MIRKO COLEMBERG

CONSULTANT/ MCT

COLEMBERG.CH GMBH

MIRKO@COLEMBERG.CH @MIRKOCOLEMBERG

BLOG.COLEMBERG.CH / CONFIGMGR.CH

UEFI / Bios was denn das?

Secunia
Stay Secure

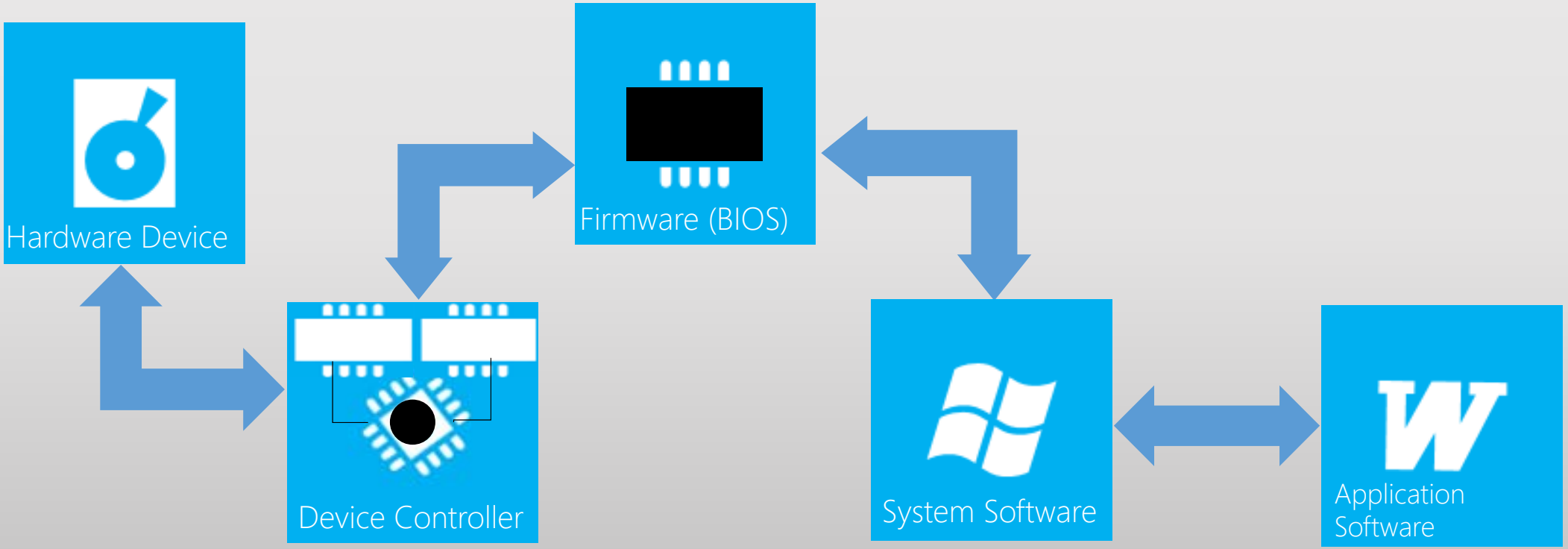
BCD SINTRAG
value add distribution

Configuration Manager

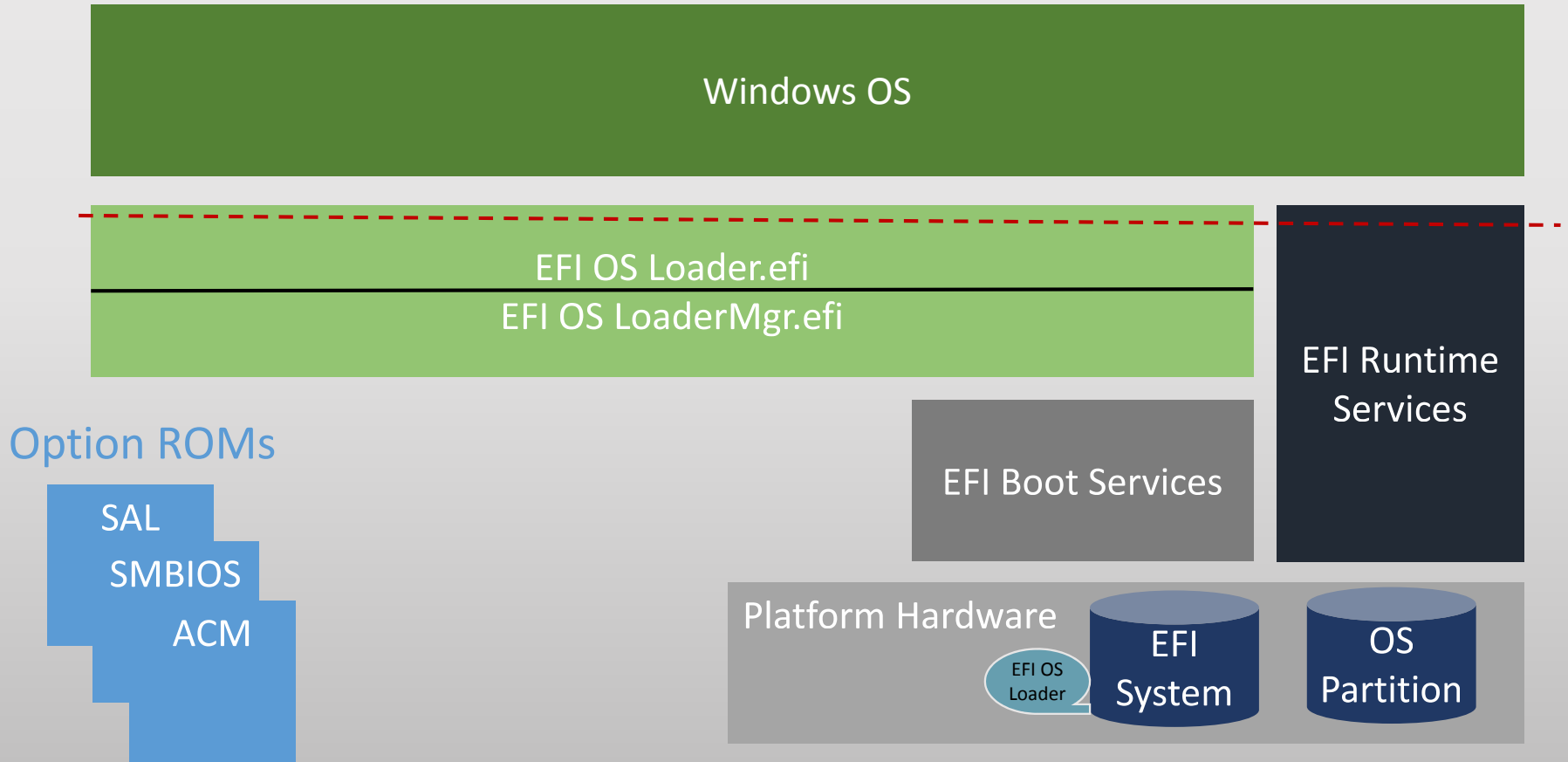
Reasons to Replace the BIOS

2.2 TB Drive Limit	16-bit Real Mode	Lack of networking support (IPv6)
Limited Option ROM Space	Aging GUI	OEM x64 Standardization

BIOS Middle Layer



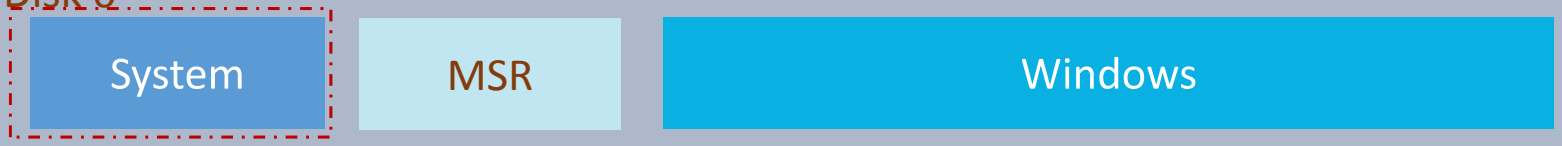
UEFI Architecture



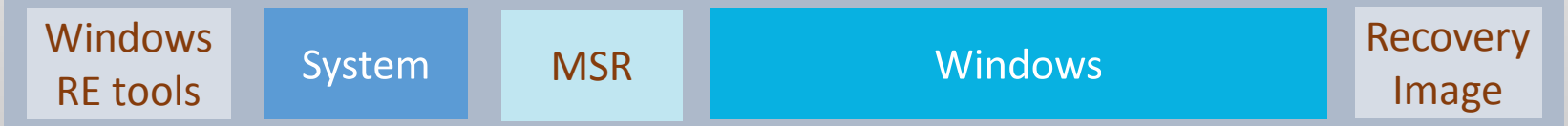
UEFI Partitions

(EFI) FAT32 500MB	(MSR)128MB	Windows (Primary) NTFS 100% of the rest	Windows (Recovery) 500MB NTFS

Default UEFI/GPT drive partitions
Disk 0

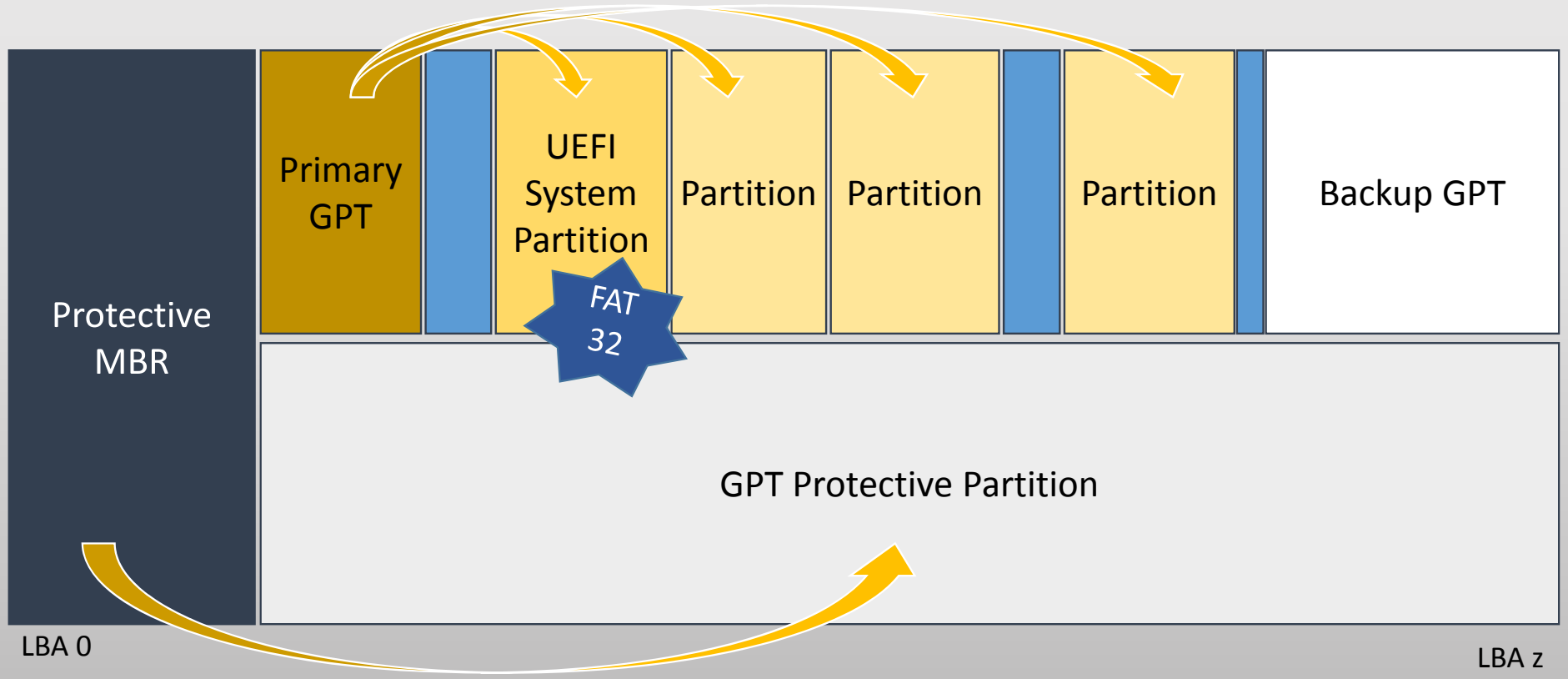


Recommended UEFI/GPT drive partitions
Disk 0

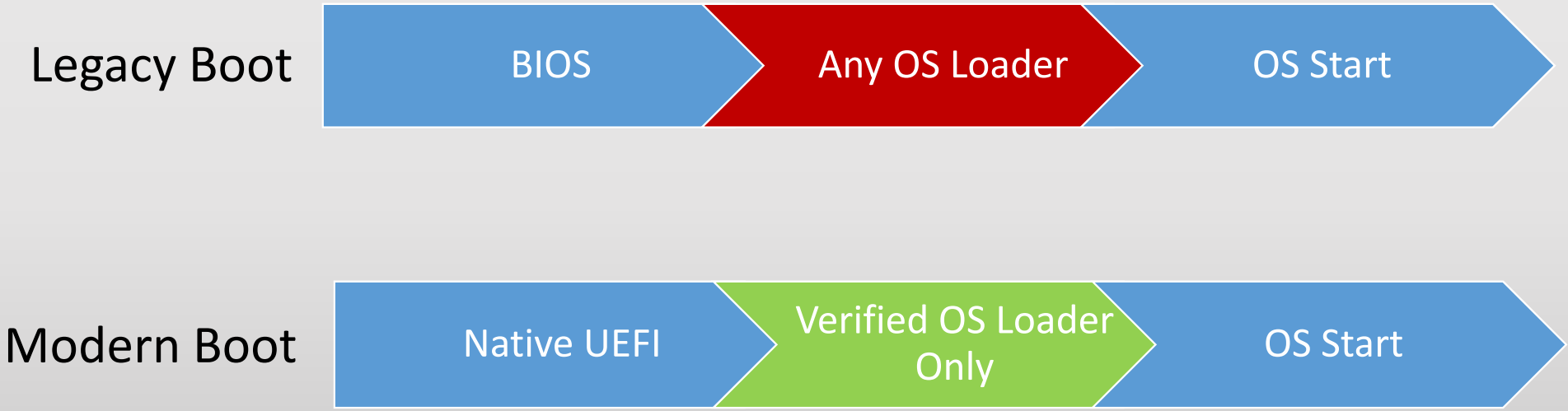


- No NTFS Support thats the «why» so many partitions
- «System» Partition also includes a TPM (simulation)
- GPO's for UEFI!
- UEFI x86 and UEFI x64 diffrent, boot with the correct WinPE

The GUID Partition Table Layout

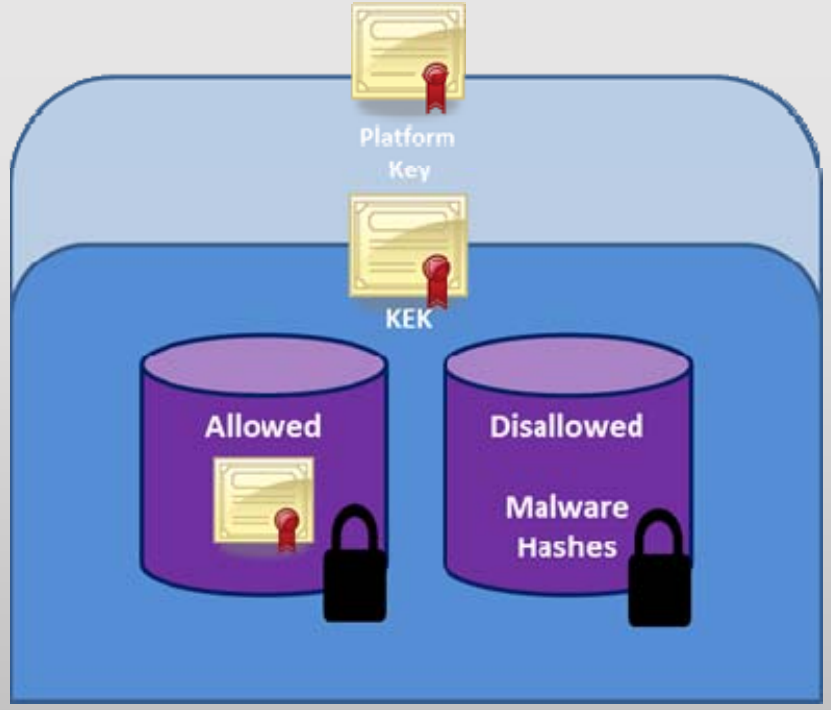


Boot Method Comparison



Secure Boot Process

Secure boot is a UEFI specification, not a Microsoft product!



- Only executes signed UEFI binary images
- Includes Option ROMs, pre-boot utilities and OS loaders.
- Benefit: Helps prevent malicious code before the OS loads
- Benefit: Provides Time-authenticated variables
- Benefit: Allows stronger keys for encryption

Early Launch Anti-Malware (ELAM)

Windows 7

- Malware is able to start before Windows and Anti-malware

Windows 8

- Trusted Boot starts Anti-Malware early in the boot process

UEFI – Technical Merits

- ✓GUID Partition Table (GPT) removes the 2TB hard-drive partition limit
- ✓Removes the Upper Memory Block limit for Option ROM's
- ✓Unifies the Setup interface for platform firmware and Option ROM's
- ✓Provides a pre-boot execution environment (not an OS)
  - ✓ Great for diagnostics and manufacturing
  - ✓ Can host a shell, run applications and scripts
  - ✓ Direct access to all of memory (64-bit addressing)
  - ✓ Direct access to bare-metal registers
  - ✓ Network stack
- ✓Easier, cleaner, more portable booting for the OS
- ✓Extensible using collision-free Globally Unique ID's

UEFI – Engineering Benefits

- C language firmware means faster deployments
  - Fewer human errors; better tools; stable, re-usable code
  - Faster time-to-market, higher quality firmware, lower system development cost
- Fully documented, testable interface
- Publicly available test suite
  - Should help maintain stability and interoperability across implementations
- Consistent behavior across platforms and architectures
- Abstraction hides underlying architecture

How do I know if I'm using UEFI

- Check the hard drive layout
- Check the BCD store for the version of winload.exe
- MSINFO32 will list the value under BIOS mode
- In WinPE 4.0, use the wpeutil updatebootinfo command.

BIOS / UEFI Setup	BIOS	UEFI with CSM	UEFI native Secure boot enabled	UEFI native Secure boot disabled
PowerShell Command	**Result**			
Confirm-SecureBootUEFI	Cmdlet not supported on this platform	FALSE	TRUE	FALSE
Get-SecureBootUEFI –Name SetupMode	Cmdlet not supported on this platform	1	0	1
Get-SecureBootUEFI –Name SecureBoot	Cmdlet not supported on this platform	0	1	0

UEFI RELATED CONTENT

UEFI Support and Requirements for Windows Operating Systems

- http://www.microsoft.com/whdc/system/platform/firmware/uefireg.mspx

Advanced Configuration and Power Interface (ACPI) Specification

- http://www.acpi.info/spec.htm

Unified Extensible Firmware Interface Specification s

- http://www.uefi.org/specs/

EFI Specification 1.10 (included here for historical purposes)

- http://www.intel.com/technology/efi/main_specification.htm

Unified EFI Forum

- http://www.uefi.org/home/

Protecting the pre-OS environment with UEFI

- http://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx

Weitere Infos

MMS USA

Minnesota System Center User Group (Midwest Management Summit)

http://mms.mnscug.org

Hier der 20% Rabat code: SCUGSEarcessequileneyl (Nur für CMCE TN)

Hotel Radisson Blu Code: MNSCUG

Digicomp Kurse neu

https://www.microsoft.com/learning/en-us/course.aspx?ID=20695A&Locale=en-us

https://www.microsoft.com/learning/en-us/course.aspx?ID=20696A&Locale=en-us

CM12 advanced Training

with Kent Agerlund und Kaido Järvemets

http://www.realstuff.ch/services/schulung/sccm-2012-r2-training/

Danke

Herzlichen Dank

Mirko Colemberg @mirkocolemberg

@configmgr_ch #cmcu_ch

blog.colemberg.ch

Bewertung der Session: Configmgr.ch

- Xing: https://www.xing.com/net/cmce
- Facebook: https://www.facebook.com/groups/411231535670608/
- Linkedin: http://www.linkedin.com
- Twitter: https://twitter.com/configmgr_ch

Nächster Event: Montag 9. Februar Digicomp Basel