EFI Specification Evolution

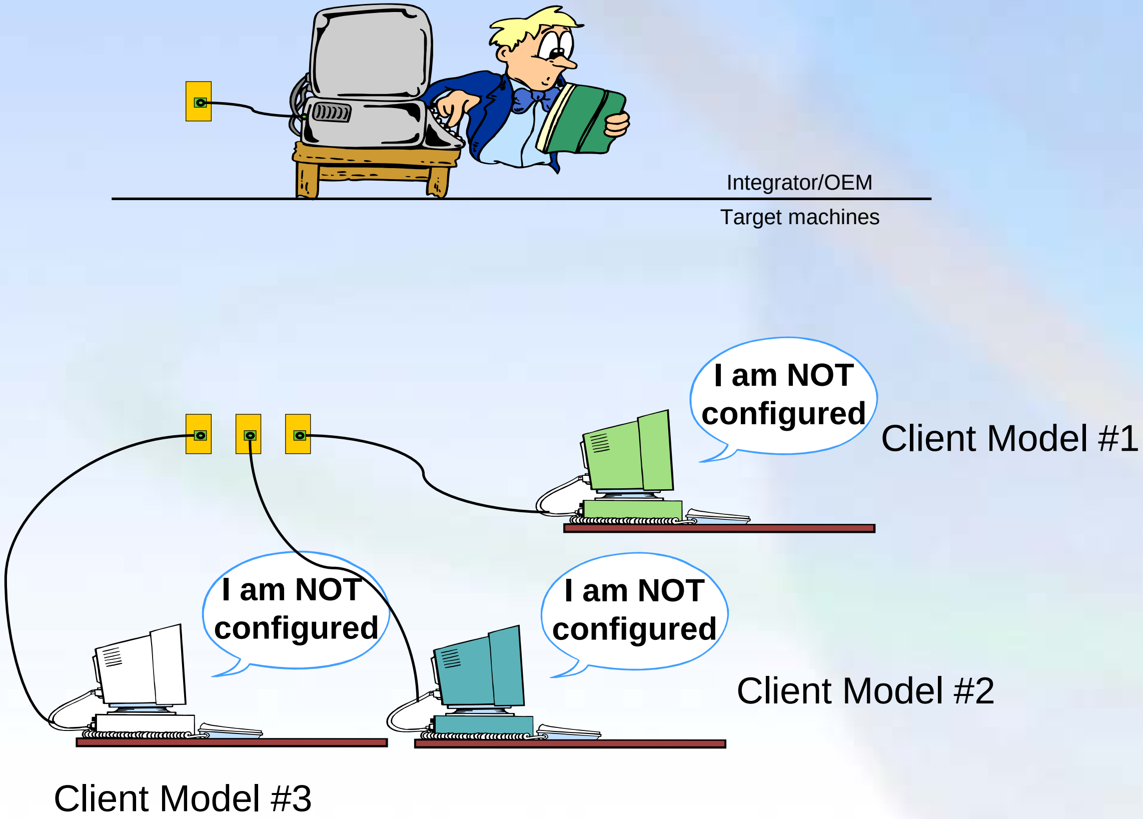
Vincent Zimmer
Staff Engineer
Intel SSG

Agenda

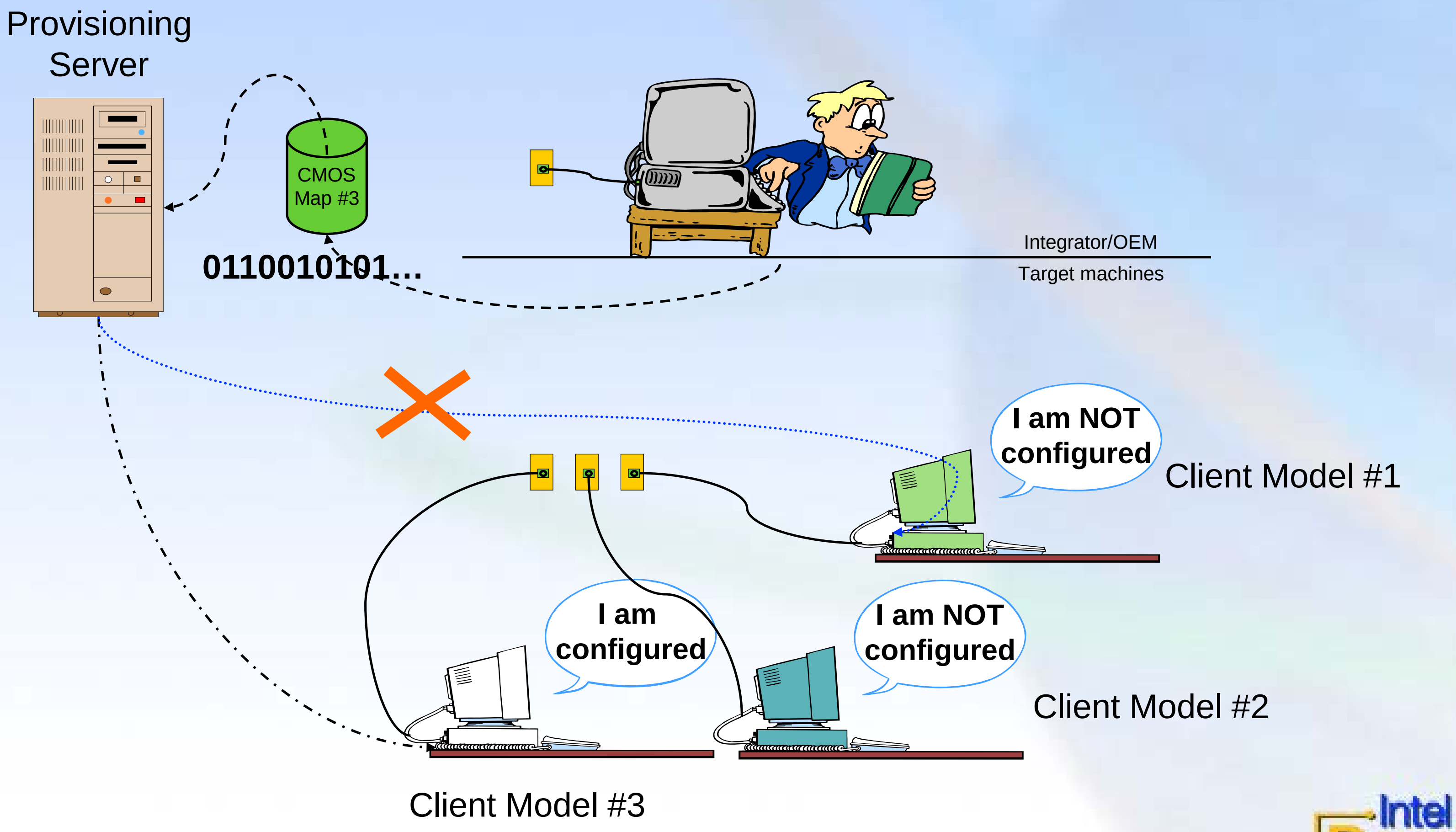
- Goals
- Current State-of-the-Art
- Proposed EFI building blocks
  - Networking
  - Security
  - Configuration
  - Setup

in the

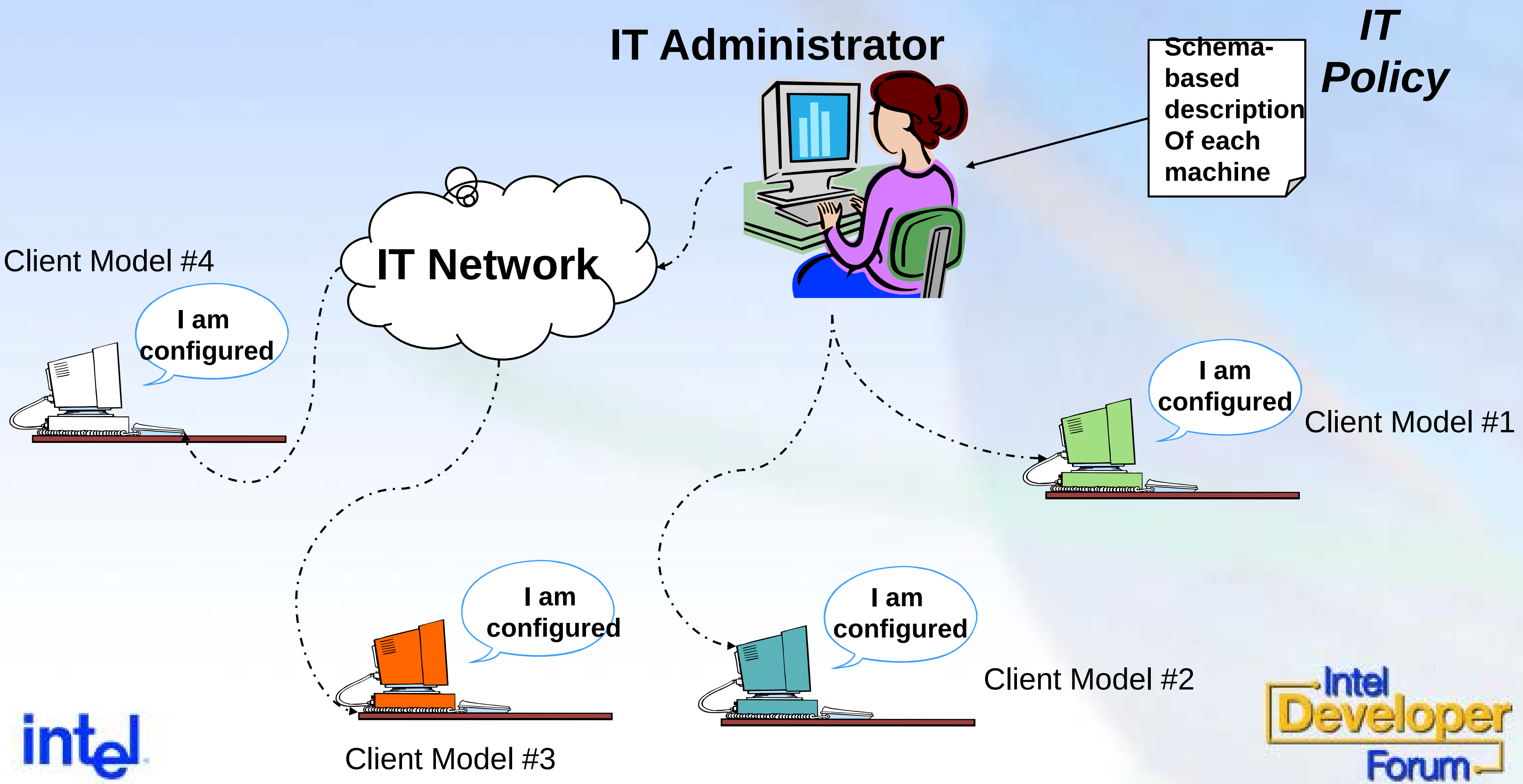
Where are we today?



Today’s Provisioning Solutions



EFI futures to enable solution stack

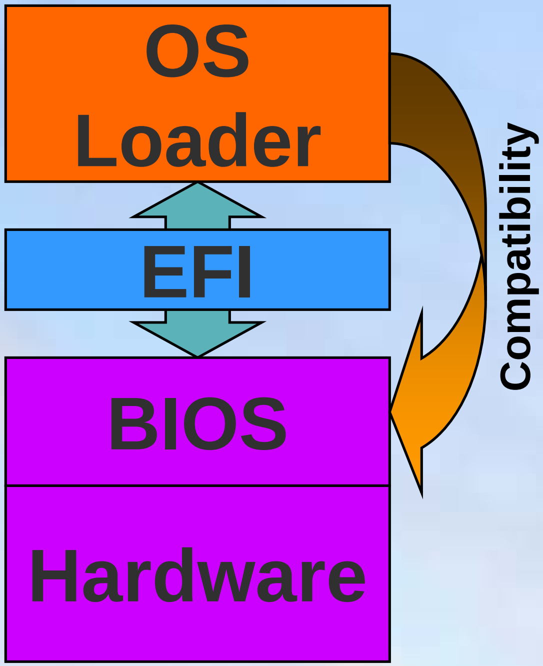


Strategy

- Make computers more easily managed by other computers
- Automated management requires security
- Make sure technology scales from across all market segments
- Solve the out-of-box configuration issues.
- Standardize the technology aspects in EFI to help reach this end
  - Sit tight & details to follow….

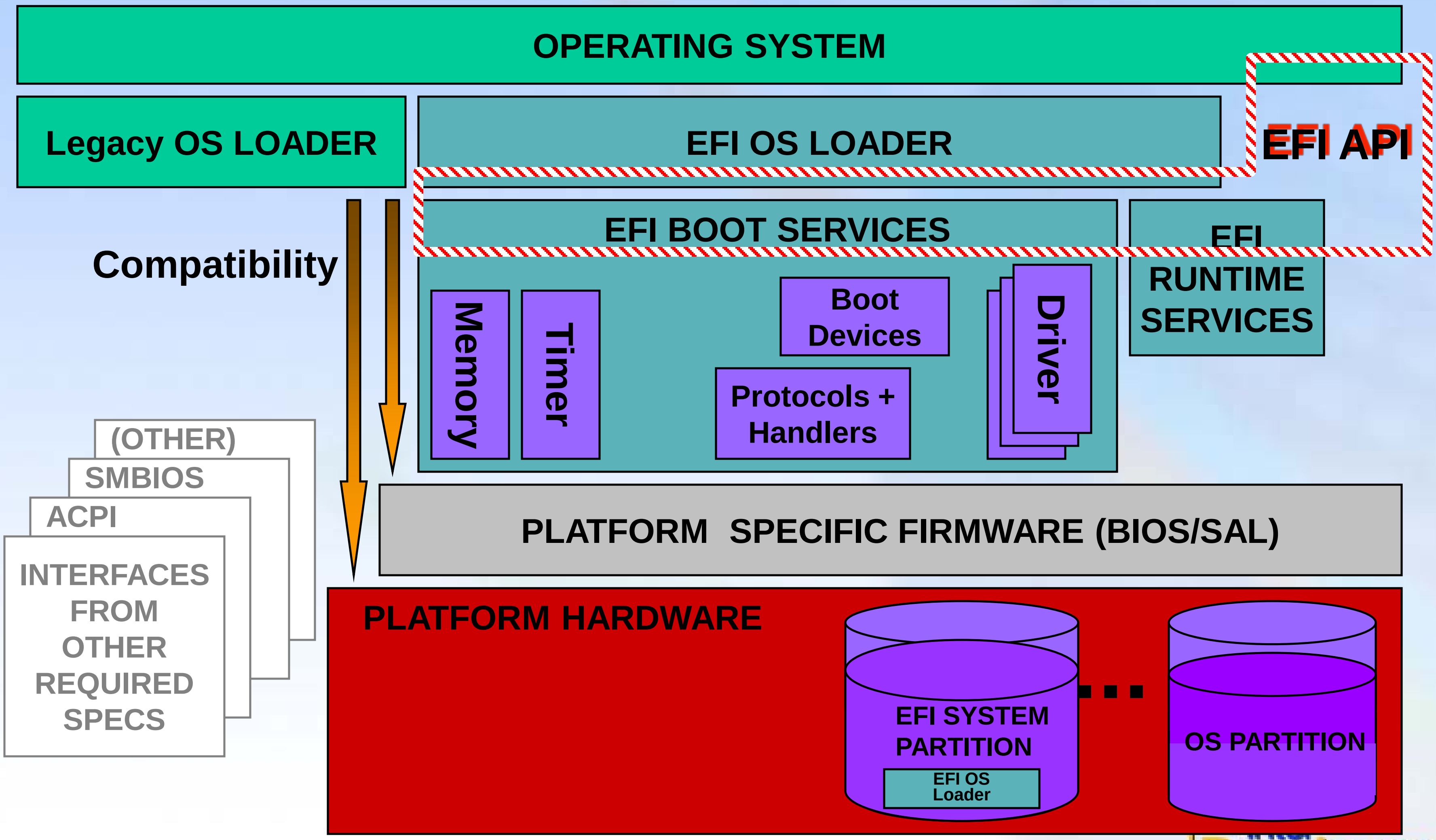
EFI Overview

- Interface specification
  - Implementation agnostic
- Abstracts BIOS from OS
  - Decouples development
- Compatible by design
  - Evolution, not revolution
- Modular and extensible
  - OS-Neutral value add
- Complements existing interfaces



Flexible to meet existing and future needs

EFI Layered Implementation



Agenda

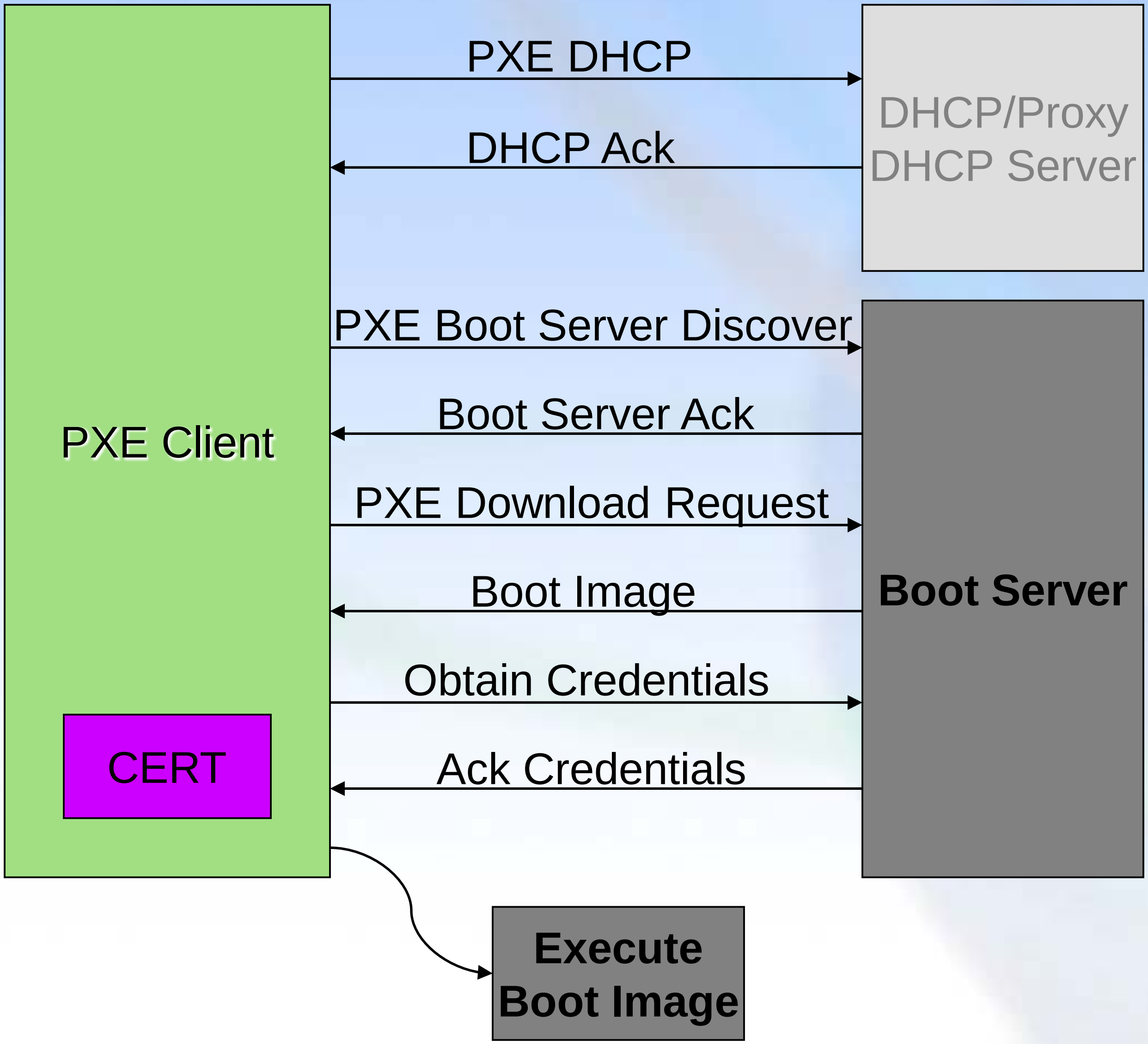
- Goals
- **Current State-of-the-Art**
- Proposed EFI building blocks
  - Networking
  - Security
  - Configuration
  - Setup
- Summary

in the

Current State-of-the-Art

- PXE and BIS
  - Network boot standard introduced by WfM
  - BIS added security test for the boot image
- BIOS Setup
  - Manual text based user interface
  - Blind CMOS copies
- Provisioning Agents and Servers
  - Products from Jareva, Platespin, etc.
  - Microsoft Network Install
  - Linux Network Boot

PXE Boot Process



Limitations of the State-of-the-Art

- PXE and BIS
  - Has scalability issues
  - No authentication of booting system
- BIOS Setup
  - Setup does not automate well
- Provisioning Agents and Servers
  - Proprietary technology needed to solve problem
  - Reboot, Reboot, Reboot

Agenda

- Goals
- Current State-of-the-Art
- Proposed EFI building blocks
  - Networking
  - Security
  - Configuration
  - Setup
- Summary

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States or other countries

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States

PXE Extensions to TFTP

- Proposing RFCs to multicast TFTP to improve scalability.
  - TFTP/MTFTP Block Count
    - Old 22 MB, New 2^{52} MB
  - Streaming Data
    - Removing acknowledgements for an approximate 50% performance improvement
  - Multi-Cast
    - Managed network saturation
- This entails software updates to BOTH the client and server software providers

Networking API extensions

- Several new pre-boot API's
  - EFI_IP_PROTOCOL
  - EFI_UDP_PROTOCOL
  - EFI_TCP_PROTOCOL
  - EFI_MTFTP_PROTOCOL
  - EFI_DHCP4_PROTOCOL
- Published by client, usable by network boot agents and embedded code
  - Not OS. Small, simple, in the flash part

Scalable services foundation

Agenda

- Goals
- Current State-of-the-Art
- Proposed EFI building blocks
  - Networking
  - **Security**
  - Configuration
  - Setup
- Summary

in the
nte is a trademark or registered trademark of nte Corporation or its subsidiaries in the
Un

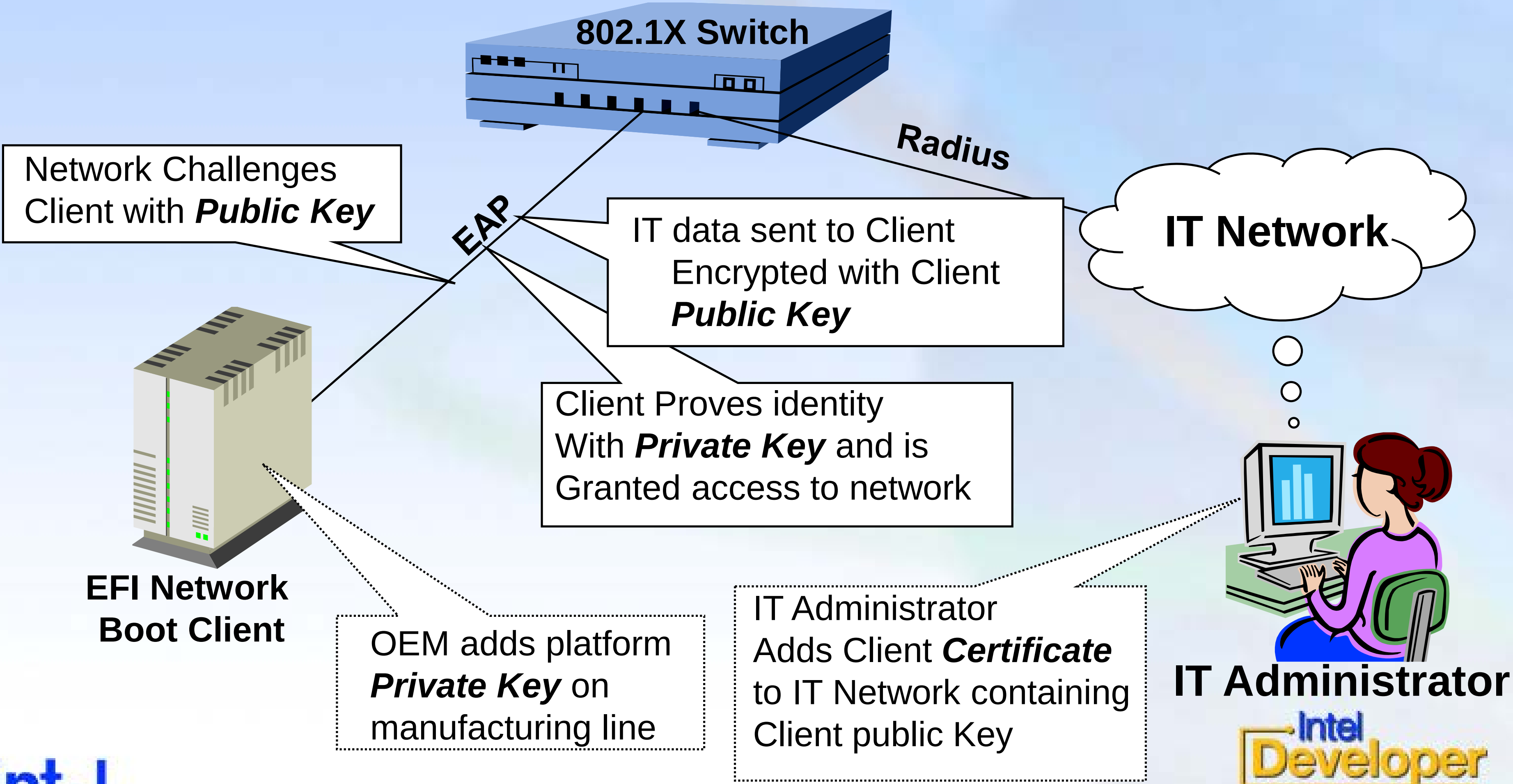
Security problems to be Solved

- Confirm identity of the client to be configured
- Send the configuration objects to the system with stronger integrity
- Securely configure the BIOS setup

Configuration and Security

- Secure Reset
  - Leverage Client Secret to send Keys over network encrypted
- Boot Image Authentication
  - Leverage Client Secret to send Keys over the network encrypted
- Secure Network Connect
  - IT Network sets Policy via 802.1X EAP messages
  - Default policy enabled if no 802.1X deployed

802.1X Client Authentication



Network Challenges
Client with ***Public Key***

IT data sent to Client
Encrypted with Client
Public Key

Client Proves identity
With ***Private Key*** and is
Granted access to network

OEM adds platform
Private Key on
manufacturing line

IT Administrator
Adds Client ***Certificate***
to IT Network containing
Client public Key

Client security services

- EFI_SECURITY_SUPPORT_PROTOCOL
  - Set of basic cryptographic and security services in the pre-boot
    - Sign
    - Hash
    - Encrypt
    - Decrypt
    - Random number generation
  - Advantages
    - Minimum amount.
    - Details names by GUID
    - Our initial set maps well to TPM
- Implement on the client

EAP Teenie RFC

- Teenie is an EAP method
  - Optimized for pre-boot code size
  - Optimized for EFI Configuration Objects
  - Will make Wi-Fi Boot much easier
- Leverage Platform Secret to authenticate Client & generate a shared secret
- Support "Remote Take Ownership"
- Implement on client and server
- Has a Phase 2 for secure data transport
  - Configuration object as format

Security via standards

Agenda

- Goals
- Current State-of-the-Art
- Proposed EFI building blocks
  - Networking
  - Security
  - **Configuration**
  - Setup
- Summary

in the
Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the
United States or other countries

Automated Configuration via Objects

- EFI Configuration Object (COB)
  - GUID’ed description of data
- EFI API to import/export configuration data for the system
- EFI 1.10 Drivers can import/Export EFI Configuration Object
- EFI Configuration Object are a new extensible Image type
  - LoadImage()/StartImage() can process EFI COBs

Proposed Protocols

- EFI_CONFIGURATION_OBJECT_PROTOCOL
  - Allows new boot capability
  - Member functions
    - Get
    - Set
    - AddHandler
    - RemoveHandler
  - Required Objects: Supported, Loaded Image, Compressed
- EFI_CONFIGURATION_OBJECT_EXPORT_PROTOCOL
  - Supports EFI 1.10 Drivers
  - Member Functions
    - Get
    - Set
  - Required Objects: Supported, Compressed, Hardware Signature

EFI Configuration Object

```
typedef struct {
  UINT32        Length;
  UINT32        Attribute;
  UINT32        Crc32;
  EFI_GUID      DataType;
  EFI_GUID      ObjectId;
} EFI_CONFIGURATION_OBJECT_HEADER;
```

OEM Provisioning

- EFI extends network boot program to be a collection of Objects
  - OEM provides standard objects
  - OSV provides modules that can be wrapped as standard objects
  - 3rd parties can provide value added objects
- Provisioning software appends EFI Objects together

Configuration items of interest

- Configuration objects INTO the client
  - BIS Certificates
  - ASF Keys
  - iSCSI boot target
- Configuration objects FROM the client
  - SMBIOS tables
  - PCI configuration settings
- Both In and Out
  - Setup information

Consistent key & data management

Agenda

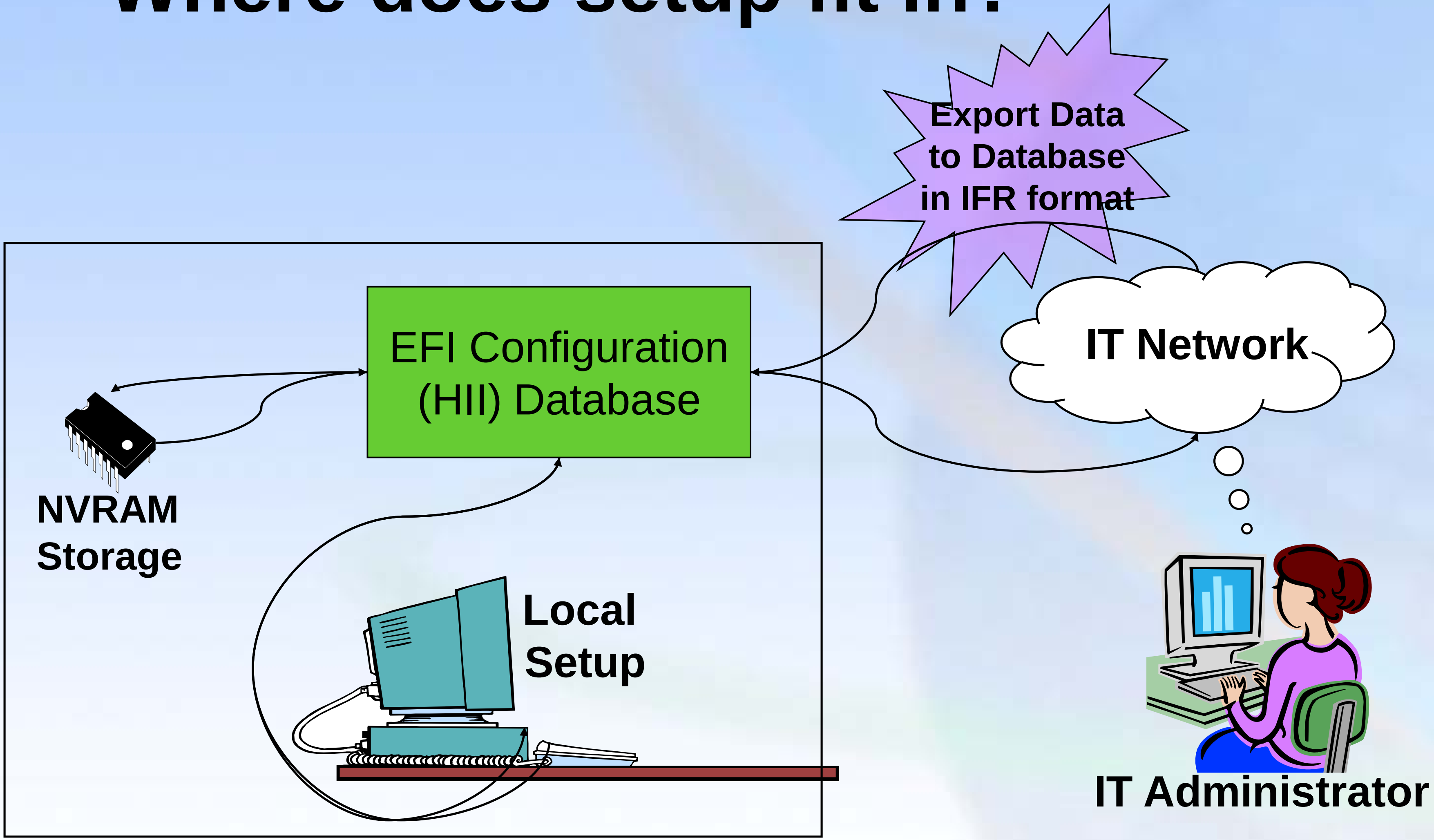
- Goals
- Current State-of-the-Art
- Proposed EFI building blocks
  - Networking
  - Security
  - Configuration
  - **Setup**
- Summary

in the
Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the
United States

Pre-Boot Setup

- New Human Interface Infrastructure (HII) with Internal Forms Representation (IFR)
  - Standardize the transport, still have to do the work as provisioning service.
- Setup for heterogeneous machines
- Allow for vendors to build schemas for classes of systems
- Scriptable & XML-like
  - Batch schema processor instead of UI
- Localizable to several languages
  - e.g., Fr, German, English, “Script”
- Form useful on platform & across net.

Where does setup fit in?

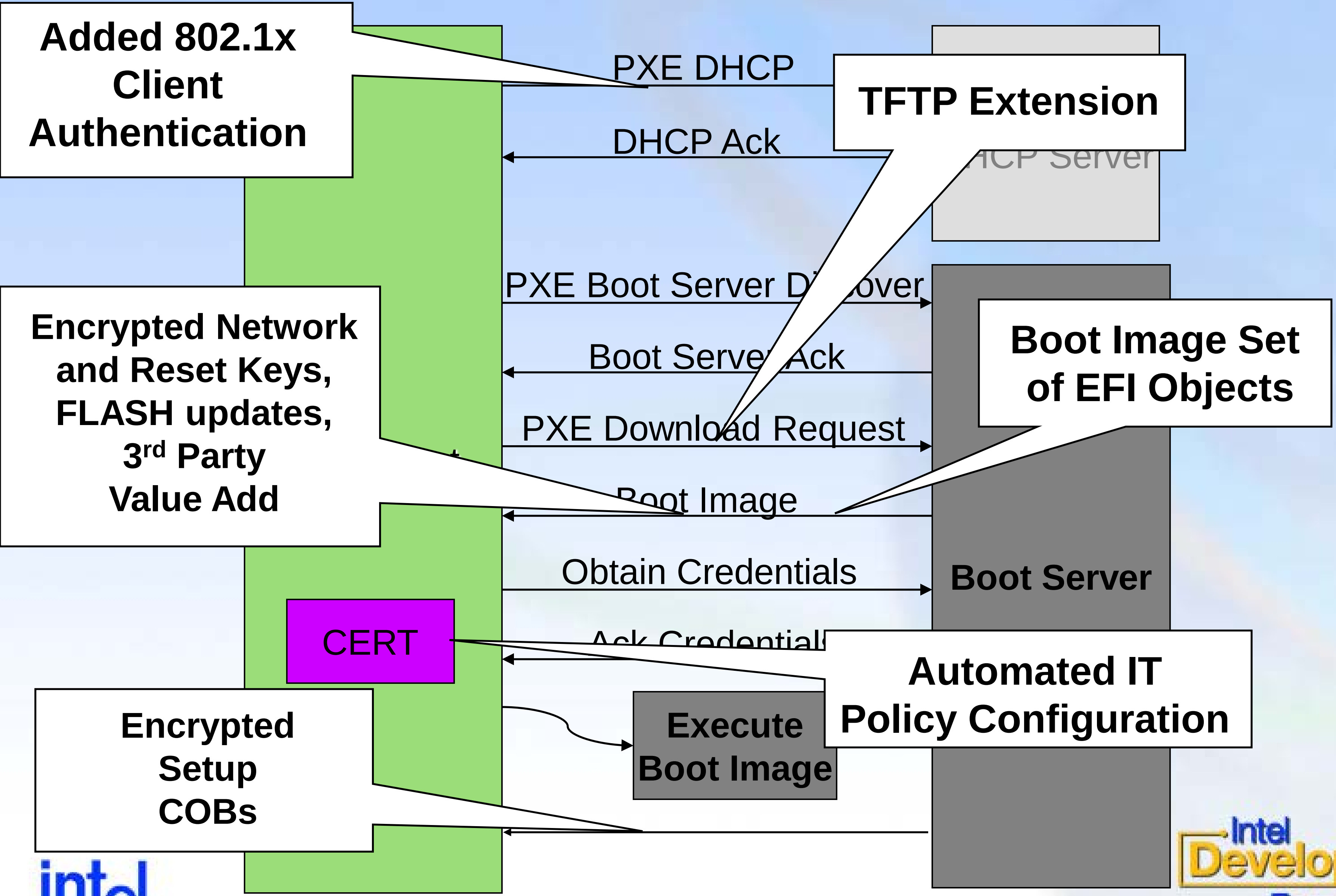


Setup advances for enterprise

Agenda

- Goals
- Current State-of-the-Art
- Proposed EFI building blocks
  - Networking
  - Security
  - Configuration
  - Setup
- **Summary**

Technology Review



Added 802.1x Client Authentication

TFTP Extension

Encrypted Network and Reset Keys, FLASH updates, 3rd Party Value Add

Boot Image Set of EFI Objects

Automated IT Policy Configuration

Encrypted Setup COBs

Summary

- Meet existing and future needs
- Scalable services foundation
- Security via standards
- Consistent key & data management
- Setup advances for the enterprise

Q & A

http://www.intel.com/technology/efi

Call to action

- **Platform builders add EFI**
- **Give us feedback**
  - **vincent.zimmer@intel.com**
- **Provisioning and OSVs investigate this technology**
- **IT investigate this technology**

More Information

Session	#	Day	Time	Room
Next Generation EFI 32 OS Loader	S186	Wed	11:00-11:50 AM	C-1/2
Introducing the Intel Platform Innovation Framework for EFI	S11	Wed	2:30-4:20 PM	C-1/2
Using the Wireless LAN to provision and manage mobile devices *	S115	Wed	2:30-3:20 PM	J-3
BIOS compatibility within the Intel Platform Innovation Framework for EFI	S12	Wed	4:30-5:20 PM	C-1/2
Non-Intel Silicon Support within the Intel Platform Innovation Framework for EFI	S13	Thu	10:00–11:50AM	C-1/2
Writing and Debugging EFI Drivers	S14	Thu	2:00-3:50 PM	C-1/2
EFI Specification Evolution	S15	Thu	4:00-4:50 PM	C-1/2

* non-EFI track

Collateral

- http://developer.intel.com/technology/efi
  - Join the EFI mailing List
  - Download EFI 1.10 Specification
  - Download EFI 1.10 Reference Code
- Intel Software College for Training
  - www.intel.com/software/products/college

Collateral

- White paper: Modular Computing: The New Enterprise Computing Model (Egenera/Intel)
- URLS:
  - IBM Autonomic Computing*: http://www-3.ibm.com/autonomic/index.shtml
  - IBM eLiza* project on X-series: http://www-1.ibm.com/servers/autonomic/
  - IBM BladeCenter*: http://www.pc.ibm.com/us/eserver/xseries/bladecenter_family.html?ca=xSeries&met=ibmblade&me=A
  - HP Utility Computing*: http://devresource.hp.com/topics/utility_comp.html
  - Microsoft .NET*: http://www.microsoft.com/net/
  - Egenera*: http://www.egenera.com/prod_spec_valprop.php
  - Sun N1*: http://wwws.sun.com/software/solutions/n1/index.html
  - Giga* analyses: (R.Fichera)
    - –Criteria for Selection: Bladed and Modular Servers (July 31, 2002)
    - –Future of the Data Center: Modularity and Virtualization (May 8, 2002)
    - –Economics of Cable Consolidation: A Major Impact on Server Cost (July 23, 2002)

EFI Specification Evolution

Vincent Zimmer

Staff Engineer

Intel SSG

Please remember to turn in your session survey form.

Acronyms

- ASF – Alert Standard Format
  http://www.dmtf.org/standards/standard_alert.php
- BIS – Boot Integrity Service
  http://www.intel.com/design/security/bis/biswks.htm
- CERT – Certificate like X.509
  http://www.ietf.org/html.charters/pkix-charter.html
- DHCP – Domain Host Controller Protocol
- RADIUS – Remote Authentication Dial-In User Service
  http://www.faqs.org/rfcs/rfc2138.html
- EAP – Extensible Authentication Protocol
  http://www.faqs.org/rfcs/rfc2284.html
- EFI – Extensible Firmware Interface
  http://www.intel.com/technology/efi/main_specification.htm
- IFR – Internal Forms Representation
- VFR – Visual Forms Representation
- 802.1x – Port Based Network Access Control

http://www.ieee802.org/1/pages/802.1x.html

Acronyms

- PXE – Preboot eXecution Environment http://www.intel.com/technology/efi/main_specification.htm
- RCMP – Remote Management and Control Protocol http://www.dmtf.org/standards/standard_alert.php
- RFC – Request for Comment http://www.ietf.org
- TCO – Total Cost of Ownership
- TFTP – Trivial File Transfer Protocol
- TPM – Trusted Computing Group http://www.trustedcomputinggroup.org
- WBEM – Web-Based Enterprise Management http://www.dmtf.org/standards/standard_wbem.php
- WfM – Wired for Management http://www.intel.com/labs/manage/wfm/index.htm