Self-Certification Tests (SCTs) in UEFI World

Fall 2017 UEFI Seminar and Plugfest
October 31 – November 3, 2017
Eric Jin (Intel Corporation)
Alex Hung (Canonical, Ltd)
Agenda

- Introduction to SCTs
- UEFI SCT
- PI SCT
- ACPI SCT
- Q&A
Introduction to SCTs
Self-Certification Tests (SCTs)

- Toolsets for firmware developers to validate the implementation for the specification compliance.
  - UEFI SCT - UEFI Spec
  - PI SCT - PI Spec
  - ACPI SCT (FWTS) - ACPI Spec
- The official or recommended versions are available on www.uefi.org/testtools
UEFI SCT
UEFI SCT

• Current stable version is UEFI 2.5 A SCT
• UEFI 2.6 A SCT is coming soon
• UEFI 2.7 SCT Alpha for Taipei Plugfest
• The components
  ✓ UEFI SCT – focus on the platform/system
  ✓ IHV SCT – focus on the device/driver
  ✓ SCRT – focus on runtime service address conversion
  ✓ EMS – focus on the network stack
UEFI SCT Framework

Test Manager on OS Side

- GUI
  - Testcase Management
  - Testcase IDE
  - Communication Configuration

- Script Interpreter
  - Extend TCL Interpreter

- Core
  - Remote EFI Interface Invocation
  - Network Packet Utility
  - Log Utility
  - Customer Defined Utility

Traffic Layer

- Message Exchange Service on Ethernet

Test Agent on UEFI Side

- EFI Interface
  - EFI Protocols
  - Runtime Services
  - Boot Services

- Agent Core
  - Local EFI Interface Invocation
  - Testcase Management Utility
  - Agent UI Utility
  - EFI Test APP Utility
  - Customer Defined Utility

UEFI Plugfest – October 2017

www.uefi.org
UEFI SCT Execution

• Execution Environments
  ✓ UEFI Shell 1.x/2.x
  ✓ SSD with 1GB free space (recommend)

• Execution Methods
  ✓ Command line interface with configurable sequence
  ✓ Menu-driven interface with hierarchical category

• Execution Modes
  ✓ Native mode – execution on the single system
  ✓ Passive mode – execution on the host/target machine
Native Execution Demo
Passive Execution Demo
### UEFI SCT Result

#### UEFI2.6 Self Certification Test (SCT2)

<table>
<thead>
<tr>
<th>MiscBootServicesTest</th>
<th>Description</th>
<th>#Iter</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>CalculateCrc32_Conf</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>CalculateCrc32_Func</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>CopyMem_Func</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>GetNextMonotonicCount_Conf</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>GetNextMonotonicCount_Func</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>InstallConfigurationTable_Conf</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>InstallConfigurationTable_Func</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>SetMem_Func</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>SetWatchdogTimer_Conf</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>SetWatchdogTimer_Func</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
<tr>
<td>Stall_Func</td>
<td></td>
<td>1</td>
<td>PASS</td>
</tr>
</tbody>
</table>

### Navigation Keys
- **Up/Down** Select Item
- **Space** Change Status
- **Enter** Select SubMenu
- **F9** Run
- **ESC** Exit
<table>
<thead>
<tr>
<th>Service\protocol Name</th>
<th>Total</th>
<th>Failed</th>
<th>Passed</th>
</tr>
</thead>
<tbody>
<tr>
<td>BootServicesTest\MiscBootService</td>
<td>132</td>
<td>0</td>
<td>132</td>
</tr>
<tr>
<td>DevicePath\Protocols\DevicePath</td>
<td>62</td>
<td>61</td>
<td>1</td>
</tr>
<tr>
<td>DevicePath\Protocols\DevicePath</td>
<td>64</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>DevicePath\Protocols\DevicePath</td>
<td>52</td>
<td>52</td>
<td>0</td>
</tr>
<tr>
<td>DevicePath\Protocols\DevicePath</td>
<td>21</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>DevicePath\Protocols\DevicePath</td>
<td>34</td>
<td>19</td>
<td>15</td>
</tr>
<tr>
<td>GenTest\ EFICompliantTest</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Total service\Protocol</td>
<td>360</td>
<td>19</td>
<td>341</td>
</tr>
</tbody>
</table>

**CheckPoint Guid**

<table>
<thead>
<tr>
<th>DevicePath</th>
<th>CheckPoint Guid</th>
<th>LogFileName</th>
</tr>
</thead>
<tbody>
<tr>
<td>F0BA4E6B-5B85-4</td>
<td>5B855127-720D-4-1A2</td>
<td>LogFileName: LineNum</td>
</tr>
<tr>
<td>0A0ABBE3-3C9D-4A4B-907A-84D52E1543B</td>
<td>0A0ABBE3-3C9D-4A4B-907A-84D52E1543B</td>
<td>LogFileName: LineNum</td>
</tr>
</tbody>
</table>

**SourceFilename**

<table>
<thead>
<tr>
<th>DevicePath</th>
<th>SourceFilename: LineNum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0A0ABBE3-3C9D-4A4B-907A-84D52E1543B</td>
<td>SourceFilename: LineNum</td>
</tr>
</tbody>
</table>

**LogFile**

<table>
<thead>
<tr>
<th>DevicePath</th>
<th>LogFileName</th>
</tr>
</thead>
<tbody>
<tr>
<td>0A0ABBE3-3C9D-4A4B-907A-84D52E1543B</td>
<td>LogFileName: LineNum</td>
</tr>
</tbody>
</table>

---

**UEFI Plugfest – October 2017**

www.uefi.org
InstallConfigurationTable_Conf_0_0_E00A6879(AF7E-423E-8D1-EE9E71D721).log

---

Revision 0x00010001
Test Entry Point GUID: E00A6879-AF7E-423E-8D1-EE9E71D721
Test Support Library GUID: "1F9C2A87-F347-4D15-ABEB-2C540D95E9E3"

UEFI 2.6
Test Configuration #0

Consistency Test for InstallConfigurationTable

Logfile: "SCTLog\MiscBootServicesTest\MiscBootServicesTest\InstallConfigurationTable_Conf_0_0_E00A6879-AF7E-423E-8D1-EE9E71D721.log"
Test Started: 09/18/17 04:25p

BS.InstallConfigurationTable - Guid is NULL -- PASS
12055F2-8EC3-4D15-ABEB-2C540D95E9E3
"c:\\workspace\\Scptk\\TestCase\\UEFI\\MiscBootServices\\MiscBootServices\BlackBoxTest\\MiscBootServices87TestConformance.c:199:Status - Invalid Parameter"

BS.InstallConfigurationTable - Guid is not present -- PASS
7A9BCF-452C-4D15-ABEB-2C540D95E9E3
"c:\\workspace\\Scptk\\TestCase\\UEFI\\MiscBootServices\\MiscBootServices\BlackBoxTest\\MiscBootServices87TestConformance.c:223:Status - Not Found"

Returned Status Code: Success

InstallConfigurationTable_Conf: [PASSED]
Passes: 2
Warnings: 0
Errors: 0

UEFI 2.6
Revision 0x00010001
Test Entry Point GUID: E00A6879-AF7E-423E-8D1-EE9E71D721

Logfile: "SCTLog\MiscBootServicesTest\MiscBootServicesTest\InstallConfigurationTable_Conf_0_0_E00A6879-AF7E-423E-8D1-EE9E71D721.log"
Test Finished: 09/18/17 04:25p
Elapsed Time: 00 Days 00:00:00
EMS Result
Getting Source Code

• Provide your github account to admin@uefi.org and ask for the access permission

• Download the code
  ✓ git clone https://www.github.com/UEFI/UEFI-SCT.git

• Compile and build
  ✓ Refer to the instruction in HowToBuild
Support and Contact

• Support
  ✓ Email utwg@uefi.org, CC project maintainers eric.jin@intel.com supreeth.venkatesh@arm.com

• Information
  ✓ Subscribe to UTWG mail list (utwg@uefi.org)
  ✓ Attend UTWG meetings
PI SCT
PI SCT

• Test PI Spec Compliance, including PEI/DXE phase.
• Current stable version is PI 1.4 SCT.
• Next release will be PI 1.6 SCT on the Q2, 2018.
• The components
  ✓ PEIM test
  ✓ DXE test
  ✓ SMM test
PEI Test

- PEI test cases are designed as PEIMs and built in flash image
- Test PEIMs are dispatched and test log are saved in HOBs
- One Shell app parses the HOBs to generate the test result
DXE Test

- DXE test is a series of DXE test drivers plus dependency
- User can give the input thru the configuration files
- DXE test result is displayed on the Menu-driven UI directly
- Log files are provided to record execution details
SMM Test

- SMM SCT is comprised of two parts
  - The SMM test entry point invoked by the DXE driver
  - The corresponding SMM test driver is loaded into SMRAM during boot
- SMM test driver is built into flash with platform SMM drivers
- Test SMI handlers are registered into SMRAM
- Shell application retrieves the test result from buffers
Getting PI SCT

- The related document/binary/source can be downloaded from [https://sourceforge.net/projects/pi-sct/](https://sourceforge.net/projects/pi-sct/)
- Please refer to the GetStarted and UserGuide for the usage and build instructions
Support and Contact

Please email project administrators

Jie.lin@intel.com
laurie.jarlstrom@intel.com
Firmware Test Suite

- FWTS 15.08.00 was recommended as the ACPI 5.1 SCT in 2015
- FWTS 17.03.00 was recommended as the ACPI 6.1 SCT in 2017
- Current version is FWTS 17.09.00
  ✓ Alpha for ACPI 6.2 SCT for this Plugfest
FWTS Framework & Tests

Firmware Test Suite

- ACPI
- UEFI
- etc...

ACPI
UEFI
etc...

Linux Kernel

ACPI
CPU

ACPI Tables and AML
UEFI Runtime
Hardware Etc.
FWTS Architecture – ACPI

ACPI

- ACPI tables & headers & checksum
- ACPI methods
- Processors (P & C states)

https://wiki.ubuntu.com/FirmwareTestSuite/Reference or fwts --show-tests / fwts --show-tests-full
Getting FWTS – LIVE

• Make bootable fwts-live USB disk
  – Linux:
    • Identify USB disk: `dmesg | tail -10 | grep Attached`
    • Copy image: `sudo dd if=fwts-live-17.09.00.img of=/dev/sdb ; sync`
  – Windows: Use “Win32 Disk Imager”
Using FWTS – LIVE

This will run a suite of firmware tests that will check the BIOS and ACPI tables. It can also find issues that can cause Linux problems.

The default below is to run just all the Batch Tests, but you can select more tests below if required.

Please select below (using cursor up/down and space) and press enter to continue.

- All
- ACPI Tests
- UEFI Tests
- Recommended Tests
- Select Individual Tests
- Abort Testing
Using FWTS – LIVE

Running ACPI Tests
578 passed, 21 failed, 3 warnings, 1 aborted, 187 skipped, 5 info only.
83.06% total run complete (6 seconds).
Processor C state support test.

Running test #52 of 62: Test all CPUs C-states.
Using FWTS – LIVE

Testing Complete
The results can be found on the USB stick in the directory: /fwts/19092017/2026/results.log

Do you want to view the results log now?

< Yes >
< No >
Using FWTS – LIVE

Choose Exit

Select if you want to exit to a command line or poweroff.

If you select to poweroff and this is running from a LIVE USB, the host will be powered down.

If you are running this from a VM and you choose to poweroff, then only the VM will be powered down.

Exit Exit to a command line
Poweroff Shutdown and power off

<OK> <Cancel> <Help>
Results.log – Header

Results generated by fwts: Version V17.08.00 (2017-08-30 06:30:53).

Some of this work - Copyright (c) 1999 - 2017, Intel Corp. All rights reserved.
Some of this work - Copyright (c) 2010 - 2017, Canonical.
Some of this work - Copyright (c) 2016 - 2017, IBM.
Some of this work - Copyright (c) 2017, ARM Ltd.

This test run on 21/09/17 at 16:38:19 on host Linux moon 4.10.0-35-generic #39~16.04.1-Ubuntu SMP Wed Sep 13 09:02:42 UTC 2017 x86_64.

Command: "fwts --acpitests".
Running tests: acpiinfo xenv xsdt wsmt wpbt wmi wdat waet uefi tpm2 tcpa stao srat spmi spcr slit slic sdei sbst rsdt rsdp rasf pptt pmtt pcct pcc nfit method msdm msct mpst mchi mcfg madt lpmi lort hmat hpet hest gttd fpdt fadl fadt facs erst einj ecdt dtrm dppt dmar dbg2 dbgp cstates csr t cpep checksum boot bgft bort aspt asf apicinstance acpitable.

acpiinfo: General ACPI information test.

Test 1 of 3: Determine Kernel ACPI version.
Kernel ACPICA driver version: 20160930, supports ACPI 5.0

Test 2 of 3: Determine machine's ACPI version.
Results.log – Test Body

```plaintext
acpiinfo: General ACPI information test.

 Test 1 of 3: Determine Kernel ACPI version.
 Kernel ACPIICA driver version: 20160930, supports ACPI 5.0

 Test 2 of 3: Determine machine's ACPI version.
 FADT X_FIRMWARE_CTRL 64 bit pointer was zero, falling back to using
 FIRMWARE_CTRL 32 bit pointer.
 FACP ACPI Version: 5.0

 Test 3 of 3: Determine AML compiler.
 Determine the compiler used to generate the ACPI AML in the DSDT and SSDT.
 Table DSDT, OEM DELL, created with INTL (Intel) compiler.
 Table SSDT0, OEM PmRef, created with INTL (Intel) compiler.
 Table SSDT1, OEM PmRef, created with INTL (Intel) compiler.
 Table SSDT2, OEM PmRef, created with INTL (Intel) compiler.
 Table SSDT3, OEM SataRe, created with INTL (Intel) compiler.
 Table SSDT4, OEM SaSsdtd, created with INTL (Intel) compiler.

------------------------------------------
0 passed, 0 failed, 0 warning, 0 aborted, 0 skipped, 3 info only.
------------------------------------------
```
### Results.log – Summary

<table>
<thead>
<tr>
<th>Test</th>
<th>Pass</th>
<th>Fail</th>
<th>Abort</th>
<th>Warn</th>
<th>Skip</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>acpiinfo</td>
<td>17</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>acpitables</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>apicinstance</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>asf</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>aspt</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>bert</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>bgrt</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>boot</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>checksum</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>cpep</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>csrt</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>cstates</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>dbg2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>dbgp</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>dmar</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>dpt</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>drtm</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>ecdt</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>einj</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>erst</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>facs</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

Total: 2364,2 98%
Information & Contacts

• Source Code
  ✓ git clone git://kernel.ubuntu.com/hwe/fwts.git
  ✓ git clone https://github.com/ColinIanKing/fwts
• https://wiki.ubuntu.com/FirmwareTestSuite
• Subscribe to fwts-devel@lists.ubuntu.com
• Activities
  ✓ Subscribe to UTWG mail list (utwg@uefi.org)
  ✓ Attend UTWG meetings
  ✓ Attend UEFI Plugfests
Q&A
Thanks for attending the Fall 2017 UEFI Plugfest

For more information on the UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

intel | CANONICAL