UEFI and Transparent Computing Technology

Wu Ming, Engineering Manager
Intel SSG/PSI Embedded Team
Liu Kehong (Steve), CTO
ASPire Digital

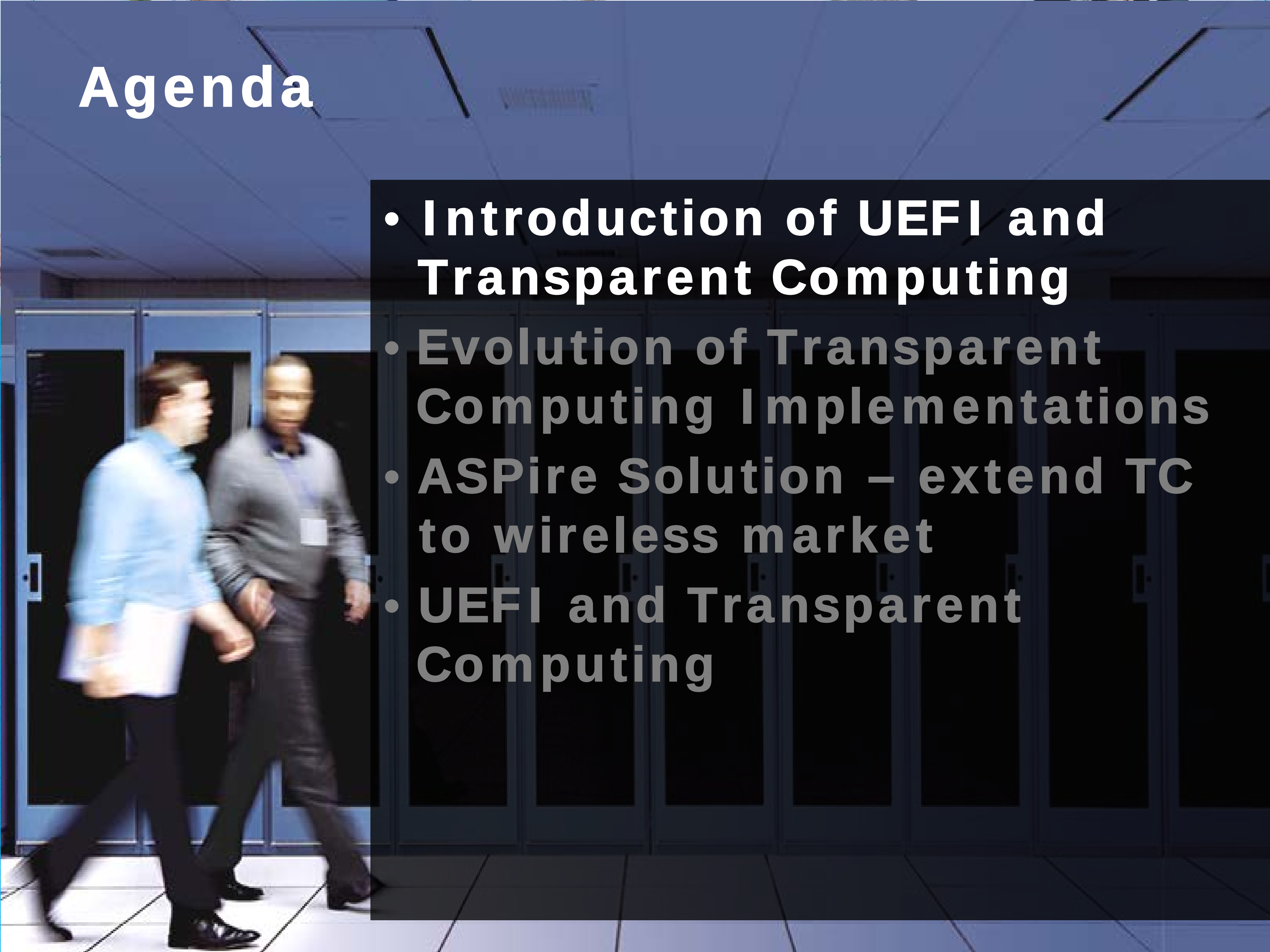
EFIS003

Sponsors of Tomorrow.™ intel

Agenda

- Introduction of UEFI and Transparent Computing
- Evolution of Transparent Computing Implementations
- ASPire Solution – extend TC to wireless market
- UEFI and Transparent Computing

Agenda



- Introduction of UEFI and Transparent Computing
- Evolution of Transparent Computing Implementations
- ASPire Solution – extend TC to wireless market
- UEFI and Transparent Computing

Industry BIOS Transition to UEFI

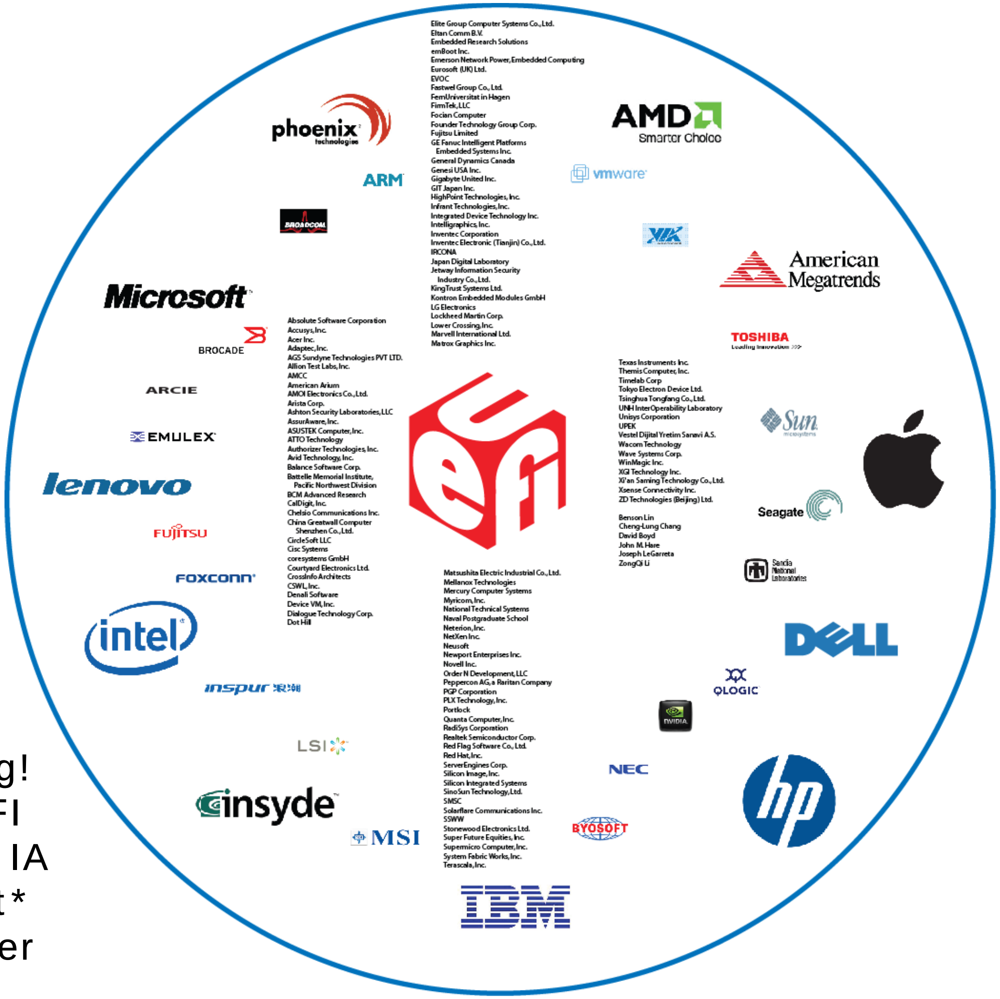
Pre-2000 All Platforms BIOS were proprietary

2000 Intel invented the Extensible Firmware Interface (EFI) and provided sample implementation under free BSD terms

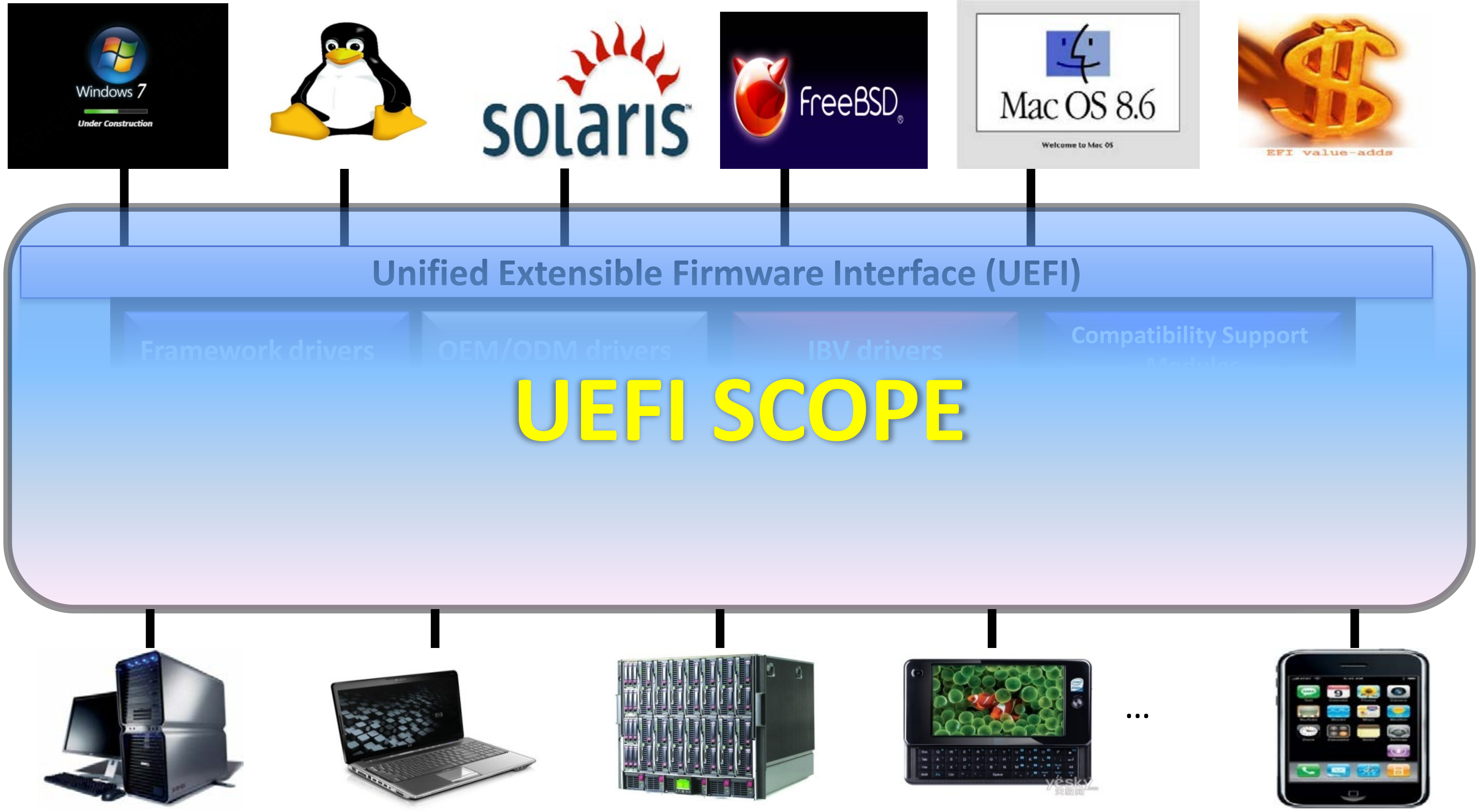
2004 **tianocore.org**, open source EFI community launched

2005 **Unified EFI (UEFI)** Industry forum, with 11 members, was formed to standardize EFI

2011 170 members and growing! Major MNCs shipping; UEFI platforms crossed 50% of IA worldwide units; Microsoft* UEFI x64 support in Server 2008, Vista* and Win7*; RedHat* and Novell* OS support



UEFI Abstracts HW Platforms



Unified Extensible Firmware Interface (UEFI)

Framework drivers

OEM/ODM drivers

IBV drivers

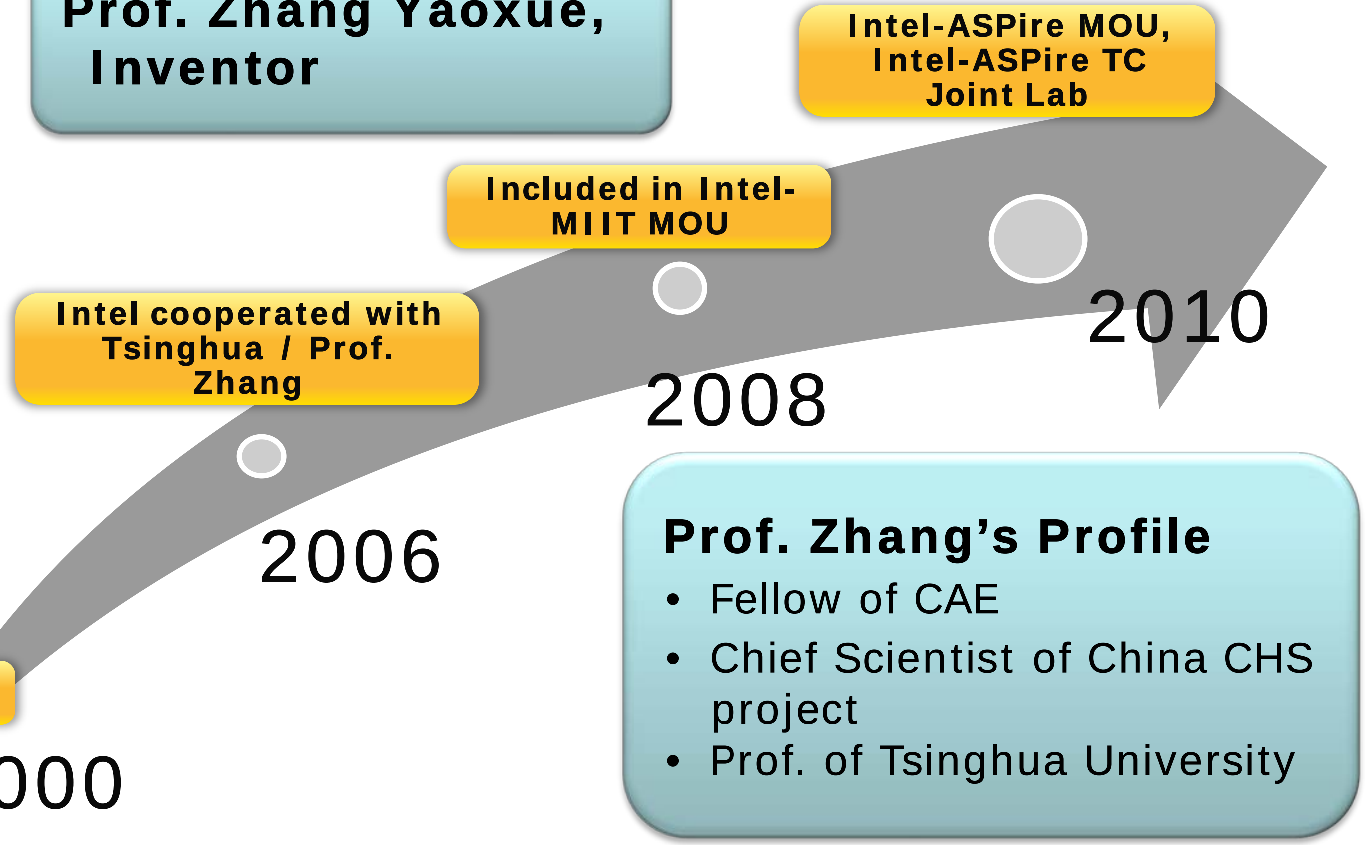
Compatibility Support Modules

UEFI SCOPE

…

Transparent Computing (TC) History

Prof. Zhang Yaoxue, Inventor



TC invented

2000

Intel cooperated with Tsinghua / Prof. Zhang

2006

Included in Intel-MIIT MOU

2008

Intel-ASPire MOU, Intel-ASPire TC Joint Lab

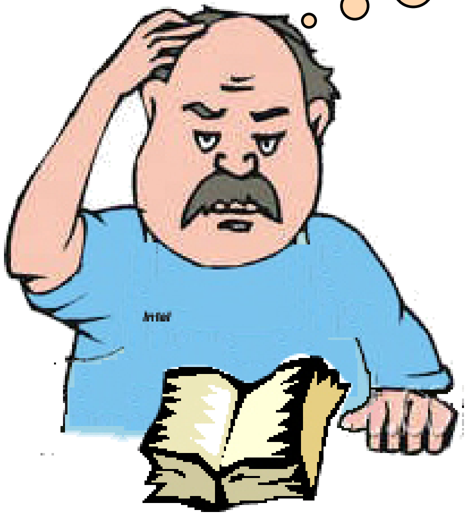
2010

Prof. Zhang's Profile

- Fellow of CAE
- Chief Scientist of China CHS project
- Prof. of Tsinghua University

Vision: Computing everywhere

TC Motivation



Question:
how to make
PC usage as
easy as TV?

TV

Turn on & watch
Only care for content
Easy for TV upgrade

PC

Format, OS installation, configure, application mgmt, virus scanning, backup
Do it again when upgrading a computer

Root-cause: Terminal too complex

Too many things in terminal which are not useful all the time

Vision of Future Computer

Turn on & use
End user: only care for content
Platform independent

Transparent Computing

Problems TC is trying to solve

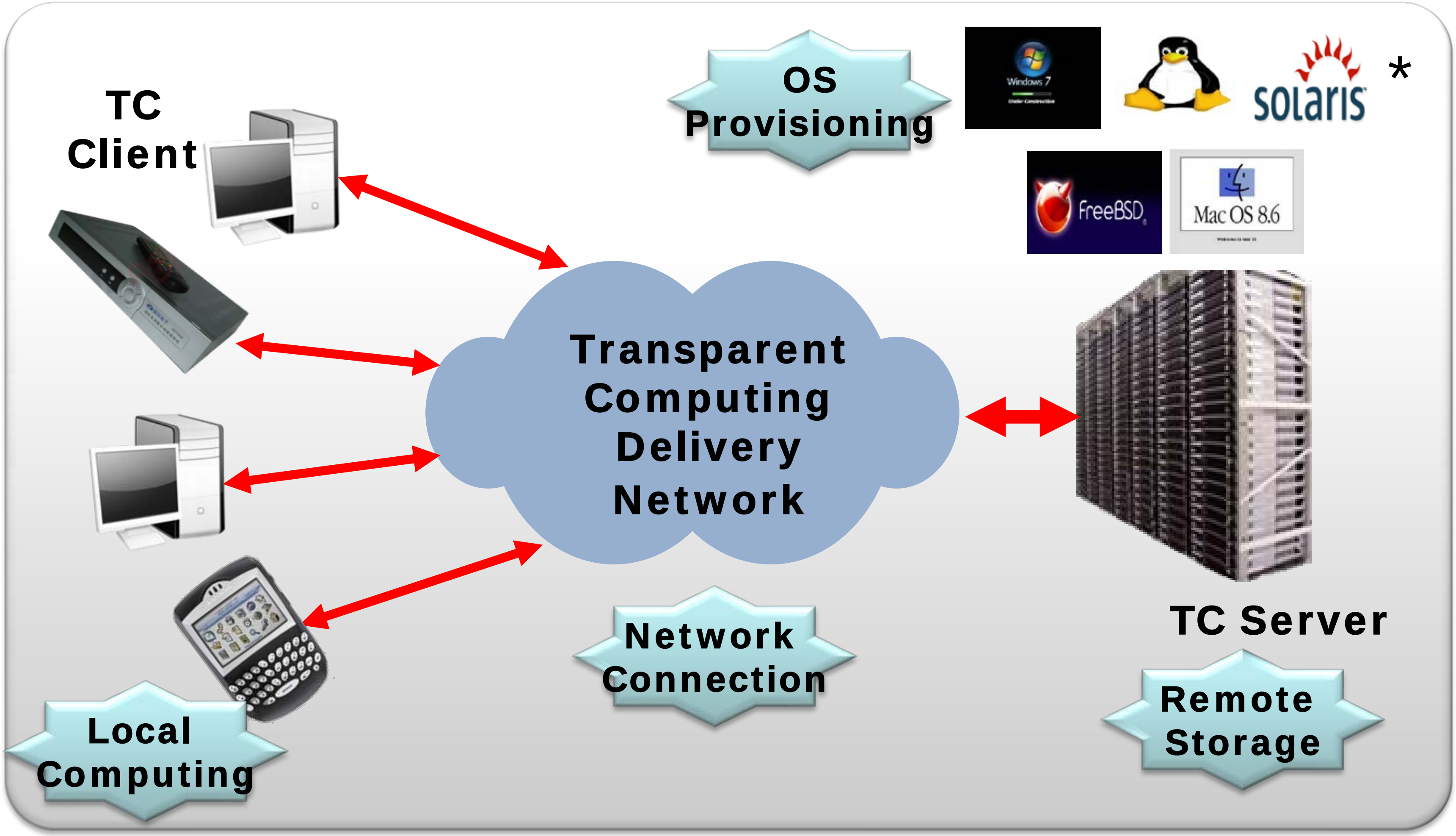
- Terminal runs more quickly
- Storage efficiency
- Security, manageability and low-cost
- Device-oriented to user-oriented
- A way to SaaS - Software as a Service

How to do it?

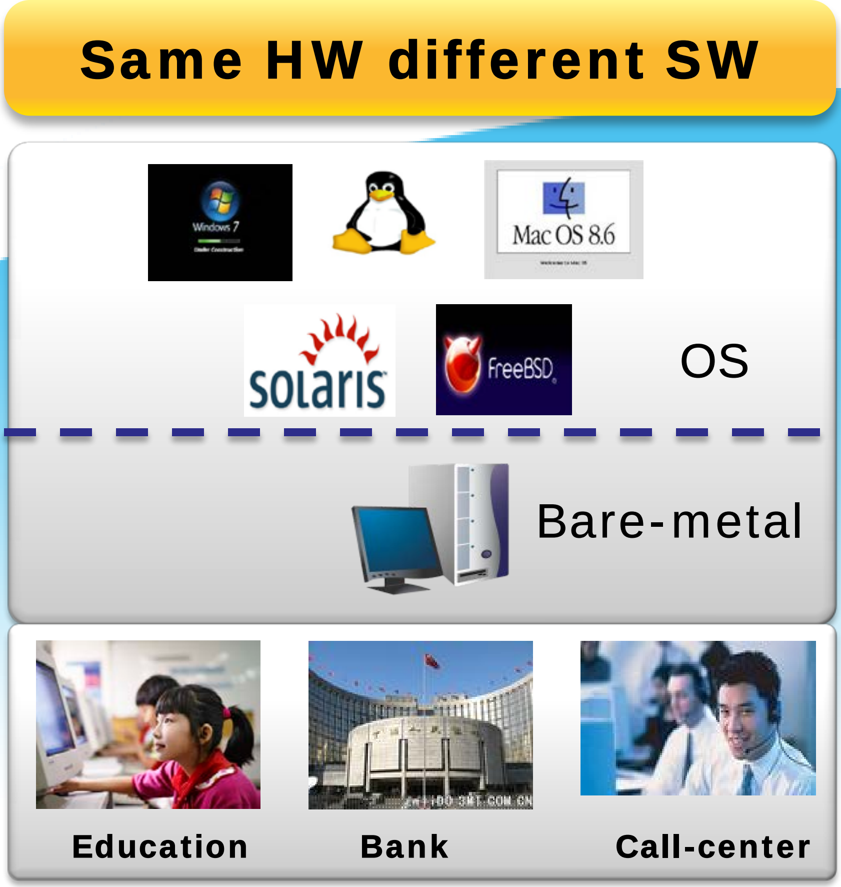
- Split SW and HW
- Split computing and storage
- Software as service, provision via network

Abstract disk I/O and redirect to network

Transparent Computing Concept



Usage Scenarios



Same HW different SW

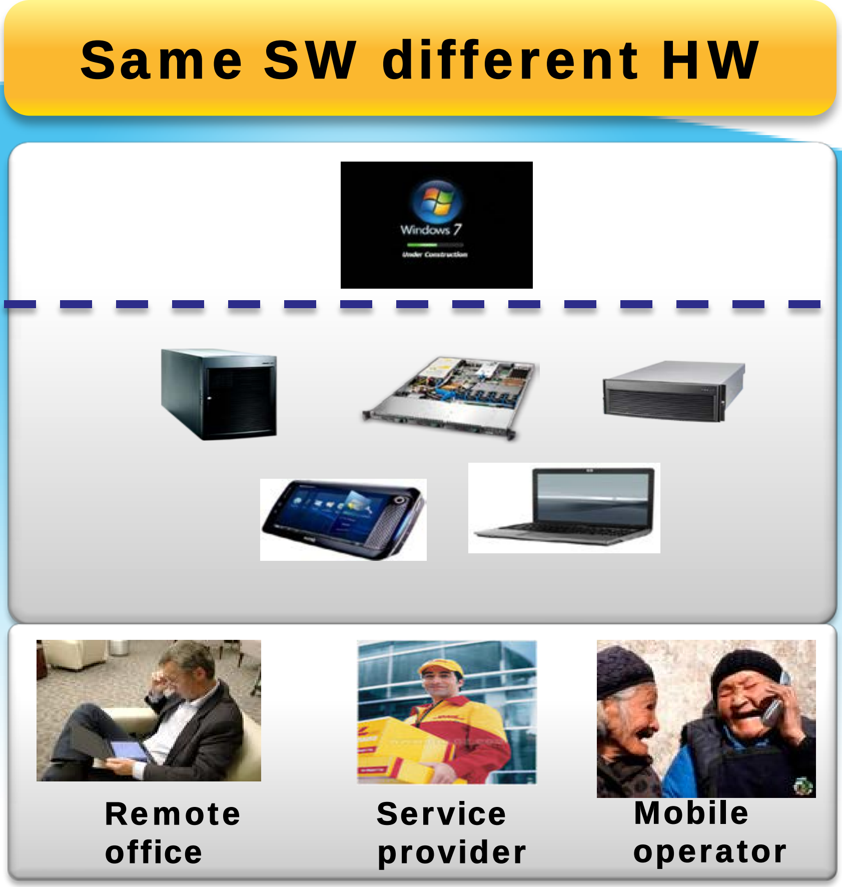
OS

Bare-metal

Education

Bank

Call-center



Same SW different HW

Remote office

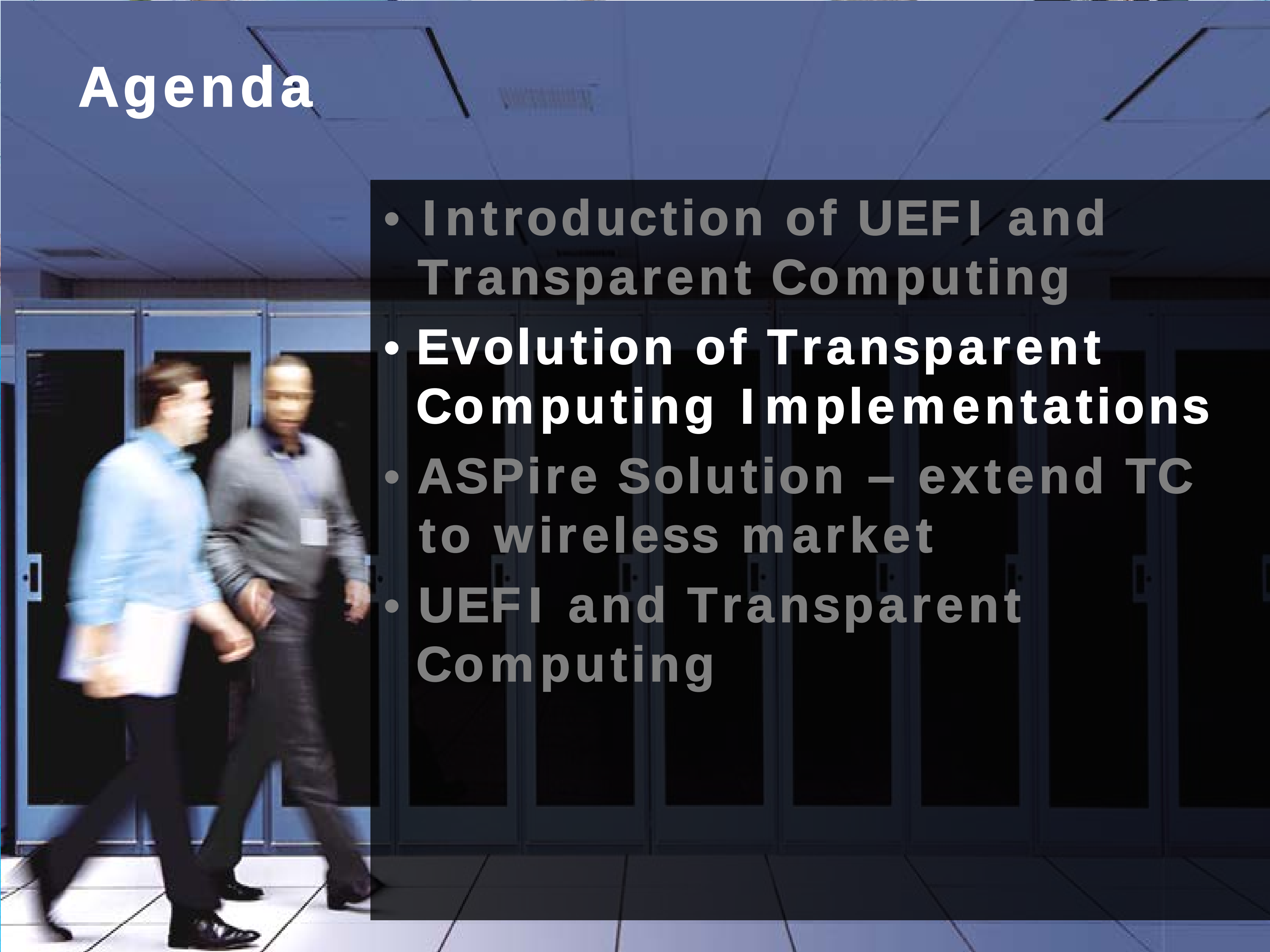
Service provider

Mobile operator

Logically separate HW and SW

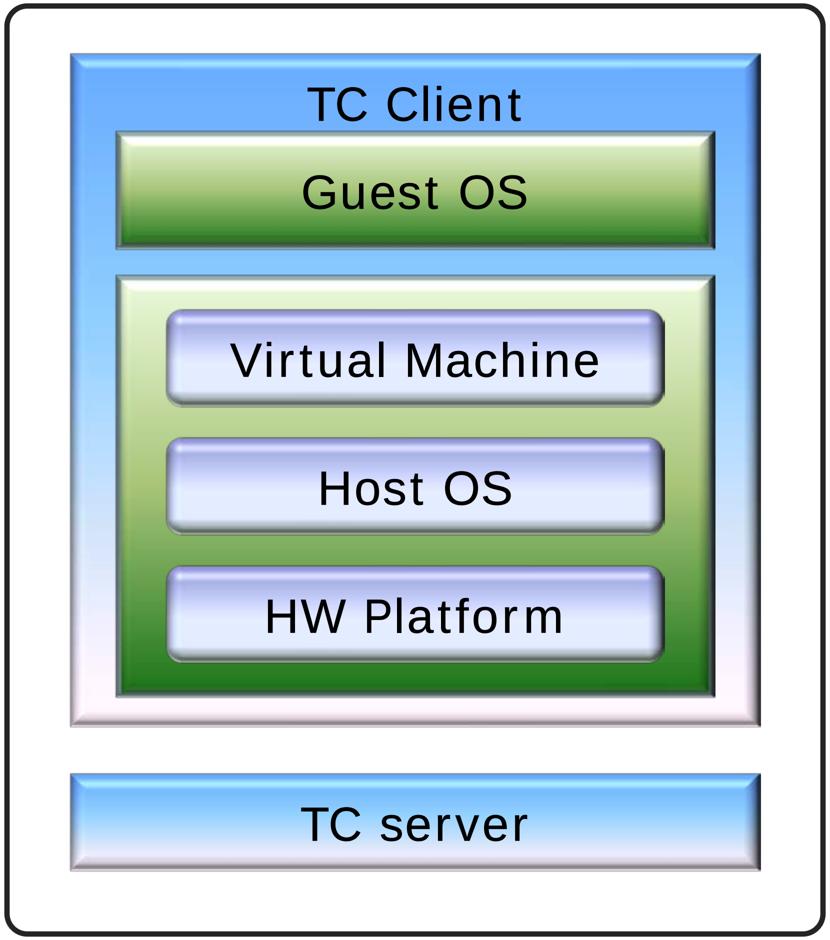
IDF2011
INTEL DEVELOPER FORUM

Agenda



- Introduction of UEFI and Transparent Computing
- Evolution of Transparent Computing Implementations
- ASPire Solution – extend TC to wireless market
- UEFI and Transparent Computing

Evolution of Transparent Computing Technology – Full Virtualization



TC Client

Guest OS

Virtual Machine

Host OS

HW Platform

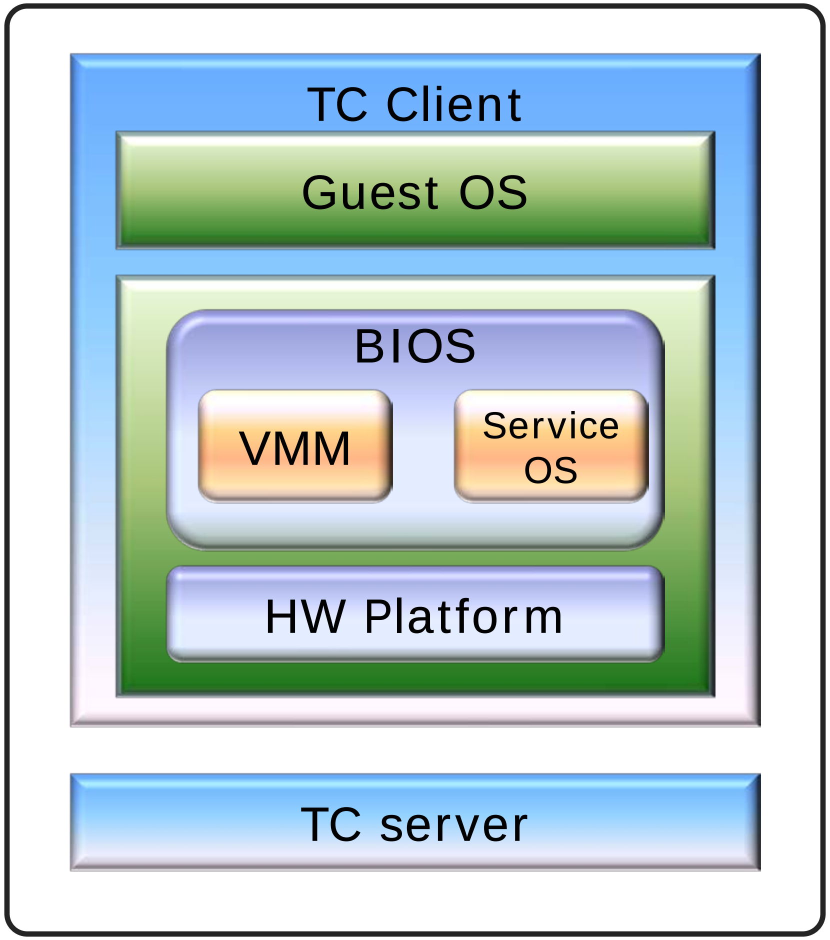
TC server

Key Points

- Guest OS runs on virtual machine
- Embed a network based Linux* in BIOS as Service OS
- Run VMM on Linux

Pros	Cons
HW independent OS Neutral 100% transparent	Performance impact

Evolution of Transparent Computing Technology – Para-virtualization

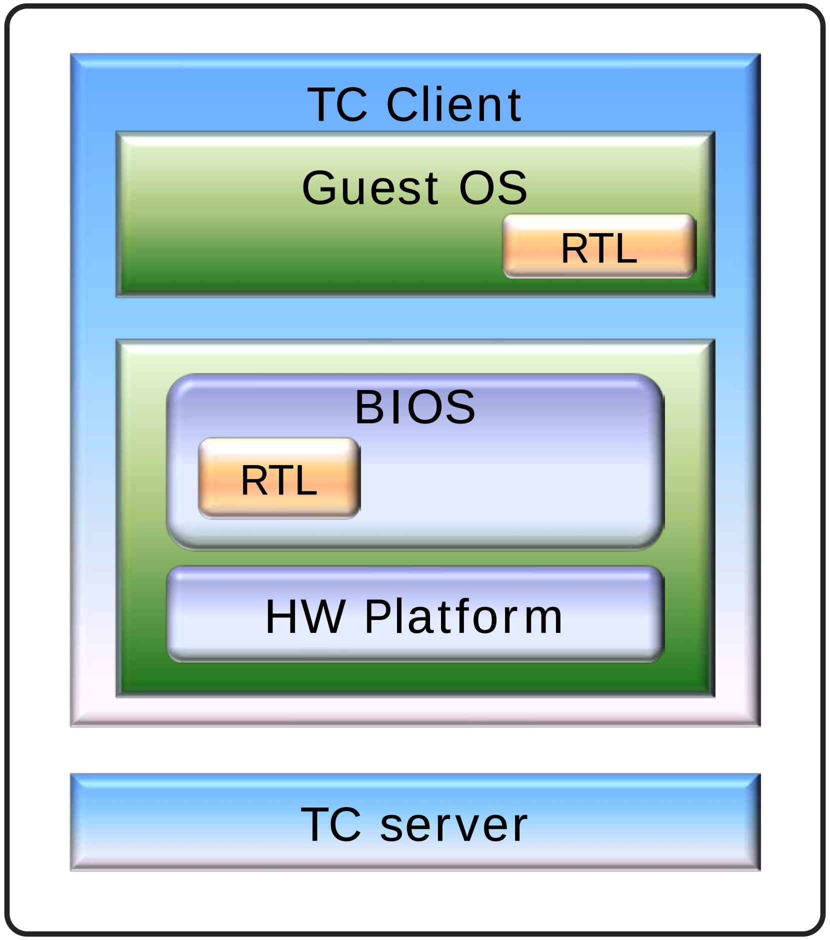


Key Points

- VMM hooks IDE and NIC and get block IO handled by Service OS
- Service OS forward block IO to network
- Other device IO handled by HW

Pros	Cons
Performance Improvement Flexible transparent OS untouched	Depend on CPU feature (VT)

Evolution of Transparent Computing Technology – Non-VT



Key Points

- Translate boot-loader disk IO at BIOS
- Translate run-time disk IO at OS
- Forward BIOS and OS disk IO to network

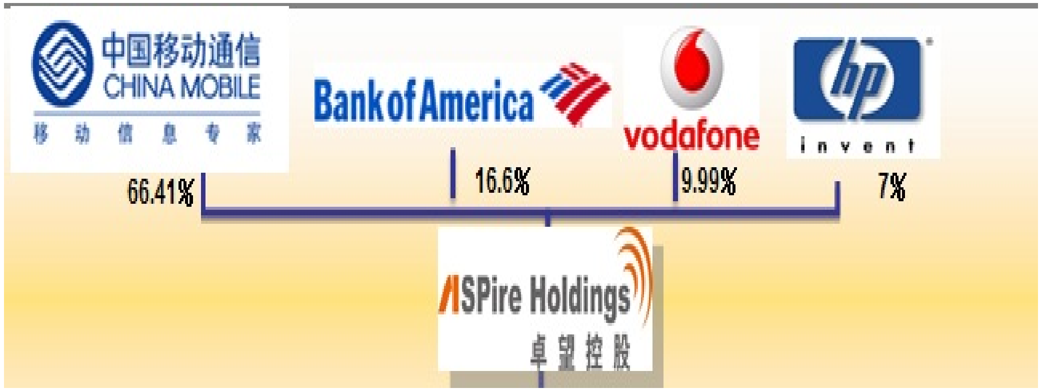
Pros	Cons
Good performance HW independent	OS porting effort

RTL: Resource Translation Layer

Agenda

- Introduction of UEFI and Transparent Computing
- Evolution of Transparent Computing Implementations
- **ASPire Solution – extend TC to wireless market**
- UEFI and Transparent Computing

ASPire Introduction



- Established in 2000
- 3000 Employees
- Provide data service, internet service development and operation for China Mobile, Singtel, Starhub, Telstra and HK Peoples.
- National High-tech Company
- National Key Software Company

ASPire / CMCC Project Requirements

Portable wireless terminal

Perf/power ratio
Generic phone feature

Software as a Service

Operator to provide additional service via SW provision
System patch like securities

中国移动通信
CHINA MOBILE

CMCC typical applications

PINM
HD video shoot and send
Video conference

Vertical market considerations

Support Windows OS
Easy for 3rd-ISV's development

Problems Mobile Computing is Facing

Mobile Computing Problems
Especially for mass-market (600M+ subscribers)

- Virus threat to mobile device
- Malware risk
- Higher-price device not good for mass market
- Valuable data lose when device lost
- Difficult to upgrade
- Application conflict
- Network traffic disaster

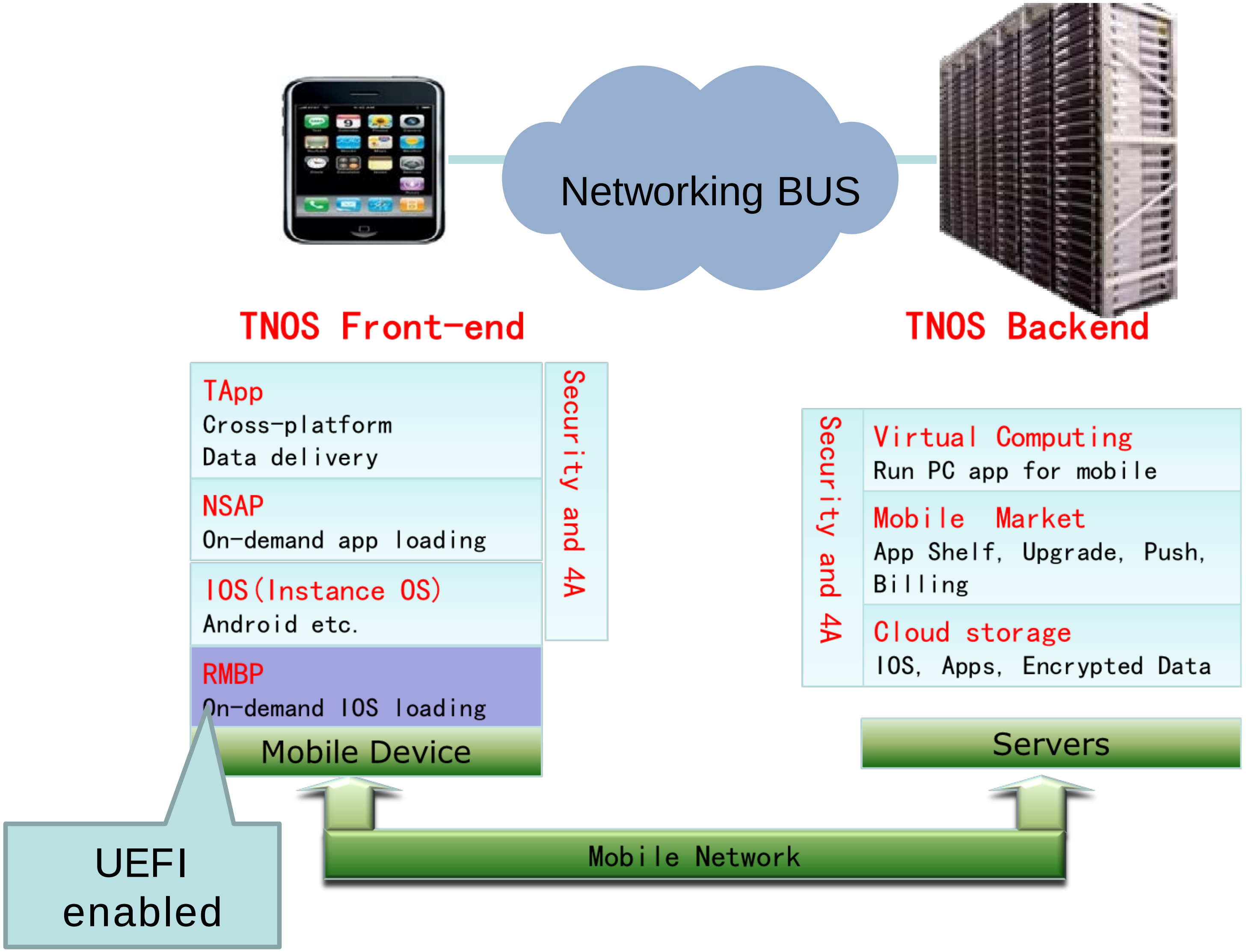
Available solutions

Current solutions do not solve problems well enough

- User-end anti-virus software
- Cloud based anti-virus service
- Cloud backup
- Paid repair/restore service
- Consulting professional

Any other solutions?

ASPire’s TC-Powered Mobile Device



Networking BUS

TNOS Front-end

TApp
Cross-platform
Data delivery

NSAP
On-demand app loading

IOS(Instance OS)
Android etc.

RMBP
On-demand IOS loading

Mobile Device

Security and 4A

TNOS Backend

Security and 4A

Virtual Computing
Run PC app for mobile

Mobile Market
App Shelf, Upgrade, Push, Billing

Cloud storage
IOS, Apps, Encrypted Data

Servers

Mobile Network

UEFI enabled

What is trans-parented (and How)

Assets	Front-end	Back-end
Instance OS	Dispatched Loaded Running Cached Check integrity	Stored Managed Maintained
Applications	Dispatched Loaded Running Cached Check integrity	Stored Managed Upgraded
User data	Generated Displayed Cached	Stored Encrypted

Transparent Data Storage Example

Take a photo and backup on server

Before

```
Capture();
fwrite(“C:\temp\picture.jpg”);
new soket to server;
Write to socket;
Close soket;
```

After

```
Capture();
fwrite(“C:\temp\picture.jpg”);
```

C: is transparently mapped to back-end storage

Benefit for Mobile Operator

- Managed OS
  - Secured
  - Invulnerable
- Device Defeat Controlled
  - Application Central Managed
  - Automatic upgrading
  - Risk application rejected.
- High Performance Network
  - Garbage traffic prohibited

Challenges and Solutions

Wireless

Limited bandwidth
Low reliability

→

- Local cache
- Virtual disk image

Manageability

Device-oriented to user-oriented

→

- BIOS–level boot image authentication
- BIOS-level user management

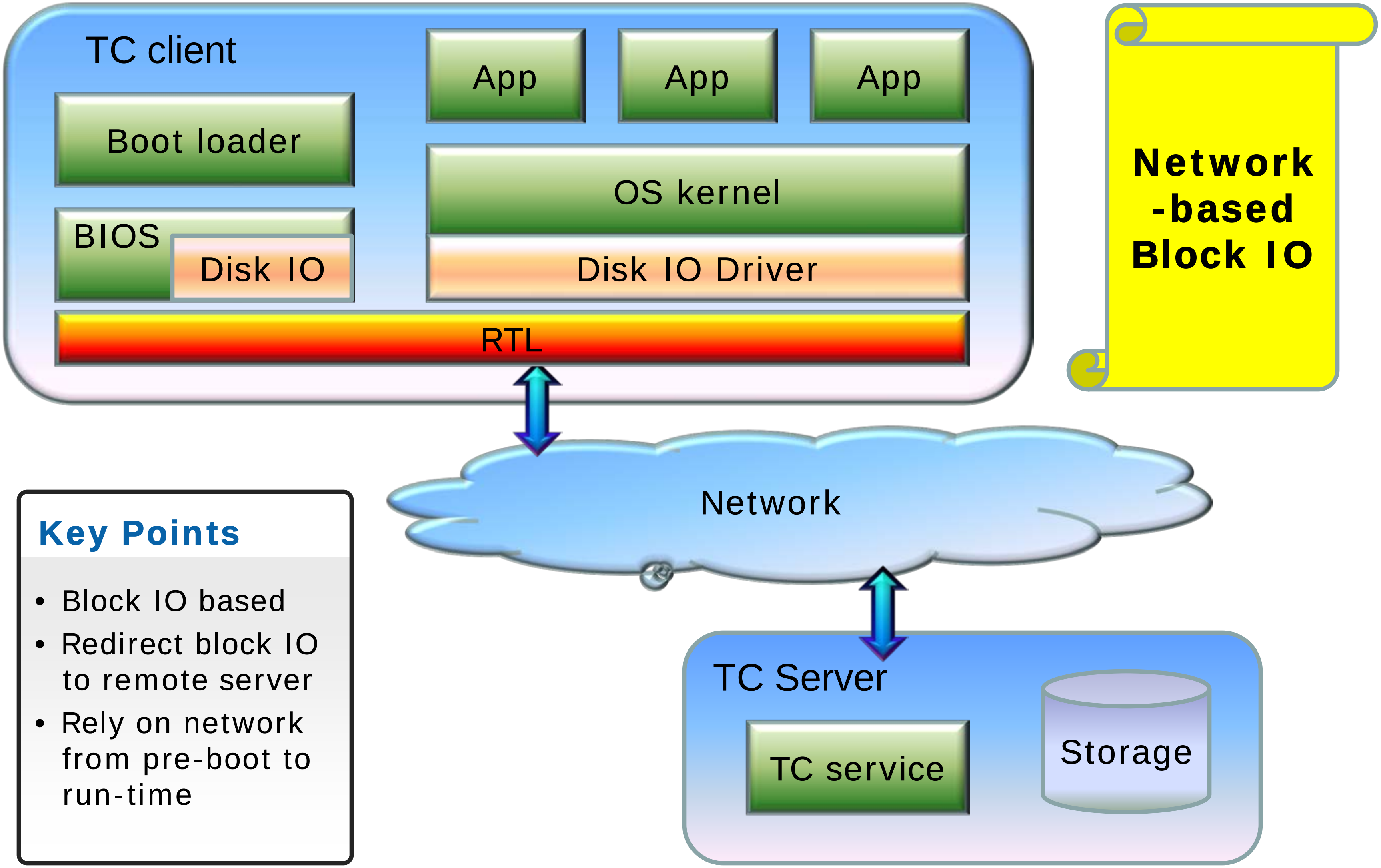
OS neutral

Multiple OS support
Close-source OS

→

- Block level disk IO
- Not dependent on a certain file system

Review of Non-VT Solution - Architecture

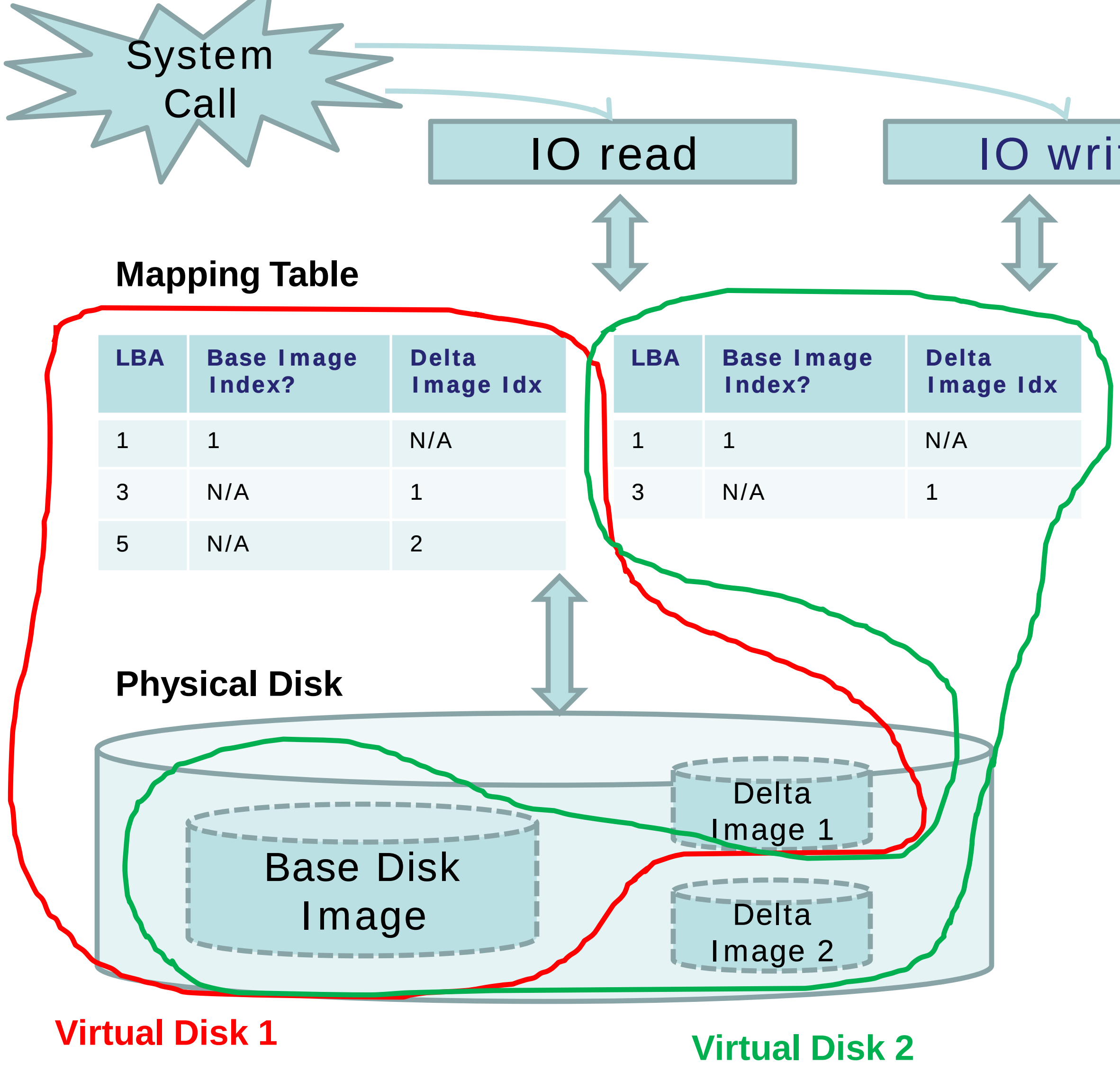


Network -based Block IO

Key Points

- Block IO based
- Redirect block IO to remote server
- Rely on network from pre-boot to run-time

Review of Non-VT Solution - Virtual Disk Management



LBA	Base Image Index?	Delta Image Idx
1	1	N/A
3	N/A	1
5	N/A	2

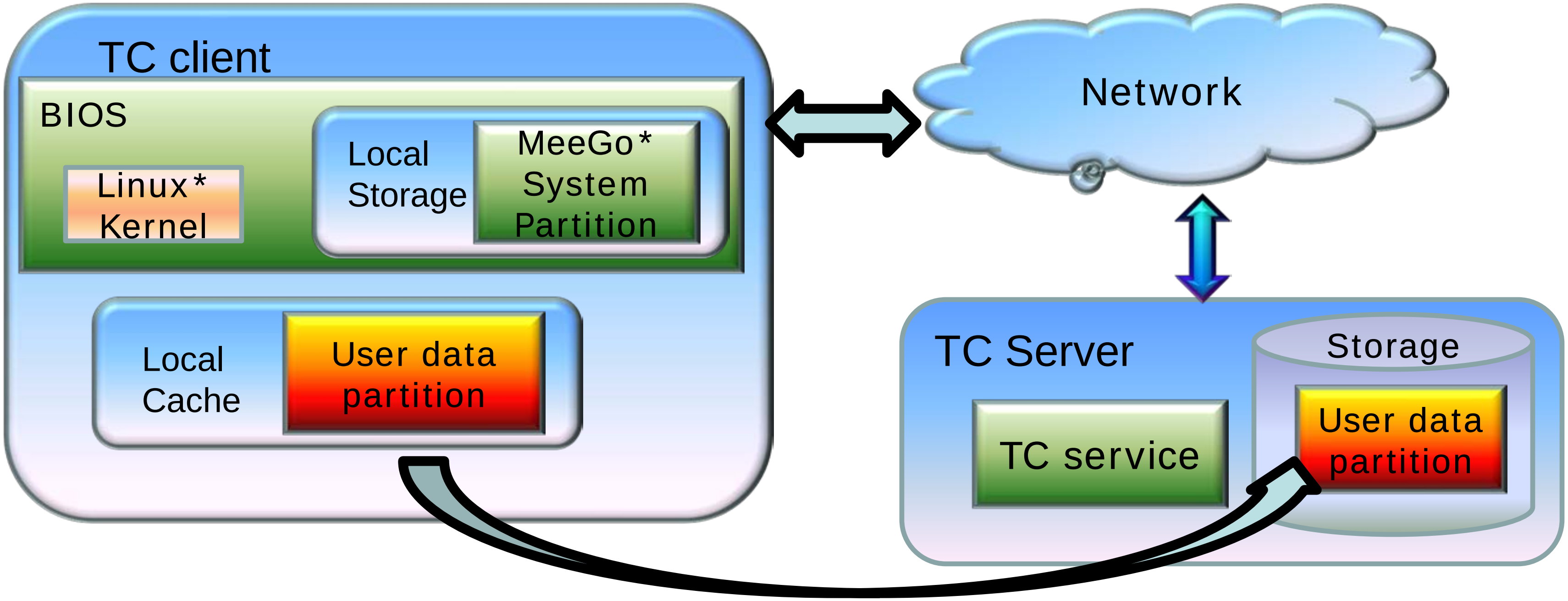
LBA	Base Image Index?	Delta Image Idx
1	1	N/A
3	N/A	1

Virtual Disk Management

Key Points

- Virtual Disk Image = mapping table + base + delta(s)
- Share base for different virtual disk images
- Delta file: software as a service
- Mapping table + delta: a way to track the disk changes

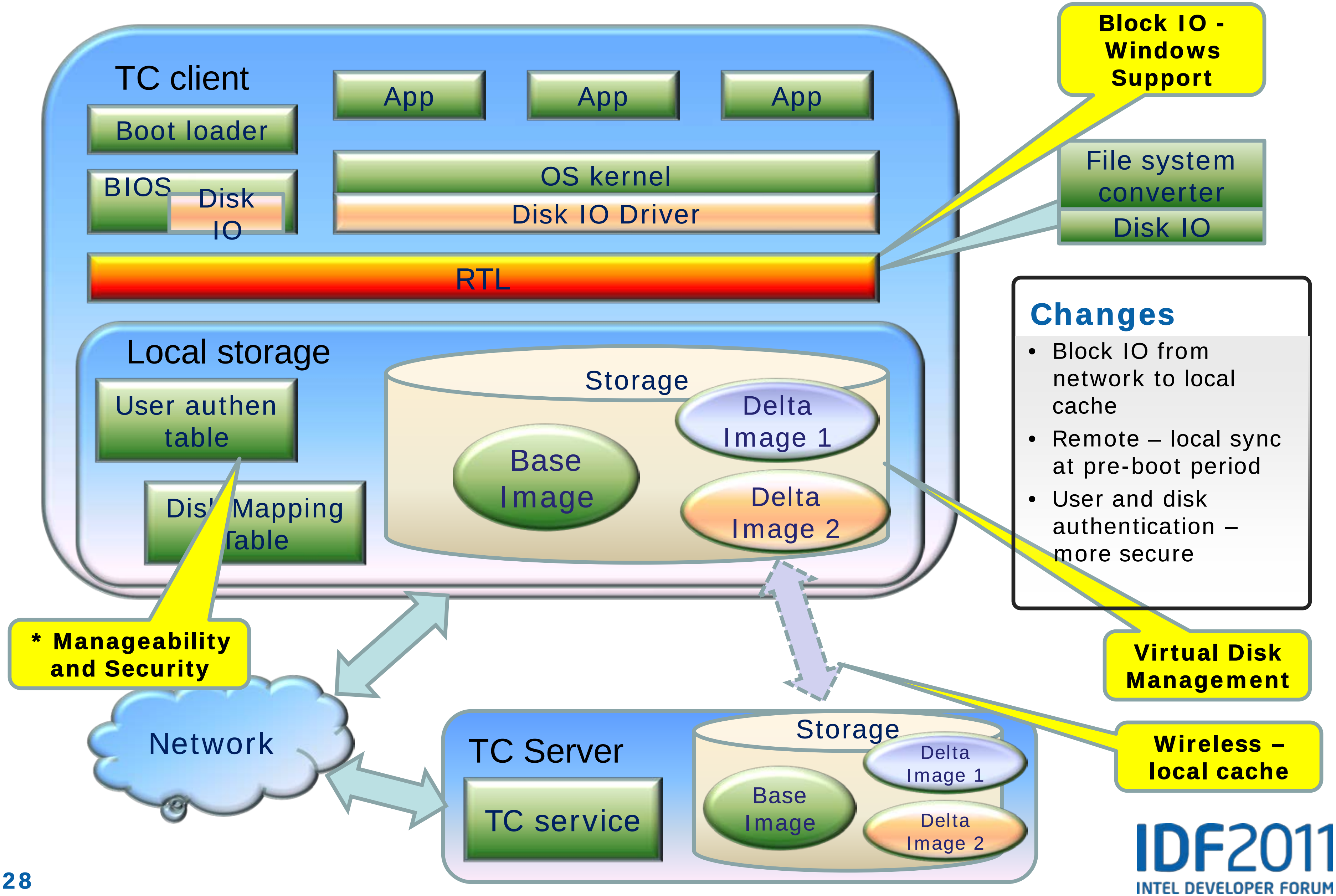
Linux*–based ASPire Solution Review



- Embedded small Linux system into BIOS
- File-system based cache-updating
- Only update user data partition (system partition not changed)

Local Cache

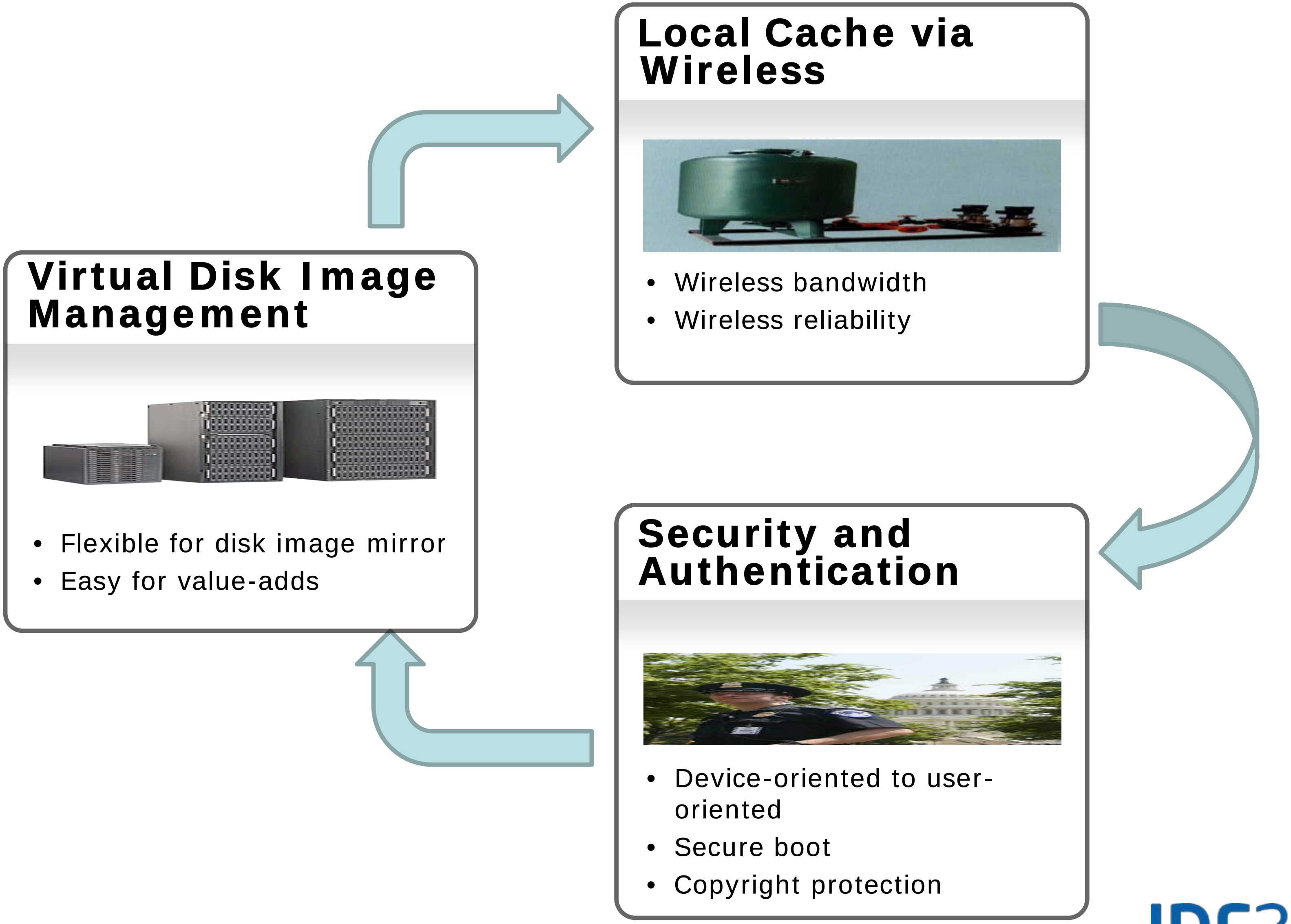
OS-neutral ASPire Solution



Changes

- Block IO from network to local cache
- Remote – local sync at pre-boot period
- User and disk authentication – more secure

UEFI's Benefits to ASPire Solution



Virtual Disk Image Management

- Flexible for disk image mirror
- Easy for value-adds

Local Cache via Wireless

- Wireless bandwidth
- Wireless reliability

Security and Authentication

- Device-oriented to user-oriented
- Secure boot
- Copyright protection

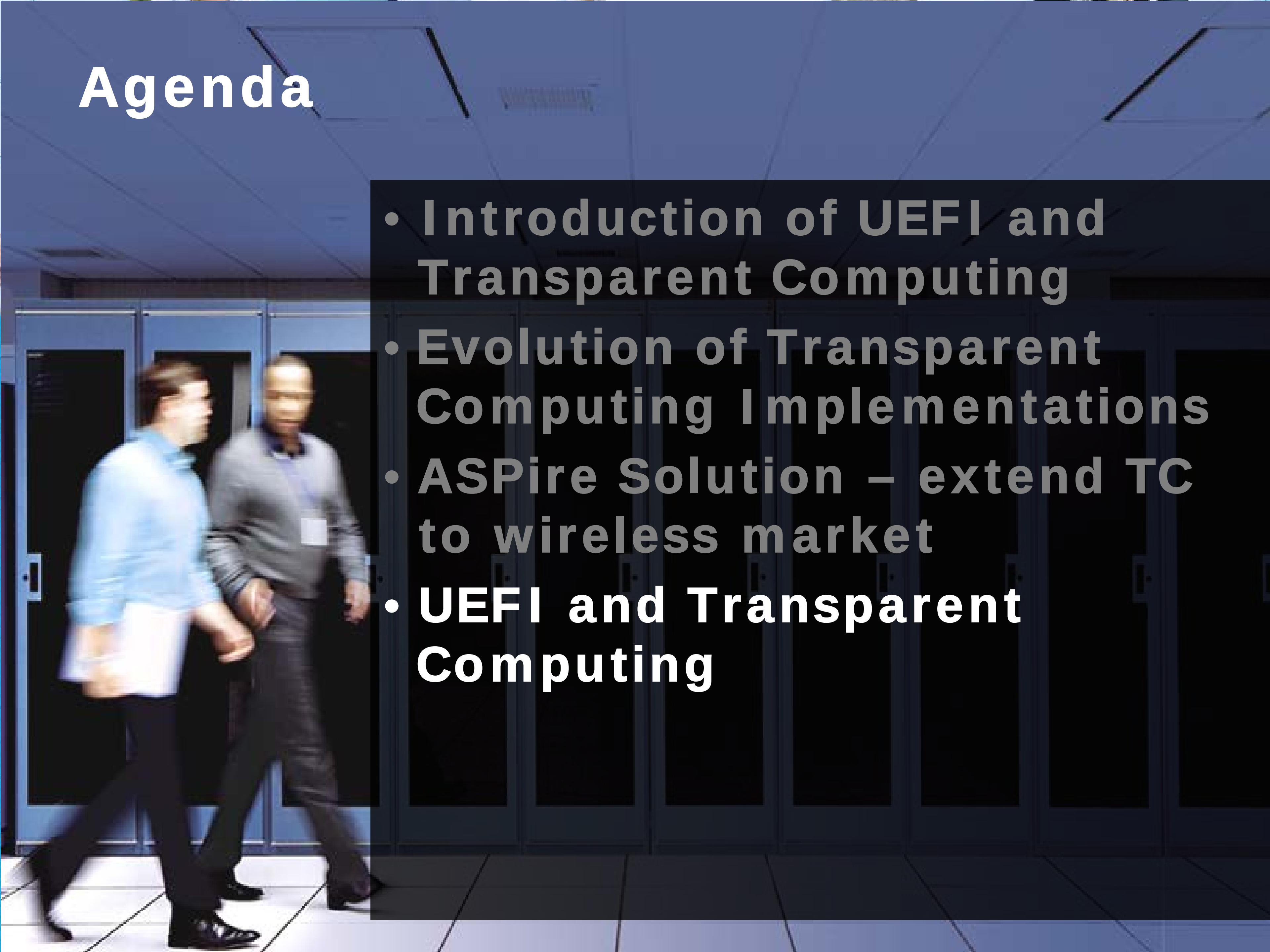
Demonstration

- Linux*/MeeGo* in Transparent Computing
  - Three typical CMCC/ASPire usage scenario
  - MeeGo/TC support
- Windows* in Transparent Computing
  - BIOS-level value-add for TC

Future Challenges

- Storage management
  - Auto selection between network block IO and disk block IO
- Securities
  - User authentication
  - Disk image secure boot
  - Anti-pirate by SaaS
- Manageability
  - Better manageability for mobile operator
  - Scalable to different market – vertical market

Agenda



- Introduction of UEFI and Transparent Computing
- Evolution of Transparent Computing Implementations
- ASPire Solution – extend TC to wireless market
- **UEFI and Transparent Computing**

Summary

- Transparent Computing – separate HW and SW and lead the way to SaaS
- ASPire solution – wireless, OS neutral, from device-oriented to user-oriented
- UEFI and Transparent Computing – embed modules at BIOS, more secure, more flexible
- Innovation with UEFI

Additional resources on UEFI:

- Other UEFI Sessions – Next slide
- More web based info:
  - Specifications sites www.uefi.org, www.intel.com/technology/efi
  - EDK II Open Source Implementation: www.tianocore.org

- Technical book from Intel Press: "Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel's Framework" www.intel.com/intelpress

EFI Track Sessions

Session ID	Title	Day/ Time	Room
EFIS001 ✓	Microsoft* Windows* Platform Evolution and UEFI	Tuesday 11:10	306A
EFIS002 ✓	UEFI Development and Innovations for System-On-Chip (SoC)	Tuesday 14:05	306A
EFIS003 ✓	UEFI and Transparent Computing Technology	Tuesday 15:10	306A
EFIS004	Intel® UEFI Development Kit 2010 and Intel® Boot Loader Development Kit: Foundations for Advanced Embedded Development	Tuesday 16:10	306A
SPCQ001	Hot Topic Q&A: Intel® Boot Loader Development Kit (Intel® BLDK)	Tuesday 17:00	306A
EFIS005	Security and Networking Advancements Today's UEFI and Intel® UEFI Development Kit 2010 (Intel® UDK2010)	Wednesday 11:10	306A

✓ = DONE

Session Presentations - PDFs

The PDF for this Session presentation is available from our IDF Content Catalog at the end of the day at:

intel.com/go/idfsessionsBJ

URL is on top of Session Agenda Pages in Pocket Guide

Please Fill out the Session Evaluation Form

Give the completed form to the room monitors as you exit!

Thank You for your input, we use it to improve future Intel Developer Forum events

Q&A

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 PROPETY 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 may make changes to specifications and product descriptions at any time, without notice.
- All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
- Intel, processors, chipsets, and desktop boards 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.
- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.
- Intel, Sponsors of Tomorrow. and the Intel logo are trademarks of Intel Corporation in the United States and other countries.
- *Other names and brands may be claimed as the property of others.
-

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the first quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Many factors could affect Intel’s actual results, and variances from Intel’s current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be the important factors that could cause actual results to differ materially from the corporation’s expectations. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; customer acceptance of Intel’s and competitors’ products; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast. Revenue and the gross margin percentage are affected by the timing of Intel product introductions and the demand for and market acceptance of Intel's products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel’s response to such actions; and Intel’s ability to respond quickly to technological developments and to incorporate new features into its products. The gross margin percentage could vary significantly from expectations based on capacity utilization; variations in inventory valuation, including variations related to the timing of qualifying products for sale; changes in revenue levels; product mix and pricing; the timing and execution of the manufacturing ramp and associated costs; start-up costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; product manufacturing quality/yields; and impairments of long-lived assets, including manufacturing, assembly/test and intangible assets. Expenses, particularly certain marketing and compensation expenses, as well as restructuring and asset impairment charges, vary depending on the level of demand for Intel's products and the level of revenue and profits. The majority of Intel’s non-marketable equity investment portfolio balance is concentrated in companies in the flash memory market segment, and declines in this market segment or changes in management’s plans with respect to Intel’s investments in this market segment could result in significant impairment charges, impacting restructuring charges as well as gains/losses on equity investments and interest and other. Intel's results could be impacted by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Intel’s results could be affected by the timing of closing of acquisitions and divestitures. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust and other issues, such as the litigation and regulatory matters described in Intel's SEC reports. An unfavorable ruling could include monetary damages or an injunction prohibiting us from manufacturing or selling one or more products, precluding particular business practices, impacting Intel’s ability to design its products, or requiring other remedies such as compulsory licensing of intellectual property. A detailed discussion of these and other factors that could affect Intel’s results is included in Intel’s SEC filings, including the report on Form 10-Q for the quarter ended September 25, 2010.

Rev. 1/13/11