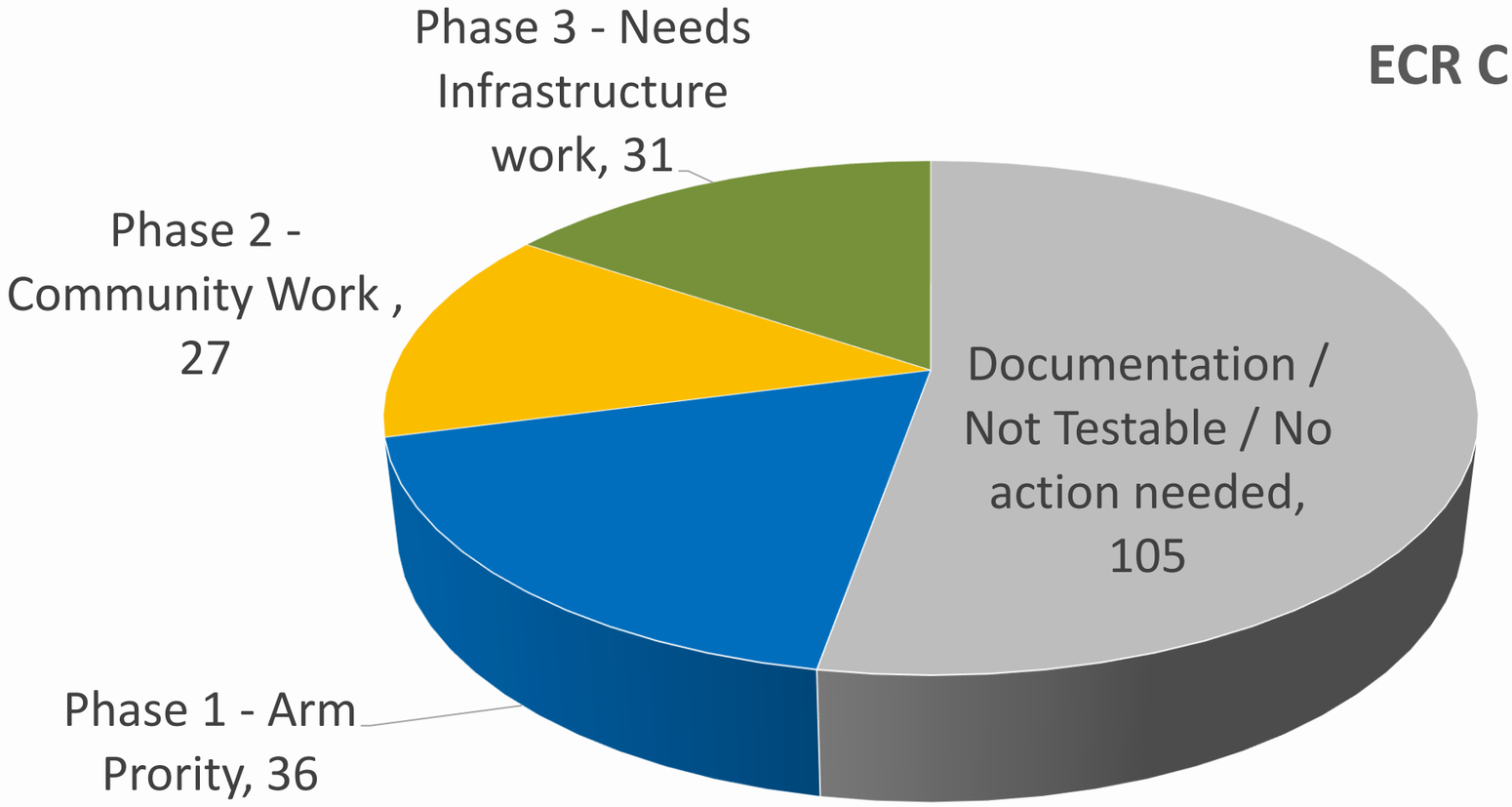
- UEFI-SCT formally satisfies UEFI spec version 2.7A (2018) – big gap with latest UEFI v2.11.
- Arm's analysis to identify new tests and scenarios, focusing on Arm-BBR specification rules.
- A total of 199 ECRs (Engineering Change Requests) between UEFI 2.7B → 2.11 were analyzed:
  - Is it feasible to implement in EDK2-test?
  - Infrastructure needed to develop a test exists in upstream EDK2?
    - If yes, priority assigned, initial estimate and scenario number.
  - Identify the items that need community contribution
  - Is the ECR applicable to Arm BBR? – If yes, implement in Phase 1
- An overview of this task was presented in the UTWG Plenary meeting.

Phases of Implementation

- **Phase 1 : Arm Priority**
  - Directly relates to Arm BBR/BBSR requirements.
  - High priority to Arm Architecture Compliance Suite.
  - Implementation in progress by Arm
- **Phase 2 : High priority UEFI - Community work**
  - EDK2 Infrastructure exists.
  - Tests in EDK2-test may be implemented with low to medium effort by the community.
- **Phase 3: Needs Infrastructure/Architecture specific**
  - May need EDK2 Infrastructure development (Some of these may be Arm BBR requirements).
  - Architecture specific RISCV/LoongArch etc.
  - Beyond present scope of EDK2-test.



Phases of Implementation



[Link to the Analysis published in the UTWG wiki]

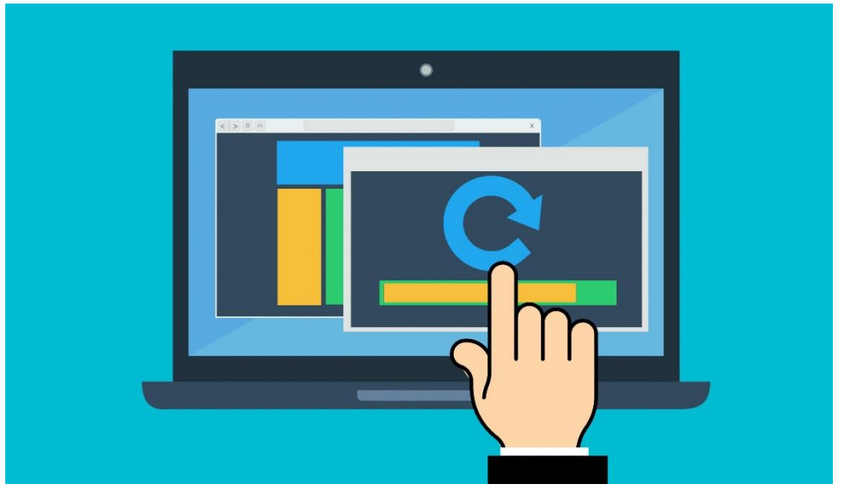
New Tests Contributions

Process

- New scenarios identified are added to SCT-test-case-spec and sent for community review
- After approval, GitHub Pull Request (PR) for test code are raised.
- Test code is discussed in EDK2-test meetings and approved by EDK2-test maintainers

Progress so far (Sept 2025)

- 8 New test scenarios implemented, covering:
  - GetVariable()
  - Adaptor Information
  - Firmware Management Protocol
  - EFI PROPERTIES TABLE
  - SimpleTextProtocolEx
- Detailed list of new tests is here



New Tests Contributions

is:issue New test coverage | Labels | Milestones | New issue

Open 3 | Closed 3 | Author | Labels | Projects | Milestones | Assignees | Types | Newest

- [Feature]: [New Test Coverage] Test EFI_ADAPTER_INFORMATION_PROTOCOL.GetInformation for EFI_NOT_FOUND type:feature-request
  #278 · edhay opened 3 weeks ago
- [Feature]: [New test coverage] Test GetVariable functionality of getting only the Attributes of the variable type:feature-request
  #260 · edhay opened on Jun 3 — 1
- [Feature]: [New test coverage] New cases for EFI_INVALID_PARAMETER for EFI_FIRMWARE_MANAGEMENT_PROTOCOL.GetImageInfo() type:feature-request
  #259 · by edhay was closed last week — 2
- [Feature]: [New test coverage] ReadKeyStrokeEx() check for KeyData.KeyState for EFI_NOT_READY return type:feature-request
  #258 · edhay opened on Jun 3
- [Feature]: [New test coverage] Test coverage for EFI_RT_PROPERTIES_TABLE UEFI v2.8 type:feature-request
  #256 · by edhay was closed on Jun 5 — 1
- [Feature]: [New test coverage] Add two new tests for GetImageInfo() in FirmwareManagementBBTestConformance type:feature-request
  #252 · by edhay was closed on May 21 — 5

New UEFI SecureBoot Tests

- New set of test covering UEFI SecureBoot (UEFI spec Section 32, mapped to Arm BBSR specifications)
- Documentation for the new tests on TianoCore here and here

Test Suite	Coverage
VariableAttributes	Validates the attributes (e.g., non-volatile, authenticated write access) of the Secure Boot variables: PK, KEK, db, dbx.
VariableUpdates	Tests runtime update paths for Secure Boot variables to ensure UEFI-enforced access control policies are in place.
ImageLoadingTest	Verifies image authentication and signature validation mechanisms during UEFI boot.

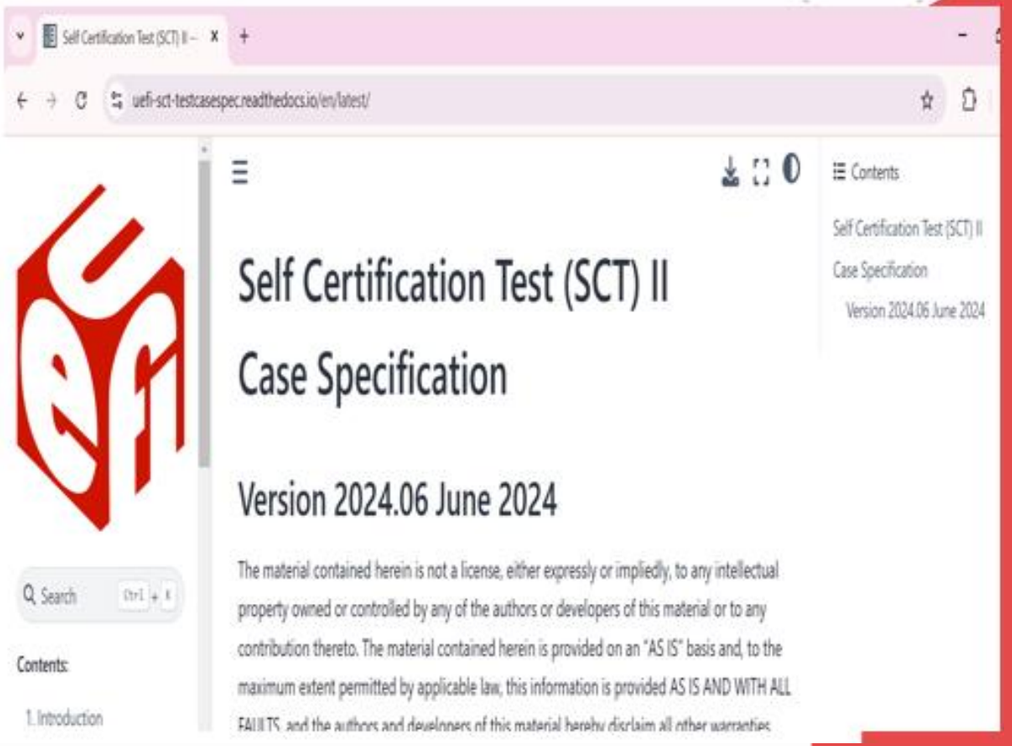
TCG2 Protocol Interface Tests

- New test coverages were added in UEFI-SCT to test TCG2 protocol interfaces
  - add test infrastructure and GetCapability Test
  - add header with TCG2 protocol definitions
  - add SubmitCommand test
  - add GetEventLog test
  - add HashLogExtendEvent test
  - add GetActivePcrBanks test
  - Platform Reset Check Test

- The tests are available here:
  https://github.com/tianocore/edk2-test/tree/master/uefi-sct/SctPkg/TestCase/UEFI/EFI/Protocol/TCG2/BlackBoxTest
  Documentation: https://uefi-sct-testcasespec.readthedocs.io/en/latest/31_TCG2_Protocol.html

Other Efforts by Arm

- The UEFI-SCT test case was updated for the latest tests and converted to markdown for integration and easy maintenance in the GitHub
- The spec is made available online: https://uefi-sct-testcasespec.readthedocs.io/en/latest/



- Arm developed the mechanism to enable automated GitHub PR review and approval is in progress. These are on the lines of automation developed for EDK2 GitHub

Firmware Test Suite (FWTS) Improvements

FWTS and ACPI 6.6

- Firmware Test Suite (FWTS) is the primary tool used to verify ACPI compliance
- Latest version FWTS v25.07.00 integrated into the Arm SystemReady ACS and covers ACPI v6.6
- FWTS is also used to test:
  - Devicetree related compliance (**`dt_base`**)
  - UEFI runtime compliance **(`uefirttime, uefirtvariable`)**
  - SMBIOS compliance
  - PSCI Compliance etc.

FWTS and Arm ACPI Tables

- FWTS is now improved to test the Arm ACPI tables
  - tables either specific to or used widely on Arm systems
  - See Arm BBR Specification.
- Each table has its own test and can be invoked in FWTS as follows:
  - Example, to invoke the AEST suite

```
sudo fwts aest
```

ACPI Table	Table Name
AEST	Arm Error Source Table
PCCT	Platform Communications Channel Table
SDEI	Software Delegated Exception Interface
IORT	Input Output Remapping Table
RAS2	Reliability Availability and Serviceability 2 Table
APMT	Arm Performance Monitoring Unit
MPAM	Memory System Resource Partitioning and Monitoring
AGDI	Arm Generic Diagnostic Dump and Reset Device Interface

FWTS and Arm SMC Interfaces

- Arm Secure Monitor Call (SMC) is a software-triggered instruction that causes the processor to switch from the Normal World to the Secure World, via the Secure Monitor.
  - Defined in Arm SMC Calling Convention (SMCC) specification + extensions specifications
- New FWTS tests added for SMC functionality
- Tests SMC functions, receive the results, and interpret according to spec

```
fwts smccc
```

Function Tested	Description
ARM_SMCCC_VERSION	Queries the SMCCC version implemented
ARM_SMCCC_ARCH_FEATURES	To check if a particular Arm SMCCC function is implemented
ARM_SMCCC_ARCH_SOCID	Used to obtain the SiP defined SoC identification details SoC_ID_type = 0 (SoC version) SoC_ID_type = 1 (SoC Revision)

FWTS and Arm PSCI Interfaces

- Power State Coordination Interface (PSCI) is a firmware standard to manage power states in systems based on Arm architecture
- PSCI is a set of SMC interfaces that allow OSes to control the power states of CPUs and other system components in a standard way.
- Defined in *Arm Power State Coordination Interface*
- New FWTS PSCI interface tests implemented

```
fwts psci
```

Function Tested	Test Description
PSCI support check	Check if PSCI is supported as per ACPI FADT table
PSCI_VERSION	Query the version of PSCI implemented
PSCI_FEATURES	Detect the PSCI functions and their properties PSCI_VERSION CPU_SUSPEND CPU_OFF CPU_ON AFFINITY_INFO MIGRATE MIGRATE_INFO_TYPE MIGRATE_INFO_UP_CPU SYSTEM_OFF SYSTEM_RESET PSCI_FEATURES CPU_FREEZE CPU_DEFAULT_SUSPEND NODE_HW_STATE SYSTEM_SUSPEND PSCI_SET_SUSPEND_MODE PSCI_STAT_RESIDENCY PSCI_STAT_COUNT SYSTEM_RESET2 MEM_PROTECT MEM_PROTECT_CHECK_RANGE SYSTEM_OFF2
psci_features_bbr_check	Check if BBR mandated PSCI functions are implemented. Enabled only with --sbbr or –ebbr
AFFINITY_INFO	Request the status of an affinity instance of a processing element

UEFI Test Work Group (UTWG) Community Driven Efforts

UTWG Community Driven Efforts

- As part of UEFI Test Work Group (UTWG) activities, FWTS version 25.01.00 was formally verified and declared as the ACPI v6.5 self certification test suite
  - Test results of all architectures are here: UEFI - FWTS v25.01.00 Test Results

- UEFI-SCT stable release EDK2-test-stable202509 is published.
  - The release verification was carried out on 16 different boards of various architectures (AARCH64, X64 Intel, X64 AMD, RISC-V, LoongArch)
  - Test results of all architectures are here: UEFI - edk2-test-stable202509

Call for Action!

- Join UTWG Forum, a working group under UEFI.org
  - Register at UEFI.org and join the UTWG sub-group : UEFI - Register for an account
- Attend the monthly UTWG meetings
  - UEFI - UTWG Calendar – Discuss forum activities, releases, open issues, collaboration.
  - Current active participants: Arm(Chair), AMD, Intel, Phoenix, Dell
- Attend monthly community edk2-test bug triage meetings
  - devel@edk2.groups.io | Calendar
  - Engineering meeting for Pull Requests, issues and release activities of UEFI-SCT
  - Active participants: Arm (maintainer, reviewers), AMD (maintainer, reviewers), Intel (reviewers), Phoenix, Dell
- Review the issues and Pull Requests https://github.com/tianocore/edk2-test and
- Participate in the FWTS community
  - https://github.com/fwts/fwts and https://wiki.ubuntu.com/FirmwareTestSuite
- Contribute code and help in filling firmware compliance testing gaps!

References

- Arm SystemReady Compliance Program
- EDK2-Test: New Test Coverages and Future Roadmap – UEFI Virtual PlugFest Feb'2025
- Arm BBR ACS
- Arm SystemReady ACS

Related Presentations in this conference:

- Evolving ACPI Standards for Arm Systems: Advancements in Specification and Implementation - Samer El-Haj-Mahmoud(Arm) & Jose Marino (Arm)
- Integrate Arm SystemReady Band – UEFI and ACPI Compliance for Better Quality and Faster Debug – Sunny Wang (Arm)
- Arm System Firmware Architecture - Dong Wei (Arm)

Questions?

Also available for chat offline