

Kerberos in Intel[®] vPro[™]

Ned Smith
Principal Engineer
Intel Business Client Platform Division

Legal Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

The Intel products in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

All dates specified are target dates, are provided for planning purposes only and are subject to change.

Δ Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See http://www.intel.com/products/processor_number for details.

Φ 64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel® 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.

Montevina, Calpella, Cantiga, Auburndale, Clarksfield, Ibex Peak, Nehalem, Iron Lake, Penryn, and other code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel, Pentium, Celeron, Centrino, Intel Core Duo, Intel Core Solo, Intel SpeedStep and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2009, Intel Corporation. All rights reserved.

Intel Software Secrets

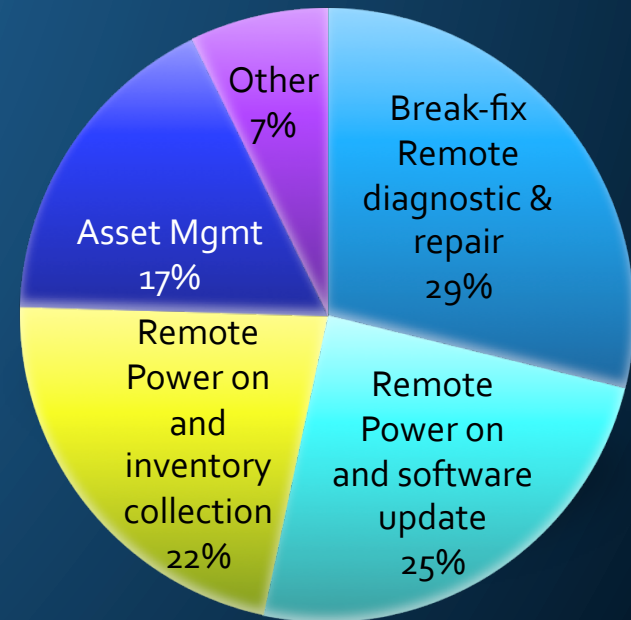
- If Intel Software were an independent software company, we'd be the 6th largest in the world
- Intel Software has the 3rd largest developer program, after MSDN and IBM
- Intel is the 3rd largest Linux institutional contributor, after Red Hat and IBM
- Intel contributed specifications to seed creation of UEFI 2.0
- Intel developed a Kerberos client for UEFI 2.0
- Intel developed a Kerberos server in vPro™ platforms

vPro™ Manageability Use Cases

Immediate Response

- Break-fix / remote KVM
- Remote platform disable
- Network outbreak containment
- Asset management / tracking
- Audit-log maintenance
- Software update
- Inventory collection

Delayed Response

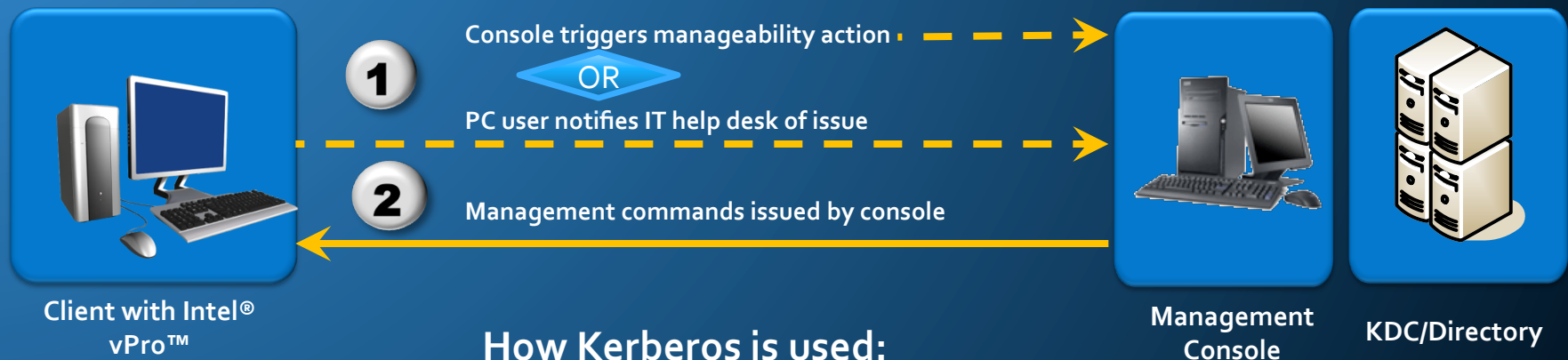


Mix of vPro usages by end customers

Platform can be powered down or in sleep states

Typical vPro™ Use Case Flow

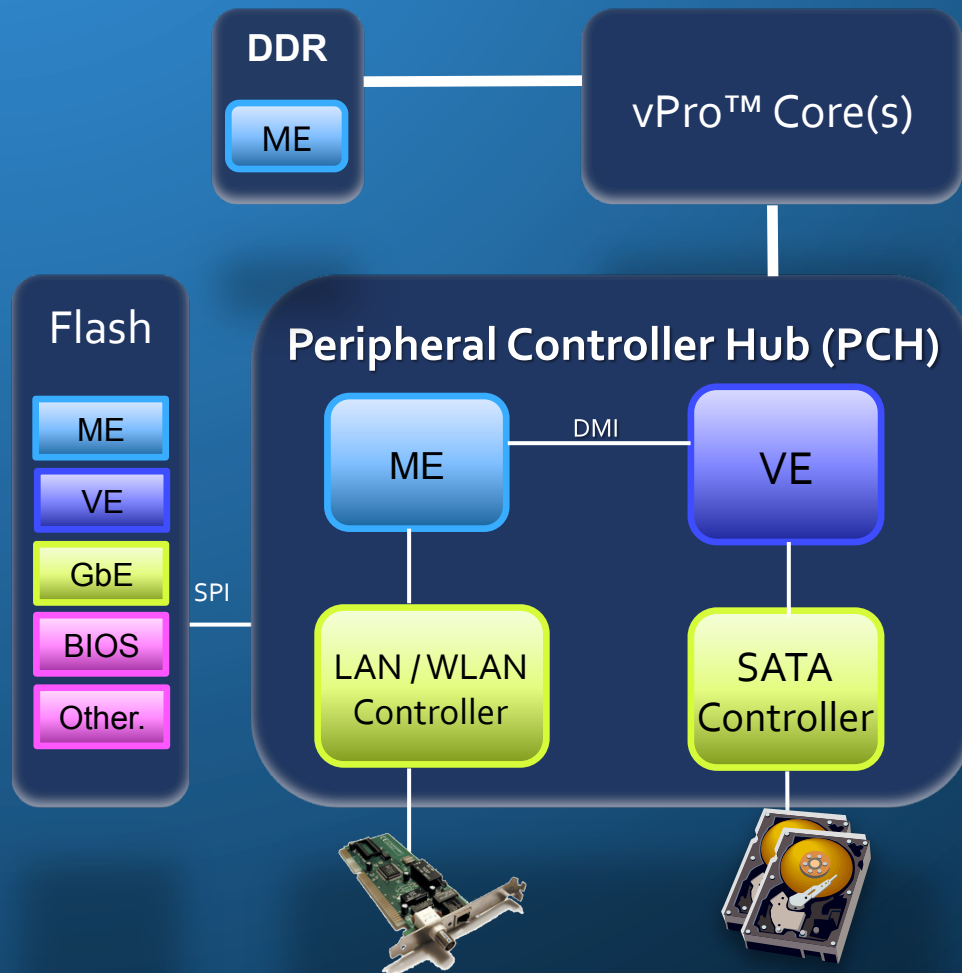
Console-Initiated Use Model



How Kerberos is used:

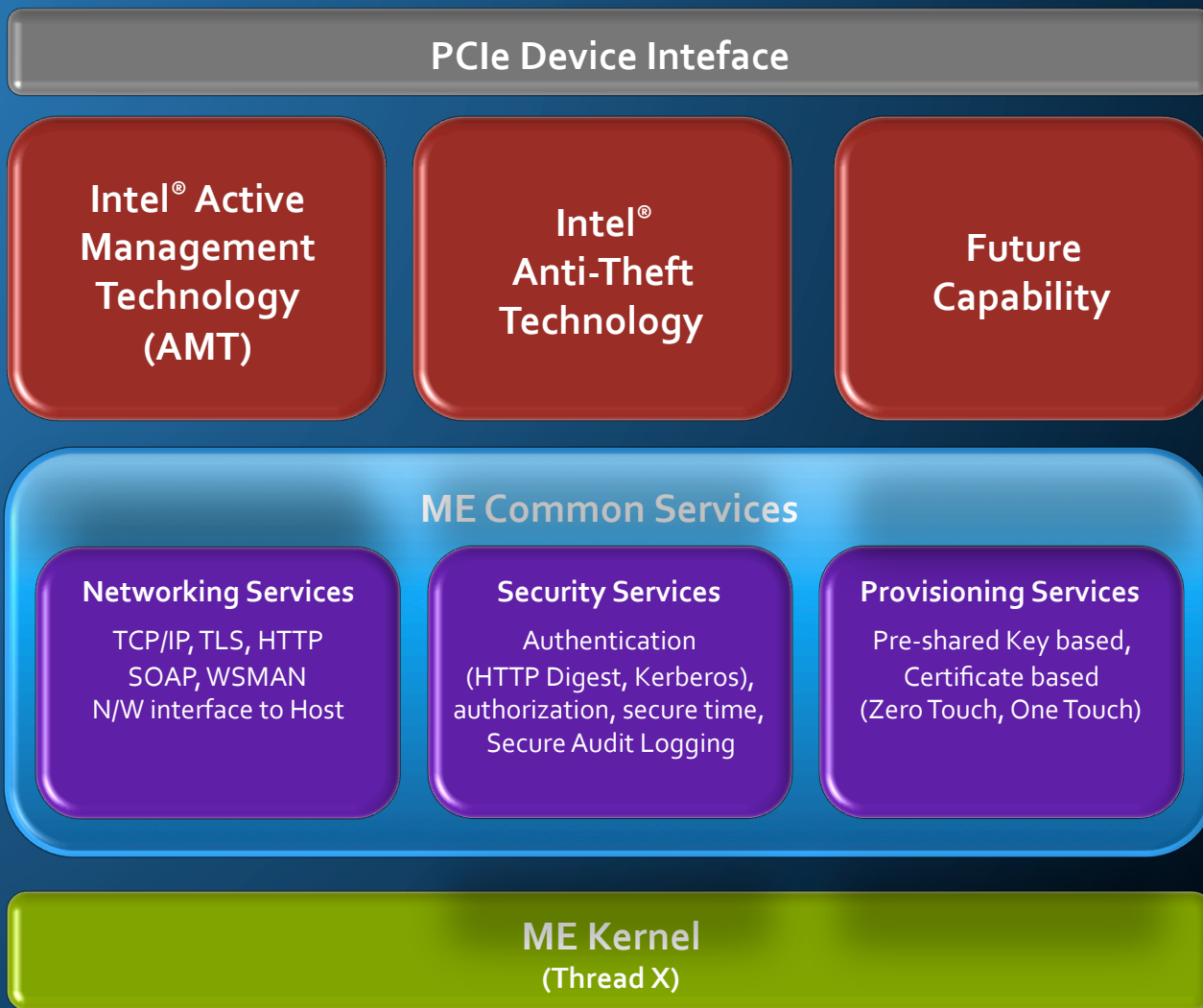
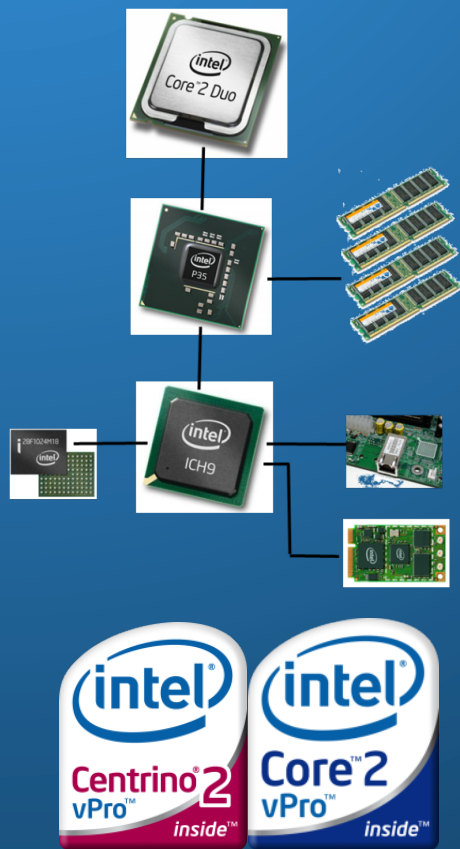
- MC obtains a Svc Ticket to access vPro platform
- Svc Ticket may contain AD PAC structure authorizing ME actions
- Svc Ticket used with WS-Man to establish a connection
- MC may wake platforms that are powered down
- ME maps PAC to ME-realms (more on ME realms later)
- Manageability action is performed using ME commands

vPro™ Hardware Architecture



- Management Engine (ME)
 - ARC4 micro-controller
 - Direct access to LAN / WLAN
- SPI Flash
 - ME code and data storage
- DDR Memory
 - ME partition hidden from CPU
- Virtualization Engine (VE)
 - ME signaling traffic

vPro™ Embedded Software Architecture



ME Realms

**ME Realm =
A Collection of ME
Commands**

**PET
Alerts**

KVM

**Anti-
Theft**

**Audit
Manage
ment**

**Wake on
Manage
ability**

Examples

- Up to 32 realms
- May contain any / all ME commands
- Realm definition performed at time of manufacture
- 3 types of user authentication are supported
 - Local (password), HTTP-digest or Kerberos

Allowing dynamic Realm definition has been considered

Challenges

- Authorization
 - Large PAC structure parsing can “run out of gas”
 - ME Realms must span different identity systems (e.g. HTTP-digest, local, AD etc...)
- Roaming / Remote Access
 - vPro™ server platform can roam where IP address changes frequently.
 - DNS updates don't propagate in real-time.
 - >45 min delay typical for large enterprise
 - Active Directory DNS update adds additional latency
 - VPN / firewall traversal solutions often don't support “inside-out” connections
- Client Authentication
 - vPro use cases also require user authentication (e.g. KVM, Anti-theft, and others)
 - Multi-factor integration (e.g. smartcards, biometrics, OTP and NFC)
 - Strength of function for authentication factors



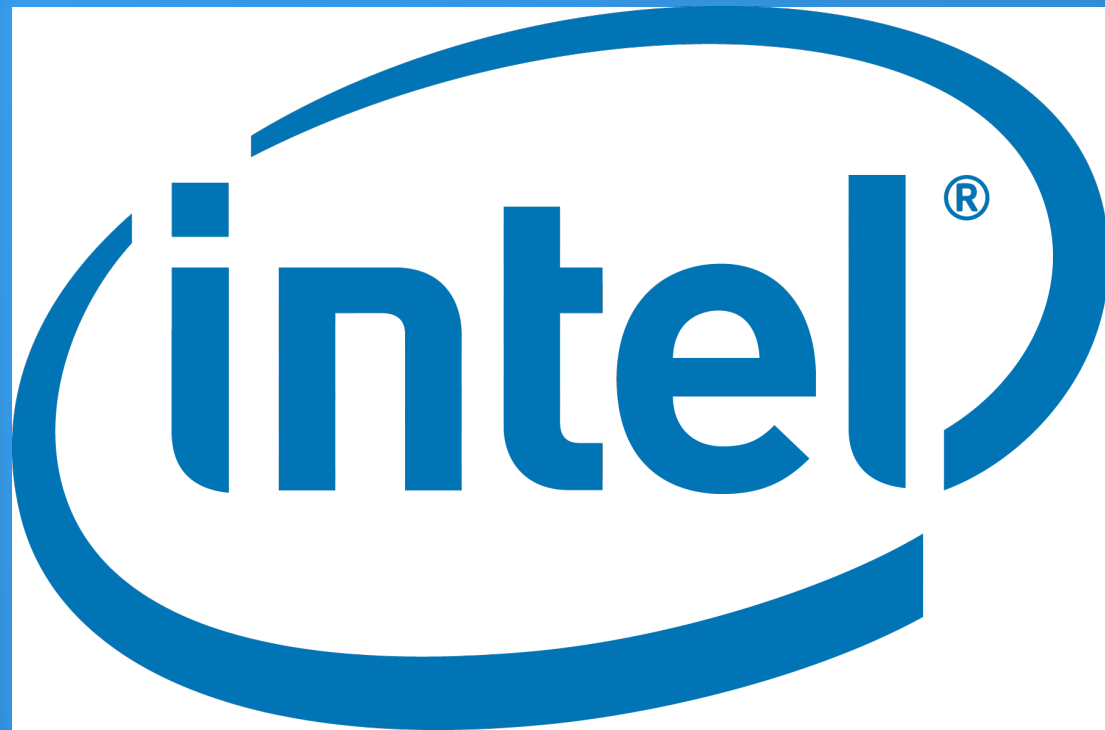
Possible Solutions

- Authorization
 - SAML assertions - Can it be implemented in constrained environments?
- DNS / Roaming kerberized servers
 - SIP – Will it work for Service Principal Names?
- Authentication
 - PKINIT – Will it work for OTP, NFC, and biometrics?



Conclusion

- Intel® vPro™ technology includes a Kerberos server
- Manageability usages appear to be compelling,
- But....
 - Heavy use of authorization / PAC can overwhelm “small” servers
 - DNS doesn’t scale appropriately for roaming servers
 - VPN and firewall traversal for “inside-out” connectivity is not easy
 - Authentication strength of function for human-computer interaction is missing



Pros and Cons



- SIP
 - Pros: Standards-based, scalable
 - Cons: SIP designed to track people not platforms – will it work
 - Not yet ubiquitous
 - Security concerns
- PKINIT
 - Pros: Allows multi-factor auth
 - Cons: Lacks proof of assurance
 - VPN / firewall traversal lacking

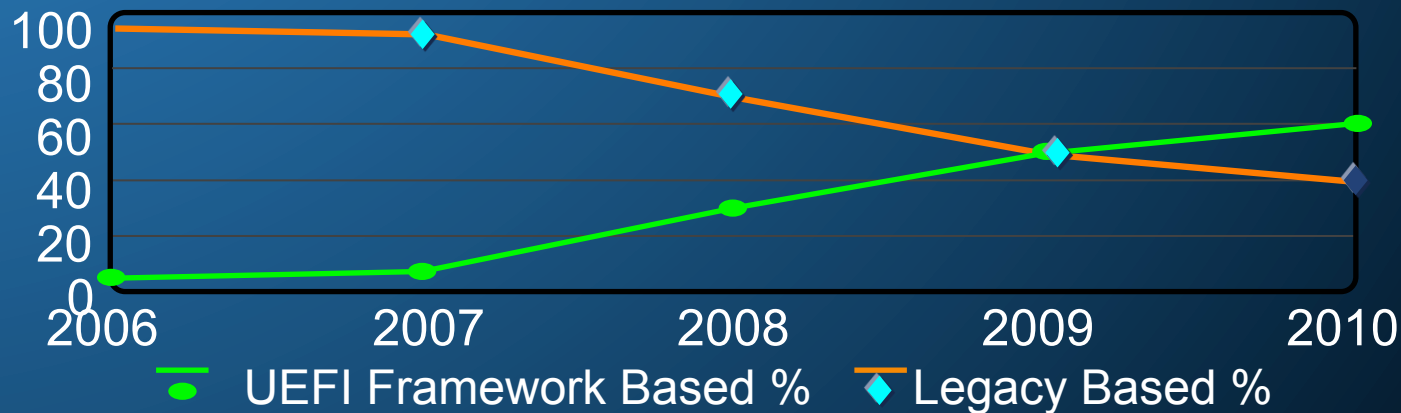
Interfaces like the Intel® Framework for EIF spur innovation

Intel® Platform Innovation Framework is Intel's implementation of EFI

Unified EFI forum promotes and manages specs (www.uefi.org) and brings standards to the system firmware

Dell, HP, IBM, Lenovo, AMI, Insyde, Phoenix; Intel, AMD, Apple, Microsoft

Intel contributed specifications to seed creation of UEFI 2.0 and Platform Initialization 1.0



Source: Various – IDC Sep'07 worldwide vendor market share; Intel customer platform adoption projection

