# OCP SUMMIT

March 20-21
2018
San Jose, CA

OPEN. FOR BUSINESS.

# OCP Initiatives and Intel Implementations

Mohan J. Kumar
Intel Fellow
Intel Corporation

# Agenda

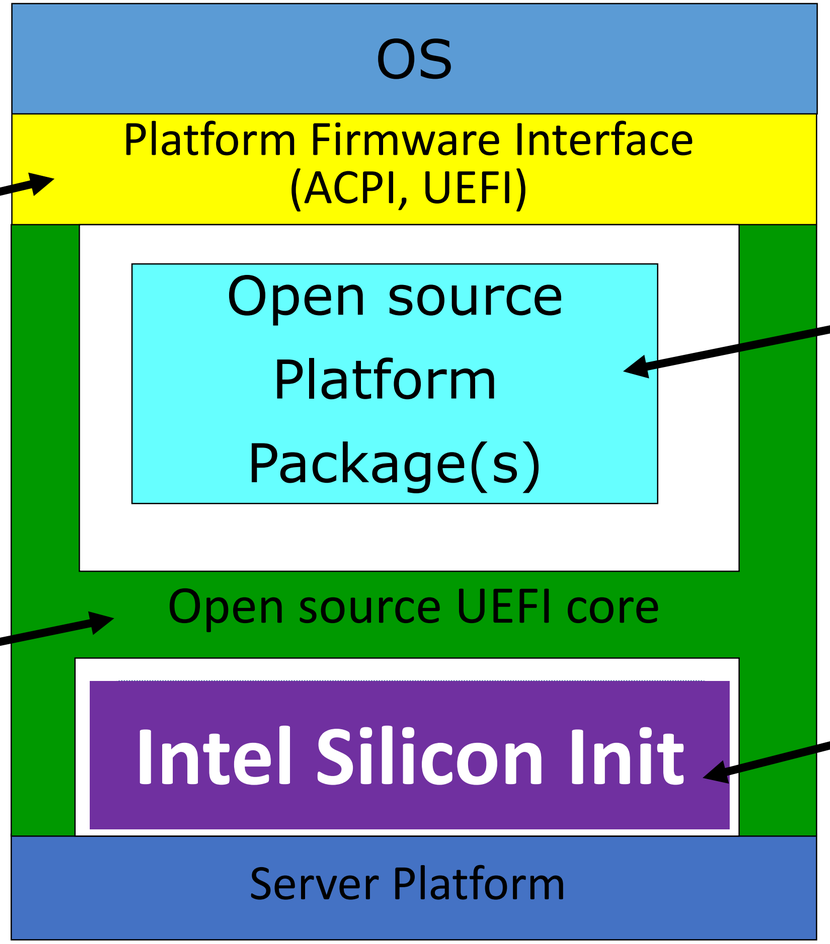
- Open Firmware
- Firmware at Scale
- Platform Attestation
- Summary

# Open Firmware

OPEN HARDWARE. OPEN SOFTWARE. OPEN FUTURE.

OPEN
Compute Project

# UEFI-based Open Firmware
## (for Intel-based Server Platforms)




Platform interfaces tables to support OS boot https://uefi.org

Platform (board) Specific Code at https://github.com/tianocore/edk2-platforms

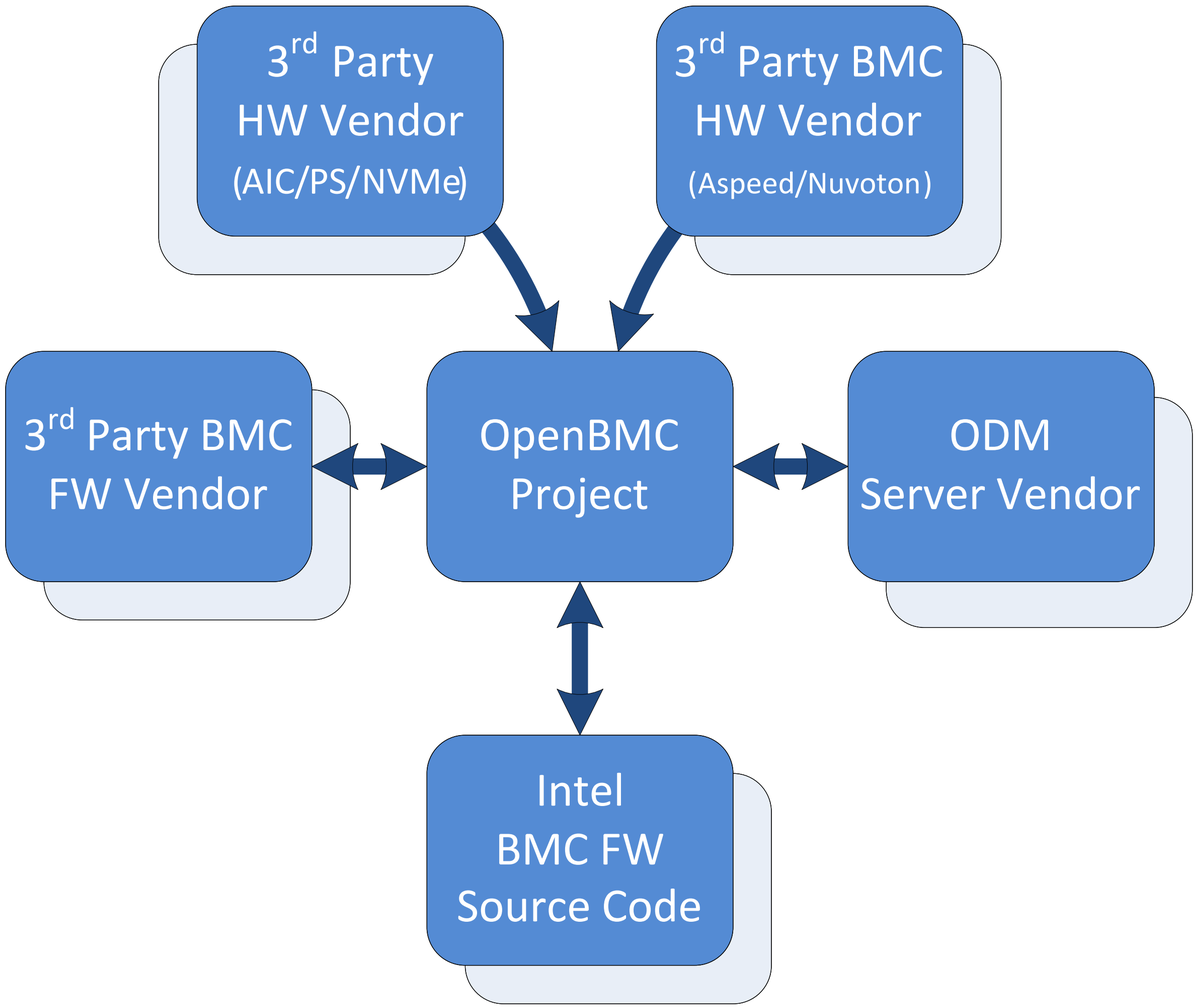
EDKII – existing upstream/open source core at https://github.com/tianocore/edk2

Intel binaries for board invariant Si code at https://github.com/intelfsp or https://github.com/tianocore/edk2-non-osi

Mt. Olympus Xeon-based platform with UEFI-based open firmware available

# Intel support for OpenBMC

- **Market Direction**
  - Customer Desire
  - Security, Easy Access to Source Code
- **Collaboration**
  - Shared Efforts
  - Enabling ODMs and 3rd Party Vendors
- **Open Manageability Standards**
  - OCP,



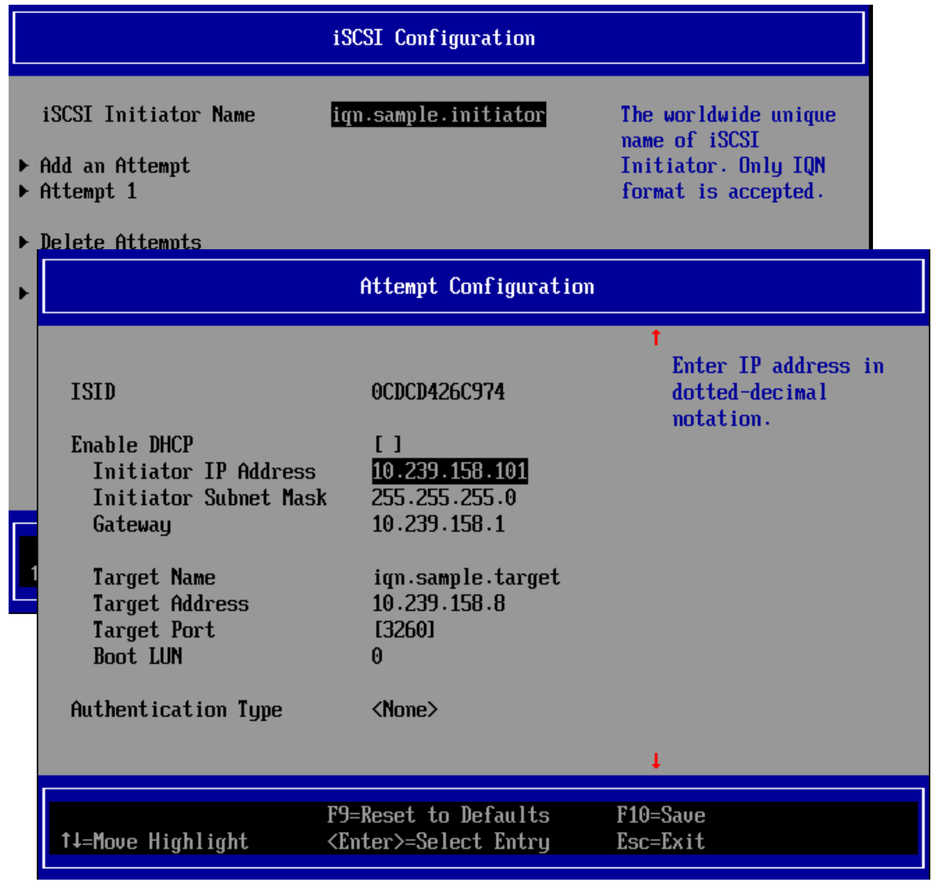
# Firmware Management at Scale

OPEN HARDWARE. OPEN SOFTWARE. OPEN FUTURE.

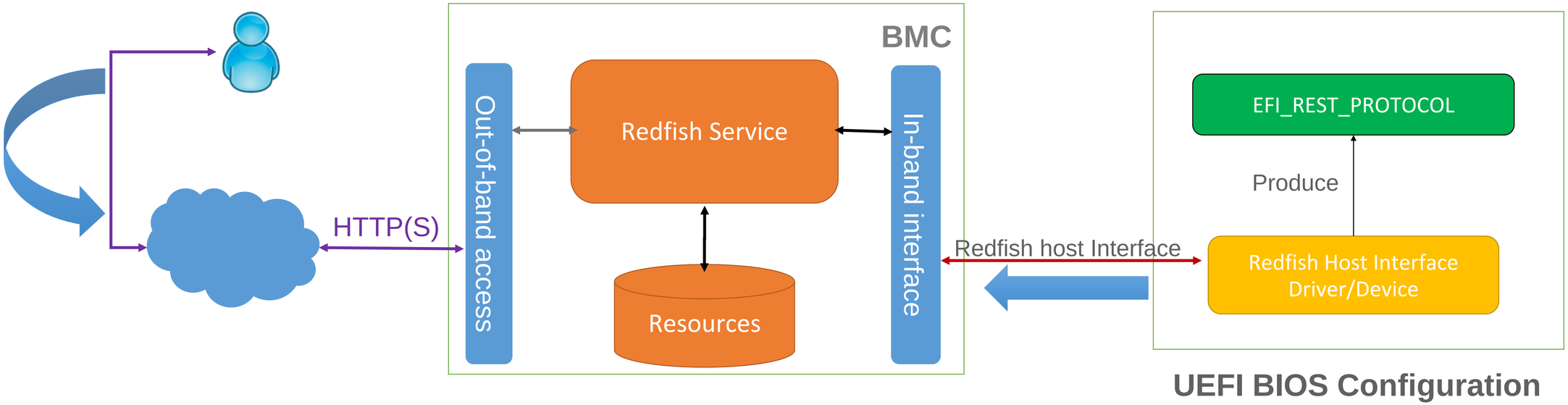
OPEN Compute Project

# Platform Firmware Configuration

- Firmware Configuration in current model is based on BIOS Setup utility
- Current model does not allow for
  - remote configuration
  - At scale configuration
- Proposing a Redfish based model for BIOS configuration
- Allows BIOS configuration using a browser
- Supports Fleet configuration using scripts



# Platform Firmware Configuration (contd.)




- User communicates to BMC via Redfish
- BIOS configuration stored in BMC is pulled by BIOS at boot and converted to UEFI BIOS Configuration settings
- Submitted to Redfish SPMF Forum

# Platform Firmware Configuration

## Proposed Redfish model

**BIOSAttributeRegistry*.json**

```
{
          "CurrentValue": null,
          "DisplayName": "Minimum Processor Idle Power Core C-State",
          ……
          "AttributeName": "MinProcIdlePower",
          ……
          "Value": [
              {
                  "ValueDisplayName": "C6 State",
                  "ValueName": "C6"
              },
              {
                  "ValueDisplayName": "C3 State",
                  "ValueName": "C3"
              },
              ……
          ],
          "AttributeDependencies": [
              {
                  "AttributeDependency": {
                      "$or": [
                          {
                              "$EQU": {"/PowerProfile/CurrentValue": "BalancedPowerPerf"}
                          },
                          {
                              "$EQU": {"/PowerProfile/CurrentValue": "MinPower"}
                          }
                      ],
                      "CurrentValue": "C6"
                  }
              },
              ……
```

Set "MinProcIdlePower/CurrentValue" to "C6" if (
"PowerProfile/CurrentValue" == "BalancedPowerPerf" ||
"PowerProfile/CurrentValue" == “MinPower"
)

# Platform Firmware Configuration in Action

GET http://10.239.158.117:5000/redfish/v1/Systems/2M220101SL

Pretty Raw Preview HTML


```
{
    "@odata.type": "#ComputerSystem.v1_1_0.ComputerSystem",
    "Id": "2M220101SL",
    "Name": "Catfish System",
    "SystemType": "Physical",
    "AssetTag": "CATFISHASSETTAG",
    "Manufacturer": "CatfishManufacturer",
    "Model": "YellowCat1000",
    "SerialNumber": "2M220101SL",
    "SKU": "",
    "PartNumber": "",
    "Description": "Catfish Implementation Recipe of simple scale-out
    "UUID": "badfaced-dead-beef-1313-131313131313",
    "HostName": "catfishHostname",
    "PowerState": "On",
    "BiosVersion": "X00.1.2.3.4(build-23)",
    "Status": {
        "State": "Enabled",
        "Health": "OK"
    },
    "IndicatorLED": "Off",
    "Boot": {
        "BootSourceOverrideEnabled": "Once",
        "BootSourceOverrideMode": "UEFI",
        "BootOptions": {
            "@odata.id": "/redfish/v1/Systems/2M220101SL/BootOptions"
        },
        "BootNext": "",
        "BootOrder": [
            "Boot0001",
            "Boot0000",
            "Boot0002",
            "Boot0004",
            "Boot0003"
        ]
    },
    "Bios": {
        "@odata.id": "/redfish/v1/Systems/2M220101SL/Bios"
    },
    "SecureBoot": {
        "@odata.id": "/redfish/v1/Systems/2M220101SL/SecureBoot"
    },
    "LogServices": {
        "@odata.id": "/redfish/v1/Systems/2M220101SL/LogServices"
    },
```



```
{
    "@odata.type": "#Bios.v1_0_2.Bios",
    "Id": "Bios",
    "Name": "BIOS Configuration Current Settings",
    "Description": "BIOS Configuration Current Settings.",
    "AttributeRegistry": "/redfish/v1/Registries/BiosAttributeRegistryUefiKeyword.v1_0_0",
    "Attributes": {
        "xUEFIns_Dev0006_iSCSIInitiatorName": "iqn.sample.initiator",
        "xUEFIns_Dev0006_iSCSIMacAddr": "8C:DC:D4:26:C9:74",
        "xUEFIns_Dev0006_iSCSIDisplayAttemptList": "Attempt:1 ",
        "xUEFIns_Dev0006_iSCSIAttemptName1": "Attempt 1",
        "xUEFIns_Dev0006_iSCSIBootEnable1": 0,
        "xUEFIns_Dev0006_iSCSIIpAddressType1": 0,
        "xUEFIns_Dev0006_iSCSIConnectRetry1": 0,
        "xUEFIns_Dev0006_iSCSIConnectTimeout1": 232,
        "xUEFIns_Dev0006_iSCSIISID1": "0CDCD426C974",
        "xUEFIns_Dev0006_iSCSIInitiatorInfoViaDHCP1": 0,
        "xUEFIns_Dev0006_iSCSIInitiatorIpAddress1": "10.239.158.101",
        "xUEFIns_Dev0006_iSCSIInitiatorNetmask1": "255.255.255.0",
        "xUEFIns_Dev0006_iSCSIInitiatorGateway1": "10.239.158.1",
        "xUEFIns_Dev0006_iSCSITargetInfoViaDHCP1": 0,
        "xUEFIns_Dev0006_iSCSITargetTcpPort1": 3260,
        "xUEFIns_Dev0006_iSCSITargetName1": "iqn.sample.target",
        "xUEFIns_Dev0006_iSCSITargetIpAddress1": "10.239.158.8",
        "xUEFIns_Dev0006_iSCSILUN1": "0",
        "xUEFIns_Dev0006_iSCSIAuthenticationMethod1": 0,
        "xUEFIns_Dev0006_iSCSIChapType1": 0,
        "xUEFIns_Dev0006_iSCSIChapUsername1": "",
        "xUEFIns_Dev0006_iSCSIChapSecret1": "",
        "xUEFIns_Dev0006_iSCSIReverseChapUsername1": "",
        "xUEFIns_Dev0006_iSCSIReverseChapSecret1": ""
    },
    "@Redfish.Settings": {
        "@odata.type": "#Settings.v1_0_4.Settings",
        "Time": "03/07/2018  14:24",
        "ETag": "\"2e884d9fb709c79ca5ed30b3435b81b37e2d2613\"",
        "Messages": [
```



```
    "@odata.type": "#AttributeRegistry.v1_0_0.AttributeRegistry",
    "@odata.id": "/redfish/v1/Registries/BiosAttributeRegistryUefiKeyword.v1_0_0",
    "Description": "This registry defines a representation of BIOS Attribute instances (UEFI configuration
    "Id": "BiosAttributeRegistryUefiKeyword.v1_0_0",
    "Language": "en",
    "Name": "BIOS Attribute Registry",
    "OwningEntity": "Intel",
    "RegistryVersion": "1.0.0",
    "RegistryEntries": {
        "Attributes": [
            {
                "AttributeName": "xUEFIns_Dev0006_iSCSIInitiatorName",
                "UefiDevicePath": "VenHw(4B47D616-A8D6-4552-9D44-CCAD2E0F4CF9)",
                "UefiKeywordName": "iSCSIInitiatorName",
                "DisplayName": "iSCSI Initiator Name",
                "HelpText": "The worldwide unique name of iSCSI Initiator. Only IQN format is accepted.",
                "ReadOnly": false,
                "ResetRequired": false,
                "MenuPath": "iSCSI_Configuration",
                "Type": "String",
                "MaxLength": 223,
                "MinLength": 4
            },
            {
                "AttributeName": "xUEFIns_Dev0006_iSCSIMacAddr",
                "UefiDevicePath": "VenHw(4B47D616-A8D6-4552-9D44-CCAD2E0F4CF9)",
                "UefiKeywordName": "iSCSIMacAddr",
                "DisplayName": "iSCSI MAC Address for the attempt",
                "HelpText": "iSCSI MAC Address for the attempt",
                "ReadOnly": false,
                "ResetRequired": false,
                "MenuPath": "iSCSI_Configuration",
                "Type": "String",
                "MaxLength": 96,
                "MinLength": 0
            },
```


Query BIOS Configuration via HTTP Get

PATCH http://127.0.0.1:5000/redfish/v1/Systems/2M220101SL/Bios/Settings Params Send

Authorization Headers (1) Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary Text

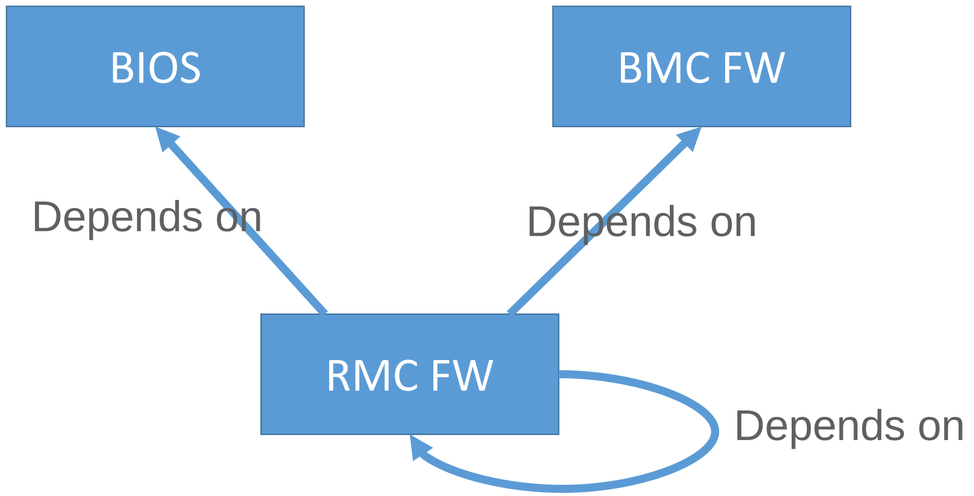
```
{
    "Attributes": {
        "xUEFIns_Dev0006_iSCSIInitiatorName": "iqn.test.patch",
        "xUEFIns_Dev0006_iSCSIInitiatorIpAddress1": "10.239.192.218",
        "xUEFIns_Dev0006_iSCSIInitiatorNetmask1": "255.255.255.0",
        "xUEFIns_Dev0006_iSCSIInitiatorGateway1": "10.239.192.1"
    }
}
```

Log Console in Managed Server Platform

```
Process PATCH request:
{
    "Attributes": {
        "xUEFIns_Dev0006_iSCSIInitiatorName": "iqn.test.patch",
        "xUEFIns_Dev0006_iSCSIInitiatorIpAddress1": "10.239.192.218",
        "xUEFIns_Dev0006_iSCSIInitiatorNetmask1": "255.255.255.0",
        "xUEFIns_Dev0006_iSCSIInitiatorGateway1": "10.239.192.1"
    }
}
Check key in patch_data:xUEFIns_Dev0006_iSCSIInitiatorName
Check key in patch_data:xUEFIns_Dev0006_iSCSIInitiatorIpAddress1
Check key in patch_data:xUEFIns_Dev0006_iSCSIInitiatorNetmask1
Check key in patch_data:xUEFIns_Dev0006_iSCSIInitiatorGateway1
127.0.0.1 - - [14/Mar/2018 11:22:10] "PATCH /redfish/v1/Systems/2M220101SL/Bios/Settings HTTP/1.1" 204 -
```

Update BIOS Configuration via HTTP Patch

# Firmware Version Dependency




*Example Firmware Update Dependency*

```
"FirmwareInventory": [
  {
     "@odata.id": "/redfish/v1/Managers/UpdateService/…",
     "Updateable": true,
     "Name": "Rack Management Controller Firmware"
     "SoftwareId": "intel/rmc-fw",
     "Version": "1.2.1",
     "UpdateDependencies": [
          "$and": [
               {"intel/bios": ">=0.6.1"},
               {"intel/bmc-fw": "==1.0.1"},
               {"intel/rmc-fw": ">=1.0.1"}
          ]
     }
  ]
  },
  . . .
```

- Dependency model for Platform Firmware Configuration also used to describe firmware update dependencies
- Submitted to Redfish SPMF Forum

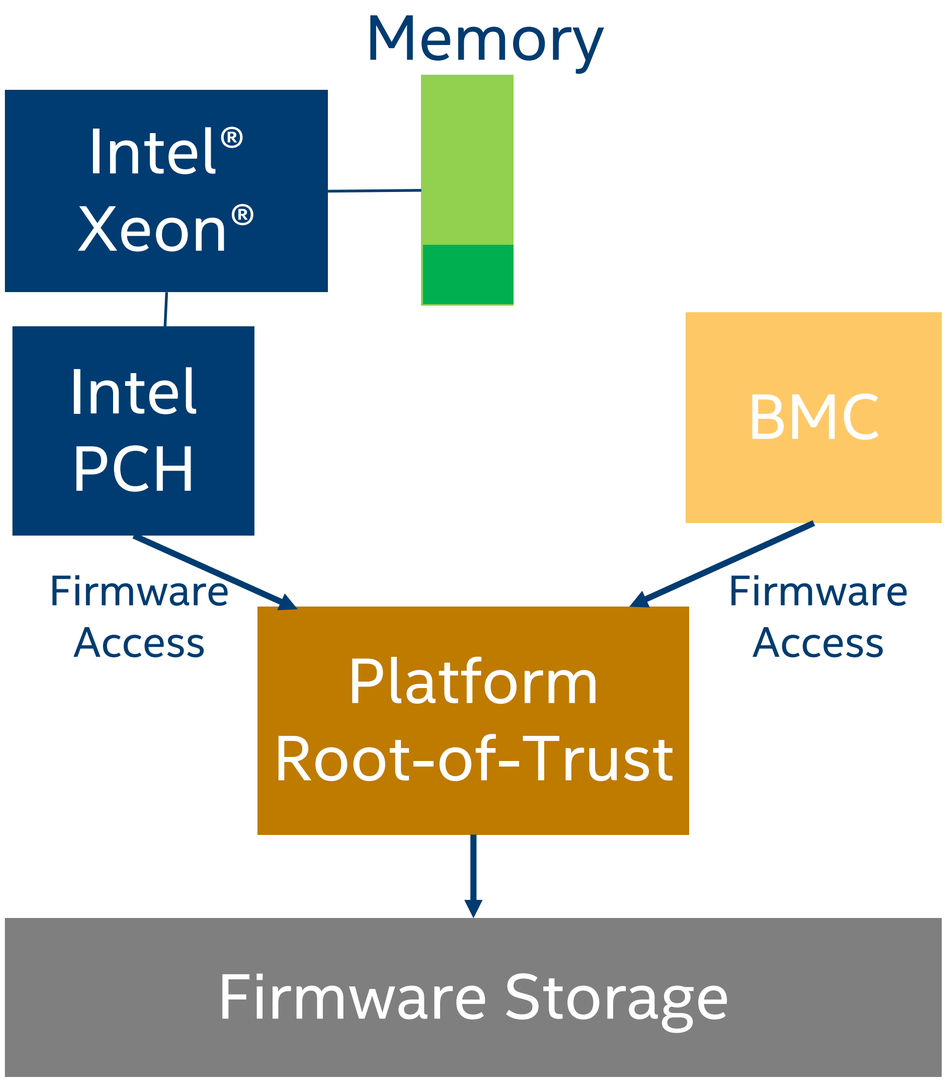
For more details, please attend “Redfish OCP profile for Server Platforms“ on March 21, 10:30AM

# Platform Attestation

OPEN HARDWARE. OPEN SOFTWARE. OPEN FUTURE.

OPEN Compute Project

# Platform Attestation Support

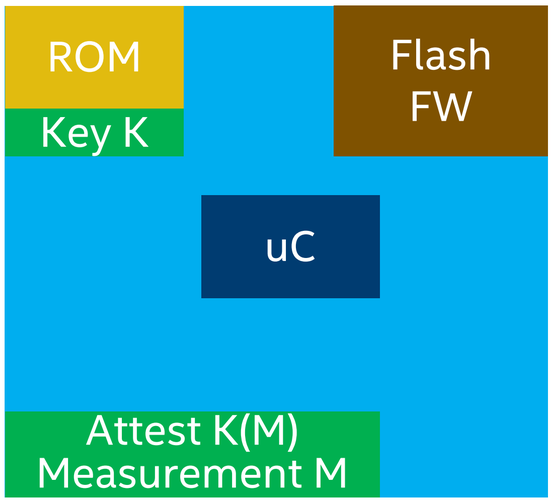



Intel is working to deliver the best implementation of OCP Platform Attestation principles (Cerberus) with Intel® Platform Firmware Resilience (Intel® PFR)

- Attestation of BIOS and BMC images before allowing firmware to run
- Intel further extends platform security with **mutual attestation** between CPU and additional platform root-of-trust solutions
- Can detect compromised firmware and **automatically recover** to known-good state
- Performs attestation during both **warm *and* hard resets**
- **Monitors and filters** SPI bus traffic during runtime to help further reduce attacks
- Attestation capabilities extendable to additional **peripheral firmware**

# Platform Attestation Support

## PCIe* Device Firmware Measurement + Attestation




Platforms need mechanisms to determine the identity and capability of devices to make trust decisions

- Device Firmware Measurement to verify both immutable and mutable firmware versions
- Device Authentication mechanism to query a Device's identities tied to a Device private key

PCI Express* Device Security Enhancements Proposal Draft Specification Posted (URL below)

- Defines register interfaces for Device Measurement and Authentication
- Follows established industry paradigms & builds on the industry architecture for USB Authentication

https://www.intel.com/content/www/us/en/io/pci-express/pci-express-architecture-devnet-resources.html

# Summary

OPEN HARDWARE. OPEN SOFTWARE. OPEN FUTURE.

OPEN Compute Project

# Summary

Intel actively engaged in OCP Platform firmware and OCP Security WG

Intel and partners providing more Open UEFI firmware solutions

Intel OpenBMC solution underway (Visit the Intel Booth A12)

Intel driving firmware management at scale solutions via SPMF

Intel plans to support OCP platform attestation (Cerberus) with best implementation using PFR

Intel’s proposal for Device Security Enhancements further improves platform security for PCIe peripherals

# Notices & Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration.

No computer system can be absolutely secure.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. For more complete information about performance and benchmark results, visit http://www.intel.com/benchmarks .

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit http://www.intel.com/benchmarks .

Benchmark results were obtained prior to implementation of recent software patches and firmware updates intended to address exploits referred to as "Spectre" and "Meltdown." Implementation of these updates may make these results inapplicable to your device or system.

Intel® Advanced Vector Extensions (Intel® AVX)* provides higher throughput to certain processor operations. Due to varying processor power characteristics, utilizing AVX instructions may cause a) some parts to operate at less than the rated frequency and b) some parts with Intel® Turbo Boost Technology 2.0 to not achieve any or maximum turbo frequencies. Performance varies depending on hardware, software, and system configuration and you can learn more at http://www.intel.com/go/turbo.

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

# OCP SUMMIT