Intel® Platform Innovation Framework for EFI Pre-EFI Initialization Core Interface Specification (PEI CIS)

A Foundation Specification

Draft for Review

Version 0.9

September 16, 2003

Revision History

Revision	Revision History	Date
0.9	First public release.	9/16/03
	Added "A Foundation Specification" line to the title page. No other changes, so the revision number and date were not changed.	6/30/04

Contents

Figures

Tables

1 Introduction

Overview

This specification defines the core code and services that are required for an implementation of the Pre-EFI Initialization (PEI) phase of the Intel® Platform Innovation Framework for EFI (hereafter referred to as the "Framework"). This PEI Core Interface Specification (CIS) does the following:

- Describes the basic components of the PEI phase
- Provides code definitions for services and functions that are architecturally required by the *Intel® Platform Innovation Framework for EFI Architecture Specification*
- Describes the machine preparation that is required for subsequent phases of firmware execution
- Discusses state variables that describe the system restart type

See Organization of the PEI CIS for more information.

Organization of the PEI CIS

This PEI Core Interface Specification (CIS) is organized as listed below. Because the PEI Foundation is just one component of a Framework-based firmware solution, there are a number of additional specifications that are referred to throughout this document:

- For references to other Framework specifications, click on the hyperlink in the page or navigate through the table of contents (TOC) in the left navigation pane to view the referenced specification.
- For references to non-Framework specifications, see References in the Interoperability and Component Specifications help system.

Table 1-1. Organization of the PEI CIS

Book	Description
Overview	Describes the major components of PEI, including the PEI Services, boot mode, PEI Dispatcher, and PEIMs.
PEI Services Table	Describes the data structure that maintains the PEI Services.
Services - PEI	Details each of the functions that comprise the PEI Services.
PEI Foundation	Describes the PEI Foundation and its methods of operation.
PEI Dispatcher	Describes the PEI Dispatcher and its associated dependency expression grammar.
PEIMs	Describes the format and use of the Pre-EFI Initialization Module (PEIM).
Architectural PPIs	Contains PEIM-to-PEIM Interfaces (PPIs) that are used by the PEI Foundation.
Additional PPIs	Contains PPIs that can exist on a platform.

Book	Description
PEI to DXE handoff	Describes the state of the machine and memory when the PEI phase invokes the DXE phase.
Boot Paths	Describes the restart modalities and behavior supported in the PEI phase.
PEI Physical Memory Usage	Describes the memory map and memory usage during the PEI phase.
Special Paths Unique to the Itanium® Processor Family	Contains flow during PEI that is unique to the Itanium® processor family.
Security (SEC) Phase Information	Contains an overview of the phase of execution that occurs prior to PEI.
Returned Status Codes	Lists success, error, and warning codes returned by PEI and EFI interfaces.
Dependency Expression Grammar	Describes the BNF grammar for a tool that can convert a text file containing a dependency expression into a dependency section of a PEIM stored in a firmware volume.

Conventions Used in This Document

This document uses the typographic and illustrative conventions described below.

Data Structure Descriptions

Intel® processors based on 32-bit Intel® architecture (IA-32) are "little endian" machines. This distinction means that the low-order byte of a multibyte data item in memory is at the lowest address, while the high-order byte is at the highest address. Processors of the Intel® Itanium® processor family may be configured for both "little endian" and "big endian" operation. All implementations designed to conform to this specification will use "little endian" operation.

In some memory layout descriptions, certain fields are marked *reserved*. Software must initialize such fields to zero and ignore them when read. On an update operation, software must preserve any reserved field.

The data structures described in this document generally have the following format:

STRUCTURE NAME: The formal name of the data structure.

Summary: A brief description of the data structure.

Prototype: A "C-style" type declaration for the data structure.

Parameters: A brief description of each field in the data structure prototype.

Description: A description of the functionality provided by the data structure, including any limitations and caveats of which the caller should be aware.

Related Definitions: The type declarations and constants that are used only by this data structure.

Procedure Descriptions

The procedures described in this document generally have the following format:

ProcedureName(): The formal name of the procedure.

Summary: A brief description of the procedure.

Prototype: A "C-style" procedure header defining the calling sequence.

Parameters: A brief description of each field in the procedure prototype.

Description: A description of the functionality provided by the interface, including any limitations and caveats of which the caller should be aware.

Related Definitions: The type declarations and constants that are used only by this procedure.

Status Codes Returned: A description of any codes returned by the interface. The procedure is required to implement any status codes listed in this table. Additional error codes may be returned, but they will not be tested by standard compliance tests, and any software that uses the procedure cannot depend on any of the extended error codes that an implementation may provide.

Instruction Descriptions

A dependency expression instruction description generally has the following format:

InstructionName The formal name of the instruction.

SYNTAX: A brief description of the instruction.

DESCRIPTION: A description of the functionality provided by the instruction accompanied by a table that details the instruction encoding.

OPERATION: Details the operations performed on operands.

BEHAVIORS AND RESTRICTIONS: An item-by-item description of the behavior of each operand involved in the instruction and any restrictions that apply to the operands or the instruction.

PPI Descriptions

A PEIM-to-PEIM Interface (PPI) description generally has the following format:

PPI Name: The formal name of the PPI.

Summary: A brief description of the PPI.

GUID: The 128-bit Globally Unique Identifier (GUID) for the PPI.

PPI Interface Structure: A "C-style" procedure template defining the PPI calling structure.

Parameters: A brief description of each field in the PPI structure.

Description: A description of the functionality provided by the interface, including any limitations and caveats of which the caller should be aware.

Related Definitions: The type declarations and constants that are used only by this interface.

Status Codes Returned: A description of any codes returned by the interface. The PPI is required to implement any status codes listed in this table. Additional error codes may be returned, but they will not be tested by standard compliance tests, and any software that uses the procedure cannot depend on any of the extended error codes that an implementation may provide.

Pseudo-Code Conventions

Pseudo code is presented to describe algorithms in a more concise form. None of the algorithms in this document are intended to be compiled directly. The code is presented at a level corresponding to the surrounding text.

In describing variables, a *list* is an unordered collection of homogeneous objects. A *queue* is an ordered list of homogeneous objects. Unless otherwise noted, the ordering is assumed to be First In First Out (FIFO).

Pseudo code is presented in a C-like format, using C conventions where appropriate. The coding style, particularly the indentation style, is used for readability and does not necessarily comply with an implementation of the *Extensible Firmware Interface Specification*.

Typographic Conventions

This document uses the typographic and illustrative conventions described below:

Plain text	The normal text typeface is used for the vast majority of the descriptive text in a specification.
Plain text (blue)	In the online help version of this specification, any plain text that is underlined and in blue indicates an active link to the cross-reference. Click on the word to follow the hyperlink. Note that these links are *not* active in the PDF of the specification.
Bold	In text, a **Bold** typeface identifies a processor register name. In other instances, a **Bold** typeface can be used as a running head within a paragraph.
Italic	In text, an *Italic* typeface can be used as emphasis to introduce a new term or to indicate a manual or specification name.
`BOLD Monospace`	Computer code, example code segments, and all prototype code segments use a `BOLD Monospace` typeface with a dark red color. These code listings normally appear in one or more separate paragraphs, though words or segments can also be embedded in a normal text paragraph.
`Bold Monospace`	In the online help version of this specification, words in a `Bold Monospace` typeface that is underlined and in blue indicate an active hyperlink to the code definition for that function or type definition. Click on the word to follow the hyperlink. Note that these links are *not* active in the PDF of the specification. Also, these inactive links in the PDF may instead have a `Bold Monospace` appearance that is underlined but in dark red. Again, these links are not active in the PDF of the specification.
`Italic Monospace`	In code or in text, words in *`Italic Monospace`* indicate placeholder names for variable information that must be supplied (i.e., arguments).
`Plain Monospace`	In code, words in a `Plain Monospace` typeface that is a dark red color but is not bold or italicized indicate pseudo code or example code. These code segments typically occur in one or more separate paragraphs.

See the master Framework glossary in the Framework Interoperability and Component Specifications help system for definitions of terms and abbreviations that are used in this document or that might be useful in understanding the descriptions presented in this document.

See the master Framework references in the Interoperability and Component Specifications help system for a complete list of the additional documents and specifications that are required or suggested for interpreting the information presented in this document.

The Framework Interoperability and Component Specifications help system is available at the following URL:

http://www.intel.com/technology/framework/spec.htm

2
Overview

Introduction

The Pre-EFI Initialization (PEI) phase of the Intel® Platform Innovation Framework for EFI (hereafter referred to as the "Framework") is invoked quite early in the boot flow. Specifically, after some preliminary processing in the Security (SEC) phase, any machine restart event will invoke the PEI phase.

The PEI phase will initially operate with the platform in a nascent state, leveraging only on-processor resources, such as the processor cache as a call stack, to dispatch Pre-EFI Initialization Modules (PEIMs). These PEIMs are responsible for the following:

- Initializing some permanent memory complement
- Describing the memory in Hand-Off Blocks (HOBs)
- Describing the firmware volume locations in HOBs
- Passing control into the Driver Execution Environment (DXE) phase

Philosophically, the PEI phase is intended to be the thinnest amount of code to achieve the ends listed above. As such, any more sophisticated algorithms or processing should be deferred to the DXE phase of execution.

The PEI phase is also responsible for crisis recovery and resuming from the S3 sleep state. For crisis recovery, the PEI phase should reside in some small, fault-tolerant block of the firmware store. As a result, it is imperative to keep the footprint of the PEI phase as small as possible. In addition, for a successful S3 resume, the speed of the resume is of utmost importance, so the code path through the firmware should be minimized. These two boot flows also speak to the need to keep the processing and code paths in the PEI phase to a minimum.

The implementation of the PEI phase is more dependent on the processor architecture than any other phase. In particular, the more resources the processor provides at its initial or near initial state, the richer the interface between the PEI Foundation and PEIMs. As such, there are several parts of the following discussion that note requirements on the architecture but are otherwise left architecturally dependent.

Design Goals

The Framework requires the PEI phase to configure a system to meet the minimum prerequisites for the Driver Execution Environment (DXE) phase of the Framework architecture. In general, the PEI phase is required to initialize a linear array of RAM large enough for the successful execution of the DXE phase elements.

The PEI phase provides a framework to allow vendors to supply separate initialization modules for each functionally distinct piece of system hardware that must be initialized prior to the DXE phase of execution in the Framework. The PEI phase provides a common framework through which the separate initialization modules can be independently designed, developed, and updated. The PEI phase was developed to meet the following goals in the Framework architecture:

- Enable maintenance of the "chain of trust." This includes protection against unauthorized updates to the PEI phase or its modules, as well as a form of authentication of the PEI Foundation and its modules during the PEI phase.
- Provide a core PEI module (the PEI Foundation) that will remain more or less constant for a particular processor architecture but that will support add-in modules from various vendors, particular for processors, chipsets, RAM initialization, and so on.
- Allow independent development of early initialization modules.

Pre-EFI Initialization (PEI) Phase

The design for the Pre-EFI Initialization (PEI) phase of a Framework boot is as an essentially miniature version of the DXE phase of the Framework and addresses many of the same issues. The PEI phase is designed to be developed in several parts. The PEI phase consists of the following:

- Some core code known as the PEI Foundation
- Specialized plug-ins known as Pre-EFI Initialization Modules (PEIMs)

Unlike DXE, the PEI phase cannot assume the availability of reasonable amounts of RAM, so the richness of the features in DXE does not exist in PEI. The PEI phase limits its support to the following actions:

- Locating, validating, and dispatching PEIMs
- Facilitating communication between PEIMs
- Providing handoff data to subsequent phases

The figure below shows a diagram of the process completed during the PEI phase.

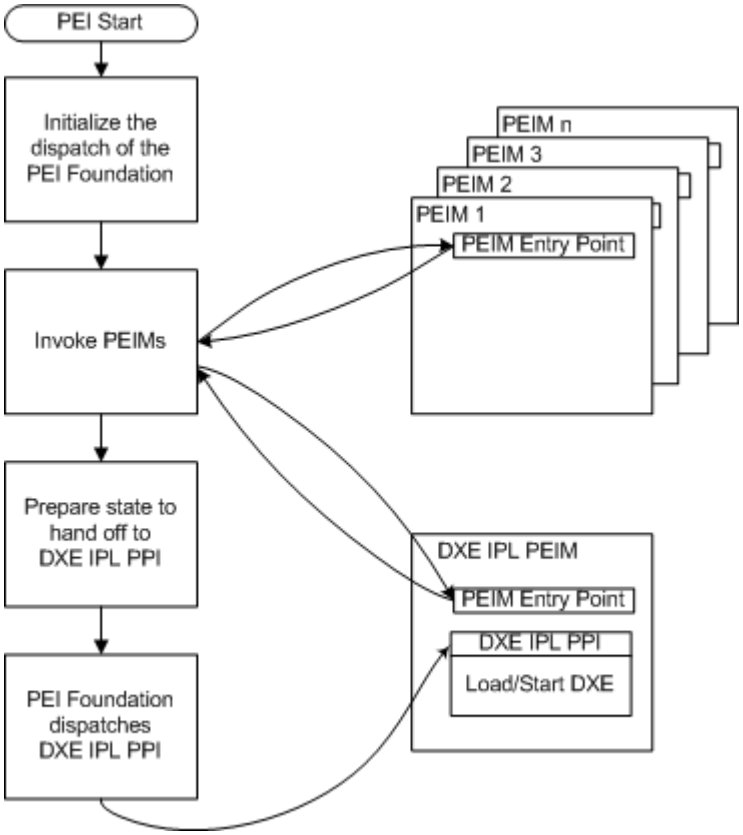


Figure 2-1. PEI Operations Diagram

PEI Services

The PEI Foundation establishes a system table named the PEI Services Table that is visible to all Pre-EFI Initialization Modules (PEIMs) in the system. A PEI Service is defined as a function, command, or other capability manifested by the PEI Foundation when that service's initialization requirements are met. Because the PEI phase has no permanent memory available until nearly the end of the phase, the range of services created during the PEI phase cannot be as rich as those created during later phases. Because the location of the PEI Foundation and its temporary RAM is not known at build time, a pointer to the PEI Services Table is passed into each PEIM's entry point and also to part of each PEIM-to-PEIM Interface (PPI).

The PEI Foundation provides the following classes of services.

PPI Services:	Manages PPIs to facilitate intermodule calls between PEIMs. Interfaces are installed and tracked on a database maintained in temporary RAM.
Boot Mode Services:	Manages the boot mode (S3, S5, normal boot, diagnostics, etc.) of the system.
HOB Services:	Creates data structures called Hand-Off Blocks (HOBs) that are used to pass information to the next phase of the Framework.
Firmware Volume Services:	Walks the Firmware File System (FFS) in firmware volumes to find PEIMs and other firmware files in the flash device.
PEI Memory Services:	Provides a collection of memory management services for use both before and after permanent memory has been discovered.
Status Code Services:	Provides common progress and error code reporting services (for example, port 080h or a serial port for simple text output for debug).
Reset Services:	Provides a common means by which to initiate a warm or cold restart of the system.

PEI Foundation

The PEI Foundation is the entity that is responsible for the following:

- Successfully dispatching Pre-EFI Initialization Modules (PEIMs)
- Maintaining the boot mode
- Initializing permanent memory
- Invoking the Driver Execution Environment (DXE) loader

The PEI Foundation is written to be portable across all platforms of a given instruction-set architecture. As such, a binary for 32-bit Intel® architecture (IA-32) should work across all Pentium® processors, from the Pentium II processor with MMX™ technology through the latest Pentium 4 processors. Similarly, the PEI Foundation binary for the Itanium® processor family should work across all Itanium processors.

Regardless of the processor microarchitecture, the set of services exposed by the PEI Foundation should be the same. This uniform surface area around the PEI Foundation allows PEIMs to be written in the C programming language and compiled across any microarchitecture.

PEI Dispatcher

The PEI Dispatcher is essentially a state machine that is implemented in the PEI Foundation. The PEI Dispatcher evaluates the dependency expressions in Pre-EFI Initialization Modules (PEIMs) that are in the firmware volume(s) being examined.

The dependency expressions are logical combinations of PEIM-to-PEIM Interfaces (PPIs). These expressions describe the PPIs that must be available before a given PEIM can be invoked. To evaluate the dependency expression for the PEIM, the PEI Dispatcher references the PPI database in the PEI Foundation to determine which PPIs have been installed. If the PPI has been installed, the dependency expression will evaluate to **`TRUE`**, which tells the PEI Dispatcher it can run the PEIM. At this point, the PEI Foundation passes control to the PEIM with a true dependency expression.

Once the PEI Dispatcher has evaluated all of the PEIMs in all of the exposed firmware volumes and no more PEIMs can be dispatched (i.e., the dependency expressions do not evaluate from **`FALSE`** to **`TRUE`**), the PEI Dispatcher will exit. It is at this point that the PEI Dispatcher cannot invoke any additional PEIMs. The PEI Foundation then reassumes control from the PEI Dispatcher and invokes the DXE IPL PPI to pass control to the DXE phase of execution.

Pre-EFI Initialization Modules (PEIMs)

Pre-EFI Initialization Modules (PEIMs) are specialized drivers that personalize the PEI Foundation to the platform. They are analogous to DXE drivers and generally correspond to the components being initialized. It is the responsibility of the PEI Foundation code to dispatch the PEIMs in a sequenced order and provide basic services. The PEIMs are intended to mirror the components being initialized.

Communication between PEIMs is not easy in a “memory poor” environment. Nonetheless, PEIMs cannot be coded without some interaction between one another and, even if they could, it would be inefficient to do so. The PEI phase provides mechanisms for PEIMs to locate and invoke interfaces from other PEIMs.

Because the PEI phase exists in an environment where minimal hardware resources are available and execution is performed from the boot firmware device, it is strongly recommended that PEIMs do the minimum necessary work to initialize the system to a state that meets the prerequisites of the DXE phase.

It is expected that, in the future, common practice will be that the vendor of a software or hardware component will provide the PEIM (possibly in source form) so the customer can debug integration problems quickly.

PEIM-to-PEIM Interfaces (PPIs)

PEIMs communicate with each other using a structure called a PEIM-to-PEIM Interface (PPI). PPIs are contained in a **`EFI_PEI_PPI_DESCRIPTOR`** data structure, which is composed of a GUID/pointer pair. The GUID "names" the interface and the associated pointer provides the associated data structure and/or service set for that PPI. A consumer of a PPI must use the PEI Service **`LocatePpi()`** to discover the PPI of interest. The producer of a PPI publishes the available PPIs in its PEIM using the PEI Services **`InstallPpi()`** or **`ReinstallPpi()`**.

All PEIMs are registered and located in the same fashion, namely through the PEI Services listed above. Within this name space of PPIs, there are two classes of PPIs:

- Architectural PPIs
- Additional PPIs

An *architectural PPI* is a PPI whose GUID is described in the PEI CIS and is a GUID known to the PEI Foundation. These architectural PPIs typically provide a common interface to the PEI Foundation of a service that has a platform-specific implementation, such as the PEI Service **`ReportStatusCode()`**.

Additional PPIs are PPIs that are important for interoperability but are not depended upon by the PEI Foundation. They can be classified as mandatory or optional. Specifically, to have a large class of interoperable PEIMs, it would be good to signal that the final boot mode was installed in some standard fashion so that PEIMs could use this PPI in their dependency expressions. The alternative to defining these additional PPIs in the PEI CIS would be to have a proliferation of similar services under different names.

Firmware Volumes

Pre-EFI Initialization Modules (PEIMs) reside in firmware volumes (FVs). The PEI Foundation, defined here, must reside in the Boot Firmware Volume (BFV). While it is expected that, in most applications, all PEIMs will reside in the BFV, the PEI phase supports the ability for PEIMs to reside in multiple FVs as long as the PEI Foundation is provided with a standard mechanism for locating these other FVs.

3
PEI Services Table

Introduction

The PEI Foundation establishes a system table named the PEI Services Table that is visible to all Pre-EFI Initialization Modules (PEIMs) in the system. A PEI Service is defined as a function, command, or other capability manifested by the PEI Foundation when that service's initialization requirements are met. Because the PEI phase has no permanent memory available until nearly the end of the phase, the range of services created during the PEI phase cannot be as rich as those created during later phases. Because the location of the PEI Foundation and its temporary RAM is not known at build time, a pointer to the PEI Services Table is passed into each PEIM's entry point and also to part of each PEIM-to-PEIM Interface (PPI).

EFI Table Header

EFI_TABLE_HEADER

Summary

Data structure that precedes all of the PEI Services.

Prototype

```
typedef struct {
  UINT64    Signature;
  UINT32    Revision;
  UINT32    HeaderSize;
  UINT32    CRC32;
  UINT32    Reserved;
} EFI_TABLE_HEADER;
```

Parameters

Signature

A 64-bit signature that identifies the type of table that follows.

Revision

The revision of the PEI Specification to which this table conforms. The upper 16 bits of this field contain the major revision value, and the lower 16 bits contain the minor revision value. The minor revision values are limited to the range of 00..99. Note that these revision fields are not encoded in Binary Coded Decimal (BCD) format but instead are stored in normal binary format

HeaderSize

The size in bytes of the entire table including the **EFI_TABLE_HEADER**.

CRC32

The 32-bit CRC for the entire table. This value is computed by setting this field to 0, and computing the 32 bit CRC for *HeaderSize* bytes. This value is ignorable for PEI and should be set to zero.

Reserved

Reserved field that must be set to 0.

Description

The data type **EFI_TABLE_HEADER** is the data structure that precedes all of the standard EFI table types. It includes a signature that is unique for each table type, a revision of the table that may be updated as extensions are added to the EFI table types, and a 32-bit CRC so a consumer of an EFI table type can validate the contents of the EFI table.

PEI Services Table

EFI_PEI_SERVICES

Summary

The PEI Services Table includes a list of function pointers in a table. The table is located in the ROM or memory, depending upon the capabilities and phase of execution of PEI. The functions in this table are defined in Services - PEI.

Related Definitions

```
//
// PEI Specification Revision information
//
#define PEI_SPECIFICATION_MAJOR_REVISION 0
#define PEI_SPECIFICATION_MINOR_REVISION 9

//
// EFI PEI Services Table
//
#define PEI_SERVICES_SIGNATURE     0x5652455320494550
#define PEI_SERVICES_REVISION
     (PEI_SPECIFICATION_MAJOR_REVISION<<16) |
(PEI_SPECIFICATION_MINOR_REVISION)

typedef struct _EFI_PEI_SERVICES {
  EFI_TABLE_HEADER                        Hdr;

  //
  // PPI Functions
  //
  EFI_PEI_INSTALL_PPI                     InstallPpi;
  EFI_PEI_REINSTALL_PPI                   ReInstallPpi;
  EFI_PEI_LOCATE_PPI                      LocatePpi;
  EFI_PEI_NOTIFY_PPI                      NotifyPpi;

  //
  // Boot Mode Functions
  //
  EFI_PEI_GET_BOOT_MODE                   GetBootMode;
  EFI_PEI_SET_BOOT_MODE                   SetBootMode;

  //
  // HOB Functions
  //
  EFI_PEI_GET_HOB_LIST                    GetHobList;
  EFI_PEI_CREATE_HOB                      CreateHob;
```

```
    //
    // Firmware Volume Functions
    //
    EFI_PEI_FFS_FIND_NEXT_VOLUME          FfsFindNextVolume;
    EFI_PEI_FFS_FIND_NEXT_FILE            FfsFindNextFile;
    EFI_PEI_FFS_FIND_SECTION_DATA         FfsFindSectionData;

    //
    // PEI Memory Functions
    //
    EFI_PEI_INSTALL_PEI_MEMORY            InstallPeiMemory;
    EFI_PEI_ALLOCATE_PAGES                AllocatePages;
    EFI_PEI_ALLOCATE_POOL                 AllocatePool;
    EFI_PEI_COPY_MEM                      CopyMem;
    EFI_PEI_SET_MEM                       SetMem;

    //
    // Status Code
    //
    EFI_PEI_REPORT_STATUS_CODE            ReportStatusCode;

    //
    // Reset
    //
    EFI_PEI_RESET_SYSTEM                  ResetSystem;
} EFI_PEI_SERVICES;
```

Parameters

Hdr

The table header for the PEI Services Table. This header contains the **PEI_SERVICES_SIGNATURE** and **PEI_SERVICES_REVISION** values along with the size of the **EFI_PEI_SERVICES** structure and a 32-bit CRC to verify that the contents of the PEI Foundation Services Table are valid.

InstallPpi

Installs an interface in the PEI PEIM-to-PEIM Interface (PPI) database by GUID. See the **InstallPpi()** function description in this document.

ReInstallPpi

Reinstalls an interface in the PEI PPI database by GUID. See the **ReinstallPpi()** function description in this document.

LocatePpi

Locates an interface in the PEI PPI database by GUID. See the **LocatePpi()** function description in this document.

NotifyPpi

Installs the notification service to be called back upon the installation or reinstallation of a given interface. See the **NotifyPpi()** function description in this document.

GetBootMode

Returns the present value of the boot mode. See the **GetBootMode()** function description in this document.

SetBootMode

Sets the value of the boot mode. See the **SetBootMode()** function description in this document.

GetHobList

Returns the pointer to the list of Hand-Off Blocks (HOBs) in memory. See the **GetHobList()** function description in this document.

CreateHob

Abstracts the creation of HOB headers. See the **CreateHob()** function description in this document.

FfsFindNextVolume

Discovers instances of firmware volumes in the system. See the **FfsFindNextVolume()** function description in this document.

FfsFindNextFile

Discovers instances of firmware files in the system. See the **FfsFindNextFile()** function description in this document.

FfsFindSectionData

Searches for the next matching file in the Firmware File System (FFS) volume. See the **FfsFindSectionData()** function description in this document.

InstallPeiMemory

Registers the found memory configuration with the PEI Foundation. See the **InstallPeiMemory()** function description in this document.

AllocatePages

Allocates memory ranges that are managed by the PEI Foundation. See the **AllocatePages()** function description in this document.

AllocatePool

Frees memory ranges that are managed by the PEI Foundation. See the **AllocatePool()** function description in this document.

CopyMem

Copies the contents of one buffer to another buffer. See the **CopyMem()** function description in this document.

SetMem

Fills a buffer with a specified value. See the **SetMem()** function description in this document.

ReportStatusCode

Provides an interface that a PEIM can call to report a status code. See the **ReportStatusCode()** function description in this document.

ResetSystem

Resets the entire platform. See the **ResetSystem()** function description in this document.

Description

EFI_PEI_SERVICES is a collection of functions whose implementation is provided by the PEI Foundation. These services fall into various classes, including the following:

- Managing the boot mode
- Allocating both early and permanent memory
- Supporting the Firmware File System (FFS)
- Abstracting the PPI database abstraction
- Creating Hand-Off Blocks (HOBs)

A pointer to the **EFI_PEI_SERVICES** table is passed into each PEIM when the PEIM is invoked by the PEI Foundation. As such, every PEIM has access to these services. Unlike the EFI Boot Services (see the *EFI 1.10 Specification*), the PEI Services have no calling restrictions, such as the EFI 1.10 Task Priority Level (TPL) limitations. Specifically, a service can be called from a PEIM or notification service.

Some of the services are also a proxy to platform-provided services, such as the Reset Services and Status Code Services. This partitioning has been designed to provide a consistent interface to all PEIMs without encumbering a PEI Foundation implementation with platform-specific knowledge. Any callable services beyond the set in this table should be invoked using a PPI.

4
Services - PEI

Introduction

A PEI Service is defined as a function, command, or other capability created by the PEI Foundation during a phase that remains available after the phase is complete. Because the PEI phase has no permanent memory available until nearly the end of the phase, the range of PEI Foundation Services created during the PEI phase cannot be as rich as those created during later phases.

The following are PEI Services, which are described in this section:

PPI Services:	Manages PEIM-to-PEIM Interface (PPIs) to facilitate intermodule calls between PEIMs. Interfaces are installed and tracked on a database maintained in temporary RAM.
Boot Mode Services:	Manages the boot mode (S3, S5, normal boot, diagnostics, etc.) of the system.
HOB Services:	Creates data structures called Hand-Off Blocks (HOBs) that are used to pass information to the next phase of the Framework.
Firmware Volume Services:	Walks the Firmware File System (FFS) in firmware volumes to find PEIMs and other firmware files in the flash device.
PEI Memory Services:	Provides a collection of memory management services for use both before and after permanent memory has been discovered.
Status Code Services:	Provides common progress and error code reporting services (for example, port 080h or a serial port for simple text output for debug).
Reset Services:	Provides a common means by which to initiate a warm or cold restart of the system.

The calling convention for PEI Services is similar to PPIs. See PEIM-to-PEIM Communication for more details on PPIs.

The means by which to bind a service call into a service involves a dispatch table, **`EFI_PEI_SERVICES`**. A pointer to the table is passed into the PEIM entry point.

PPI Services

PPI Services

The following services provide the interface set for abstracting the PPI database:

- InstallPpi()
- ReinstallPpi()
- LocatePpi()
- NotifyPpi()

InstallPpi()

Summary

This service is the first one provided by the PEI Foundation. This function installs an interface in the PEI PPI database by GUID. The purpose of the service is to publish an interface that other parties can use to call additional PEIMs.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_INSTALL_PPI) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN EFI_PEI_PPI_DESCRIPTOR       *PpiList
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

PpiList

A pointer to the list of interfaces that the caller shall install. Type **EFI_PEI_PPI_DESCRIPTOR** is defined in PEIM Descriptors.

Description

This service enables a given PEIM to register an interface into the PEI Foundation. The interface takes a pointer to a list of records that adhere to the format of a **EFI_PEI_PPI_DESCRIPTOR**. The list is embedded into the image of a PEIM. The length of the list of described by the **EFI_PEI_PPI_DESCRIPTOR** that has the **EFI_PEI_PPI_DESCRIPTOR_TERMINATE_LIST** flag set in its *Flags* field. There shall be at least one **EFI_PEI_PPI_DESCRIPTOR** in the list.

There are two types of **EFI_PEI_PPI_DESCRIPTOR**s that can be installed, including the **EFI_PEI_PPI_DESCRIPTOR_NOTIFY_DISPATCH** and **EFI_PEI_PPI_DESCRIPTOR_NOTIFY_CALLBACK**.

Status Codes Returned

EFI_SUCCESS	The interface was successfully installed.
EFI_INVALID_PARAMETER	The *PpiList* pointer is **NULL**.
EFI_INVALID_PARAMETER	Any of the PEI PPI descriptors in the list do not have the **EFI_PEI_PPI_DESCRIPTOR_PPI** bit set in the *Flags* field.
EFI_OUT_OF_RESOURCES	There is no additional space in the PPI database.

ReinstallPpi()

Summary

This function reinstalls an interface in the PEI PPI database by GUID. The purpose of the service is to publish an interface that other parties can use to replace a same-named interface in the protocol database with a different interface.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_REINSTALL_PPI) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN EFI_PEI_PPI_DESCRIPTOR       *OldPpi,
  IN EFI_PEI_PPI_DESCRIPTOR       *NewPpi
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

OldPpi

A pointer to the former PPI in the database. Type **EFI_PEI_PPI_DESCRIPTOR** is defined in PEIM Descriptors.

NewPpi

A pointer to the new interfaces that the caller shall install.

Description

This service enables PEIMs to replace an entry in the PPI database with an alternate entry. This service is similar to the EFI 1.0 Boot Service **ReinstallProtocolInterface()**. The use of this service is similar inasmuch as a PEIM might wish to multiplex several services that are already installed, such as a console splitter.

ReinstallPpi() will only reinstall a single PPI instance. **EFI_PEI_PPI_DESCRIPTOR**s can be concatenated to install a series of PPIs.

Status Codes Returned

EFI_SUCCESS	The interface was successfully installed.
EFI_INVALID_PARAMETER	The *PpiList* pointer is **NULL**.
EFI_INVALID_PARAMETER	Any of the PEI PPI descriptors in the list do not have the **EFI_PEI_PPI_DESCRIPTOR_PPI** bit set in the *Flags* field.
EFI_OUT_OF_RESOURCES	There is no additional space in the PPI database.
EFI_NOT_FOUND	The PPI for which the reinstallation was requested has not been installed.

LocatePpi()

Summary

This function locates an interface in the PEI PPI database by GUID.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_LOCATE_PPI) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN EFI_GUID                     *Guid,
  IN UINTN                        Instance,
  IN OUT EFI_PEI_PPI_DESCRIPTOR   **PpiDescriptor,
  IN OUT VOID                     **Ppi
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** published by the PEI Foundation.

Guid

A pointer to the GUID whose corresponding interface needs to be found.

Instance

The N-th instance of the interface that is required.

PpiDescriptor

A pointer to instance of the **EFI_PEI_PPI_DESCRIPTOR**.

Ppi

A pointer to the instance of the interface.

Description

This service enables PEIMs to discover a given instance of an interface. This interface differs from the interface discovery mechanism in the *EFI 1.0 Specification,* namely **HandleProtocol()**, in that the PEI PPI database does not expose the handle's name space. Instead, PEI manages the interface set by maintaining a partial order on the interfaces such that the *Instance* of the interface, among others, can be traversed.

LocatePpi() provides the ability to traverse all of the installed instances of a given GUID-named PPI. For example, there can be multiple instances of a PPI named *Foo* in the PPI database. An *Instance* value of 0 will provide the first instance of the PPI that is installed. Correspondingly, an *Instance* value of 2 will provide the second, 3 the third, and so on. The *Instance* value designates when a PPI was installed. For an implementation that must reference all possible manifestations of a given GUID-named PPI, the code should invoke **LocatePpi()** with a monotonically increasing *Instance* number until **EFI_NOT_FOUND** is returned.

Status Codes Returned

EFI_SUCCESS	The interface was successfully returned.
EFI_NOT_FOUND	The PPI descriptor is not found in the database.

NotifyPpi()

Summary

This function installs a notification service to be called back when a given interface is installed or reinstalled. The purpose of the service is to publish an interface that other parties can use to call additional PPIs that may materialize later.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_NOTIFY_PPI) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN EFI_PEI_NOTIFY_DESCRIPTOR    *NotifyList
  );  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

NotifyList

A pointer to the list of notification interfaces that the caller shall install. Type **EFI_PEI_NOTIFY_DESCRIPTOR** is defined in PEIM Descriptors.

Description

This service enables PEIMs to register a given service to be invoked when another service is installed or reinstalled. This service is similar to the EFI 1.0 **RegisterProtocolNotify()**. The semantics of this event are slightly different than that of EFI 1.0 in that the callback is only invoked one time per installation of the notify service. **EFI_PEI_NOTIFY_DESCRIPTOR** is defined in PEIM Descriptors.

In addition, the PPI pointer is passed back to the agent that registered for the notification so that it can deference private data, if so needed.

Status Codes Returned

EFI_SUCCESS	The interface was successfully installed.
EFI_INVALID_PARAMETER	The *NotifyList* pointer is **NULL**.
EFI_INVALID_PARAMETER	Any of the PEI notify descriptors in the list do not have the **EFI_PEI_PPI_DESCRIPTOR_NOTIFY_TYPES** bit set in the *Flags* field.
EFI_OUT_OF_RESOURCES	There is no additional space in the PPI database.

Boot Mode Services

These services provide abstraction for ascertaining and updating the boot mode:

- GetBootMode()
- SetBootMode()

See Boot Paths for additional information on the boot mode.

GetBootMode()

Summary

This function returns the present value of the boot mode.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_GET_BOOT_MODE) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN OUT EFI_BOOT_MODE            *BootMode
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

BootMode

A pointer to contain the value of the boot mode. Type **EFI_BOOT_MODE** is defined in "Related Definitions" below.

Description

This service enables PEIMs to ascertain the present value of the boot mode. The list of possible boot modes is described in "Related Definitions" below.

Related Definitions

```
//***********************************************************
// EFI_BOOT_MODE
//***********************************************************
typedef UINT32     EFI_BOOT_MODE;

#define BOOT_WITH_FULL_CONFIGURATION                          0x00
#define BOOT_WITH_MINIMAL_CONFIGURATION                       0x01
#define BOOT_ASSUMING_NO_CONFIGURATION_CHANGES                0x02
#define BOOT_WITH_FULL_CONFIGURATION_PLUS_DIAGNOSTICS         0x03
#define BOOT_WITH_DEFAULT_SETTINGS                            0x04
#define BOOT_ON_S4_RESUME                                     0x05
#define BOOT_ON_S5_RESUME                                     0x06
#define BOOT_ON_S2_RESUME                                     0x10
#define BOOT_ON_S3_RESUME                                     0x11
#define BOOT_ON_FLASH_UPDATE                                  0x12
#define BOOT_IN_RECOVERY_MODE                                 0x20
0x21 - 0xF..F Reserved Encodings
```

The following table describes the bit values in the Boot Mode Register.

Table 4-1. Boot Mode Register

REGISTER BIT(S)	VALUES	DESCRIPTIONS
MSBit-0	000000b	Boot with full configuration
	000001b	Boot with minimal configuration
	000010b	Boot assuming no configuration changes from last boot
	000011b	Boot with full configuration plus diagnostics
	000100b	Boot with default settings
	000101b	Boot on S4 resume
	000110b	Boot in S5 resume
	000111b-001111b	Reserved for boot paths that configure memory
	010000b	Boot on S2 resume
	010001b	Boot on S3 resume
	010010b	Boot on flash update restart
	010011b-011111b	Reserved for boot paths that preserve memory context
	100000b	Boot in recovery mode
	100001b-111111b	Reserved for special boots

Status Codes Returned

EFI_SUCCESS	The boot mode was returned successfully.

SetBootMode()

Summary

This function sets the value of the boot mode.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_SET_BOOT_MODE) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN EFI_BOOT_MODE                BootMode
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

BootMode

The value of the boot mode to set. Type **EFI_BOOT_MODE** is defined in **GetBootMode()**.

Description

This service enables PEIMs to update the boot mode variable. This would be used by either the boot mode PPIs described in Architectural PPIs or by a PEIM that needs to engender a recovery condition.

Status Codes Returned

EFI_SUCCESS	The value was successfully updated.

HOB Services

The following services describe the capabilities in the PEI Foundation for providing Hand-Off Block (HOB) manipulation:

- GetHobList()
- CreateHob()

The purpose of the abstraction is to automate the common case of HOB creation and manipulation. See the *Intel® Platform Innovation Framework for EFI Hand-Off Block (HOB) Specification* for details on HOBs and their type definitions.

GetHobList()

Summary

This function returns the pointer to the list of Hand-Off Blocks (HOBs) in memory.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_GET_HOB_LIST) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN OUT VOID                     **HobList
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

HobList

A pointer to the list of HOBs that the PEI Foundation will initialize.

Description

This service enables a PEIM to ascertain the address of the list of HOBs in memory. This service should not be required by many modules in that the creation of HOBs is provided by the PEI Service **CreateHob()**.

Status Codes Returned

EFI_SUCCESS	The list was successfully returned.
EFI_NOT_AVAILABLE_YET	The HOB list is not yet published.

CreateHob()

Summary

This service published by the PEI Foundation abstracts the creation of a Hand-Off Block's (HOB's) headers.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_CREATE_HOB) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN UINT16                       Type,
  IN UINT16                       Length,
  IN OUT VOID                     **Hob
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

Type

The type of HOB to be installed. See the *Intel® Platform Innovation Framework for EFI Hand-Off Block (HOB) Specification* for a definition of this type.

Length

The length of the HOB to be added. See the *Intel® Platform Innovation Framework for EFI Hand-Off Block (HOB) Specification* for a definition of this type.

Hob

The address of a pointer that will contain the HOB header.

Description

This service enables PEIMs to create various types of HOBs. This service handles the common work of allocating memory on the HOB list, filling in the type and length fields, and building the end of the HOB list. The final aspect of this service is to return a pointer to the newly allocated HOB. At this point, the caller can fill in the type-specific data. This service is always available because the HOBs can also be created on temporary memory.

There will be no error checking on the *Length* input argument. Instead, the Framework implementation of this service will round up the allocation size that is specified in the *Length* field to be a multiple of 8 bytes in length. This rounding is consistent with the requirement that all of the HOBs, including the PHIT HOB, begin on an 8-byte boundary. See the PHIT HOB definition in the *Intel® Platform Innovation Framework for EFI Hand-Off Block (HOB) Specification* for more information.

Status Codes Returned

EFI_SUCCESS	The HOB was successfully created.
EFI_OUT_OF_RESOURCES	There is no additional space for HOB creation.

Firmware Volume Services

The following services abstract traversing the Firmware File System (FFS):

- FfsFindNextVolume()
- FfsFindNextFile()
- FfsFindSectionData()

The description of the FFS can be found in the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification* and *Intel® Platform Innovation Framework for EFI Firmware File System Specification.*

FfsFindNextVolume()

Summary

The purpose of the service is to abstract the capability of the PEI Foundation to discover instances of firmware volumes in the system. Given the input file pointer, this service searches for the next matching file in the Firmware File System (FFS) volume.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_FFS_FIND_NEXT_VOLUME) (
  IN struct _EFI_PEI_SERVICES          **PeiServices,
  IN UINTN                             Instance,
  IN OUT EFI_FIRMWARE_VOLUME_HEADER    **FwVolHeader
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

Instance

This instance of the firmware volume to find. The value 0 is the Boot Firmware Volume (BFV).

FwVolHeader

Pointer to the firmware volume header of the volume to return. Type **EFI_FIRMWARE_VOLUME_HEADER** is defined in the *Intel® Platform Innovation Framework for EFI Firmware Volume Block Specification.*

Description

This service enables PEIMs to discover additional firmware volumes. This capability might be employed by the DXE IPL PPI to discover the DXE Foundation FFS file, for example, or for a PEIM to inspect all available volumes.

The PEI Foundation publishes this service to abstract the location of various firmware volumes. These volumes can include the boot firmware volume and any additional volumes exposed by the **EFI_FIND_FV_PPI** instances, if the latter are available.

Status Codes Returned

EFI_SUCCESS	The volume was found.
EFI_NOT_FOUND	The volume was not found.
EFI_INVALID_PARAMETER	*FwVolHeader* is **NULL**

FfsFindNextFile()

Summary

The purpose of the service is to abstract the capability of the PEI Foundation to discover instances of firmware files in the system. Given the input file pointer, this service searches for the next matching file in the Firmware File System (FFS) volume.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_FFS_FIND_NEXT_FILE) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN EFI_FV_FILETYPE              SearchType,
  IN EFI_FIRMWARE_VOLUME_HEADER   *FwVolHeader,
  IN OUT EFI_FFS_FILE_HEADER      **FileHeader
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

SearchType

A filter to find files only of this type. Type **EFI_FV_FILETYPE** is defined in the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification.* Type **EFI_FV_FILETYPE_ALL** causes no filtering to be done.

FwVolHeader

Pointer to the firmware volume header of the volume to search. This parameter must point to a valid FFS volume. Type **EFI_FIRMWARE_VOLUME_HEADER** is defined in the *Intel® Platform Innovation Framework for EFI Firmware Volume Block Specification.*

FileHeader

Pointer to the current file from which to begin searching. This pointer will be updated upon return to reflect the file found. Type **EFI_FFS_FILE_HEADER** is defined in the *Intel® Platform Innovation Framework for EFI Firmware File System Specification.*

Description

This service enables PEIMs to discover additional firmware files. This capability might be employed by the DXE IPL PPI to discover the DXE Foundation FFS file, for example. To find the first instance of a firmware file, pass a *FileHeader* value of **NULL** into the service.

For integrity checking of the file, only the header checksum is calculated. No other FFS integrity values are checked by this service.

Status Codes Returned

EFI_SUCCESS	The file was found.
EFI_NOT_FOUND	The file was not found.
EFI_NOT_FOUND	The header checksum was not zero.

FfsFindSectionData()

Summary

Given the input file pointer, this service searches for the next matching file in the Firmware File System (FFS) volume.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_FFS_FIND_SECTION_DATA) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN EFI_SECTION_TYPE             SectionType,
  IN EFI_FFS_FILE_HEADER          *FfsFileHeader,
  IN OUT VOID                     **SectionData
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

SectionType

The value of the section type to find. Type **EFI_SECTION_TYPE** is defined in the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification.*

FfsFileHeader

A pointer to the file header that contains the set of sections to be searched. Type **EFI_FFS_FILE_HEADER** is defined in the *Intel® Platform Innovation Framework for EFI Firmware File System Specification.*

SectionData

A pointer to the discovered section, if successful.

Description

This service enables PEIMs to discover sections of a given type within a valid FFS file. The semantics of this interface are precise in that there can be only one instance of a given section type within a file, versus **FfsFindNextFile()**, which needs to be iteratively invoked.

Status Codes Returned

EFI_SUCCESS	The section was found.
EFI_NOT_FOUND	The section was not found.

PEI Memory Services

The following services are a collection of memory management services for use both before and after permanent memory has been discovered:

- InstallPeiMemory()
- AllocatePages()
- AllocatePool()
- CopyMem()
- SetMem()

InstallPeiMemory()

Summary

This function registers the found memory configuration with the PEI Foundation.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_INSTALL_PEI_MEMORY) (
  IN struct _EFI_PEI_SERVICES     **PeiServices,
  IN EFI_PHYSICAL_ADDRESS         MemoryBegin,
  IN UINT64                       MemoryLength
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

MemoryBegin

The value of a region of installed memory.

MemoryLength

The corresponding length of a region of installed memory.

Description

This service enables PEIMs to register the permanent memory configuration that has been initialized with the PEI Foundation. The result of this call-set is the creation of the appropriate Hand-Off Block (HOB) describing the physical memory.

The usage model is that the PEIM that discovers the permanent memory shall invoke this service. The memory reported is a single contiguous run. It should be enough to allocate a PEI stack and some HOB list. The full memory map will be reported using the appropriate memory HOBs. The PEI Foundation will follow up with an installation of **EFI_PEI_PERMANENT_MEMORY_INSTALLED_PPI**.

Status Codes Returned

EFI_SUCCESS	The region was successfully installed in a HOB.
EFI_INVALID_PARAMETER	*MemoryBegin* and *MemoryLength* are illegal for this system.
EFI_OUT_OF_RESOURCES	There is no additional space for HOB creation.

AllocatePages()

Summary

The purpose of the service is to publish an interface that allows PEIMs to allocate memory ranges that are managed by the PEI Foundation.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_ALLOCATE_PAGES) (
  IN struct _EFI_PEI_SERVICES    **PeiServices,
  IN EFI_ALLOCATE_TYPE           Type,
  IN EFI_MEMORY_TYPE             MemoryType,
  IN UINTN                       Pages,
  OUT EFI_PHYSICAL_ADDRESS       *Memory,
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

Type

The type of allocation to perform. Type **EFI_ALLOCATE_TYPE** is defined in **AllocatePages()** in the *EFI 1.10 Specification.*

MemoryType

The type of memory to allocate. The only types allowed are **EfiLoaderCode**, **EfiLoaderData**, **EfiRuntimeServicesCode**, **EfiRuntimeServicesData**, **EfiBootServicesCode**, **EfiBootServicesData**, **EfiACPIReclaimMemory**, and **EfiACPIMemoryNVS**. Normal allocations (that is, allocations by any EFI application) are of type **EfiLoaderData**. Type **EFI_MEMORY_TYPE** is defined in the *EFI 1.10 Specification.*

Pages

The number of contiguous 4 KB pages to allocate. Type **EFI_PHYSICAL_ADDRESS** is defined in **AllocatePages()** in the *EFI 1.10 Specification.*

Memory

Pointer to a physical address. On output, the address is set to the base of the page range that was allocated.

Description

This service enables PEIMs to allocate memory after the permanent memory has been installed by a PEIM. The purpose of this service is to allow more stateful, later PEIMs to have a single set of memory allocation services upon which to rely. This is especially of interest for services like the recovery PEIMs that might have to allocate large buffers for disk transactions and file system metadata. The memory regions that the memory allocation primitives manage will be described in the appropriate HOB type from the *Intel® Platform Innovation Framework for EFI Hand-Off Block (HOB) Specification.*

This service is not usable prior to the installation of main memory. There is no free memory.

The expectation is that the implementation of this service will automate the creation of the Memory Allocation HOB types. As such, this is in the same spirit as the PEI Services to create the FV HOB, for example.

The service also supports the creation of Memory Allocation HOBs that describe the stack, boot-strap processor (BSP) BSPStore ("Backing Store Pointer Store"), and the DXE Foundation allocation. This additional information is conveyed through the final two arguments in this API and the description of the appropriate HOB types can be founding the *Intel® Platform Innovation Framework for EFI Hand-Off Block (HOB) Specification.*

Status Codes Returned

EFI_SUCCESS	The memory range was successfully allocated.
EFI_OUT_OF_RESOURCES	The pages could not be allocated.
EFI_INVALID_PARAMETER	*Type* is not equal to **AllocateAnyPages**.

AllocatePool()

Summary

The purpose of this service is to publish an interface that allows PEIMs to allocate memory ranges that are managed by the PEI Foundation.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_ALLOCATE_POOL) (
  IN struct _EFI_PEI_SERVICES    **PeiServices,
  IN UINTN                       Size,
  OUT VOID                       **Buffer
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

Size

The number of bytes to allocate from the pool.

Buffer

If the call succeeds, a pointer to a pointer to the allocated buffer; undefined otherwise.

Description

This service allocates memory from the Hand-Off Block (HOB) heap. Because HOBs can be allocated from either temporary or permanent memory, this service is available throughout the entire PEI phase.

This service allocates memory in multiples of eight bytes to maintain the required HOB alignment. The early allocations from temporary memory will be migrated to permanent memory when permanent main memory is installed; this migration shall occur when the HOB list is migrated to permanent memory.

Status Codes Returned

EFI_SUCCESS	The allocation was successful.
EFI_OUT_OF_RESOURCES	There is not enough heap to allocate the requested size.

CopyMem()

Summary

This service copies the contents of one buffer to another buffer.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_COPY_MEM) (
  IN VOID                                   *Destination,
  IN VOID                                   *Source,
  IN UINTN                                  Length
  );
```

Parameters

Destination

Pointer to the destination buffer of the memory copy.

Source

Pointer to the source buffer of the memory copy.

Length

Number of bytes to copy from *Source* to *Destination*.

Description

This function copies *Length* bytes from the buffer *Source* to the buffer *Destination*.

Status Codes Returned

None.

SetMem()

Summary

The service fills a buffer with a specified value.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_SET_MEM) (
  IN VOID                                   *Buffer,
  IN UINTN                                  Size,
  IN UINT8                                  Value
  );
```

Parameters

Buffer

Pointer to the buffer to fill.

Size

Number of bytes in *Buffer* to fill.

Value

Value to fill *Buffer* with.

Description

This function fills *Size* bytes of *Buffer* with *Value*.

Status Codes Returned

None.

Status Code Service

The PEI Foundation publishes the following status code service:

- ReportStatusCode()

This service will report **EFI_NOT_AVAILABLE_YET** until a PEIM publishes the services for other modules. For the GUID of the PPI, see **EFI_PEI_PROGRESS_CODE_PPI**.

ReportStatusCode()

Summary

This service publishes an interface that allows PEIMs to report status codes.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_REPORT_STATUS_CODE) (
  IN struct _EFI_PEI_SERVICES **PeiServices,
  IN EFI_STATUS_CODE_TYPE     Type,
  IN EFI_STATUS_CODE_VALUE    Value,
  IN UINT32                   Instance,
  IN EFI_GUID                 *CallerId  OPTIONAL,
  IN EFI_STATUS_CODE_DATA     *Data      OPTIONAL
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

Type

Indicates the type of status code being reported. The type **EFI_STATUS_CODE_TYPE** is defined in "Related Definitions" below.

Value

Describes the current status of a hardware or software entity. This includes information about the class and subclass that is used to classify the entity as well as an operation. For progress codes, the operation is the current activity. For error codes, it is the exception. For debug codes, it is not defined at this time. Type **EFI_STATUS_CODE_VALUE** is defined in "Related Definitions" below. Specific values are discussed in the *Intel® Platform Innovation Framework for EFI Status Code Specification*.

Instance

The enumeration of a hardware or software entity within the system. A system may contain multiple entities that match a class/subclass pairing. The instance differentiates between them. An instance of 0 indicates that instance information is unavailable, not meaningful, or not relevant. Valid instance numbers start with 1.

CallerId

This optional parameter may be used to identify the caller. This parameter allows the status code driver to apply different rules to different callers.

Data

This optional parameter may be used to pass additional data. Type **EFI_STATUS_CODE_DATA** is defined in "Related Definitions" below. The contents of this data type may have additional GUID-specific data. The standard GUIDs and their associated data structures are defined in the *Intel® Platform Innovation Framework for EFI Status Codes Specification*.

Description

ReportStatusCode() is called by PEIMs that wish to report status information on their progress. The principal use model is for a PEIM to emit one of the standard 32-bit error codes that are defined in the *Intel® Platform Innovation Framework for EFI Status Code Specification.* This will allow a platform owner to ascertain the state of the system, especially under conditions where the full consoles might not have been installed.

This is the entry point that PEIMs shall use. This service can use all platform PEI Services, and when main memory is available, it can even construct a GUIDed HOB that conveys the pre-DXE data as an input to the data hub. This service can also publish an interface that is usable only from the DXE phase. This entry point should not be the same as that published to the PEIMs, and the implementation of this code path should *not* do the following:

- Use any PEI Services or PPIs from other modules.
- Make any presumptions about global memory allocation.

It can only operate on its local stack activation frame and must be careful about using I/O and memory-mapped I/O resources. These concerns, including the latter warning, arise because this service could be used during the “blackout” period between the termination of PEI and the beginning of DXE, prior to the loading of the DXE progress code driver. As such, the ownership of the memory map and platform resource allocation is indeterminate at this point in the platform evolution.

Related Definitions

```
//
// Status Code Type Definition
//
typedef UINT32 EFI_STATUS_CODE_TYPE;

//
// A Status Code Type is made up of the code type and severity
// All values masked by EFI_STATUS_CODE_RESERVED_MASK are
// reserved for use by this specification.
//
#define EFI_STATUS_CODE_TYPE_MASK       0x000000FF
#define EFI_STATUS_CODE_SEVERITY_MASK   0xFF000000
#define EFI_STATUS_CODE_RESERVED_MASK   0x00FFFF00

//
// Definition of code types, all other values masked by
// EFI_STATUS_CODE_TYPE_MASK are reserved for use by
```

```
// this specification.
//
#define EFI_PROGRESS_CODE               0x00000001
#define EFI_ERROR_CODE                  0x00000002
#define EFI_DEBUG_CODE                  0x00000003

//
// Definitions of severities, all other values masked by
// EFI_STATUS_CODE_SEVERITY_MASK are reserved for use by
// this specification.
// Uncontained errors are major errors that could not contained
// to the specific component that is reporting the error
// For example, if a memory error was not detected early enough,
// the bad data could be consumed by other drivers.
//
#define EFI_ERROR_MINOR                 0x40000000
#define EFI_ERROR_MAJOR                 0x80000000
#define EFI_ERROR_UNRECOVERED           0x90000000
#define EFI_ERROR_UNCONTAINED           0xa0000000

//
// Status Code Value Definition
//
typedef UINT32 EFI_STATUS_CODE_VALUE;

//
// A Status Code Value is made up of the class, subclass, and
// an operation.
//
#define EFI_STATUS_CODE_CLASS_MASK      0xFF000000
#define EFI_STATUS_CODE_SUBCLASS_MASK   0x00FF0000
#define EFI_STATUS_CODE_OPERATION_MASK  0x0000FFFF

//
// Definition of Status Code extended data header.
// The data will follow HeaderSize bytes from the beginning of
// the structure and is Size bytes long.
//
typedef struct {
  UINT16    HeaderSize;
  UINT16    Size;
  EFI_GUID  Type;
} EFI_STATUS_CODE_DATA;
```

HeaderSize

The size of the structure. This is specified to enable future expansion.

Size

The size of the data in bytes. This does not include the size of the header structure.

Type

The GUID defining the type of the data. The standard GUIDs and their associated data structures are defined in the *Intel® Platform Innovation Framework for EFI Status Codes Specification*.

Status Codes Returned

EFI_SUCCESS	The function completed successfully.
EFI_NOT_AVAILABLE_YET	No progress code provider has installed an interface in the system.

Reset Services

The PEI Foundation publishes the following reset service:

- ResetSystem()

ResetSystem()

Summary

Resets the entire platform.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_RESET_SYSTEM) (
  IN struct _EFI_PEI_SERVICES     **PeiServices
  );
```

Parameters

PeiServices

An indirect pointer to the **EFI_PEI_SERVICES** table published by the PEI Foundation.

Description

This service resets the entire platform, including all processors and devices, and reboots the system. It is important to have a standard variant of this function for cases such as the following:

- Resetting the processor to change frequency settings
- Restarting hardware to complete chipset initialization
- Responding to exceptions from a catastrophic error

Returned Status Codes

EFI_SUCCESS	The function completed successfully.

5
PEI Foundation

Introduction

The PEI Foundation centers around the PEI Dispatcher. The dispatcher's job is to hand control to the PEIMs in an orderly manner. The PEI Foundation also assists in PEIM-to-PEIM communication. The central resource for the module-to-module communication involves the PPI. The marshalling of references to PPIs can occur using the installable or notification interface.

The PEI Foundation is constructed as an autonomous binary image that is of file type **`EFI_FV_FILETYPE_PEI_CORE`** and is composed of the following:

- An authentication section
- A code image that is possibly PE32+

See the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification* for information on section and file types. If the code that comprises the PEI Foundation is not a PE32+ image, then it is a raw binary whose lowest address is the entry point to the PEI Foundation. The PEI Foundation is discovered and authenticated by the Security (SEC) phase.

Prerequisites

The PEI phase is handed control from the Security (SEC) phase of the Framework boot process. The PEI phase must satisfy the following minimum prerequisites before it can begin execution:

- Processor execution mode
- Access to the Boot Firmware Volume (BFV) that contains the PEI Foundation

It is expected that the SEC infrastructure code and PEI Foundation are not linked together as a single ROMable executable image. The entry point from SEC into PEI is not architecturally fixed but is instead dependent on the PEI Foundation location within FV0, or the Boot Firmware Volume.

Processor Execution Mode

Processor Execution Mode in IA-32 Intel® Architecture

In IA-32 Intel® architecture, the Security (SEC) phase of the Framework is responsible for placing the processor in a native linear address mode by which the full address range of the processor is accessible for code, data, and stack. For example, “flat 32” is the IA-32 processor generation mode in which the PEI phase will execute. The processor must be in its most privileged "ring 0” mode, or equivalent, and be able to access all memory and I/O space.

This prerequisite is strictly dependent on the processor generation architecture.

Processor Execution Mode in Itanium® Processor Family

The PEI Foundation will begin executing after the Security (SEC) phase has completed. The SEC phase subsumed the System Abstraction Layer entry point (SALE_ENTRY) in Itanium® architecture. In addition, the SEC phase makes the appropriate Processor Abstraction Layer (PAL) calls or platform services to enable the temporary memory store. The SEC passes its handoff state to the PEI Foundation in physical mode with some configured memory stack, such as the processor cache configured as memory.

Access to the Boot Firmware Volume

The program that the Security (SEC) phase hands control to is known as the PEI Foundation. The firmware volume (FV) in which the PEI Foundation resides is known as the Boot Firmware Volume (BFV). PEIMs may reside in the BFV or other FVs. A "special" PEIM must be resident in the BFV to provide information about the location of the other FVs.

Each file contained in the BFV that is required to boot must be able to be discovered and validated by the PEI phase. This allows the PEI phase to determine if the FV has been corrupted.

The PEI Foundation and the PEIMs are expected to be stored in some reasonably tamper-proof (albeit not necessarily in the strict security-based definition of the term) nonvolatile storage (NVS). The storage is expected to be fairly analogous to a flat file system with the unique IDs substituting for names. Rules for using the particular NVS might affect certain storage considerations, but a standard data-only mechanism for locating PEIMs by ID is required. Framework architecture uses the EFI firmware volume and firmware file system, with the GUID convention of naming files in NVS. These standards are architectural for PEI inasmuch as the PEI phase needs to directly support this file system.

The PEI Foundation and some PEIMs required for recovery must be either locked into a nonupdateable BFV or must be able to be updated via a "fault-tolerant" mechanism. The fault-tolerant mechanism is designed such that, if the system halts at any point, either the old (preupdate) PEIM or the newly updated PEIM is entirely valid and that the PEI phase can determine which is valid.

Access to the Boot Firmware Volume in IA-32 Intel® Architecture

In IA-32 Intel® architecture, the Security (SEC) file is at the top of the Boot Firmware Volume (BFV). This SEC file will have the 16-byte entry point for IA-32 and restarts at address 0xFFFFFFF0.

Access to the Boot Firmware Volume in Itanium® Processor Family

In the Itanium® processor family, the microcode starts up the Processor Abstraction Layer A (PAL-A) code, which is the first layer of PAL code and is provided by the processor vendor, that resides in the Boot Firmware Volume (BFV). This code minimally initializes the processor and then finds and authenticates the second layer of PAL code, called PAL-B. The location of both PAL-A and PAL-B can be found by consulting either of the following:

- The architected pointers in the ROM (near the 4 GB region)
- The Firmware Interface Table (FIT) pointer in the ROM

The PAL layer communicates with the OEM boot firmware using a single entry point called the System Abstraction Layer entry point (SALE_ENTRY). The PEI Foundation will be located at the SALE_ENTRY point on the boot firmware device for an Itanium®-based system. The Itanium processor family PEIMs, like other PEIMs, may reside in the BFV or other firmware volumes. A "special" PEIM must be resident in the BFV to provide information about the location of the other firmware volumes; this will be described in the context of the **`EFI_PEI_FIND_FV_PPI`** description. It must also be noted that in an Itanium-based system, all the processors in each node start up and execute the PAL code and subsequently enter the PEI Foundation. The BFV of a particular node must be accessible by all the processors running in that node. This also means that some of the PEIMs in the Itanium® architecture boot path will be multiprocessor (MP) aware.

In an Itanium-based system, it is also imperative that the organization of firmware modules in the BFV must be such that at least the PAL-A is contained in the fault-tolerant regions. This processor-specific PAL-A code authenticates the PAL-B code, which is usually contained in the non-fault-tolerant regions of the firmware system. The PAL-A and PAL-B binary components are always visible to all the processors in a node at the time of power-on; the system fabric should not need to be initialized.

PEI Foundation Entry Point

PEI Foundation Entry Point

The Security (SEC) phase must hand the following key data to the PEI Foundation:

- A set of PPIs
- Information on the Boot Firmware Volume (BFV)
- Size of the cache-as-RAM

The SEC phase hands this data to the PEI Foundation using the structure **EFI_PEI_STARTUP_DESCRIPTOR**.

This PPI list is a collection of data structures that contain PPIs that abstract several things. The most important data is the base of the BFV and other state information known by the SEC phase. Another PPI can include the service used to corroborate the integrity of the PEI Foundation, if the foundation is wrapped in a GUIDed section type. This latter function allows for root-of-trust maintenance from the SEC component into the PEI phase. The SEC Platform Information PPI is the mandatory component.

The figure below depicts the data that is passed to the PEI Foundation from the SEC phase.

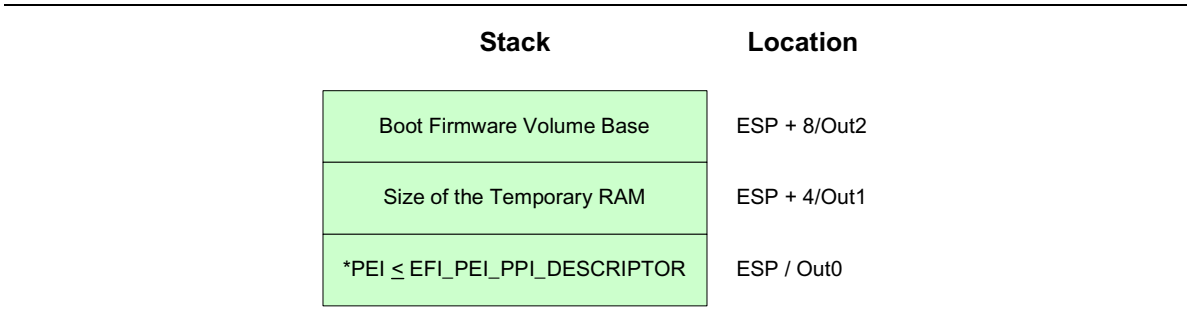


Figure 5-1. Handoff from SEC to PEI for IA-32/Itanium® Processor Family

EFI_PEI_STARTUP_DESCRIPTOR

Summary

Provides the minimum amount of information from the Security (SEC) phase that is required to initialize the PEI Foundation and PEI operational environment.

Prototype

```
typedef struct {
  UINTN                    BootFirmwareVolume;
  UINTN                    SizeOfCacheAsRam;
  EFI_PEI_PPI_DESCRIPTOR   *DispatchTable;
} EFI_PEI_STARTUP_DESCRIPTOR;
```

Parameters

BootFirmwareVolume

Informs the PEI Foundation where to find the Boot Firmware Volume (BFV) and to commence discovery and dispatch of PEIMs.

SizeOfCacheAsRam

Describes the extent of unoccupied cache-as-RAM. The PEI Foundation will apportion this region for use as private data, stack, and heap.

DispatchTable

A pointer to a possibly **NULL** list of PEI PPI descriptors. These descriptors describe services that are resident in SEC but can be used by either the PEI Foundation or other PEIMs. Type **EFI_PEI_PPI_DESCRIPTOR** is defined in PEIM Descriptors.

Description

EFI_PEI_STARTUP_DESCRIPTOR is a **mandatory** data structure that is placed on the stack by the SEC phase to invoke the PEI Foundation.

The SEC phase provides the required processor and/or platform initialization such that there is a temporary RAM region available to the PEI phase. This temporary RAM could be a particular configuration of the processor cache, SRAM, or other source. What is important with respect to this handoff is that the PEI ascertain the available amount of cache as RAM from this data structure. *SizeOfCacheAsRam* does not describe total temporary memory, just the available amount of temporary memory. The stack pointer value upon entry to the PEI Foundation minus the *SizeOfCacheAsRam* field describes the lowest usable address for the PEI Foundation.

Similarly, the PEI Foundation needs to receive *a priori* information about where to commence the dispatch of PEIMs. A platform can have various size BFVs. As such, the *BootFirmwareVolume* value tells the PEI Foundation where it can expect to discover a firmware volume header data structure, **EFI_FIRMWARE_VOLUME_HEADER**, and it is this firmware volume that contains the PEIMs necessary to perform the basic system initialization. Type **EFI_FIRMWARE_VOLUME_HEADER** is defined in the *Intel® Platform Innovation Framework for EFI Firmware Volume Block Specification.*

Finally, later phases of platform evolution might need many of the features and data that the SEC phase might possibly have. Health Flag Bit Format describes the health and self-test information for certain processors. To support this, the SEC phase can construct a **EFI_PEI_PPI_DESCRIPTOR** and pass its address into the PEI Foundation as the final argument. The SEC can also pass an optional PPI, **SEC_PLATFORM_INFORMATION_PPI**, as part of the PPI list that is included as the final argument of **EFI_PEI_STARTUP_DESCRIPTOR**. This PPI abstracts platform-specific information that the PEI Foundation needs to discover where to begin dispatching PEIMs. Other possible values to pass into the PEI Foundation would include any security or verification services, such as the Trusted Computing Group (TCG) access services, because the SEC would constitute the Core Root-of-Trust Module (CRTM) in a TCG-conformant system.

There is no limit to the number of additional PPIs that can be passed from SEC into the PEI Foundation. As part of its initialization phase, the PEI Foundation will add these SEC-hosted PPIs to its PPI database such that both the PEI Foundation and any modules can leverage the associated service calls and/or code in these early PPIs.

6
PEI Dispatcher

Introduction

The PEI Dispatcher's job is to hand control to the PEIMs in an orderly manner. The PEI Dispatcher consists of a single phase. It is during this phase that the PEI Foundation will examine each file in the firmware volumes that contain files of type **`EFI_FV_FILETYPE_PEIM`** (see the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification* for file type definitions). It will examine the dependency expression (depex) within each firmware file to decide when a PEIM is eligible to be dispatched. The binary encoding of the depex will be the same as that of a depex associated with a PEIM.

Ordering

Requirements

It is not reasonable to expect PEIMs to be executed in any order. A chipset initialization PEIM usually requires processor initialization and a memory initialization PEIM usually requires chipset initialization. On the other hand, the PEIMs that satisfy these requirements might have been authored by different organizations and might reside in different FVs. The requirement is thus to, without memory, create a mechanism to allow for the definition of ordering among the different PEIMs so that, by the time a PEIM executes, all of the requirements for it to execute have been met.

Although the update and build processes assist in resolving ordering issues, they cannot be relied upon completely. Consider a system with a removable processor card containing a processor and firmware volume that plugs into a main system board. If the processor card is upgraded, it is entirely reasonable that the user should expect the system to work even though no update program was executed.

Requirement Representation and Notation

Requirements are represented by GUIDs, with each GUID representing a particular requirement. The requirements are represented by two sets of data structures:

- The dependency expression (depex) of a given PEIM
- The installed set of PPIs maintained by the PEI Foundation in the PPI database

This mechanism provides for a "weak ordering" among PEIMs. If PEIMs A and B consume X (written AcX and BcX), once a PEIM (C) that produces X (CpX) is executed, A and B can be executed. There is no definition about the order in which A and B are executed.

PEIM Dependency Expressions

The sequencing of PEIMs is determined by evaluating a *dependency expression* associated with each PEIM. This expression describes the requirements necessary for that PEIM to run, which imposes a weak ordering on the PEIMs. Within this weak ordering, the PEIMs may be initialized in any order.

Types of Dependencies

The base unit of the dependency expression is a dependency. A representative syntax (used in this document for descriptive purposes) for each dependency is shown in the following section. The syntax is case-insensitive and mnemonics are used in place of non-human-readable data such as GUIDs. White space is optional.

The operands are GUIDs of PPIs. The operand becomes "true" when a PPI with the GUID is registered.

Dependency Expressions

Introduction

A PEIM is stored in a firmware volume as a file with one or more sections. One of the sections must be a PE32+ image. If a PEIM has a dependency expression, then it is stored in a dependency section. A PEIM may contain additional sections for compression and security wrappers. The PEI Dispatcher can identify the PEIMs by their file type. In addition, the PEI Dispatcher can look up the dependency expression for a PEIM by looking for a dependency section in a PEIM file. The dependency section contains a section header followed by the actual dependency expression that is composed of a packed byte stream of opcodes and operands.

Dependency expressions stored in dependency sections are designed to meet the following goals:

- Be small to conserve space.
- Be simple and quick to evaluate to reduce execution overhead.

These two goals are met by designing a small, stack-based instruction set to encode the dependency expressions. The PEI Dispatcher must implement an interpreter for this instruction set to evaluate dependency expressions. The instruction set is defined in the following topics.

See Dependency Expression Grammar for an example BNF grammar for a dependency expression compiler. There are many possible methods of specifying the dependency expression for a PEIM. This example grammar demonstrates one possible design for a tool that can be used to help build PEIM images.

Dependency Expression Instruction Set

The following topics describe each of the dependency expression (depex) opcodes in detail. Information includes a description of the instruction functionality, binary encoding, and any limitations or unique behaviors of the instruction.

Several of the opcodes require a GUID operand. The GUID operand is a 16-byte value that matches the type **EFI_GUID** that is described in Chapter 2 of the *EFI 1.10 Specification*. These GUIDs represent PPIs that are produced by PEIMs and the file names of PEIMs stored in firmware volumes. A dependency expression is a packed byte stream of opcodes and operands. As a result, some of the GUID operands will not be aligned on natural boundaries. Care must be taken on processor architectures that do allow unaligned accesses.

The dependency expression is stored in a packed byte stream using postfix notation. As a dependency expression is evaluated, the operands are pushed onto a stack. Operands are popped off the stack to perform an operation. After the last operation is performed, the value on the top of the stack represents the evaluation of the entire dependency expression. If a push operation causes a stack overflow, then the entire dependency expression evaluates to **FALSE**. If a pop operation causes a stack underflow, then the entire dependency expression evaluates to **FALSE**. Reasonable implementations of a dependency expression evaluator should not make arbitrary assumptions about the maximum stack size it will support. Instead, it should be designed to grow the dependency expression stack as required. In addition, PEIMs that contain dependency expressions should make an effort to keep their dependency expressions as small as possible to help reduce the size of the PEIM.

All opcodes are 8-bit values, and if an invalid opcode is encountered, then the entire dependency expression evaluates to **FALSE**.

If an END opcode is not present in a dependency expression, then the entire dependency expression evaluates to **FALSE**.

If an instruction encoding extends beyond the end of the dependency section, then the entire dependency expression evaluates to **FALSE**.

The final evaluation of the dependency expression results in either a **TRUE** or **FALSE** result.

NOTE

The PEI Foundation will only support the evaluation of dependency expressions that are less than or equal to 256 terms.

The table below is a summary of the opcodes that are used to build dependency expressions. The following sections describe each of these instructions in detail.

Table 6-1. Dependency Expression Opcode Summary

Opcode	Description
0x02	PUSH <PPI GUID>
0x03	AND
0x04	OR
0x05	NOT
0x06	TRUE
0x07	FALSE
0x08	END

PUSH

SYNTAX:

PUSH <PPI GUID>

DESCRIPTION:

Pushes a Boolean value onto the stack. If the GUID is present in the handle database, then a **TRUE** is pushed onto the stack. If the GUID is not present in the handle database, then a **FALSE** is pushed onto the stack. The test for the GUID in the handle database may be performed with the Boot Service **LocatePpi()**.

OPERATION:

```
Status = (*PeiServices)->LocatePpi (PeiServices, GUID, 0, NULL,
&Interface);
if (EFI_ERROR (Status)) {
  PUSH FALSE;
} Else {
  PUSH TRUE;
}
```

The following table defines the PUSH instruction encoding.

Table 6-2. PUSH Instruction Encoding

BYTE	DESCRIPTION
0	0x02
1..16	A 16-byte GUID that represents a protocol that is produced by a different PEIM. The format is the same at type **EFI_GUID**.

BEHAVIORS AND RESTRICTIONS:

None.

AND

SYNTAX:

AND

DESCRIPTION:

Pops two Boolean operands off the stack, performs a Boolean AND operation between the two operands, and pushes the result back onto the stack.

OPERATION:

Operand1 <= POP Boolean stack element

Operand2 <= POP Boolean stack element

Result <= Operand1 AND Operand2

PUSH Result

The following table defines the AND instruction encoding.

Table 6-3. AND Instruction Encoding

BYTE	DESCRIPTION
0	0x03

BEHAVIORS AND RESTRICTIONS:

None.

OR

SYNTAX:

OR

DESCRIPTION:

Pops two Boolean operands off the stack, performs a Boolean OR operation between the two operands, and pushes the result back onto the stack.

OPERATION:

Operand1 <= POP Boolean stack element

Operand2 <= POP Boolean stack element

Result <= Operand1 OR Operand2

PUSH Result

The following table defines the OR instruction encoding.

Table 6-4. OR Instruction Encoding

BYTE	DESCRIPTION
0	0x04

BEHAVIORS AND RESTRICTIONS:

None.

NOT

SYNTAX:

NOT

DESCRIPTION:

Pops a Boolean operands off the stack, performs a Boolean NOT operation on the operand, and pushes the result back onto the stack.

OPERATION:

Operand <= POP Boolean stack element

Result <= NOT Operand

PUSH Result

The following table defines the NOT instruction encoding.

Table 6-5. NOT Instruction Encoding

BYTE	DESCRIPTION
0	0x05

BEHAVIORS AND RESTRICTIONS:

None.

TRUE

SYNTAX:

TRUE

DESCRIPTION:

Pushes a Boolean **TRUE** onto the stack.

OPERATION:

PUSH **TRUE**

The following table defines the TRUE instruction encoding.

Table 6-6. TRUE Instruction Encoding

BYTE	DESCRIPTION
0	0x06

BEHAVIORS AND RESTRICTIONS:

None.

FALSE

SYNTAX:

FALSE

DESCRIPTION:

Pushes a Boolean **FALSE** onto the stack.

OPERATION:

PUSH **FALSE**

The following table defines the FALSE instruction encoding.

Table 6-7. FALSE Instruction Encoding

BYTE	DESCRIPTION
0	0x07

BEHAVIORS AND RESTRICTIONS:

None.

END

SYNTAX:

END

DESCRIPTION:

Pops the final result of the dependency expression evaluation off the stack and exits the dependency expression evaluator.

OPERATION:

POP Result

RETURN Result

The following table defines the END instruction encoding.

Table 6-8. END Instruction Encoding

BYTE	DESCRIPTION
0	0x08

BEHAVIORS AND RESTRICTIONS:

This opcode must be the last one in a dependency expression.

Dependency Expression with No Dependencies

A PEIM that does not have any dependencies will have a dependency expression that evaluates to **TRUE** with no dependencies on any PPI GUIDs.

Empty Dependency Expressions

If a PEIM file does not contain a dependency section, then the PEIM has an empty dependency expression.

Dependency Expression Reverse Polish Notation (RPN)

The actual equations will be presented by the PEIM in a simple-to-evaluate form, namely postfix.

The following is a BNF encoding of this grammar. See Dependency Expression Instruction Set for definitions of the dependency expressions.

```
<statement> ::= <expression> END

<expression> ::= PUSH <guid> |
                 TRUE |
                 FALSE |
                 <expression> NOT |
                 <expression> <expression> OR |
                 <expression> <expression> AND
```

Dispatch Algorithm

Overview

Ordering Algorithm

The dispatch algorithm repeatedly scans through the PEIMs to find those that have not been dispatched. For each PEIM that is found, it scans through the PPI database of PPIs that have been published, searching for elements in the yet-to-be-dispatched PEIM's depex. If all of the elements in the depex are in the PEI Foundation's PPI database, the PEIM is dispatched. The phase terminates when all PEIMs are scanned and none dispatched.

NOTE

The PEIM may be dispatched without a search if its depex is NULL.

Multiple Firmware Volume Support

The scanning process is complicated by the requirement that multiple firmware volumes (FVs) be supported. A special PPI, **EFI_FIND_FV_PPI**, is defined. This interface's role is to describe to the PEI Foundation where other FVs are located so that they can be searched for PEIMs. **EFI_FIND_FV_PPI** may be published by several possible PEIMs.

Recovery Dispatching

Any PEIM or the PEI Foundation can engender a crisis recovery. This transition could occur because of either of the following:

- A PEIM sets the boot mode to **BOOT_IN_RECOVERY_MODE** using the PEI Service **SetBootMode()**.
- The PEI Dispatcher detects that a PEIM failed to validate.

The PEI Dispatcher will attempt to dispatch all PEIMs again. The platform PEIM will install the **EFI_PEI_BOOT_IN_RECOVERY_MODE_PEIM_PPI** so that modules that wish to be dispatched only during a crisis recovery will be invoked.

The initial state of the boot mode variable is the key distinction from a dispatch that starts from a cold reset and one engendered by a forced recovery. For a cold reset, the boot mode will not be defined until the Master Boot Mode PPI has been installed, with the corresponding requirement that the module that published this PPI also used the PEI Service **SetBootMode()** to initialize the boot mode. For the recovery condition, the boot mode will have been received by a PEIM as being updated to "Need to Recover" or reset to Recovery by the PEI Foundation based on same failure condition (failure to authenticate a subsequent firmware volume, for example). In either of the latter cases, the dispatch will restart with the boot mode set to **BOOT_IN_RECOVERY_MODE**.

Requirements

Requirements of a Dispatching Algorithm

The dispatching algorithm must meet the following requirements:

1. Preserve the dispatch weak ordering.
2. Prevent an infinite loop.
3. Control processor resources.
4. Preserve proper dispatch order.
5. Make use of available memory.
6. Invoke each PEIM's entry point.
7. Know when the PEI Dispatcher tasks are finished.

Preserving Weak Ordering

The algorithm must preserve the weak ordering implied by the depex.

Preventing Infinite Loops

It is illegal for AcXpY (A consumes X and produces Y) and BcYpX. This is known as a cycle and is unresolvable even if memory is available. At a minimum, the dispatching algorithm must not end up in an infinite loop in such a scenario. With the algorithm described above, neither PEIM would be executed.

Controlling Processor Register Resources

The algorithm must require that a minimum of the processor's register resources be preserved while PEIMs are dispatched.

Preserving Proper Dispatch Order

The algorithm must preserve proper dispatch order in cases such as the following:

```
AcQpZ BcLpR CpL DcRpQ
```

The issue with the above scenario is that A and B are not obviously related until D is processed. If A and B were in one firmware volume and C and D were in another, the ordering could not be resolved until execution. The proper dispatch order in this case is CBDA. The algorithm must resolve this type of case.

Using Available Memory

The PEI Foundation begins operation using a temporary memory store that contains the initial call stack from the Security (SEC) phase. Upon this stack is information about the size of the initial memory store. Based on the size of the initial memory handoff from SEC, the PEI Foundation will divide this region into the following:

- PEI stack
- PEI heap

The PEI stack will be available for subsequent PEIM invocations, and the PEI heap will be used for PEIM memory allocations and Hand-Off Block (HOB) creation.

There can be no memory writes to the address space beyond this initial temporary memory until a PEIM registers a permanent memory range using the PEI Service **InstallPeiMemory()**. When permanent memory is installed, the PEI Foundation will copy the call stack that is located in temporary memory into a segment of permanent memory. If necessary, the size of the call stack can be expanded to 128 KB to support the subsequent transition into DXE.

In addition to the call stack, the PEI Foundation will copy the following from temporary to permanent memory:

- PEI Foundation private data
- PEI Foundation heap
- HOB list

Any permanent memory consumed in this fashion by the PEI Foundation will be described in a HOB, which the PEI Foundation will create.

In addition, if there were any **EFI_PEI_PPI_DESCRIPTOR**s created in the temporary memory heap, their respective locations have been translated by an offset equal to the difference between the original heap location in temporary memory and the destination location in permanent memory. In addition to this heap copy, the PEI Foundation will traverse the PEI PPI database. Any references to **EFI_PEI_PPI_DESCRIPTOR**s that are in temporary memory will be fixed up by the PEI Foundation to reflect the location of the **EFI_PEI_PPI_DESCRIPTOR**s destination in permanent memory.

The PEI Foundation will invoke the DXE IPL PPI after dispatching all candidate PEIMs. The DXE IPL PPI may have to allocate additional regions from permanent memory to be able to load and relocate the DXE Foundation from its firmware store. The DXE IPL PPI will describe these memory allocations in the appropriate HOB such that when control is passed to DXE, an accurate record of the memory usage will be known to the DXE Foundation.

Invoking the PEIM's Entry Point

PEIMs are written using Microsoft* CDECL conventions, which detail how parameters are passed on the stack. After assessing a PEIM's dependency expression to see if it can be invoked, the PEI Foundation will pass control to the PEIM's entry point. This entry point is a value described in the PEIM's image header. This header could be either of the following:

- Microsoft* PE/COFF image
- Terse Executable (TE) image format

The PEI Foundation will push an indirect pointer to the PEI Services Table and the address of the firmware file onto the stack before it invokes the PEIM.

In the entry point of the PEIM, or what can be called its constructor, the PEIM has the opportunity do the following:

- Locate other PPIs
- Install PPIs that reference services within the body of this PEIM
- Register for a notification

Once the PEIM has completed its constructor processing, it returns back to the PEI Foundation.

See the *Microsoft Portable Executable and Common Object File Format Specification* for information on PE/COFF images; see the *Intel® Platform Innovation Framework for EFI Architecture Specification* for information on TE images.

Knowing When Dispatcher Tasks Are Finished

The PEI Dispatcher is finished with a pass when it has finished dispatching all the PEIMs that it can. During a pass, some PEIMs might not have been dispatched if they had requirements that no other PEIM has met.

However, with the weak ordering defined in previous requirements, system RAM could possibly be initialized before all PEIMs are given a chance to run. This situation can occur because the system RAM initialization PEIM is not required to consume all resources provided by all other PEIMs. The PEI Dispatcher must recognize that its tasks are not complete until all PEIMs have been given an opportunity to run.

Example Dispatch Algorithm

The following pseudo code is an example of an algorithm that uses few registers and implements the requirements listed in the previous section. The pseudo code uses simple C-like statements but more assembly-like flow-of-control primitives. Some error recovery paths, such as verification failure, have been left out for clarity. PEIMs may designate themselves as "for recovery" and "for nonrecovery." This check has also been omitted for clarity.

The dispatch algorithm's main data structure is the DispatchedBitMap as described in the following table.

Table 6-9. Example Dispatch Map

PEIM#	Item	PEIM#	Item
	FV0	4	FV1
	PEI Foundation		<non PEIM>
	<non PEIM>		<non PEIM>
0	PEIM		<non PEIM>
1	PEIM	5	PEIM
2	Platform PEIM with **EFI_PEI_FIND_FV_PPI**		<non PEIM>
	<non PEIM>	6	PEIM
3	PEIM	7	PEIM

The table above is an example of a dispatch in a given set of firmware volumes (FVs). Following are the steps in this dispatch:

1. If the dispatcher has not seen the FV before, it validates all of the PEIMs in that FV. For this reason, the order that **EFI_PEI_FIND_FV_PPI** reports FVs must not change throughout the first PEI pass.
2. The algorithm scans through the PEIMs that it knows about.

3. When it comes to a PEIM that has not been dispatched, it invokes a routine known as **LocatePpi()**, which finds PPIs that have been installed, to verify that all of the requirements listed in the dependency expression (depex) are in the PPI database.
4. If all of the GUIDed interfaces listed in the depex are available, the PEIM is invoked.
5. When the routine completes a pass through an FV, it calls **EFI_PEI_FIND_FV_PPI** (if the routine has found and dispatched it).
6. If **EFI_PEI_FIND_FV_PPI** reports a new FV, the dispatcher invokes the **EFI_PEI_SECURITY_PPI** authentication routine to corroborate the integrity of the FV.
7. Iterations continue through all known PEIMs in all known FVs until a pass is made with no PEIMs dispatched, thus signifying completion.
8. After the dispatch completes, the PEI Foundation locates and invokes the GUID for the DXE IPL PPI, passing in the HOB address and a valid stack. Failing to discover the GUID for the DXE IPL PPI shall be an error.

Dispatching When Memory Exists

The purpose of the PEI phase of execution is to discover and initialize main memory. As such, a large number of the modules execute from the nonvolatile firmware store and cannot be shadowed. However, there are several circumstances in which the shadowing of a PEIM and the relocation of this image into memory are of interest. This can include but is not limited to compressing PEIMs, such as the DXE IPL PPI, and those modules that are required for crisis recovery.

The PEI architecture shall not dictate what compression mechanism is to be used, but there will be a Decompress service that is published by some PEIM that the PEI Foundation will discover and use when it becomes available. In addition, loading images also requires a full image-relocation service and the ability to flush the cache. The former will allow the PEIM that was relocated into RAM to have its relocations adjust pursuant to the new load address. The latter service will be invoked by the PEI Foundation so that this relocated code can be run, especially on Itanium-based platforms that do not have a coherent data and code cache.

A compressed section shall have an implied dependency on permanent memory having been installed. To speed up boot time, however, there can be an explicit annotation of this dependency.

7
PEIMs

Introduction

A Pre-EFI Initialization Module (PEIM) represents a unit of code and/or data. It abstracts domain-specific logic and is analogous to a DXE driver. As such, a given group of PEIMs for a platform deployment might include a set of the following:

- Platform-specific PEIMs
- Processor-specific PEIMs
- Chipset-specific PEIMs
- PEI CIS–prescribed architectural PEIMs
- Miscellaneous PEIMs

The PEIM encapsulation allows for a platform builder to use services for a given hardware technology without having to build the source of this technology or necessarily understand its implementation. A PEIM-to-PEIM Interface (PPI) is the means by which to abstract hardware-specific complexities to a platform builder's PEIM. As such, PEIMs can work in concert with other PEIMs using PPIs.

In addition, PEIMs can ascertain a fixed set of services that are always available through the PEI Services Table.

Finally, because the PEIM represents the basic unit of execution beyond the Security (SEC) phase and the PEI Foundation, there will always be some non-zero-sized collection of PEIMs in a platform.

PEIM Structure

PEIM Structure Overview

Each Pre-EFI Initialization Module (PEIM) is stored in a file. It consists of the following:

- Standard header
- Execute-in-place code/data section
- Optional relocation information
- Authentication information, if present

The PEIM binary image can be executed in place from its location in the firmware volume (FV) or from a compressed component that will be shadowed after permanent memory has been installed. The executable section of the PEIM may be either position-dependent or position-independent code. If the executable section of the PEIM is position-dependent code, relocation information must be provided in the PEIM image to allow FV store software to relocate the image to a different location than it is compiled.

The figure below depicts the basic layout of a PEIM. See the following specifications for the indicated code definition:

- Firmware file header definition: Intel® Platform Innovation Framework for EFI Firmware File System Specification
- Section type definitions: Intel® Platform Innovation Framework for EFI Firmware Volume Specification

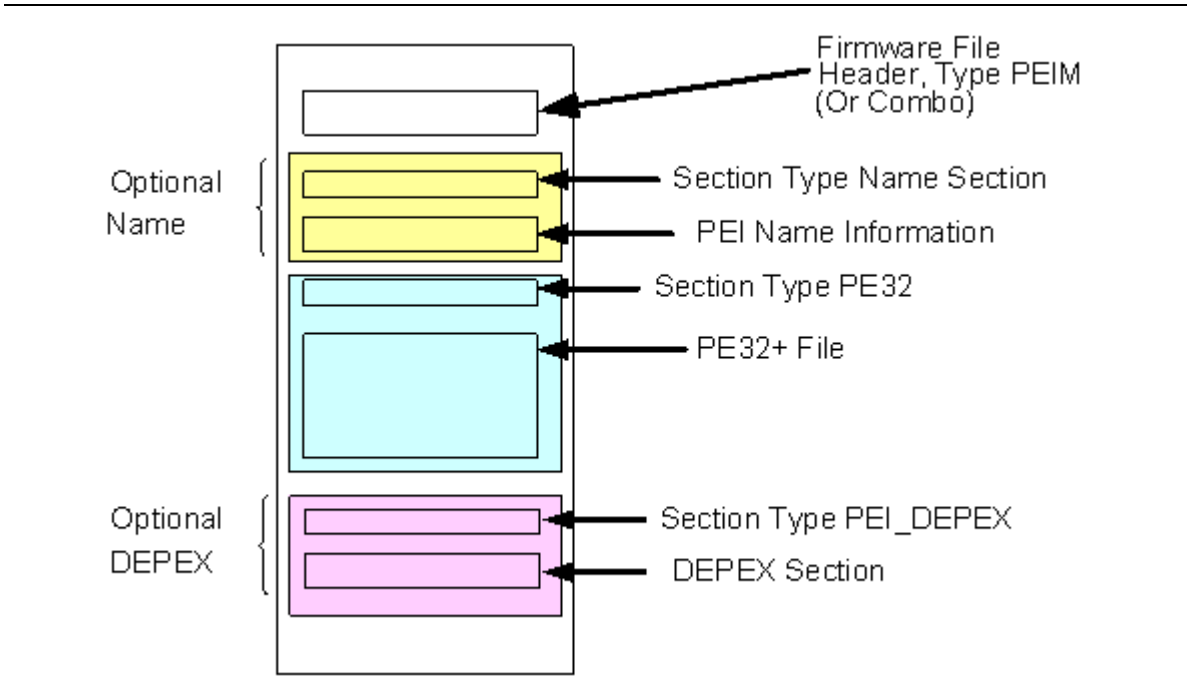


Figure 7-1. PEIM Layout in a Firmware File

Relocation Information

Position-Dependent Code

PEIMs that are developed using position-dependent code require relocation information. When an image in a firmware volume (FV) is updated, the update software will use the relocation information to fix the code image according to the module's location in the FV. The relocation is done on the authenticated image; therefore, software verifying the integrity of the image must undo the relocation during the verification process.

There is no explicit pointer to this data. Instead, the update and verification tool will know that the image is actually stored as PE32 if the `Pe32Image` bit is set in the header **`EFI_COMMON_SECTION_HEADER`**; type **`EFI_COMMON_SECTION_HEADER`** is defined in the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification.* The PE32 specification, in turn, will be used to ascertain the relocation records.

Position-Independent Code

If the PEIM is written in position-independent code, then its entry point shall be at the lowest address in the section. This method is useful for creating PEIMs for the Itanium® processor family.

Relocation Information Format

The relocations will be contained in a PE32+ image. See the *Microsoft Portable Executable and Common Object File Format Specification* for more information. The determination of whether the image subscribes to the PE32 image format or is position-independent assembly language should be provided by the firmware volume section type. The PEIM that is formatted as PE/COFF will always be linked against a base address of zero. This allows for support of signature checking.

The section may also be compressed if there is a compression encapsulation section.

Authentication Information

The authentication information will be contained in a section of type **`EFI_SECTION_GUID_DEFINED`** (see the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification* for more information on section types). The information contained in this section could be one of the following:

- A cryptographic-quality hash computed across the PEIM image
- A simple checksum
- A CRC

The GUID defines the meaning of the associated encapsulated data. The relocation section is needed to undo the fix-ups done on the image so the hash that was computed at build time can be confirmed. In other words, the build of a PEIM image is linked against zero, but the update tool will relocate the PEIM image for its execute-in-place address (at least for images that are not position-independent code). Any signing information is calculated on the image after the image has been linked against an address of zero. The relocations on the image will have to be "undone" to determine if the image has been modified.

The image must be linked against address zero by the PEIM provider. The build or update tool will apply the appropriate relocations. The linkage against address zero is key because it allows a subsequent undoing of the relocations.

PEIM Invocation Entry Point

EFI_PEIM_ENTRY_POINT

Summary

The PEI Dispatcher will invoke each PEIM one time. During this pass, the PEI Dispatcher will pass control to the PEIM at the *AddressOfEntryPoint* in the PE Header. *AddressOfEntryPoint* is defined in the *Microsoft Portable Executable and Common Object File Format Specification.*

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEIM_ENTRY_POINT) (
  IN EFI_FFS_FILE_HEADER        *FfsHeader,
  IN struct _EFI_PEI_SERVICES   **PeiServices
  );
```

Parameters

FfsHeader

Pointer to the FFS file header. Type **EFI_FFS_FILE_HEADER** is defined in the *Intel® Platform Innovation Framework for EFI Firmware File System Specification.*

PeiServices

Describes the list of possible PEI Services.

Description

This function is the entry point for a PEIM. **EFI_IMAGE_ENTRY_POINT** is the equivalent of this state in the EFI/DXE environment; see the DXE CIS for its definition.

The motivation behind this definition is that the firmware file system has the provision to mark a file as being both a PEIM and DXE driver. The result of this name would be that both the PEI Dispatcher and the DXE Dispatcher would attempt to execute the module. In doing so, it is incumbent upon the code in the entry point of the driver to decide what services are exposed, namely whether to make boot service and runtime calls into the EFI System Table or to make calls into the PEI Services Table. The means by which to make this decision entail examining the second argument on entry, which is a pointer to the respective foundation's exported service-call table. Both PEI and EFI/DXE have a common header, **EFI_TABLE_HEADER**, for the table. The code in the PEIM or DXE driver will examine the *Arg2->Hdr->Signature*. If it is **EFI_SYSTEM_TABLE_SIGNATURE**, the code will assume DXE driver behavior; if it is **PEI_SERVICES_SIGNATURE**, the code will assume PEIM behavior.

Status Codes Returned

EFI_SUCCESS	The service completed successfully
< 0	There was an error

PEIM Descriptors

PEIM Descriptors Overview

A PEIM descriptor is the data structure used by PEIMs to export service entry points and data. The descriptor contains the following:

- Flags
- A pointer to a GUID
- A pointer to data

The latter data can include a list of pointers to functions and/or data. It is the function pointers that are commonly referred to as PEIM-to-PEIM Interfaces (PPIs), and the PPI is the unit of software across which PEIMs can invoke services from other PEIMs.

A PEIM also uses a PEIM descriptor to export a service to the PEI Foundation into which the PEI Foundation will pass control in response to an event, namely "notifying" the callback when a PPI is installed or reinstalled. As such, PEIM descriptors serve the dual role of exposing the following:

- A callable interface/data for other PEIMs
- A callback interface from the perspective of the PEI Foundation

EFI_PEI_DESCRIPTOR

Summary

This data structure is the means by which callable services are installed and notifications are registered in the PEI phase.

Prototype

```
typedef union {
  EFI_PEI_NOTIFY_DESCRIPTOR   Notify;
  EFI_PEI_PPI_DESCRIPTOR      Ppi;
} EFI_PEI_DESCRIPTOR;
```

Parameters

Notify

The typedef structure of the notification descriptor. See the **EFI_PEI_NOTIFY_DESCRIPTOR** type definition.

Ppi

The typedef structure of the PPI descriptor. See the **EFI_PEI_PPI_DESCRIPTOR** type definition.

Description

EFI_PEI_DESCRIPTOR is a data structure that can be either a PPI descriptor or a notification descriptor. A PPI descriptor is used to expose callable services to other PEIMs. A notification descriptor is used to register for a notification or callback when a given PPI is installed.

EFI_PEI_NOTIFY_DESCRIPTOR

Summary

The data structure in a given PEIM that tells the PEI Foundation where to invoke the notification service.

Prototype

```
typedef struct _EFI_PEI_NOTIFY_DESCRIPTOR {
  UINTN                          Flags;
  EFI_GUID                       *Guid;
  EFI_PEIM_NOTIFY_ENTRY_POINT    Notify;
} EFI_PEI_NOTIFY_DESCRIPTOR;
```

Parameters

Flags

Details if the type of notification is callback or dispatch.

Guid

The address of the **EFI_GUID** that names the interface.

Notify

Address of the notification callback function itself within the PEIM. Type **EFI_PEIM_NOTIFY_ENTRY_POINT** is defined in "Related Definitions" below.

Description

EFI_PEI_NOTIFY_DESCRIPTOR is a data structure that is used by a PEIM that needs to be called back when a PPI is installed or reinstalled. The notification is similar to the **RegisterProtocolNotify()** function in the *EFI 1.10 Specification.* The use model is complementary to the dependency expression (depex) and is as follows:

- A PEIM expresses the PPIs that it *must* have to execute in its depex list.
- A PEIM expresses any other PEIMs that it needs, perhaps at some later time, in **EFI_PEI_NOTIFY_DESCRIPTOR**.

The latter data structure includes the GUID of the PPI for which the PEIM publishing the notification would like to be reinvoked.

Following is an example of the notification use model for **EFI_PEI_PERMANENT_MEMORY_INSTALLED_PPI**. In this example, a PEIM called *SamplePeim* executes early in the PEI phase before main memory is available. However, SamplePeim also needs to create some large data structure later in the PEI phase. As such, SamplePeim has a NULL depex, but after its entry point is processed, it needs to call **NotifyPpi()** with a **EFI_PEI_NOTIFY_DESCRIPTOR**, where the notification descriptor includes the following:

- A reference to **EFI_PEI_PERMANENT_MEMORY_INSTALLED_PPI**
- A reference to a function within this same PEIM called *SampleCallback*

When the PEI Foundation finally migrates the system from temporary to permanent memory and installs the **EFI_PEI_PERMANENT_MEMORY_INSTALLED_PPI**, the PEI Foundation assesses if there are any pending notifications on this PPI. After the PEI Foundation discovers the descriptor from SamplePeim, the PEI Foundation invokes SampleCallback.

With respect to the *Flags* parameter, the difference between callback and dispatch mode is as follows:

- **Callback mode:** Invokes all of the agents that are registered for notification immediately after the PPI is installed.
- **Dispatch mode:** Calls the agents that are registered for notification only after the PEIM that installs the PPI in question has returned to the PEI Foundation.

The callback mechanism will give a better quality of service, but it has the downside of possibly deepening the use of the stack (i.e., the agent that installed the PPI that engenders the notification is a PEIM itself that has used the stack already). The dispatcher mode, however, is better from a stack-usage perspective in that when the PEI Foundation invokes the agents that want notification, the stack has returned to the minimum stack usage of just the PEI Foundation.

Related Definitions

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEIM_NOTIFY_ENTRY_POINT) (
  IN struct _EFI_PEI_SERVICES        **PeiServices,
  IN struct _EFI_PEI_NOTIFY_DESCRIPTOR  *NotifyDescriptor,
  IN VOID                            *Ppi
  );
```

PeiServices

Indirect reference to the PEI Services Table.

NotifyDescriptor

Address of the notification descriptor data structure. Type **EFI_PEI_NOTIFY_DESCRIPTOR** is defined above.

Ppi

Address of the PPI that was installed.

EFI_PEI_PPI_DESCRIPTOR

Summary

The data structure through which a PEIM describes available services to the PEI Foundation.

Prototype

```
typedef struct _EFI_PEI_PPI_DESCRIPTOR {
  UINTN                         Flags;
  EFI_GUID                      *Guid;
  VOID                          *Ppi;
} EFI_PEI_PPI_DESCRIPTOR;
```

Parameters

Flags

This field is a set of flags describing the characteristics of this imported table entry. See "Related Definitions" below for possible flag values.

Guid

The address of the **EFI_GUID** that names the interface.

Ppi

A pointer to the PPI. It contains the information necessary to install a service.

Description

EFI_PEI_PPI_DESCRIPTOR is a data structure that is within the body of a PEIM or created by a PEIM. It includes the following:

- Information about the nature of the service
- A reference to a GUID naming the service
- An associated pointer to either a function or data related to the service

There can be a catenation of one or more of these **EFI_PEI_PPI_DESCRIPTOR**s. The final descriptor will have the **EFI_PEI_PPI_DESCRIPTOR_TERMINATE_LIST** flag set to indicate to the PEI Foundation how many of the descriptors need to be added to the PPI database within the PEI Foundation. The PEI Services that references this data structure include **InstallPpi()**, **ReinstallPpi()**, and **LocatePpi()**.

Related Definitions

```
//
// PEI PPI Services List Descriptors
//

#define EFI_PEI_PPI_DESCRIPTOR_PIC             0x00000001
#define EFI_PEI_PPI_DESCRIPTOR_PPI             0x00000010
#define EFI_PEI_PPI_DESCRIPTOR_NOTIFY_CALLBACK 0x00000020
#define EFI_PEI_PPI_DESCRIPTOR_NOTIFY_DISPATCH 0x00000040
#define EFI_PEI_PPI_DESCRIPTOR_NOTIFY_TYPES    0x00000060
#define EFI_PEI_PPI_DESCRIPTOR_TERMINATE_LIST  0x80000000
```

Following is a description of the fields in the above definition:

EFI_PEI_PPI_DESCRIPTOR_PIC	When set to 1, this designates that the PPI described by the structure is position-independent code (PIC).
EFI_PEI_PPI_DESCRIPTOR_PPI	When set to 1, this designates that the PPI described by this structure is a normal PPI. As such, it should be callable by the conventional PEI infrastructure.
EFI_PEI_PPI_DESCRIPTOR_NOTIFY_CALLBACK	When set to 1, this flag designates that the service registered in the descriptor is to be invoked at callback. This means that if the PPI is installed for which the listener registers a notification, then the callback routine will be immediately invoked. The danger herein is that the callback will inherit whatever depth had been traversed up to and including this call.
EFI_PEI_PPI_DESCRIPTOR_NOTIFY_DISPATCH	When set to 1, this flag designates that the service registered in the descriptor is to be invoked at dispatch. This means that if the PPI is installed for which the listener registers a notification, then the callback routine will be deferred until the PEIM calling context returns to the PEI Foundation. Prior to invocation of the next PEIM, the notifications will be dispatched. The advantage herein is that the callback will have the maximum available stack depth as any other PEIM.
EFI_PEI_PPI_DESCRIPTOR_NOTIFY_TYPES	When set to 1, this flag designates that this is a notification-style PPI.
EFI_PEI_PPI_DESCRIPTOR_TERMINATE_LIST	This flag is set to 1 in the last structure entry in the list of PEI PPI descriptors. This flag is used by the PEI Foundation Services to know that there are no additional interfaces to install.

PEIM-to-PEIM Communication

Overview

PEIMs may invoke other PEIMs. The interfaces themselves are named using GUIDs. Because the PEIMs may be authored by different organizations at different times and updated at different times, references to these interfaces cannot be resolved during their execution by referring to the PEI PPI database. The database is loaded and queried using PEI Services such as **`InstallPpi()`** and **`LocatePpi()`**.

Dynamic PPI Discovery

PPI Database

The PPI database is a data structure that PEIMs can use to discover what interfaces are available or to manage a specific interface. The actual layout of the PPI database is opaque to a PEIM but its contents can be queried and manipulated using the following PEI Services:

- **`InstallPpi()`**
- **`ReinstallPpi()`**
- **`LocatePpi()`**
- **`NotifyPpi()`**

Invoking a PPI

When the PEI Foundation examines a PEIM for dispatch eligibility, it examines the dependency expression section of the firmware file. If there are non-NULL contents, the Reverse Polish Notation (RPN) expression is evaluated. Any requested PPI GUIDs in this data structure are queried in the PPI database. The existence in the database of the particular PUSH_GUID depex opcode leads to this expression evaluating to true.

Address Resolution

When a PEIM needs to leverage a PPI, it uses the PEI Foundation Service **`LocatePpi()`** to discover if an instance of the interface exists. The PEIM could do either of the following:

- Install the PPI in its depex to ensure that its entry point will not be invoked until the needed PPI is already installed
- Have a very thin set of code in its entry point that simply registers a notification on the desired PPI.

In the case of either the depex or the notification, the **`LocatePpi()`** call will then succeed and the pointer returned on this call references the **`EFI_PEI_PPI_DESCRIPTOR`**. It is through this data structure that the actual code entry point can be discovered. If this PEIM is being loaded before permanent memory is available, it will not have resources to cache this discovered interface and will have to search for this interface every time it needs to invoke the service.

It should also be noted that you cannot uninstall a PPI, so the services will be left in the database. If a PPI needs to be shrouded, a version can be “reinstalled” that just returns failure.

Also, there is peril in caching a PPI. For example, if you cache a PPI and the producer of the PPI "reinstalls" it to be something else (i.e., shadows to memory), then you have the possibility that the agent who cached the data will have "stale" or "illegal" data. For example, imagine the Stall PPI, **EFI_PEI_STALL_PPI**, relocating itself to memory using the Load File PPI, **EFI_PEI_FV_FILE_LOADER_PPI**, and reinstalling the interface for performance considerations. A way to solve the latter issue, as a platform builder, is by having a different stall PPI for the memory-based one versus that of the Execute In Place (XIP) one.

8
Architectural PPIs

Introduction

The PEI Foundation and PEI Dispatcher rely on the following PEIM-to-PEIM Interfaces (PPIs) to perform its work. The abstraction provided by these interfaces allows dispatcher algorithms to be improved over time or have some platform variability without affecting the rest of PEI.

The key to these PPIs is that they are architecturally defined interfaces consumed by the PEI Foundation, but they do not necessarily get published by the PEI Foundation.

Required Architectural PPIs

Master Boot Mode PPI (Required)

EFI_PEI_MASTER_BOOT_MODE_PPI (Required)

Summary

The PEI Master Boot Mode PPI is installed by a PEIM to signal that a final boot has been determined and set. This signal is useful in that PEIMs with boot-mode-specific behavior (for example, S3 versus normal) can put this PPI in their dependency expression.

GUID

```
#define EFI_PEI_MASTER_BOOT_MODE_PEIM_PPI \
{0x7408d748, 0xfc8c, 0x4ee6, 0x92, 0x88, 0xc4, 0xbe, 0xc0, 0x92,
0xa4, 0x10};
```

PPI Interface Structure

None.

Description

The Master Boot Mode PPI is a PPI GUID and must be in the dependency expression of every PEIM that modifies the basic hardware. The dispatch, or entry point, of the module that installs the Master Boot Mode PPI modifies the boot path value in the following ways:

- Directly, through the PEI Service **SetBootMode()**
- Indirectly through its optional subordinate boot path modules

The PEIM that publishes the Master Boot Mode PPI has a non-null dependency expression if there are subsidiary modules that publish alternate boot path PPIs. The primary reason for this PPI is to be the root of dependencies for any child boot mode provider PPIs.

Status Codes Returned

None.

DXE IPL PPI (Required)

EFI_DXE_IPL_PPI (Required)

Summary

Final service to be invoked by the PEI Foundation.

GUID

```
#define EFI_DXE_IPL_PPI_GUID \
{ 0xae8ce5d, 0xe448, 0x4437, 0xa8, 0xd7, 0xeb, 0xf5, 0xf1, 0x94,
0xf7, 0x31 }
```

PPI Interface Structure

```
typedef struct _EFI_DXE_IPL_PPI {
  EFI_DXE_IPL_ENTRY  Entry;
} EFI_DXE_IPL_PPI;
```

Parameters

Entry

The entry point to the DXE IPL PPI. See the **Entry()** function description.

Description

After completing the dispatch of all available PEIMs, the PEI Foundation will invoke this PPI through its entry point using the same handoff state used to invoke other PEIMs. This special treatment by the PEI Foundation effectively makes the DXE IPL PPI the last PPI to execute during PEI. When this PPI is invoked, the system state should be as follows:

- Single thread of execution
- Interrupts disabled
- Processor mode as defined for PEI

The DXE IPL PPI is responsible for locating and loading the DXE Foundation. The DXE IPL PPI may use PEI services to locate and load the DXE Foundation. As long as the DXE IPL PPI is using PEI Services, it must obey all PEI interoperability rules of memory allocation, HOB list usage, and PEIM-to-PEIM communication mechanisms.

EFI_DXE_IPL_PPI.Entry()

Summary

The architectural PPI that the PEI Foundation invokes when there are no additional PEIMs to invoke.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_DXE_IPL_ENTRY) (
  IN struct _EFI_DXE_IPL_PPI   *This,
  IN EFI_PEI_SERVICES          **PeiServices,
  IN EFI_PEI_HOB_POINTERS      HobList
  );
```

Parameters

This

Pointer to the DXE IPL PPI instance.

PeiServices

Pointer to the PEI Services Table.

HobList

Pointer to the list of Hand-Off Block (HOB) entries.

Description

This function is invoked by the PEI Foundation. The PEI Foundation will invoke this service when there are no additional PEIMs to invoke in the system. If this PPI does not exist, it is an error condition and an ill-formed firmware set. The DXE IPL PPI should never return after having been invoked by the PEI Foundation. The DXE IPL PPI can do many things internally, including the following:

- Invoke the DXE entry point from a firmware volume.
- Invoke the recovery processing modules.
- Invoke the S3 resume modules.

Status Codes Returned

EFI_SUCCESS	Upon this return code, the PEI Foundation should enter some exception handling. Under normal circumstances, the DXE IPL PPI should not return.

Memory Discovered PPI (Required)

EFI_PEI_PERMANENT_MEMORY_INSTALLED_PPI (Required)

Summary

This PPI is published by the PEI Foundation when the main memory is installed. It is essentially a PPI with no associated interface. Its purpose is to be used as a signal for other PEIMs who can register for a notification on its installation.

GUID

```
#define EFI_PEI_PERMANENT_MEMORY_INSTALLED_PPI \
{0xf894643d, 0xc449, 0x42d1, 0x8e, 0xa8, 0x85, 0xbd, 0xd8, 0xc6,
0x5b, 0xde};
```

PPI Interface Structure

None.

Description

This PPI is installed by the PEI Foundation at the point of system evolution when the permanent memory size has been registered and waiting PEIMs can use the main memory store. Using this GUID allows PEIMs to do the following:

- Be notified when this PPI is installed.
- Include this PPI's GUID in the **EFI_DEPEX**.

The expectation is that a compressed PEIM would depend on this PPI, for example. The PEI Foundation will relocate the temporary cache to permanent memory prior to this installation.

Status Codes Returned

None.

Optional Architectural PPIs

Boot in Recovery Mode PPI (Optional)

EFI_PEI_BOOT_IN_RECOVERY_MODE_PPI (Optional)

Summary

This PEIM is installed by the platform PEIM to designate that a recovery boot is in progress.

GUID

```
#define EFI_PEI_BOOT_IN_RECOVERY_MODE_PEIM_PPI \
{0x17ee496a, 0xd8e4, 0x4b9a, 0x94, 0xd1, 0xce, 0x82, 0x72, 0x30,
0x8, 0x50}
```

PPI Interface Structure

None.

Description

This optional PPI is installed by the platform PEIM to designate that a recovery boot is in progress. Its purpose is to allow certain PEIMs that wish to be dispatched **only during a recovery boot** to include this PPI in their dependency expression (depex). Including this PPI in the depex allows the PEI Dispatcher to skip recovery-specific PEIMs during normal restarts and thus save on boot time. This PEIM has no associated PPI and is used only to designate the system state as being "in a crisis recovery dispatch."

Status Codes Returned

None.

Section Extraction PPI (Optional)

EFI_PEI_SECTION_EXTRACTION_PPI (Optional)

Summary

This PPI supports encapsulating sections, such as GUIDed sections used to authenticate the file encapsulation of other domain-specific wrapping.

GUID

```
#define EFI_PEI_SECTION_EXTRACTION_PPI_GUID  \
 { 0x4F89E208, 0xE144, 0x4804, 0x9EC8, 0x0F894F7E36D7 }
```

PPI Interface Structure

```
typedef struct _EFI_PEI_SECTION_EXTRACTION_PPI {
  EFI_PEI_GET_SECTION                    GetSection;
} EFI_PEI_SECTION_EXTRACTION_PPI;
```

Parameters

GetSection

Retrieves a section from within a section file. See the **GetSection()** function description.

Description

This PPI is used to retrieve a section from within a section file. The section file is akin to the stream paradigm defined in DXE except that there can only be one stream, or encapsulated set of sections; as a result, the stream concept will be omitted.

EFI_PEI_SECTION_EXTRACTION_PPI.GetSection() will retrieve both encapsulation sections and leaf sections in their entirety, exclusive of the section header.

Because the requested section may be contained within compression and/or GUIDed encapsulations, the implementation must be capable of processing these encapsulations to produce the requested section. While decompression of an encapsulating compression section is completely transparent, the results of all encapsulating GUIDed sections used for authentication must be exposed to the caller so the caller can make appropriate policy decisions.

EFI_PEI_SECTION_EXTRACTION_PPI.GetSection()

Summary

Retrieves a section from within a section file.

Prototype

```
EFI_STATUS
(EFIAPI *EFI_PEI_GET_SECTION)(
  IN EFI_PEI_SERVICES                   **PeiServices,
  IN EFI_PEI_SECTION_EXTRACTION_PPI     *This,
  IN EFI_SECTION_TYPE                   *SectionType,
  IN EFI_GUID                           *SectionDefinitionGuid,
OPTIONAL
  IN UINTN                              SectionInstance,
  IN VOID                               **Buffer,
  IN OUT UINT32                         *BufferSize,
  OUT UINT32                            *AuthenticationStatus
  );
```

Parameters

PeiServices

Pointer to the PEI Services Table.

This

Indicates the calling context.

SectionType

Pointer to an **EFI_SECTION_TYPE**. If *SectionType* == **NULL**, the contents of the entire section are returned in *Buffer*. If *SectionType* is not **NULL**, only the requested section is returned. Type **EFI_SECTION_TYPE** is defined in the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification.*

SectionDefinitionGuid

Pointer to an **EFI_GUID**. If *SectionType* == **EFI_SECTION_GUID_DEFINED**, *SectionDefinitionGuid* indicates for which section GUID to search. If *SectionType* != **EFI_SECTION_GUID_DEFINED**, *SectionDefinitionGuid* is unused and is ignored. See *Intel® Platform Innovation Framework for EFI Firmware Volume Specification* for details about GUID-defined sections.

SectionInstance

If *SectionType* is not **NULL**, indicates which instance of the requested section type to return. The file's section layout can be thought of as a tree that is built recursively left to right. *SectionInstance* is zero-based and calculated using a left-to-right depth-first search algorithm of the file's section layout. See the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification* for more details. If *SectionType* is **NULL**, then *SectionInstance* is ignored.

Buffer

Pointer to a pointer to a buffer in which the section contents are returned. See "Description" below for more details on using the *Buffer* parameter.

BufferSize

A pointer to a caller-allocated **UINT32**. On input, **BufferSize* indicates the size in bytes of the memory region pointed to by *Buffer*. On output, **BufferSize* contains the number of bytes required to read the section.

AuthenticationStatus

A pointer to a caller-allocated **UINT32** in which any metadata from encapsulating GUID-defined sections is returned. See the *Intel® Platform Innovation Framework for EFI Firmware Volume Specification* for more information regarding GUID-defined sections. All individual *AuthenticationStatus* values from each layer of GUID defined section are bitwise OR-ed together to form an aggregate result. See "Related Definitions" below for possible bit values for *AuthenticationStatus*.

Description

The **GetSection()** function is used to retrieve a section from within a section file. It will retrieve both encapsulation sections and leaf sections in their entirety, exclusive of the section header.

The authentication results are passed back in the *AuthenticationStatus* output variable. If there are multiple layers of encapsulation, the *AuthenticationStatus* values from each layer are bitwise OR-ed together to produce the final output.

The output buffer is specified by a double indirection of the parameter *Buffer*. The input value of **Buffer* is used to determine whether or not the output buffer is caller allocated or is dynamically allocated by **GetSection()**.

If the input value of **Buffer!=NULL*, it indicates that the output buffer is caller allocated. In this case, the input value of **BufferSize* indicates the size of the caller-allocated output buffer. If the output buffer is not large enough to contain the entire requested output, it is filled up to the point that the output buffer is exhausted, **EFI_BUFFER_TOO_SMALL** is returned, and **BufferSize* is returned with the size required to successfully complete the read. All other output parameters are returned with valid values.

If the input value of **Buffer==NULL*, it indicates the output buffer is to be allocated by **GetSection()**. In this case, **GetSection()** will allocate an appropriately sized buffer from

boot services pool memory which will be returned in **Buffer*. The size of the new buffer is returned in **BufferSize* and all other output parameters are returned with valid values.

Related Definitions

```
//*******************************************************
// Bit values for AuthenticationStatus
//*******************************************************
#define EFI_AUTH_STATUS_PLATFORM_OVERRIDE  0x01
#define EFI_AUTH_STATUS_IMAGE_SIGNED       0x02
#define EFI_AUTH_STATUS_NOT_TESTED         0x04
#define EFI_AUTH_STATUS_TEST_FAILED        0x08

// all other bits are reserved and must be 0
```

The bit definitions above lead to the following evaluations of *AuthenticationStatus*:

Table 8-1. *AuthenticationStatus* **Bit Definitions**

Bit	Definition
xx00	Image was not signed.
xxx1	Platform security policy override. Assumes same meaning as 0010 (the image was signed, the signature was tested, and the signature passed authentication test).
0010	Image was signed, the signature was tested, and the signature passed authentication test.
0110	Image was signed and the signature was not tested. This can occur if there is no GUIDed Section Extraction Protocol available to process a GUID-defined section, but it was still possible to retrieve the data from the GUID-defined section directly.
1010	Image was signed, the signature was tested, and the signature failed the authentication test.
1110	To generate this code, there must be at least two layers of GUIDed encapsulations. In one layer, the *AuthenticationStatus* was returned as 0110; in another layer, it was returned as 1010. When these two results are OR-ed together, the aggregate result is 1110.

Status Codes Returned

EFI_SUCCESS	The section was successfully processed and the section contents were returned in *Buffer*.
EFI_PROTOCOL_ERROR	A GUID-defined section was encountered in the file with its **EFI_GUIDED_SECTION_PROCESSING_REQUIRED** bit set, but there was no corresponding GUIDed Section Extraction Protocol in the handle database. **Buffer* is unmodified.
EFI_NOT_FOUND	The requested section does not exist. **Buffer* is unmodified.
EFI_OUT_OF_RESOURCES	The system has insufficient resources to process the request.
EFI_INVALID_PARAMETER	The *SectionStreamHandle* does not exist.
EFI_WARN_TOO_SMALL	The size of the input buffer is insufficient to contain the requested section. The input buffer is filled and contents are section contents are truncated.

End of PEI Phase PPI (Optional)

EFI_PEI_END_OF_PEI_PHASE_PPI (Optional)

Summary

This PEIM will be installed at the end of PEI for all boot paths, including normal, recovery, and S3. It allows for PEIMs to possibly quiesce hardware, build handoff information for the next phase of execution, or provide some terminal processing behavior.

GUID

```
#define EFI_PEI_END_OF_PEI_PHASE_PPI_GUID \
{0x605EA650, 0xC65C, 0x42e1, 0xBA, 0x80, 0x91, 0xA5, 0x2A,
0xB6,0x18, 0xC6}
```

PPI Interface Structure

None.

Description

This PPI is installed by the DXE IPL PPI to indicate the end of the PEI usage of memory and ownership of memory allocation by the DXE phase.

The intended use model is for any agent that needs to do cleanup, such as memory services to convert internal metadata for tracking memory allocation into HOBs, to have some distinguished point in which to do so. The PEI Memory Services would register for a callback on the installation of this PPI.

Status Codes Returned

None.

Find FV PPI (Optional)

EFI_PEI_FIND_FV_PPI (Optional)

Summary

Abstracts additional firmware volumes (FVs) to the PEI Foundation.

GUID

```
#define EFI_PEI_FIND_FV_PPI_GUID  \
  { 0x36164812, 0xa023, 0x44e5, 0xbd85, 0x050bf3c7700aa }
```

PPI Interface Structure

```
typedef struct _EFI_PEI_FIND_FV_PPI {
  EFI_PEI_FIND_FV_FINDFV  FindFv;
} EFI_PEI_FIND_FV_PPI;
```

Parameters

FindFv

Service that abstracts the location of additional firmware volumes. See the **FindFv()** function description.

Description

Hardware mechanisms for locating FVs in a platform vary widely. **EFI_PEI_FIND_FV_PPI** serves to abstract this variation so that the PEI Foundation can remain standard across a wide variety of platforms. The *Intel® Platform Innovation Framework for EFI Firmware Volume Block Specification* describes the FV header **EFI_FIRMWARE_VOLUME_HEADER** that prefixes a well-formed volume. The PEI Foundation uses **FfsFindNextVolume()** to find new FVs, but this function will call **EFI_PEI_FIND_FV_PPI**. **FfsFindNextVolume()** gives a common interface and **EFI_PEI_FIND_FV_PPI** is dependent on vendor implementation.

The reason that this service is different from the PEI Service **FfsFindNextVolume()** is that the information in **EFI_PEI_FIND_FV_PPI** is not complete; it cannot describe the base of the boot firmware volume, for example.

There shall only be one instance of this PPI in the system.

Status Codes Returned

EFI_SUCCESS	The firmware volume was found.
EFI_OUT_OF_RESOURCES	There are no firmware volumes for the given *FvNumber*.

EFI_PEI_FIND_FV_PPI.FindFv()

Summary

This service is published by a platform agenda that abstracts the location of additional firmware volumes.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_FIND_FV_FINDFV) (
  IN EFI_PEI_SERVICES                **PeiServices,
  IN struct _EFI_PEI_FIND_FV_PPI     *This,
  IN UINT8                           *FvNumber,
  IN OUT EFI_FIRMWARE_VOLUME_HEADER  **FvAddress
  );
```

Parameters

PeiServices

Pointer to the PEI Services Table.

This

Interface pointer that implements the Find FV service.

FvNumber

The index of the firmware volume to locate.

FvAddress

The address of the volume to discover. Type **EFI_FIRMWARE_VOLUME_HEADER** is defined in the *Intel® Platform Innovation Framework for EFI Firmware Volume Block Specification.*

Description

The function returns the base address of the firmware volume whose index was passed in *FvNumber*. Once this function reports a firmware volume index/base address pair, that index/address pairing must continue throughout PEI.

This interface is provided by some platform agent because, other than the location of the boot firmware volume provided by the Security (SEC) phase, the location of additional firmware volumes is under the control of the platform builder. Some PEIM with platform awareness will publish an instance of the Find FV PPI if the following two conditions are met:

- There is at least one well-formed firmware volume beyond the Boot Firmware Volume (BFV).
- This latter firmware volume contains PEIMs that should be evaluated on the given boot mode.

The reason for this distinction is that there can be additional firmware volumes that are exposed to the DXE IPL PPI and DXE Foundation using firmware volume HOBs, but these same volumes may not contain additional PEIMs. In fact, it is unlikely to have a scenario where there are PEIMs

in firmware volumes beyond the boot firmware volume because of the time-space constraints of the PEI phase of execution.

Status Codes Returned

EFI_SUCCESS	An additional firmware volume was found.
EFI_OUT_OF_RESOURCES	There are no firmware volumes for the given *FvNumber*.
EFI_INVALID_PARAMETER	*****FvAddress* is **NULL**.

Load File PPI (Optional)

EFI_PEI_FV_FILE_LOADER_PPI (Optional)

Summary

This PPI is installed by a PEIM that supports the Load File PPI.

GUID

```
#define EFI_PEI_FV_FILE_LOADER_GUID  \
{ 0x7e1f0d85, 0x4ff, 0x4bb2, 0x86, 0x6a, 0x31, 0xa2, 0x99, 0x6a, 0x48, 0xa8 }
```

PPI Interface Structure

```
typedef struct _EFI_PEI_FV_FILE_LOADER_PPI {
  EFI_PEI_FV_LOAD_FILE        FvLoadFile;
} EFI_PEI_FV_FILE_LOADER_PPI;
```

Parameters

FvLoadFile

Loads a PEIM into memory for subsequent execution. See the **FvLoadFile()** function description.

Description

This PPI is a pointer to the Load File service. This service will be published by a PEIM. The PEI Foundation will use this service to launch the known non-XIP PE/COFF PEIM images. This service may depend upon the presence of the **EFI_PEI_PERMANENT_MEMORY_INSTALLED_PPI**. This service does not accept a pointer to the PEI Services Table because the service implementation can cache a module-global version of the pointer on its entry point; for speed considerations, an implementation of this service will be shadowed into memory using a self-shadowing technique.

EFI_PEI_FV_FILE_LOADER_PPI.FvLoadFile()

Summary

Loads a PEIM into memory for subsequent execution.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_FV_LOAD_FILE) (
  IN  struct _EFI_PEI_FV_FILE_LOADER_PPI        *This,
  IN  EFI_FFS_FILE_HEADER                       *FfsHeader,
  OUT EFI_PHYSICAL_ADDRESS                      *ImageAddress,
  OUT UINT64                                    *ImageSize,
  OUT EFI_PHYSICAL_ADDRESS                      *EntryPoint
  );
```

Parameters

This

Interface pointer that implements the Load File PPI instance.

FfsHeader

Pointer to the FFS header of the file to load. Type **EFI_FFS_FILE_HEADER** is defined in the *Intel® Platform Innovation Framework for EFI Firmware File System Specification.*

ImageAddress

Pointer to the address of the loaded Image.

ImageSize

Pointer to the size of the loaded image.

EntryPoint

Pointer to the entry point of the image.

Description

This service is the single member function of **EFI_PEI_FV_FILE_LOADER_PPI**. This service separates image loading and relocating from the PEI Foundation. For example, if there are compressed images or images that need to be relocated into memory for performance reasons, this service performs that transformation. This service is very similar to the **LOAD_FILE** protocol in the *EFI 1.10 Specification.* The abstraction allows for an implementation of the **FvLoadFile()** service to support different image types in the future. To conform with the PEI CIS, however, there must be an **FvLoadFile()** instance that at least supports the PE/COFF and Terse Executable (TE) image format.

Status Codes Returned

EFI_SUCCESS	The image was loaded successfully.
EFI_OUT_OF_RESOURCES	There was not enough memory.
EFI_INVALID_PARAMETER	The contents of the FFS file did not contain a valid PE/COFF image that could be loaded.

PEI Reset PPI

EFI_PEI_RESET_PPI (Optional)

Summary

This PPI is installed by some platform- or chipset-specific PEIM that abstracts the Reset Service to other agents.

GUID

```
#define EFI_PEI_RESET_PPI_GUID \
{0xef398d58, 0x9dfd, 0x4103, 0xbf, 0x94, 0x78, 0xc6, 0xf4, 0xfe, 0x71, 0x2f};
```

PPI Interface Structure

```
typedef struct _EFI_PEI_RESET_PPI {
  EFI_PEI_RESET_SYSTEM  ResetSystem;
} EFI_PEI_RESET_PPI;
```

Parameters

ResetSystem

A service to reset the platform. See the **ResetSystem()** function description in Services - PEI: Reset Services.

Description

These services provide a simple reset service. See the **ResetSystem()** function description for a description of this service.

Related Definitions

```
//*******************************************************
// EFI_PEI_RESET_TYPE
//*******************************************************
typedef enum {
  EfiPeiResetCold,
  EfiPeiResetWarm,
} EFI_PEI_RESET_TYPE;
```

PEI Status Code PPI (Optional)

EFI_PEI_PROGRESS_CODE_PPI (Optional)

Summary

This service is published by a PEIM. There can be only one instance of this service in the system. If there are multiple variable access services, this PEIM must multiplex these alternate accessors and provide this single, read-only service to the other PEIMs and the PEI Foundation. This singleton nature is important because the PEI Foundation will notify when this service is installed.

GUID

```
#define EFI_PEI_REPORT_PROGRESS_CODE_PPI_GUID  \
{0x229832d3, 0x7a30, 0x4b36, 0xb8, 0x27, 0xf4, 0xc, 0xb7, 0xd4, 0x54, 0x36);
```

PPI Interface Structure

```
typedef struct _EFI_PEI_PROGRESS_CODE_PPI {
  EFI_PEI_REPORT_STATUS_CODE      ReportStatusCode;
} EFI_PEI_PROGRESS_CODE_PPI;
```

Parameters

ReportStatusCode

Service that allows PEIMs to report status codes. See the **ReportStatusCode()** function description in Services - PEI: Status Code Services.

Description

See the **ReportStatusCode()** function description for a description of this service.

Security PPI (Optional)

EFI_PEI_SECURITY_PPI (Optional)

Summary

This PPI is installed by some platform PEIM that abstracts the security policy to the PEI Foundation, namely the case of a PEIM's authentication state being returned during the PEI section extraction process.

GUID

```
#define EFI_PEI_SECURITY_PPI_GUID \
{0x1388066e, 0x3a57, 0x4efa, 0x98, 0xf3, 0xc1, 0x2f, 0x3a, 0x95, 0x8a, 0x29}
```

PPI Interface Structure

```
typedef struct _EFI_PEI_SECURITY_PPI {
  EFI_PEI_SECURITY_AUTHENTICATION_STATE  AuthenticationState;
} EFI_PEI_SECURITY_PPI;
```

Parameters

AuthenticationState

Allows the platform builder to implement a security policy in response to varying file authentication states. See the **AuthenticationState()** function description.

Description

This PPI is a means by which the platform builder can indicate a response to a PEIM's authentication state. This can be in the form of a requirement for the PEI Foundation to skip a module using the *DeferExecution* Boolean output in the **AuthenticationState()** member function. Alternately, the Security PPI can invoke something like a cryptographic PPI that hashes the PEIM contents to log attestations, for which the *FfsFileHeader* parameter in **AuthenticationState()** will be useful. If this PPI does not exist, PEIMs will be considered trusted.

EFI_PEI_SECURITY_PPI.AuthenticationState()

Summary

Allows the platform builder to implement a security policy in response to varying file authentication states.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_SECURITY_AUTHENTICATION_STATE) (
  IN EFI_PEI_SERVICES              **PeiServices,
  IN struct _EFI_PEI_SECURITY_PPI  *This,
  IN UINT32                        AuthenticationStatus,
  IN EFI_FFS_FILE_HEADER           *FfsFileHeader,
  IN OUT BOOLEAN                   *DeferExecution
);
```

Parameters

PeiServices

Pointer to the PEI Services Table.

This

Interface pointer that implements the particular **EFI_PEI_SECURITY_PPI** instance.

AuthenticationStatus

Status returned by the verification service as part of section extraction.

FfsFileHeader

Pointer to the file under review. Type **EFI_FFS_FILE_HEADER** is defined in the *Intel® Platform Innovation Framework for EFI Firmware File System Specification.*

DeferExecution

Pointer to a variable that alerts the PEI Foundation to defer execution of a PEIM.

Description

This service is published by some platform PEIM. The purpose of this service is to expose a given platform's policy-based response to the PEI Foundation. For example, if there is a PEIM in a GUIDed encapsulation section and the extraction of the PEI file section yields an authentication failure, there is no *a priori* policy in the PEI Foundation. Specifically, this situation leads to the question whether PEIMs that are either not in GUIDed sections or are in sections whose authentication fails should still be executed.

In fact, it is the responsibility of the platform builder to make this decision. This platform-scoped policy is a result that a desktop system might not be able to skip or not execute PEIMs because the skipped PEIM could be the agent that initializes main memory. Alternately, a system may require

that unsigned PEIMs not be executed under any circumstances. In either case, the PEI Foundation simply multiplexes access to the Section Extraction PPI and the Security PPI. The Section Extraction PPI determines the contents of a section, and the Security PPI tells the PEI Foundation whether or not to invoke the PEIM.

The PEIM that publishes the **`AuthenticationState()`** service uses its parameters in the following ways:

- *`AuthenticationStatus`* conveys the source information upon which the PEIM acts.
- The *`DeferExecution`* value tells the PEI Foundation whether or not to dispatch the PEIM.

In addition, between receiving the **`AuthenticationState()`** from the PEI Foundation and returning with the *`DeferExecution`* value, the PEIM that publishes **`AuthenticationState()`** can do the following:

- Log the file state.
- Lock the firmware hubs in response to an unsigned PEIM being discovered.

These latter behaviors are platform- and market-specific and thus outside the scope of the PEI CIS.

Status Codes Returned

EFI_SUCCESS	The service performed its action successfully.
EFI_SECURITY_VIOLATION	The object cannot be trusted

9
Additional PPIs

Introduction

Architectural PPIs described a collection of architecturally required PPIs. These were interfaces consumed by the PEI Foundation and are not intended to be consumed by other PEIMs.

In addition to these architectural PPIs, however, there is another name space of PPIs that are optional or mandatory for a given platform. This section describes these additional PPIs:

- Required PPIs:
  - CPU I/O PPI
  - PCI Configuration PPI
  - Stall PPI
  - PEI Variable Services
- Optional PPIs:
  - Security (SEC) Platform Information PPI

These shall be referred to as first-class PEIMs in some contexts.

Required Additional PPIs

PEI CPU I/O PPI (Required)

EFI_PEI_CPU_IO_PPI (Required)

Summary

This PPI is installed by some platform or chipset-specific PEIM that abstracts the processor-visible I/O operations.

GUID

```
#define EFI_PEI_CPU_IO_PPI_GUID  \
{0x3ae721c8, 0xe303, 0x4399, 0xbe, 0xfd, 0xa9, 0x30, 0xbb, 0x85, 0x82, 0x1c}
```

PPI Interface Structure

```
typedef
struct _EFI_PEI_CPU_IO_PPI {
  EFI_PEI_CPU_IO_PPI_ACCESS           Mem;
  EFI_PEI_CPU_IO_PPI_ACCESS           Io;
  EFI_PEI_CPU_IO_PPI_IO_READ8         IoRead8;
  EFI_PEI_CPU_IO_PPI_IO_READ16        IoRead16;
  EFI_PEI_CPU_IO_PPI_IO_READ32        IoRead32;
  EFI_PEI_CPU_IO_PPI_IO_READ64        IoRead64;
  EFI_PEI_CPU_IO_PPI_IO_WRITE8        IoWrite8;
  EFI_PEI_CPU_IO_PPI_IO_WRITE16       IoWrite16;
  EFI_PEI_CPU_IO_PPI_IO_WRITE32       IoWrite32;
  EFI_PEI_CPU_IO_PPI_IO_WRITE64       IoWrite64;
  EFI_PEI_CPU_IO_PPI_MEM_READ8        MemRead8;
  EFI_PEI_CPU_IO_PPI_MEM_READ16       MemRead16;
  EFI_PEI_CPU_IO_PPI_MEM_READ32       MemRead32;
  EFI_PEI_CPU_IO_PPI_MEM_READ64       MemRead64;
  EFI_PEI_CPU_IO_PPI_MEM_WRITE8       MemWrite8;
  EFI_PEI_CPU_IO_PPI_MEM_WRITE16      MemWrite16;
  EFI_PEI_CPU_IO_PPI_MEM_WRITE32      MemWrite32;
  EFI_PEI_CPU_IO_PPI_MEM_WRITE64      MemWrite64;
} EFI_PEI_CPU_IO_PPI;
```

Parameters

Mem

Collection of memory-access services. See the **Mem()** function description. Type **EFI_PEI_CPU_IO_PPI_ACCESS** is defined in "Related Definitions" below.

Io

Collection of I/O-access services. See the **Io()** function description. Type **EFI_PEI_CPU_IO_PPI_ACCESS** is defined in "Related Definitions" below.

IoRead8

8-bit read service. See the **IoRead8()** function description.

IoRead16

16-bit read service. See the **IoRead16()** function description.

IoRead32

32-bit read service. See the **IoRead32()** function description.

IoRead64

64-bit read service. See the **IoRead64()** function description.

IoWrite8

8-bit write service. See the **IoWrite8()** function description.

IoWrite16

16-bit write service. See the **IoWrite16()** function description.

IoWrite32

32-bit write service. See the **IoWrite32()** function description.

IoWrite64

64-bit write service. See the **IoWrite64()** function description.

MemRead8

8-bit read service. See the **MemRead8()** function description.

MemRead16

16-bit read service. See the **MemRead16()** function description.

MemRead32

32-bit read service. See the **MemRead32()** function description.

MemRead64

64-bit read service. See the **MemRead64()** function description.

MemWrite8

8-bit write service. See the **MemWrite8()** function description.

MemWrite16

16-bit write service. See the **MemWrite16()** function description.

MemWrite32

32-bit write service. See the **MemWrite32()** function description.

MemWrite64

64-bit write service. See the **MemWrite64()** function description.

Description

This PPI provides a set of memory- and I/O-based services. The perspective of the services is that of the processor, not the bus or system.

Related Definitions

```
//*******************************************************
// EFI_PEI_CPU_IO_PPI_ACCESS
//*******************************************************

typedef
struct {
  EFI_PEI_CPU_IO_PPI_IO_MEM             Read;
  EFI_PEI_CPU_IO_PPI_IO_MEM             Write;
} EFI_PEI_CPU_IO_PPI_ACCESS;
```

Read

This service provides the various modalities of memory and I/O read. It is similar to the **EFI_CPU_IO_PROTOCOL** service of the same name in the *EFI 1.10 Specification.*

Write

This service provides the various modalities of memory and I/O write. It is similar to the **EFI_CPU_IO_PROTOCOL** service of the same name in the *EFI 1.10 Specification.*

EFI_PEI_CPU_IO_PPI.Mem()

Summary

Memory-based access services.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_MEM) (
  IN  EFI_PEI_SERVICES                  **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI        *This,
  IN  EFI_PEI_CPU_IO_PPI_WIDTH          Width,
  IN  UINT64                            Address,
  IN  UINTN                             Count,
  IN  OUT VOID                          *Buffer
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Width

The width of the access. Enumerated in bytes. Type **EFI_PEI_CPU_IO_PPI_WIDTH** is defined in "Related Definitions" below.

Address

The physical address of the access.

Count

The number of accesses to perform.

Buffer

A pointer to the buffer of data.

Description

The **Mem()** function provides a list of memory-based accesses.

Related Definitions

```
//*******************************************************
// EFI_PEI_CPU_IO_PPI_WIDTH
//*******************************************************

typedef enum {
  EfiPeiCpuIoWidthUint8,
  EfiPeiCpuIoWidthUint16,
  EfiPeiCpuIoWidthUint32,
  EfiPeiCpuIoWidthUint64,
  EfiPeiCpuIoWidthFifoUint8,
  EfiPeiCpuIoWidthFifoUint16,
  EfiPeiCpuIoWidthFifoUint32,
  EfiPeiCpuIoWidthFifoUint64,
  EfiPeiCpuIoWidthFillUint8,
  EfiPeiCpuIoWidthFillUint16,
  EfiPeiCpuIoWidthFillUint32,
  EfiPeiCpuIoWidthFillUint64,
  EfiPeiCpuIoWidthMaximum
} EFI_PEI_CPU_IO_PPI_WIDTH;
```

Status Codes Returned

EFI_SUCCESS	The function completed successfully.

EFI_PEI_CPU_IO_PPI.Io()

Summary

I/O-based access services.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_MEM) (
  IN  EFI_PEI_SERVICES                  **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI        *This,
  IN  EFI_PEI_CPU_IO_PPI_WIDTH          Width,
  IN  UINT64                            Address,
  IN  UINTN                             Count,
  IN  OUT VOID                          *Buffer
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Width

The width of the access. Enumerated in bytes. Type **EFI_PEI_CPU_IO_PPI_WIDTH** is defined in **Mem()**.

Address

The physical address of the access.

Count

The number of accesses to perform.

Buffer

A pointer to the buffer of data.

Description

The **Io()** function provides a list of I/O-based accesses. Input or output data can be found in the last argument.

Status Codes Returned

EFI_SUCCESS	The function completed successfully.

EFI_PEI_CPU_IO_PPI.IoRead8()

Summary

8-bit I/O read operations.

Prototype

```
typedef
UINT8
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_READ8) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Description

The **IoRead8()** function returns an 8-bit value from the I/O space.

EFI_PEI_CPU_IO_PPI.IoRead16()

Summary

16-bit I/O read operations.

Prototype

```
typedef
UINT16
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_READ16) (
  IN  EFI_PEI_SERVICES             **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI   *This,
  IN  UINT64                       Address
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Description

The **IoRead16()** function returns a 16-bit value from the I/O space.

EFI_PEI_CPU_IO_PPI.IoRead32()

Summary

32-bit I/O read operations.

Prototype

```
typedef
UINT32
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_READ32) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Description

The **IoRead32()** function returns a 32-bit value from the I/O space.

EFI_PEI_CPU_IO_PPI.IoRead64()

Summary

64-bit I/O read operations.

Prototype

```
typedef
UINT64
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_READ64) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Description

The **IoRead64()** function returns a 64-bit value from the I/O space.

EFI_PEI_CPU_IO_PPI.IoWrite8()

Summary

8-bit I/O write operations.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_WRITE8) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address,
  IN  UINT8                         Data
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Data

The data to write.

Description

The **IoWrite8()** function writes an 8-bit value to the I/O space.

EFI_PEI_CPU_IO_PPI.IoWrite16()

Summary

16-bit I/O write operation.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_WRITE16) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address,
  IN  UINT16                        Data
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Data

The data to write.

Description

The **IoWrite16()** function writes a 16-bit value to the I/O space.

EFI_PEI_CPU_IO_PPI.IoWrite32()

Summary

32-bit I/O write operation.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_WRITE32) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address,
  IN  UINT32                        Data
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Data

The data to write.

Description

The **IoWrite32()** function writes a 32-bit value to the I/O space.

EFI_PEI_CPU_IO_PPI.IoWrite64()

Summary

64-bit I/O write operation.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_WRITE64) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address,
  IN  UINT64                        Data
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Data

The data to write.

Description

The **IoWrite64()** function writes a 64-bit value to the I/O space.

EFI_PEI_CPU_IO_PPI.MemRead8()

Summary

8-bit memory read operations.

Prototype

```
typedef
UINT8
(EFIAPI *EFI_PEI_CPU_IO_PPI_MEM_READ8) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Description

The **MemRead8()** function returns an 8-bit value from the memory space.

EFI_PEI_CPU_IO_PPI.MemRead16()

Summary

16-bit memory read operations.

Prototype

```
typedef
UINT16
(EFIAPI *EFI_PEI_CPU_IO_PPI_MEM_READ16) (
  IN  EFI_PEI_SERVICES             **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI   *This,
  IN  UINT64                       Address
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Description

The **MemRead16()** function returns a 16-bit value from the memory space.

EFI_PEI_CPU_IO_PPI.MemRead32()

Summary

32-bit memory read operations.

Prototype

```
typedef
UINT32
(EFIAPI *EFI_PEI_CPU_IO_PPI_MEM_READ32) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Description

The **MemRead32()** function returns a 32-bit value from the memory space.

EFI_PEI_CPU_IO_PPI.MemRead64()

Summary

64-bit memory read operations.

Prototype

```
typedef
UINT64
(EFIAPI *EFI_PEI_CPU_IO_PPI_MEM_READ64) (
  IN  EFI_PEI_SERVICES            **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI  *This,
  IN  UINT64                      Address
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Description

The **MemRead64()** function returns a 64-bit value from the memory space.

EFI_PEI_CPU_IO_PPI.MemWrite8()

Summary

8-bit memory write operations.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_CPU_IO_PPI_MEM_WRITE8) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address,
  IN  UINT8                         Data
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Data

The data to write.

Description

The **MemWrite8()** function writes an 8-bit value to the memory space.

EFI_PEI_CPU_IO_PPI.MemWrite16()

Summary

16-bit memory write operation.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_CPU_IO_PPI_MEM_WRITE16) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address,
  IN  UINT16                        Data
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Data

The data to write.

Description

The **MemWrite16()** function writes a 16-bit value to the memory space.

EFI_PEI_CPU_IO_PPI.MemWrite32()

Summary

32-bit memory write operation.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_CPU_IO_PPI_MEM_WRITE32) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address,
  IN  UINT32                        Data
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Data

The data to write.

Description

The **MemWrite32()** function writes a 32-bit value to the memory space.

EFI_PEI_CPU_IO_PPI.MemWrite64()

Summary

64-bit memory write operation.

Prototype

```
typedef
VOID
(EFIAPI *EFI_PEI_CPU_IO_PPI_IO_WRITE64) (
  IN  EFI_PEI_SERVICES              **PeiServices,
  IN  struct _EFI_PEI_CPU_IO_PPI    *This,
  IN  UINT64                        Address,
  IN  UINT64                        Data
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Address

The physical address of the access.

Data

The data to write.

Description

The **MemWrite64()** function writes a 64-bit value to the memory space.

PEI PCI Configuration PPI (Required)

EFI_PEI_PCI_CFG_PPI (Required)

Summary

This PPI is installed by some platform or chipset-specific PEIM that abstracts the PCI operations service to other agents.

GUID

```
#define EFI_PEI_PCI_CFG_PPI_GUID  \
  { 0xe0f08f7d, 0x7c5b, 0x45b9, 0x9c, 0xd, 0x4a, 0xcc, 0xe6, 0x80, 0xa3, 0x1 }
```

PPI Interface Structure

```
typedef struct _EFI_PEI_PCI_CFG_PPI {
  EFI_PEI_PCI_CFG_PPI_IO  Read;
  EFI_PEI_PCI_CFG_PPI_IO  Write;
  EFI_PEI_PCI_CFG_PPI_RW  Modify;
} EFI_PEI_PCI_CFG_PPI;
```

Parameters

Read

PCI read services. See the **Read()** function description.

Write

PCI write services. See the **Write()** function description.

Modify

PCI read-modify-write services. See the **Modify()** function description.

Description

The **EFI_PEI_PCI_CFG_PPI** interfaces are used to abstract accesses to PCI controllers behind a PCI root bridge controller. The rationale for this abstraction is that the programmatic sequence for configuration space reads and writes is not standardized. As such, this interface provides a common surface area against which to code initialization PEIMs. The **Modify()** service allows for space-efficient implementation of the following common operations:

- Reading a register
- Changing some bit fields within the register
- Writing the register value back into the hardware

The **Modify()** service is a composite of the **Read()** and **Write()** services.

EFI_PEI_PCI_CFG_PPI.Read()

Summary

PCI read operation.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_PCI_CFG_PPI_IO) (
  IN EFI_PEI_SERVICES              **PeiServices,
  IN struct _EFI_PEI_PCI_CFG_PPI   *This,
  IN EFI_PEI_PCI_CFG_PPI_WIDTH     Width,
  IN UINT64                        Address,
  IN OUT VOID                      *Buffer
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Width

The width of the access. Enumerated in bytes. Type **EFI_PEI_PCI_CFG_PPI_WIDTH** is defined in "Related Definitions" below.

Address

The physical address of the access.

Buffer

A pointer to the buffer of data.

Description

The **Read()** function reads from a given location in the PCI configuration space.

Related Definitions

```
//*****************************************************************
// EFI_PEI_PCI_CFG_PPI_WIDTH
//*****************************************************************
typedef enum {
  EfiPeiPciCfgWidthUint8      = 0,
  EfiPeiPciCfgWidthUint16     = 1,
  EfiPeiPciCfgWidthUint32     = 2,
  EfiPeiPciCfgWidthUint64     = 3,
  EfiPeiPciCfgWidthMaximum
} EFI_PEI_PCI_CFG_PPI_WIDTH;


//*****************************************************************
// EFI_PEI_PCI_CFG_PPI_PCI_ADDRESS
//*****************************************************************
typedef struct {
  UINT8   Register;
  UINT8   Function;
  UINT8   Device;
  UINT8   Bus;
  UINT8   Reserved[4];
} EFI_PEI_PCI_CFG_PPI_PCI_ADDRESS;
```

Register

8-bit register offset within the PCI configuration space for a given device's function space.

Function

Only the 3 least-significant bits are used to encode one of 8 possible functions within a given device.

Device

Only the 5 least-significant bits are used to encode one of 32 possible devices.

Bus

8-bit value to encode between 0 and 255 buses.

Reserved

These fields should not be read or written.

```
#define EFI_PEI_PCI_CFG_ADDRESS(bus,dev,func,reg) \
((UINT64) ( (((UINTN)bus) << 24) + (((UINTN)dev) << 16) +
(((UINTN)func) << 8) + ((UINTN)reg) )& 0x00000000ffffffff
```

Status Codes Returned

EFI_SUCCESS	The function completed successfully.

EFI_PEI_PCI_CFG_PPI.Write()

Summary

PCI write operation.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_PCI_CFG_PPI_IO) (
  IN EFI_PEI_SERVICES              **PeiServices,
  IN struct _EFI_PEI_PCI_CFG_PPI   *This,
  IN EFI_PEI_PCI_CFG_PPI_WIDTH     Width,
  IN UINT64                        Address,
  IN OUT VOID                      *Buffer
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Width

The width of the access. Enumerated in bytes. Type **EFI_PEI_PCI_CFG_PPI_WIDTH** is defined in **Read()**.

Address

The physical address of the access.

Buffer

A pointer to the buffer of data.

Description

The **Write()** function writes to a given location in the PCI configuration space.

Status Codes Returned

EFI_SUCCESS	The function completed successfully.

EFI_PEI_PCI_CFG_PPI.Modify()

Summary

PCI read-modify-write Operation.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_PCI_CFG_PPI_RW) (
  IN EFI_PEI_SERVICES              **PeiServices,
  IN struct _EFI_PEI_PCI_CFG_PPI   *This,
  IN EFI_PEI_PCI_CFG_PPI_WIDTH     Width,
  IN UINT64                        Address,
  IN UINTN                         SetBits,
  IN UINTN                         ClearBits
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to local data for the interface.

Width

The width of the access. Enumerated in bytes. Type **EFI_PEI_PCI_CFG_PPI_WIDTH** is defined in **Read()**.

Address

The physical address of the access.

SetBits

Value of the bits to set.

ClearBits

Value of the bits to clear.

Description

The **Modify()** function performs a read-modify-write operation on the contents from a given location in the PCI configuration space.

Status Codes Returned

EFI_SUCCESS	The function completed successfully.

PEI Stall PPI (Required)

EFI_PEI_STALL_PPI (Required)

Summary

This PPI is installed by some platform or chipset-specific PEIM that abstracts the blocking stall service to other agents.

GUID

```
#define EFI_PEI_STALL_PPI_GUID \
{ 0x1f4c6f90, 0xb06b, 0x48d8, 0xa2, 0x01, 0xba, 0xe5, 0xf1, 0xcd, 0x7d, 0x56 }
```

PPI Interface Structure

```
typedef
struct _EFI_PEI_STALL_PPI {
  UINTN                                 Resolution;
  EFI_PEI_STALL                         Stall;
} EFI_PEI_STALL_PPI;
```

Parameters

Resolution

The resolution in microseconds of the stall services.

Stall

The actual stall procedure call. See the **Stall()** function description.

Description

This service provides a simple, blocking stall with platform-specific resolution.

EFI_PEI_STALL_PPI.Stall()

Summary

Blocking stall.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_STALL) (
  IN EFI_PEI_SERVICES              **PeiServices,
  IN struct _EFI_PEI_STALL_PPI     *This,
  IN UINTN                         Microseconds
  );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

This

Pointer to the local data for the interface.

Microseconds

Number of microseconds for which to stall.

Description

The **Stall()** function provides a blocking stall for at least the number of microseconds stipulated in the final argument of the API.

Status Codes Returned

EFI_SUCCESS	The service provided at least the required delay.

PEI Variable Services (Required)

EFI_PEI_READ_ONLY_VARIABLE_PPI (Required)

Summary

The following is a list of read-only variable services. These services will report **EFI_NOT_AVAILABLE_YET** until a PEIM publishes the services for other modules.

GUID

```
#define EFI_PEI_READ_ONLY_VARIABLE_ACCESS_PPI_GUID  \
{0x3cdc90c6, 0x13fb, 0x4a75, 0x9e, 0x79, 0x59, 0xe9, 0xdd, 0x78, 0xb9, 0xfa};
```

PPI Interface Structure

```
typedef struct _EFI_PEI_READ_ONLY_VARIABLE_PPI {
   EFI_PEI_GET_VARIABLE            GetVariable;
   EFI_PEI_GET_NEXT_VARIABLE_NAME  GetNextVariableName;
 } EFI_PEI_READ_ONLY_VARIABLE_PPI;
```

Parameters

GetVariable

A service to ascertain a given variable name. See the **GetVariable()** function description.

GetNextVariableName

A service to ascertain a variable based upon a given, known variable. See the **GetNextVariableName()** function description.

Description

These services provide a lightweight, read-only variant of the full EFI variable services. The reason that these services are read-only is to reduce the complexity of flash management. Also, some implementation of the PEI may use the same physical flash part for variable and PEIM storage; as such, a write command to certain technologies would alter the contents of the entire part, thus making the in situ PEIM execution not follow the required flow.

EFI_PEI_READ_ONLY_VARIABLE_PPI. GetVariable()

Summary

The purpose of the service is to publish an interface that allows PEIMs to free memory ranges that are managed by the PEI Foundation.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_GET_VARIABLE) (
    IN struct _EFI_PEI_SERVICES      **PeiServices,
    IN CHAR16                        *VariableName,
    IN EFI_GUID                      *VendorGuid,
    OUT UINT32                       *Attributes OPTIONAL,
    IN OUT UINTN                     *DataSize,
    OUT VOID                         *Data
    );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

VariableName

A **NULL**-terminated Unicode string that is the name of the vendor's variable.

VendorGuid

A unique identifier for the vendor.

Attributes

If not **NULL**, a pointer to the memory location to return the attributes bitmask for the variable. See "Related Definitions" below for possible attribute values.

DataSize

On input, the size in bytes of the return *Data* buffer. On output, the size of data returned in *Data*.

Data

The buffer to return the contents of the variable.

Description

Each vendor may create and manage its own variables without the risk of name conflicts by using a unique *VendorGuid*. When a variable is set its *Attributes* are supplied to indicate how the data variable should be stored and maintained by the system. The attributes affect when the variable may be accessed and volatility of the data. Any attempts to access a variable that does not have the attribute set for runtime access will yield the **EFI_NOT_FOUND** error.

If the *Data* buffer is too small to hold the contents of the variable, the error **EFI_BUFFER_TOO_SMALL** is returned and *DataSize* is set to the required buffer size to obtain the data.

Related Definitions

```
// Variable attributes
#define EFI_VARIABLE_NON_VOLATILE          0x00000001
#define EFI_VARIABLE_BOOTSERVICE_ACCESS    0x00000002
#define EFI_VARIABLE_RUNTIME_ACCESS        0x00000004
```

Status Codes Returned

EFI_SUCCESS	The function completed successfully.
EFI_NOT_FOUND	The variable was not found.
EFI_BUFFER_TOO_SMALL	The *BufferSize* is too small for the result. *BufferSize* has been updated with the size needed to complete the request.
EFI_INVALID_PARAMETER	One of the parameters has an invalid value.
EFI_DEVICE_ERROR	The variable could not be retrieved due to a hardware error.

EFI_PEI_READ_ONLY_VARIABLE_PPI. NextVariableName()

Summary

The purpose of the service is to publish an interface that allows PEIMs to free memory ranges that are managed by the PEI Foundation.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_PEI_GET_NEXT_VARIABLE_NAME) (
    IN struct _EFI_PEI_SERVICES      **PeiServices,
    IN OUT UINTN                     *VariableNameSize,
    IN OUT CHAR16                    *VariableName,
    IN OUT EFI_GUID                  *VendorGuid
    );
```

Parameters

PeiServices

An indirect pointer to the PEI Services Table published by the PEI Foundation.

VariableNameSize

The size of the *VariableName* buffer.

VariableName

On input, supplies the last *VariableName* that was returned by **GetNextVariableName()**. On output, returns the Null-terminated Unicode string of the current variable.

VendorGuid

On input, supplies the last *VendorGuid* that was returned by **GetNextVariableName()**. On output, returns the *VendorGuid* of the current variable.

Description

GetNextVariableName() is called multiple times to retrieve the *VariableName* and *VendorGuid* of all variables currently available in the system. On each call to **GetNextVariableName()** the previous results are passed into the interface, and on output the interface returns the next variable name data. When the entire variable list has been returned, the error **EFI_NOT_FOUND** is returned.

Note that if **EFI_BUFFER_TOO_SMALL** is returned, the *VariableName* buffer was too small for the next variable. When such an error occurs, the *VariableNameSize* is updated to reflect the size of buffer needed. In all cases when calling **GetNextVariableName()** the

VariableNameSize must not exceed the actual buffer size that was allocated for *VariableName*.

To start the search, a Null-terminated string is passed in *VariableName*; that is, *VariableName* is a pointer to a Null Unicode character. This is always done on the initial call to **GetNextVariableName()**. When *VariableName* is a pointer to a Null Unicode character, *VendorGuid* is ignored. **GetNextVariableName()** cannot be used as a filter to return variable names with a specific GUID. Instead, the entire list of variables must be retrieved, and the caller may act as a filter if it chooses.

Once **ExitBootServices()** is performed, variables that are only visible during boot services will no longer be returned. To obtain the data contents or attribute for a variable returned by **GetNextVariableName()**, the **GetVariable()** interface is used.

Status Codes Returned

EFI_SUCCESS	The function completed successfully.
EFI_NOT_FOUND	The next variable was not found.
EFI_BUFFER_TOO_SMALL	The *VariableNameSize* is too small for the result. *VariableNameSize* has been updated with the size needed to complete the request.
EFI_INVALID_PARAMETER	One of the parameters has an invalid value.
EFI_DEVICE_ERROR	The variable name could not be retrieved due to a hardware error.

Optional Additional PPIs

SEC Platform Information PPI (Optional)

EFI_SEC_PLATFORM_INFORMATION_PPI (Optional)

Summary

This service is the primary handoff state into the PEI Foundation. The Security (SEC) component creates the early, transitory memory environment and also encapsulates knowledge of at least the location of the Boot Firmware Volume (BFV).

GUID

```
#define EFI_SEC_PLATFORM_INFORMATION_GUID \
{0x6f8c2b35, 0xfef4, 0x448d, 0x82, 0x56, 0xe1, 0x1b, 0x19, 0xd6,   0x10, 0x77};
```

Prototype

```
typedef struct _EFI_SEC_PLATFORM_INFORMATION_PPI {
  EFI_SEC_PLATFORM_INFORMATION          PlatformInformation;
} EFI_SEC_PLATFORM_INFORMATION_PPI;
```

Parameters

PlatformInformation

Conveys state information out of the SEC phase into PEI. See the **PlatformInformation()** function description.

Description

This service abstracts platform-specific information. It is necessary to convey this information to the PEI Foundation so that it can discover where to begin dispatching PEIMs. In addition, if the PEI Foundation wishes to move the stack, it can discover the maximum stack capabilities of this platform.

This same information will be placed in a GUIDed HOB with the PPI GUID as the HOB GUID. This allows agents, such as the DXE multiprocessor (MP) driver, to get health information for the boot-strap processor (BSP).

EFI_SEC_PLATFORM_INFORMATION_PPI. PlatformInformation()

Summary

This service is the single member of the **EFI_SEC_PLATFORM_INFORMATION_PPI** that conveys state information out of the Security (SEC) phase into PEI.

Prototype

```
typedef
EFI_STATUS
(EFIAPI *EFI_SEC_PLATFORM_INFORMATION) (
  IN EFI_PEI_SERVICES                          **PeiServices,
  IN OUT UINT64                                *StructureSize,
  IN OUT EFI_SEC_PLATFORM_INFORMATION_RECORD
 *PlatformInformationRecord
  );
```

Parameters

PeiServices

Pointer to the PEI Services Table.

StructureSize

Pointer to the variable describing size of the input buffer.

PlatformInformationRecord

Pointer to the **EFI_SEC_PLATFORM_INFORMATION_RECORD**. Type **EFI_SEC_PLATFORM_INFORMATION_RECORD** is defined in "Related Definitions" below.

Description

This service is published by the SEC phase. The SEC phase handoff has an optional **EFI_PEI_PPI_DESCRIPTOR** list as its final argument when control is passed from SEC into the PEI Foundation. As such, if the platform supports the built-in self test (BIST) on IA-32 Intel® architecture or the PAL-A handoff state for Itanium® architecture, this information is encapsulated into the data structure abstracted by this service. This information is collected for the boot-strap processor (BSP) on IA-32, and for Itanium architecture, it is available on all processors that execute the PEI Foundation.

The motivation for this service is that a specific processor register contains this information for each microarchitecture, but the PEI CIS avoids using specific processor registers. Instead, the PEI CIS describes callable interfaces across which data is conveyed. As such, this processor state information that is collected at the reset of the machine is mapped into a common interface. The expectation is that a manageability agent, such as a platform PEIM that logs information for the

platform, would use this interface to determine the viability of the BSP and possibly select an alternate BSP if there are significant errors.

Related Definitions

```
//*******************************************************
// EFI_SEC_PLATFORM_INFORMATION_RECORD
//*******************************************************
typedef struct {
  EFI_HEALTH_FLAGS              HealthFlags;
} EFI_SEC_PLATFORM_INFORMATION_RECORD;
```

HealthFlags

Contains information generated by microcode, hardware, and/or the Itanium® processor PAL code about the state of the processor upon reset. Type **EFI_HEALTH_FLAGS** is defined below.

```
//*******************************************************
// EFI_HEALTH_FLAGS
//*******************************************************
typedef union {
  struct {
    UINT32    Status                    : 2;
    UINT32    Tested                    : 1;
    UINT32    Reserved1                 :13;
    UINT32    VirtualMemoryUnavailable  : 1;
    UINT32    Ia32ExecutionUnavailable  : 1;
    UINT32    FloatingPointUnavailable  : 1;
    UINT32    MiscFeaturesUnavailable   : 1;
    UINT32    Reserved2                 :12;
  }                     Bits;
  UINT32                Uint32;
} EFI_HEALTH_FLAGS;
```

Tested is the only common bit between IA-32 and Itanium architecture. IA-32 has the BIST but none of the other capabilities and ignores all bits except *Tested*. See Health Flag Bit Format for more information on **EFI_HEALTH_FLAGS**.

Status Codes Returned

EFI_SUCCESS	The data was successfully returned.
EFI_BUFFER_TOO_SMALL	The buffer was too small.

10
PEI to DXE Hand-Off

Introduction

The PEI phase of the system firmware boot process performs rudimentary initialization of the system to meet specific minimum system state requirements of the DXE Foundation. The PEI Foundation must have a mechanism of locating and passing off control of the system to the DXE Foundation. PEI must also provide a mechanism for components of DXE and the DXE Foundation to discover the state of the system when the DXE Foundation is invoked. Certain aspects of the system state at handoff are architectural, while other system state information may vary and hence must be described to DXE components.

Discovery and Dispatch of the DXE Foundation

The PEI Foundation uses a special PPI named the DXE Initial Program Load (IPL) PPI to discover and dispatch the DXE Foundation and components that are needed to run the DXE Foundation

The final action of the PEI Foundation is to locate and pass control to the DXE IPL PPI. To accomplish this, the PEI Foundation scans all PPIs by GUID for the GUID matching the DXE IPL PPI. The GUID for this PPI is defined in **`EFI_DXE_IPL_PPI`**.

Passing the Hand-Off Block (HOB) List

The DXE IPL PPI passes the Hand-Off Block (HOB) list from PEI to the DXE Foundation when it invokes the DXE Foundation. The handoff state is described in the form of HOBs in the HOB list. The HOB list must contain at least the HOBs listed in the following table.

Table 10-1. Required HOB Types in the HOB List

Required HOB Type	Usage
Phase Handoff Information Table (PHIT) HOB	This HOB is required.
One or more Resource Descriptor HOB(s) describing physical system memory	The DXE Foundation will use this physical system memory for DXE.
Boot-strap processor (BSP) Stack HOB	The DXE Foundation needs to know the current stack location so that it can move it if necessary, based upon its desired memory address map.
BSP BSPStore (“Backing Store Pointer Store”) HOB **Note:** Itanium® processor family only	The DXE Foundation needs to know the current store location so that it can move it if necessary, based upon its desired memory address map.
One or more Resource Descriptor HOB(s) describing firmware devices	The DXE Foundation will place this into the GCD.
One or more Firmware Volume HOB(s)	The DXE Foundation needs this information to begin loading other drivers in the platform.
A Memory Allocation Module HOB	This HOB tells the DXE Foundation where it is when allocating memory into the initial system address map.

The above HOB types are defined in the *Intel® Platform Innovation Framework for EFI Hand-Off Block (HOB) Specification.*

Handoff Processor State to the DXE IPL PPI

The table below defines the state that processors must be in at handoff to the DXE IPL PPI, for the following processors:

- IA-32 processors
- Itanium® processor family
- Intel® processors using Intel® XScale™ technology

Table 10-2. Handoff Processor State to the DXE IPL PPI

Processor	State at Handoff
IA-32	In 32-bit flat mode
Itanium	In Itanium processor family physical mode
Intel XScale	In SuperVisor Mode with a one-to-one virtual-to-physical mapping if there is a memory management unit (MMU) in the system

11
Boot Paths

Introduction

The PEI Foundation is unaware of the boot path required by the system. It relies on the PEIMs to determine the boot mode (e.g. R0, R1, S3, etc.) and take appropriate action depending on the mode.

To implement this, each PEIM has the ability to manipulate the boot mode using the PEI Service **SetBootMode()** described in Services - PEI.

The PEIM does not change the order in which PEIMs are dispatched depending on the boot mode.

Defined Boot Modes

The list of possible boot modes is described in the **GetBootMode()** function description. Framework architecture specifically does not define an upgrade path if new boot modes are defined. This is necessary as the nature of those additional boot modes may work in conjunction with or may conflict with the previously defined boot modes.

Priority of Boot Paths

Within a given PEIM, the priority ordering of the sources of boot mode should be as follows (from highest priority to lowest):

1. **BOOT_IN_RECOVERY_MODE**
2. **BOOT_ON_FLASH_UPDATE**
3. **BOOT_ON_S3_RESUME**
4. **BOOT_WITH_MINIMAL_CONFIGURATION**
5. **BOOT_WITH_FULL_CONFIGURATION**
6. **BOOT_ASSUMING_NO_CONFIGURATION_CHANGES**
7. **BOOT_WITH_FULL_CONFIGURATION_PLUS_DIAGNOSTICS**
8. **BOOT_WITH_DEFAULT_SETTINGS**
9. **BOOT_ON_S4_RESUME**
10. **BOOT_ON_S5_RESUME**
11. **BOOT_ON_S2_RESUME**

The boot modes listed above are defined in the PEI Service **SetBootMode()**.

Assumptions

The following table lists the assumptions that can be made about the system for each sleep state.

Table 11-1. Boot Path Assumptions

System State	Description	Assumptions
R0	Cold Boot	Cannot assume that the previously stored configuration data is valid.
R1	Warm Boot	May assume that the previously stored configuration data is valid.
S3	ACPI Save to RAM Resume	The previously stored configuration data is valid and RAM is valid. RAM configuration must be restored from nonvolatile storage (NVS) before RAM may be used. The firmware may only modify previously reserved RAM. There are two types of reserved memory. One is the equivalent of the BIOS INT15h, E820 type-4 memory and indicates that the RAM is reserved for use by the firmware. The suggestion is to add another type of memory that allows the OS to corrupt the memory during runtime but that may be overwritten during resume.
S4, S5	Save to Disk Resume, “Soft Off”	S4 and S5 are identical from a PEIM's point of view. The two are distinguished to support follow-on phases. The entire system must be reinitialized but the PEIMs may assume that the previous configuration is still valid.
Boot on Flash Update		This boot mode can be either an INIT, S3, or other means by which to restart the machine. If it is an S3, for example, the flash update cause will supersede the S3 restart. It is incumbent upon platform code, such as the Memory Initialization PEIM, to determine the exact cause and perform correct behavior (i.e., S3 state restoration versus INIT behavior).

Architectural Boot Mode PPIs

There is a possible hierarchy of boot mode PPIs that abstracts the various producers of this variable. It is a hierarchy in that there should be an order of precedence in which each mode can be set. The PPIs and their respective GUIDs are described in Required Architectural PPIs and Optional Architectural PPIs. The hierarchy includes the master PPI, which publishes a PPI that will be depended upon by the appropriate PEIMs, and some subsidiary PPI. For PEIMs that require that the boot mode is finally known, the Master Boot Mode PPI can be used as a dependency.

The following table lists the architectural boot mode PPIs.

Table 11-2. Architectural Boot Mode PPIs

PPI Name	Required or Optional?	PPI Definition in Section...
Master Boot Mode PPI	Required	Architectural PPIs: Required Architectural PPIs
Boot in Recovery Mode PPI	Optional	Architectural PPIs: Optional Architectural PPIs

Recovery

Scope

Recovery is the process of reconstituting a system's firmware devices when they have become corrupted. The corruption can be caused by various mechanisms. Most firmware volumes (FVs) in nonvolatile storage (NVS) devices (flash or disk, for example) are managed as blocks. If the system loses power while a block, or semantically bound blocks, are being updated, the storage might become invalid. On the other hand, an errant program or hardware could corrupt the device. The system designers must determine the level of support for recovery based on their perceptions of the probabilities of these events occurring and the consequences.

The designers of a system may choose not to support recovery for the following reasons:

- A system's FV storage media might not support modification after being manufactured. It might be the functional equivalent of a ROM.
- Most mechanisms of implementing recovery require additional FV space that might be too expensive for a particular application.
- A system may have enough FV space and hardware features that the FV can be made sufficiently fault tolerant to make recovery unnecessary.

Discovery

Discovering that recovery is required may be done using a PEIM (for example, by checking a "force recovery" jumper) or the PEI Foundation itself. The PEI Foundation might discover that a particular PEIM has not validated correctly or that an entire firmware has become corrupted.

General Recovery Architecture

The concept behind recovery is to preserve enough of the system firmware so that the system can boot to a point where it can do the following:

- Read a copy of the data that was lost from chosen peripherals.
- Reprogram the firmware volume (FV) with that data.

Preserving the recovery firmware is a function of the way the FV store is managed, which is generally beyond the scope of this document. For the purpose of this description, it is expected that the PEIMs and other contents of the FVs that are required for recovery will be marked. The FV store architecture must then preserve marked items, either by making them unalterable (possibly with hardware support) or protect them using a fault-tolerant update process. Note that a PEIM is required to be in a fault-tolerant area if it indicates it is required for recovery or if a PEIM that is required for recovery depends on it. This architecture also assumes that it is fairly easy to determine that FVs have become corrupted.

The PEI Dispatcher then proceeds as normal. If it encounters PEIMs that have been corrupted (for example, by receiving an incorrect hash value), it must change the boot mode to "recovery." Once set to recovery, other PEIMs must not change it to one of the other states. After the PEI Dispatcher has discovered the system is in recovery mode, it will restart itself and dispatch only those PEIMs that are required for recovery.

A PEIM can also detect a catastrophic condition or a forced-recovery event and inform the PEI Dispatcher that it needs to proceed with a recovery dispatch. A PEIM can alert the PEI Foundation to start recovery by setting the present boot mode to recovery. The PEI Foundation will then reset the boot mode to **BOOT_IN_RECOVERY_MODE** and start the dispatch from the beginning with **BOOT_IN_RECOVERY_MODE** as the sole value for the mode.

NOTE

At this point a physical reset of the system has not occurred. The PEI Dispatcher has only cleared all state information and restarted itself.

It is possible that a PEIM could be built to handle the portion of the recovery that would initialize the recovery peripherals (and the buses they reside on) and then to read the new images from the peripherals and update the FVs.

It is considered far more likely that the PEI will transition to DXE because DXE is designed to handle access to peripherals. This has the additional benefit that, if DXE then discovers that a device has become corrupted, it may institute recovery without transferring control back to the PEI.

Since the PEI Foundation does not have a list of what to dispatch, how does it know if an area of invalid space in an FV should have contained a PEIM or not? The PEI Foundation should discover most corruption as an incidental result of its search for PEIMs. In this case, if the PEI Foundation completes its dispatch process without discovering enough static system memory to start DXE, then it should go into recovery mode.

12
PEI Physical Memory Usage

Introduction

This section describes how physical system memory is used during PEI. The rules for using physical system memory are different before and after permanent memory registration within the PEI execution.

Before Permanent Memory Is Installed

Discovering Physical Memory

Before permanent memory is installed, the minimum exit condition for the PEI phase is that it has enough physical system memory to run PEIMs and the DXE IPL PPI that require permanent memory. These memory-aware PEIMs may discover and initialize additional system memory, but in doing so they must not cause loss of data in the physical system memory initialized during the earlier phase. The required amount of memory initialized and tested by PEIMs in these two phases is platform dependent.

Before permanent memory is installed, a PEIM may not assume any area of physical memory is present and initialized. During this early phase, a PEIM—usually one specific to the chipset memory controller—will initialize and test physical memory. When this PEIM has initialized and tested the physical memory, it will register the memory using the PEI Memory Service **`InstallPeiMemory()`**, which in turn will cause the PEI Foundation to create an initial Hand-Off Block (HOB) list and describe the memory. The memory that is present, initialized, and tested will reside in resource descriptor HOBs in the initial HOB list (see the *Intel® Platform Innovation Framework for EFI Hand-Off Block (HOB) Specification* for more information). This memory allocation PEIM may also choose to allocate some of this physical memory by doing the following:

- Creating memory allocation HOBs, as described in After Permanent Memory Is Installed: Within PEI Memory
- Using the memory allocation services **`AllocatePages()`** and **`AllocatePool()`**

Once permanent memory has been installed, the resources described in the HOB list are considered permanent system memory.

Using Physical Memory

A PEIM that requires permanent, fixed memory allocation must schedule itself to run after **EFI_PEI_PERMANENT_MEMORY_INSTALLED_PPI** is installed. To schedule itself, the PEIM can do one of the following:

- Put this PPI's GUID into the depex of the PEIM.
- Register for a notification.

The PEIM can then allocate Hand-Off Blocks (HOBs) and other memory using the same mechanisms described in Allocating Physical Memory.

The **AllocatePool()** service can be invoked at any time during the boot phase to discover temporary memory that will have its location translated, even before permanent memory is installed.

After Permanent Memory Is Installed

Allocating Physical Memory

After permanent memory is installed, PEIMs may allocate memory in four ways:

- Using a GUID Extension HOB
- Within the PEI free memory space
- Outside of PEI memory
- Using the PEI Service **AllocatePages()**

Allocating Memory Using GUID Extension HOBs

A PEIM may allocate memory for its private use by constructing a GUID Extension HOB and using the private data area defined by the GUIDed name of the HOB for private data storage.

See the *Intel® Platform Innovation Framework for EFI Hand-Off Block (HOB) Specification* for HOB construction rules.

Allocating Memory within PEI Memory

A PEIM may allocate memory from PEI free memory space, from the top of the memory range between *PHIT->EfiFreeMemoryTop* and *PHIT->EfiFreeMemoryBottom*. To do so, the PEIM must create a memory allocation HOB that describes the allocated memory range. The allocated memory is assumed to be fixed by DXE and will not be moved unless explicitly directed to do so by a PEIM.

Perform the following steps to allocate memory within PEI memory:

1. Determine *NewHobSize*, where *NewHobSize* is the size in bytes of the memory allocation HOB to be created.
2. Determine *MemoryAllocationSize*, where *MemoryAllocationSize* is the size in bytes of the memory allocation range.
3. Check free memory to ensure there is enough free memory available. This is performed by checking that *(NewHobSize + MemoryAllocationSize) <= PHIT->EfiFreeMemoryTop - PHIT->EfiFreeMemoryBottom)*.

4. Construct the memory allocation HOB at *PHIT->EfiFreeMemoryBottom*.
5. Set *PHIT->EfiFreeMemoryTop = PHIT->EfiFreeMemoryTop - MemoryAllocationSize*.
6. Set *PHIT->EfiFreeMemoryBottom = PHIT->EfiFreeMemoryBottom + NewHobSize*.

Allocating Memory outside of PEI Memory

Although it is discouraged, a PEIM can allocate memory outside the memory declared for use in PEI, between *PHIT->EfiMemoryTop* and *PHIT->EfiMemoryBottom*, by creating a memory allocation HOB.

Perform the following steps to allocate memory outside of PEI memory:

1. Determine *NewHobSize*, where *NewHobSize* is the size in bytes of the memory allocation HOB to be created.
2. Determine *MemoryAllocationSize*, where *MemoryAllocationSize* is the size in bytes of the memory allocation range.
3. Check free memory to ensure that there is enough free memory available. To do so, check that *(NewHobSize <= PHIT->EfiFreeMemoryTop - PHIT->EfiFreeMemoryBottom*).
4. Scan the *HobList* for the next resource descriptor that describes memory outside of PEI memory whose size is greater than or equal to *MemoryAllocationSize*. The memory in the physical resource descriptor must be present, initialized, and tested.
5. Scan the *HobList* for memory allocation HOBs that overlap the selected memory range found in step 3. If no free memory is found, return to step 3.
6. Construct the memory allocation HOB at *PHIT->EfiFreeMemoryBottom*.
7. Set *PHIT->EfiFreeMemoryBottom = PHIT->EfiFreeMemoryBottom + NewHobSize*.

Allocating Memory Using PEI Service

A PEIM may allocate memory using the PEI Service **`AllocatePages()`**. Use the **`EFI_MEMORY_TYPE`** values to specify the type of memory to allocate; type **`EFI_MEMORY_TYPE`** is defined is defined in **`AllocatePages()`** in the *EFI 1.10 Specification.*

13
Special Paths Unique to the Itanium® Processor Family

Introduction

The Itanium® processor family supports the full complement of boot modes listed in the PEI CIS. In addition, however, Itanium® architecture requires an augmented flow. This flow includes a "recovery check call" in which all processors execute the PEI Foundation when an Itanium platform restarts. Each processor has its own version of temporary memory such that there are as many concurrent instances of PEI execution as there are Itanium processors.

There is a point in the multiprocessor flow, however, when all processors have to call back into the Processor Abstraction Layer A (PAL-A) component to assess whether the processor revisions and PAL-B binaries are compatible. This callback into the PAL-A does not preserve the state of the temporary memory, however. When the PAL-A returns control back to the various processors, the PEI Foundation and its associated data structures have to be reinstantiated.

At this point, however, the flow of the PEI phase is the same as for IA-32 Intel® architecture in that all processors make forward progress up through invoking the DXE IPL PPI.

Unique Boot Paths for Itanium® Architecture

Intel® Itanium® processors possess two unique boot paths that also invoke the dispatcher located at the System Abstraction Layer entry point (SALE_ENTRY):

- Processor INIT
- Machine Check (MCHK)

INIT and MCHK are two asynchronous events that start up the Security (SEC) code/dispatcher in an Itanium®-based system. The Framework security module is transparent during all the code paths except for the recovery check call that happens during a cold boot. The PEIMs that handle these events are architecture aware and do not return control to the PEI Dispatcher. They call their respective architectural handlers in the operating system.

The figure below shows the boot path for INIT and MCHK events.

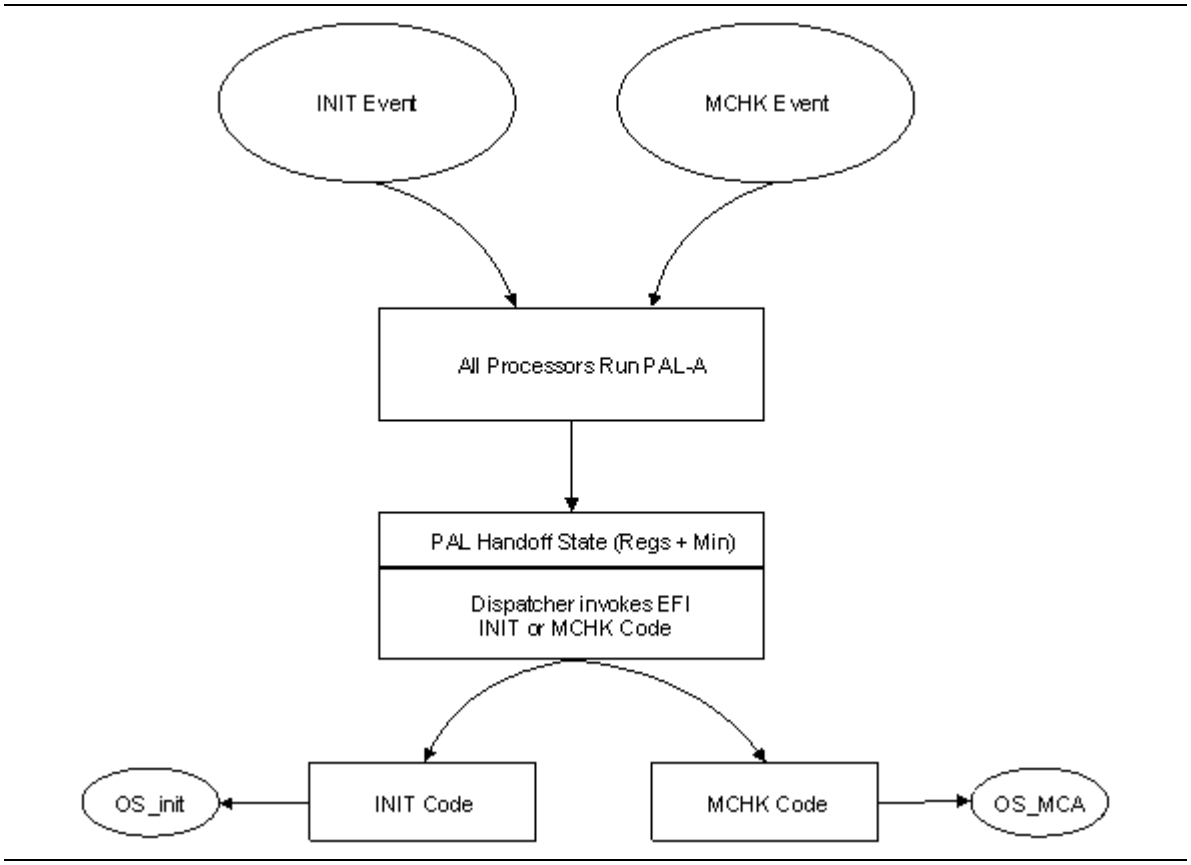


Figure 13-1. Itanium Processor Boot Path (INIT and MCHK)

Min-State Save Area

When the Processor Abstraction Layer (PAL) hands control to the dispatcher, it will supply the following:

- Unique handoff state in the registers
- A pointer, called the *min-state pointer,* to the minimum-state saved buffer area

This buffer is a unique per-processor save area that is registered to each processor during the normal OS boot path. The Framework architecture defines a unique, Framework-specific data pointer, **`EFI_PEI_MIN_STATE_DATA`**, that is attached to this min-state pointer. This data structure is defined in the next topic.

The figure below shows a typical organization of a min-state buffer. The EFI Data Pointer references **`EFI_PEI_MIN_STATE_DATA`**.

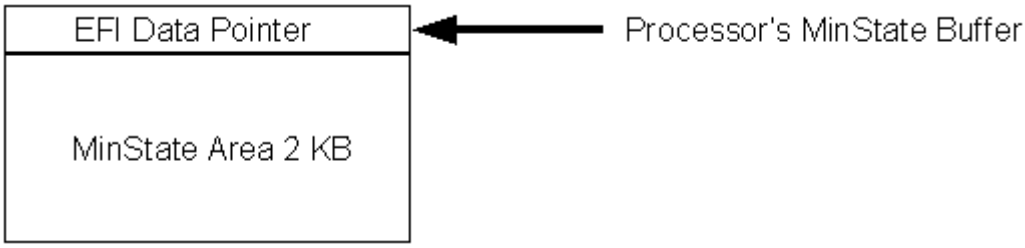


Figure 13-2. Min-State Buffer Organization

EFI_PEI_MIN_STATE_DATA

NOTE

This data structure is for the Itanium® processor family only.

Summary

A structure that encapsulates the Processor Abstraction Layer (PAL) min-state data structure for purposes of firmware state storage and reference.

Prototype

```
typedef struct {
  UINT64      OsInitHandlerPointer;
  UINT64      OsInitHandlerGP;
  UINT64      OsInitHandlerChecksum;
  UINT64      OSMchkHandlerPointer;
  UINT64      OSMchkHandlerGP;
  UINT64      OSMchkHandlerChecksum;
  UINT64      PeimInitHandlerPointer;
  UINT64      PeimInitHandlerGP;
  UINT64      PeimInitHandlerChecksum;
  UINT64      PeimMchkHandlerPointer;
  UINT64      PeimMchkHandlerGP;
  UINT64      PeimMckhHandlerChecksum;
  UINT64      TypeOfOSBooted;
  UINT8       MinStateReserved[0x400];
  UINT8       OEMReserved[0x400];
} EFI_PEI_MIN_STATE_DATA;
```

Parameters

OsInitHandlerPointer

The address of the operating system's INIT handler. The INIT is a restart type for the Itanium processor family.

OsInitHandlerGP

The value of the operating system's INIT handler's General Purpose (GP) register. Per the calling conventions for the Itanium processor family, the GP must be set before invoking the function.

OsInitHandlerChecksum

A 64-bit checksum across the contents of the operating system's INIT handler. This can be used by the EFI firmware to corroborate the integrity of the INIT handler prior to invocation.

OSMchkHandlerPointer

The address of the operating system's Machine Check (MCHK) handler. MCHK is a restart type for the Itanium processor family.

OSMchkHandlerGP

The value of the operating system's MCHK handler's GP register. Per the calling conventions for the Itanium processor family, the GP must be set before invoking the function.

OSMchkHandlerChecksum

A 64-bit checksum across the contents of the operating system's MCHK handler. This can be used by the EFI firmware to corroborate the integrity of the MCHK handler prior to invocation.

PeimInitHandlerPointer

The address of the PEIM's INIT handler.

PeimInitHandlerGP

The value of the PEIM's INIT handler's GP register. Per the calling conventions for the Itanium processor family, the GP must be set before invoking the function.

PeimInitHandlerChecksum

A 64-bit checksum across the contents of the PEIM's INIT handler. This can be used by the EFI firmware to corroborate the integrity of the INIT handler prior to invocation.

PeimMchkHandlerPointer

The address of the PEIM's MCHK handler.

PeimMchkHandlerGP

The value of the PEIM's MCHK handler's GP register. Per the calling conventions for the Itanium processor family, the GP must be set before invoking the function.

PeimMckhHandlerChecksum

A 64-bit checksum across the contents of the PEIM's MCHK handler. This can be used by the EFI firmware to corroborate the integrity of the MCHK handler prior to invocation.

TypeOfOSBooted

Details the type of operating system that was originally booted. This allows for different preliminary processing in firmware based upon the target OS.

MinStateReserved

Reserved bytes that must not be interpreted by OEM firmware. Future versions of EFI may choose to expand in this range.

OEMReserved

Reserved bytes for the OEM. EFI core components should not attempt to interpret the contents of this region.

Description

A 64-bit EFI data pointer is defined at the beginning of the Itanium processor family min-state data structure. This data pointer references an **EFI_PEI_MIN_STATE_DATA** structure that is defined above. This latter structure contains the entry points of INIT and MCHK code blocks. The pointers are defined such that the INIT and MCHK code can be either written as ROM-based PEIMs or as DXE drivers. The distinction between PEIM and DXE driver are at the OEM's discretion.

In Itanium® architecture, the EFI firmware must register a min-state with the PAL. This min-state is memory when the PAL code can deposit processor-specific information upon various restart events (INIT, RESET, Machine Check). Upon receipt of INIT or MCHK, the EFI firmware shall first invoke the PEIM INIT or MCHK handlers, respectively, and then the OS INIT or MCHK handler. The min-state data structure is a natural location from which to reference the EFI data structure that contains these latter entry points.

Dispatching Itanium® Processor Family PEIMs

The Itanium® processor family dispatcher starts dispatching all the PEIMs as it resolves the dependency grammar contained within their headers. Because all Itanium processors enter into SALE_ENTRY for a recovery check, some of the PEIMs will contain multiprocessor (MP) code and will work on all processors. The behavior of a particular PEIM that is dispatched depends on the following:

- Handoff state given by the Processor Abstraction Layer (PAL)
- The boot mode flag

Once the processor runs some code and one of the recovery check PEIM determines that the firmware needs to be recovered, it flips the boot flag to recovery and invokes the dispatcher again in recovery mode.

If it is a nonrecovery situation (normal boot), then the recovery check PEIM wakes up all the processors and returns them to PAL-A for further initialization. Note that when control for a normal boot returns back to the PAL to run PAL-B code, all of the register contents are lost. When control returns to the dispatcher, the PEIMs gain control in the dispatched order and can determine the memory topology (if needed in a platform implementation) by reading the memory controller registers of the chipset. The PEIMs can then build Hand-Off Blocks (HOBs).

When the first phase is done, there will be coherent memory on the system that all the node processors can see. The system then begins to execute the dispatcher in a second phase, during which it builds HOBs. On a multinode system with many processors, the configuration of memory may take several steps and therefore quite a bit of code.

When the second phase is done, the last PEIM will build DXE as described in PEI to DXE Handoff and hand control to the Framework DXE phase for further initialization of the platform.

The figure below depicts the initial flow between PAL-A , PAL-B, and the PEI Foundation located at SALE_ENTRY point.

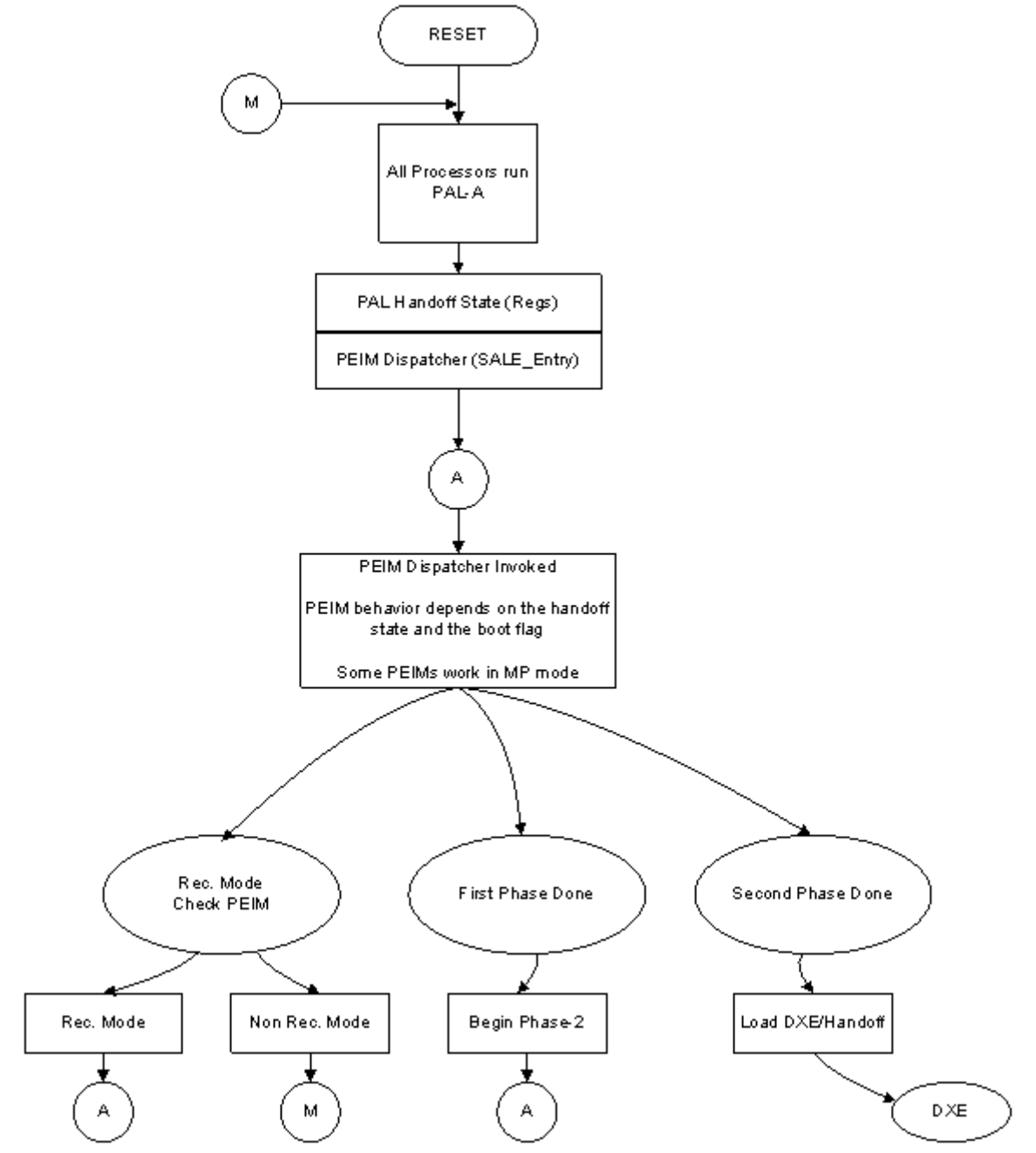


Figure 13-3. Boot Path in Itanium Processors

14
Security (SEC) Phase Information

Introduction

The Security (SEC) phase is the first phase in the Framework architecture and is responsible for the following:

- Handling all platform restart events
- Creating a temporary memory store
- Serving as the root of trust in the system
- Passing handoff information to the PEI Foundation

In addition to the minimum architecturally required handoff information, the SEC phase can pass optional information to the PEI Foundation, such as the SEC Platform Information PPI or information about the health of the processor.

The tasks listed above are common to all processor microarchitectures. However, there are some additions or differences between IA-32 and Itanium® processors, which are discussed in Processor-Specific Details.

Responsibilities

Handling All Platform Restart Events

The Security (SEC) phase is the unit of processing that handles all platform restart events, including the following:

- Applying power to the system from an unpowered state
- Restarting the system from an active state
- Receiving various exception conditions

The SEC phase is responsible for aggregating any state information so that some PEIM can deduce the health of the processor upon the respective restart.

Creating a Temporary Memory Store

The Security (SEC) phase is also responsible for creating some temporary memory store. This temporary memory store can include but is not limited to programming the processor cache to behave as a linear store of memory. This cache behavior is referred to as "no evictions mode" in that access to the cache should always represent a hit and not engender an eviction to the main memory backing store; this "no eviction" is important in that during this early phase of platform evolution, the main memory has not been configured and such as eviction could engender a platform failure.

Serving As the Root of Trust in the System

Finally, the Security (SEC) phase represents the root of trust in the system. Any inductive security design in which the integrity of the subsequent module to gain control is corroborated by the caller

must have a root, or "first," component. For any Framework deployment, the SEC phase represents the initial code that takes control of the system. As such, a platform or technology deployment may choose to authenticate the PEI Foundation from the SEC phase before invoking the PEI Foundation.

Passing Handoff Information to the PEI Foundation

Regardless of the other responsibilities listed in this section, the Security (SEC) phase's final responsibility is to convey the following handoff information to the PEI:

- State of the platform
- Location of the Boot Firmware Volume (BFV)
- Size of the temporary RAM

This handoff information listed above is passed to the PEI as arguments in the **EFI_PEI_STARTUP_DESCRIPTOR** data structure. The SEC phase uses this data structure to push the handoff information on the stack and invoke the PEI.

SEC Platform Information PPI

Handoff information is passed from the Security (SEC) phase to the PEI Foundation using the data structure **EFI_PEI_STARTUP_DESCRIPTOR**. It is a **mandatory** data structure that provides the minimum amount of information from the SEC phase that is required to initialize the PEI Foundation and PEI operational environment.

In addition, however, an **optional** PPI, **EFI_SEC_PLATFORM_INFORMATION_PPI**, can be used to pass handoff information from SEC to the PEI Foundation. This PPI abstracts platform-specific information that the PEI Foundation needs to discover where to begin dispatching PEIMs. It can be part of the PPI list that is included as the final argument of the **EFI_PEI_STARTUP_DESCRIPTOR** data structure.

Health Flag Bit Format

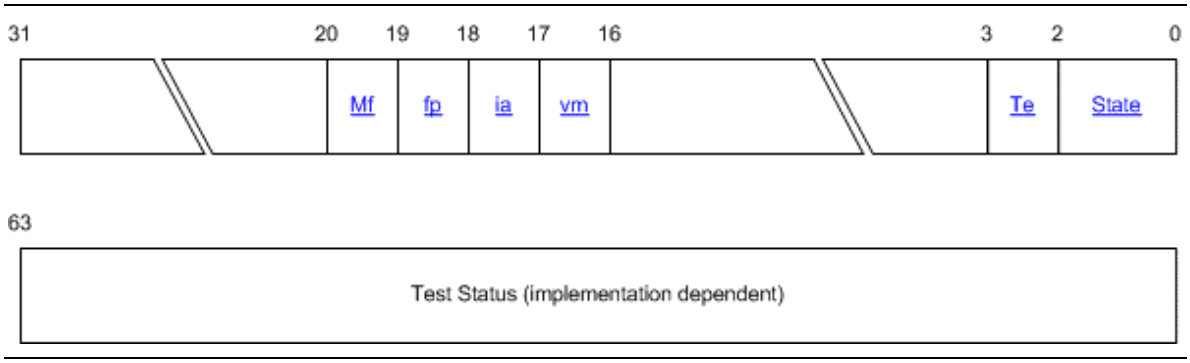
Health Flag Bit Format

The Health flag contains information that is generated by microcode, hardware, and/or the Itanium® processor Processor Abstraction Layer (PAL) code about the state of the processor upon reset. Type **EFI_HEALTH_FLAGS** is defined in **SEC_PLATFORM_INFORMATION_PPI.PlatformInformation()**.

In an Itanium®-based system, the Health flag is passed from PAL-A after restarting. It is the means by which the PAL conveys the state of the processor to the firmware, such as EFI. The handoff state is separated between the PAL and EFI because the code is provided by different vendors; Intel provides the PAL and various OEMs design the EFI firmware.

The Health flag is used by both IA-32 and Itanium® architectures, but *Tested* (Te) is the only common bit. IA-32 has the built-in self-test (BIST), but none of the other capabilities.

The figure below depicts the bit format in the Health flag.



Health Flag Bit Format

The table below explains the bit fields in the Health flag. IA-32 ignores all bits except *Tested* (Te).

Table 14-1. Health Flag Bit Description

Field	Parameter Name in EFI_HEALTH_FLAGS	Bit #	Description
State	*Status*	0:1	A 2-bit field indicating self-test state after reset. For more information, see Self-Test State Parameter.
Te	*Tested*	2	A 1-bit field indicating whether testing has occurred. If this field is zero, the processor has not been tested, and no further fields in the self-test State parameter are valid.
Vm	*VirtualMemoryUnavailable*	16	A 1-bit field. If set to 1, indicates that virtual memory features are not available.
Ia	*Ia32ExecutionUnavailable*	17	A 1-bit field. If set to 1, indicates that IA-32 execution is not available.
Fp	*FloatingPointUnavailable*	18	A 1-bit field. If set to 1, indicates that the floating point unit is not available.

Field	Parameter Name in EFI_HEALTH_FLAGS	Bit #	Description
Mf	*MiscFeaturesUnavailable*	19	A 1-bit field. If set to 1, indicates miscellaneous functional failure other than vm, ia, or fp. The test status field provides additional information on test failures when the State field returns a value of performance restricted or functionally restricted. The value returned is implementation dependent.

Self-Test State Parameter

Self-test state parameters are defined in the same format for IA-32 Intel® processors and the Intel® Itanium® processor family. Some of the test status bits may not be relevant to IA-32 processors. In that case, these bits will read **NULL** on IA-32 processors.

The table below indicates the meanings for various values of the self-test State parameter (bits 0:1) of the Health flag.

Table 14-2. Self-Test State Bit Values

State	Value	Description
Catastrophic Failure	N/A	Processor is not executing.
Healthy	00	No failure in functionality or performance.
Performance Restricted	01	No failure in functionality but performance is restricted.
Functionally Restricted	10	Some code may run but functionality is restricted and performance may also be affected.

If the state field indicates that the processor is functionally restricted, then the vm, ia, and fp fields in the Health flag specify additional information about the functional failure. See the table in Health Flag Bit Format for a description of these fields.

To further qualify "Functionally Restricted," the following requirements will be met:

- The processor or PAL (for the Itanium processor family) has detected and isolated the failing component so that it will not be used.

- The processor must have at least one functioning memory unit, arithmetic logic unit (ALU), shifter, and branch unit.
- The floating-point unit may be disabled.
- For the Itanium processor family, the Register Stack Engine (RSE) is not required to work, but register renaming logic must work properly.
- The paths between the processor-controlled caches and the register files must work during the tests.
- Loads from the firmware address space must work correctly.

Processor-Specific Details

SEC Phase in IA-32 Intel® Architecture

In 32-bit Intel® architecture (IA-32), the Security (SEC) phase of the Framework is responsible for several activities:

- Locating the PEI Foundation
- Passing control directly to PEI using an architecturally defined handoff state
- Initializing processor-controlled memory resources, such as the processor data cache, that can be used as a linear extent of memory for a call stack (if supported)

The figure below shows the steps completed during PEI initialization for IA-32.

Figure 14-1. PEI Initialization Steps in IA-32

SEC Phase in the Itanium® Processor Family

Itanium® architecture contains enough hooks to authenticate the PAL-A and PAL-B code distributed by the processor vendor.

The internal microcode on the processor silicon that starts up on a power-good reset finds the first layer of processor abstraction code (called PAL-A) located in the Boot Firmware Volume (BFV) using architecturally defined pointers in the BFV. It is the responsibility of this microcode to authenticate that the PAL-A code layer from the processor vendor has not been tampered.

If the authentication of the PAL-A layer passes, then control passes on to the PAL-A layer. The PAL-A layer then authenticates the next layer of processor abstraction code (called PAL-B) before passing control to it.

In addition, the SEC phase of the Framework is also responsible for locating the PEI Foundation and verifying its authenticity.

The figure below summarizes the SEC phase in the Itanium® processor family.

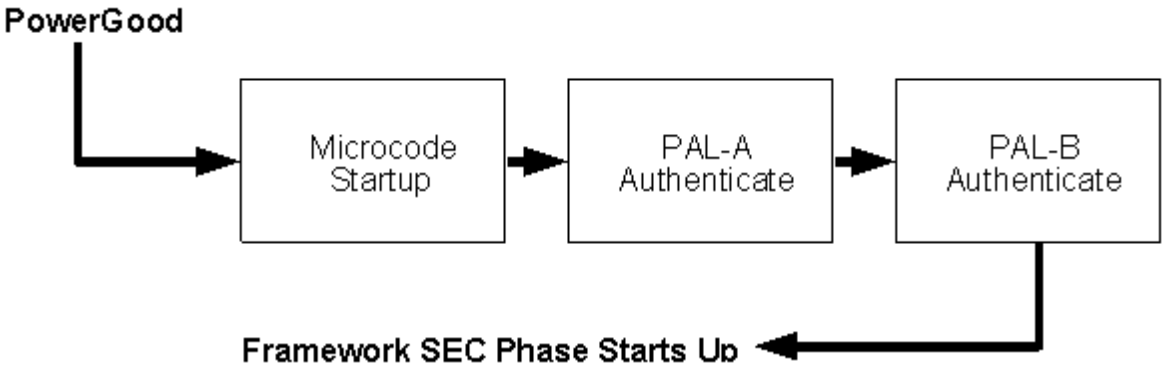


Figure 14-2. Security (SEC) Phase in the Itanium Processor Family

15 Returned Status Codes

Returned Status Codes

EFI interfaces return an **EFI_STATUS** code. The topics in this section discuss the following:

- Ranges of EFI_STATUS codes
- Success codes
- Error codes
- Warning codes

Error codes also have their highest bit set, so all error codes have negative values. The range of status codes that have the highest bit set and the next to highest bit clear are reserved for use by EFI. The range of status codes that have both the highest bit set and the next to highest bit set are reserved for use by OEMs.

Success and warning codes have their highest bit clear, so all success and warning codes have positive values. The range of status codes that have both the highest bit clear and the next to highest bit clear are reserved for use by EFI. The range of status code that have the highest bit clear and the next to highest bit set are reserved for use by OEMs.

EFI_STATUS Codes Ranges

The following table lists the ranges of **EFI_STATUS** codes.

Table 15-1. EFI_STATUS Codes Ranges

0x00000000- 0x3fffffff	0x0000000000000000- 0x3fffffffffffffff	Success and warning codes reserved for use by EFI. See EFI_STATUS Success Codes (High Bit Clear) and EFI_STATUS Warning Codes (High Bit Clear) for valid values in this range.
0x40000000- 0x7fffffff	0x4000000000000000- 0x7fffffffffffffff	Success and warning codes reserved for use by OEMs.
0x80000000- 0xbfffffff	0x8000000000000000- 0xbfffffffffffffff	Error codes reserved for use by EFI. See EFI_STATUS Error Codes (High Bit Set) for valid values for this range.
0xc0000000- 0xffffffff	0xc000000000000000- 0xffffffffffffffff	Error codes reserved for use by OEMs.
0x00000000- 0x3fffffff	0x0000000000000000- 0x3fffffffffffffff	Success and warning codes reserved for use by EFI. See EFI_STATUS Success Codes (High Bit Clear) and EFI_STATUS Warning Codes (High Bit Clear) for valid values in this range.

EFI_STATUS Success Codes (High Bit Clear)

The following table lists the success codes for **EFI_STATUS**.

Table 15-2. EFI_STATUS Success Codes (High Bit Clear)

Mnemonic	Value	Description
EFI_SUCCESS	0	The operation completed successfully.

EFI_STATUS Error Codes (High Bit Set)

The following table lists the error codes for **EFI_STATUS**.

Table 15-3. EFI_STATUS Error Codes (High Bit Set)

Mnemonic	Value	Description
EFI_LOAD_ERROR	1	The image failed to load.
EFI_INVALID_PARAMETER	2	A parameter was incorrect.
EFI_UNSUPPORTED	3	The operation is not supported.
EFI_BAD_BUFFER_SIZE	4	The buffer was not the proper size for the request.
EFI_BUFFER_TOO_SMALL	5	The buffer is not large enough to hold the requested data. The required buffer size is returned in the appropriate parameter when this error occurs.
EFI_NOT_READY	6	There is no data pending upon return.
EFI_DEVICE_ERROR	7	The physical device reported an error while attempting the operation.
EFI_WRITE_PROTECTED	8	The device cannot be written to.
EFI_OUT_OF_RESOURCES	9	A resource has run out.
EFI_VOLUME_CORRUPTED	10	An inconstancy was detected on the file system causing the operating to fail.
EFI_VOLUME_FULL	11	There is no more space on the file system.
EFI_NO_MEDIA	12	The device does not contain any medium to perform the operation.
EFI_MEDIA_CHANGED	13	The medium in the device has changed since the last access.
EFI_NOT_FOUND	14	The item was not found.

Mnemonic	Value	Description
EFI_ACCESS_DENIED	15	Access was denied.
EFI_NO_RESPONSE	16	The server was not found or did not respond to the request.
EFI_NO_MAPPING	17	A mapping to a device does not exist.
EFI_TIMEOUT	18	The timeout time expired.
EFI_NOT_STARTED	19	The protocol has not been started.
EFI_ALREADY_STARTED	20	The protocol has already been started.
EFI_ABORTED	21	The operation was aborted.
EFI_ICMP_ERROR	22	An ICMP error occurred during the network operation.
EFI_TFTP_ERROR	23	A TFTP error occurred during the network operation.
EFI_PROTOCOL_ERROR	24	A protocol error occurred during the network operation.
EFI_INCOMPATIBLE_VERSION	25	The function encountered an internal version that was incompatible with a version requested by the caller.
EFI_SECURITY_VIOLATION	26	The function was not performed due to a security violation.
EFI_CRC_ERROR	27	A CRC error was detected.
EFI_NOT_AVAILABLE_YET	28	The service is not available yet because one of its dependencies has not been satisfied yet.
EFI_UNLOAD_IMAGE	29	If this value is returned by an EFI image, then the image should be unloaded.

EFI_STATUS Warning Codes (High Bit Clear)

The following table lists the warning codes for **EFI_STATUS**.

Table 15-4. EFI_STATUS Warning Codes (High Bit Clear)

Mnemonic	Value	Description
EFI_WARN_UNKOWN_GLYPH	1	The Unicode string contained one or more characters that the device could not render and were skipped.
EFI_WARN_DELETE_FAILURE	2	The handle was closed, but the file was not deleted.
EFI_WARN_WRITE_FAILURE	3	The handle was closed, but the data to the file was not flushed properly.
EFI_WARN_BUFFER_TOO_SMALL	4	The resulting buffer was too small, and the data was truncated to the buffer size.

16
Dependency Expression Grammar

Dependency Expression Grammar

This topic contains an example BNF grammar for a PEIM dependency expression compiler that converts a dependency expression source file into a dependency section of a PEIM stored in a firmware volume.

Example Dependency Expression BNF Grammar

```
<depex>     ::= <bool>
<bool>      ::= <bool> AND <term>
              | <bool> OR <term>
              | <term>
<term>      ::= NOT <factor>
              | <factor>
<factor>    ::= <bool>
              | TRUE
              | FALSE
              | GUID
              | END
<guid>      ::= '{' <hex32> ',' <hex16> ',' <hex16> ','
                <hex8> ',' <hex8> ',' <hex8> ',' <hex8> ','
                <hex8> ',' <hex8> ',' <hex8> ',' <hex8> '}'
<hex32>     ::= <hexprefix> <hexvalue>
<hex16>     ::= <hexprefix> <hexvalue>
<hex8>      ::= <hexprefix> <hexvalue>
<hexprefix>::= '0' 'x'
              | '0' 'X'
<hexvalue>  ::= <hexdigit> <hexvalue>
              | <hexdigit>
<hexdigit>  ::= [0-9]
              | [a-f]
              | [A-F]
```

Sample Dependency Expressions

The following contains three examples of source statements using the BNF grammar from above along with the opcodes, operands, and binary encoding that a dependency expression compiler would generate from these source statements.

```
//
// Source
//
EFI_PEI_CPU_IO_PPI_GUID AND EFI_PEI_READ_ONLY_VARIABLE_ACCESS_PPI_GUID
END

//
// Opcodes, Operands, and Binary Encoding
//
```

```
ADDR   BINARY                      MNEMONIC
====   =======================
=============================================
0x00 : 02                          PUSH
0x01 : 26 25 73 b0 c8 38 40 4b     EFI_PEI_CPU_IO_PPI_GUID
       88 77 61 c7 b0 6a ac 45
0x11 : 02                          PUSH
0x12 : b1 cc ba 26 42 6f d4 11
EFI_PEI_READ_ONLY_VARIABLE_ACCESS_PPI_GUID
       bc e7 00 80 c7 3c 88 81
0x22 : 03                          AND
0x23 : 08                          END
```