New Firmware Security Requirements for the Modern Data Center

UEFI & ACPI:

www.uefi.org

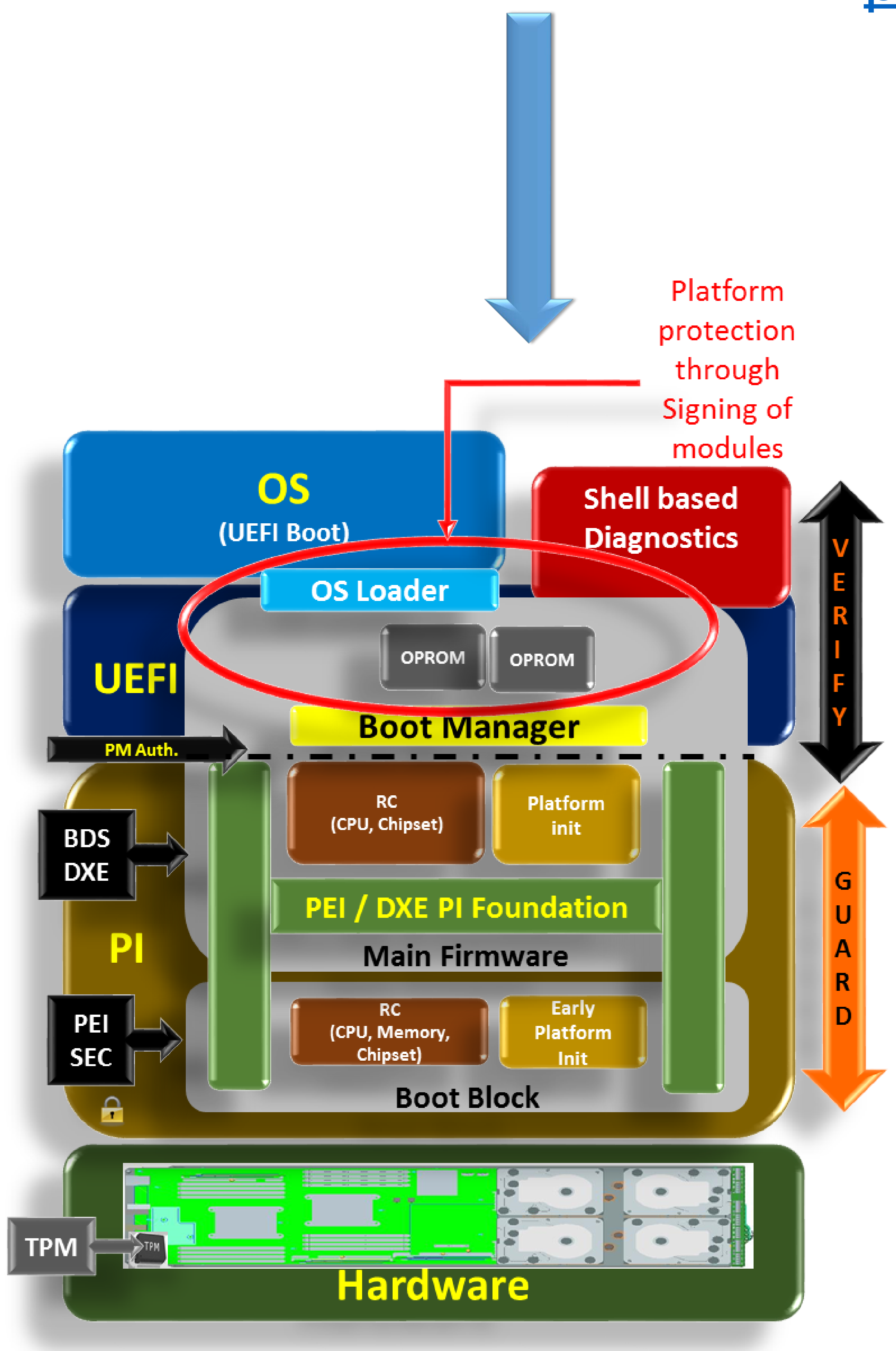
- UEFI 2.6
- ACPI 6.1
- PI 1.4

EDKII code base:

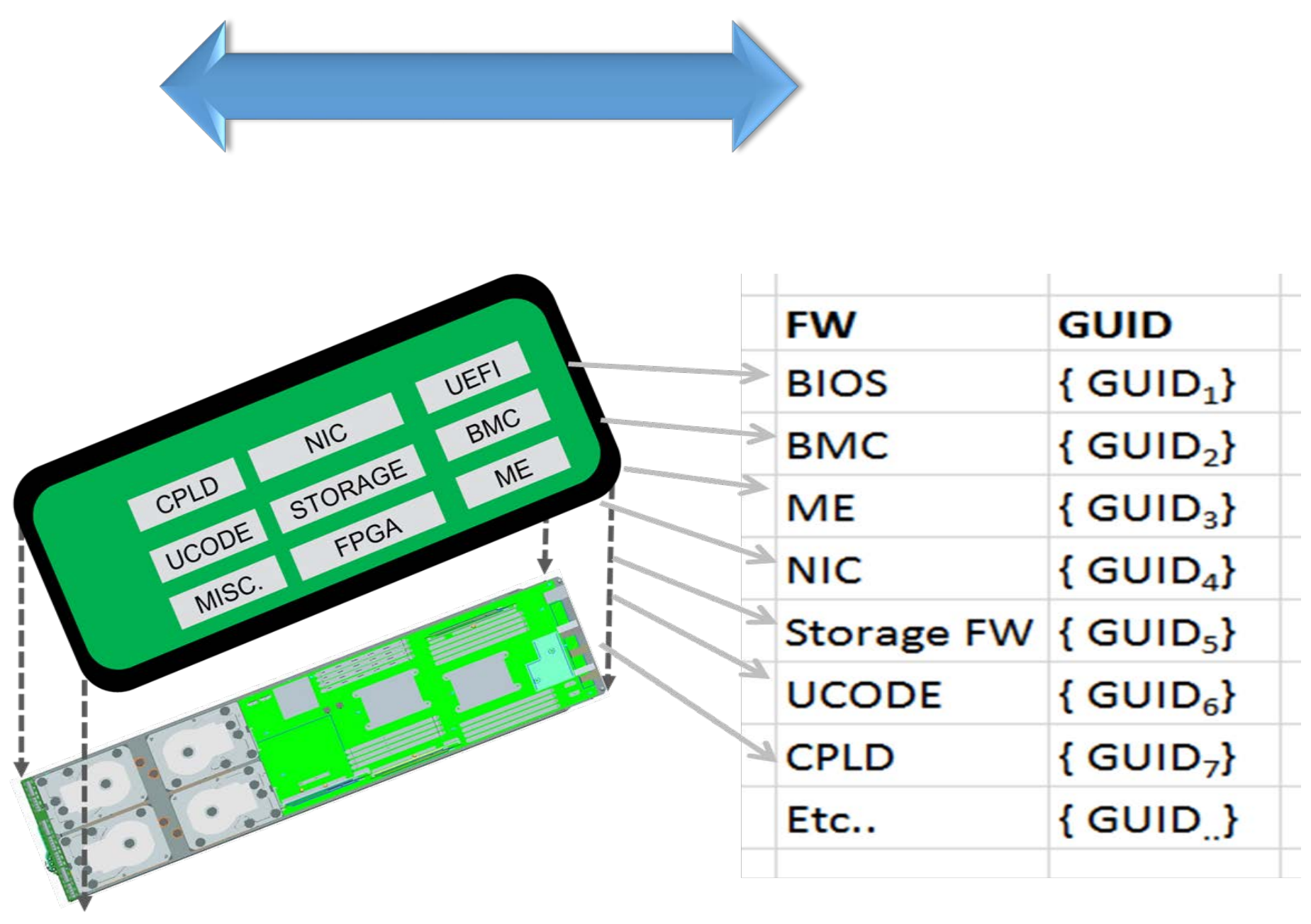
www.tianocore.org

- TPM2.0
- EFI Measured boot
- UEFI Secure boot
- EFI System Resource Table (ESRT)
- Capsule update

White papers - https://github.com/tianocore/tianocore.github.io/wiki/EDK-II-white-papers



Server firmware
And platform elements



FW	GUID
BIOS	{ $GUID_1$}
BMC	{ $GUID_2$}
ME	{ $GUID_3$}
NIC	{ $GUID_4$}
Storage FW	{ $GUID_5$}
UCODE	{ $GUID_6$}
CPLD	{ $GUID_7$}
Etc..	{ $GUID_{..}$}

Example ESRT

Updatable
Firmware on
server

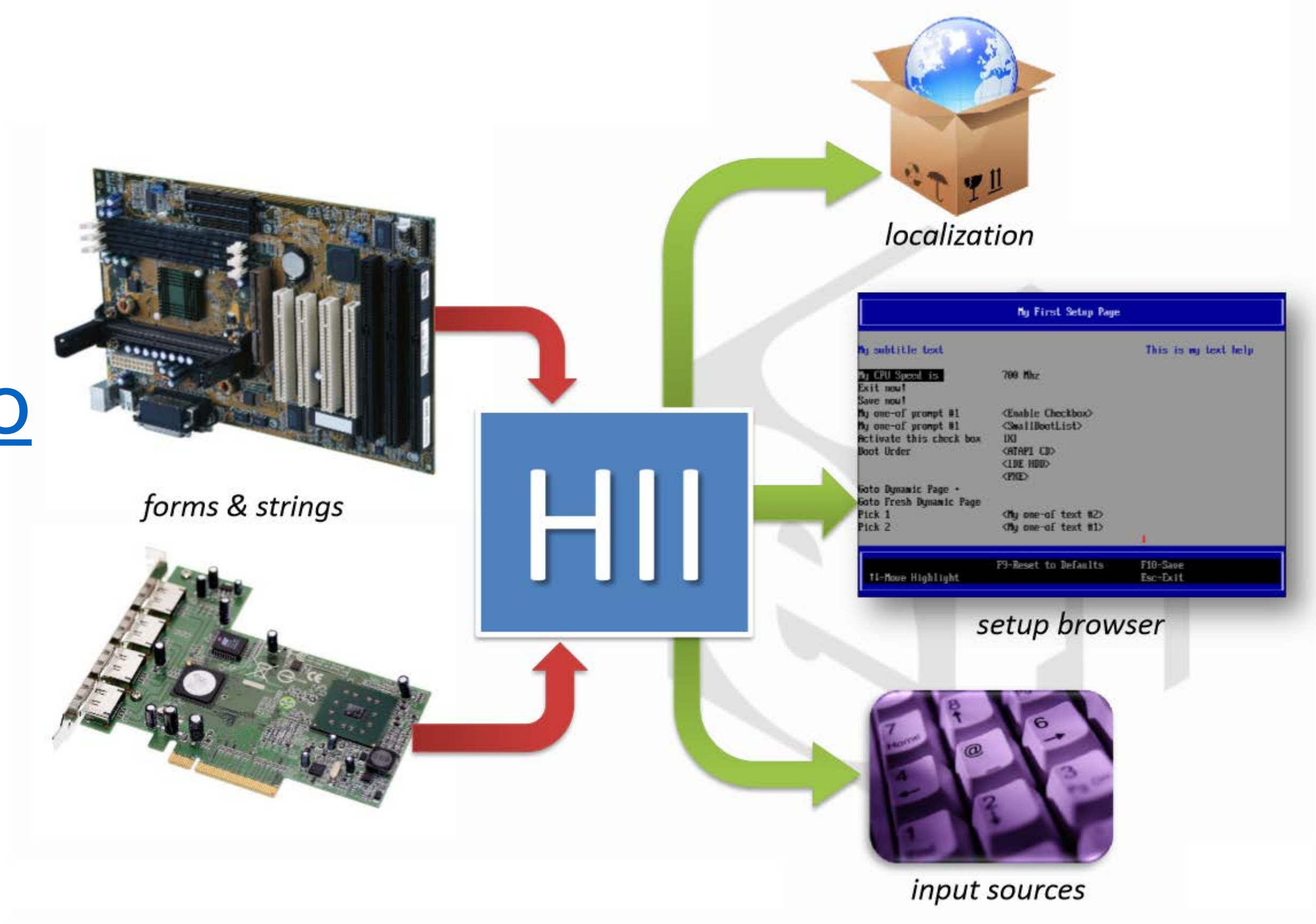
Speakers

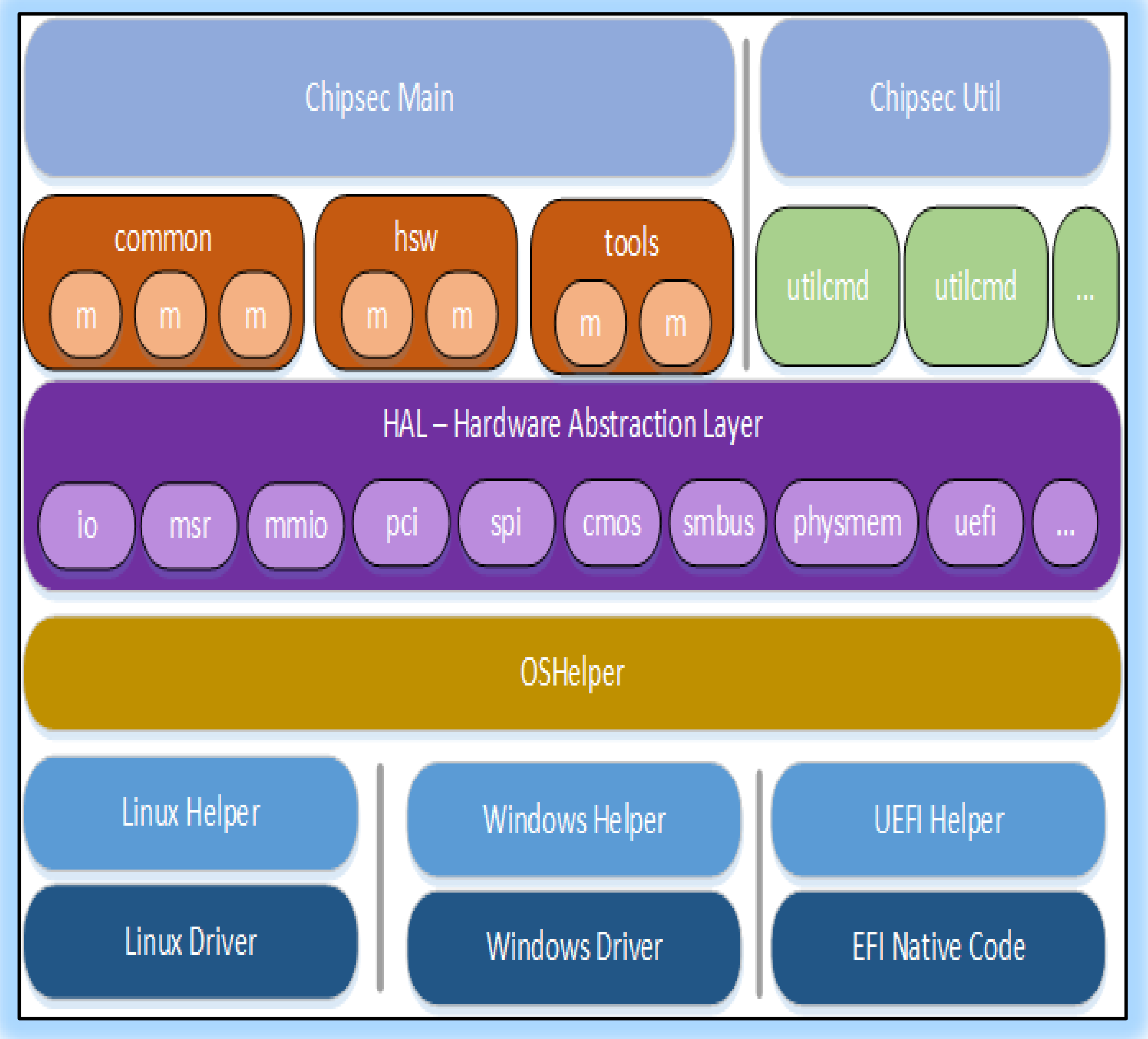
Vincent Zimmer

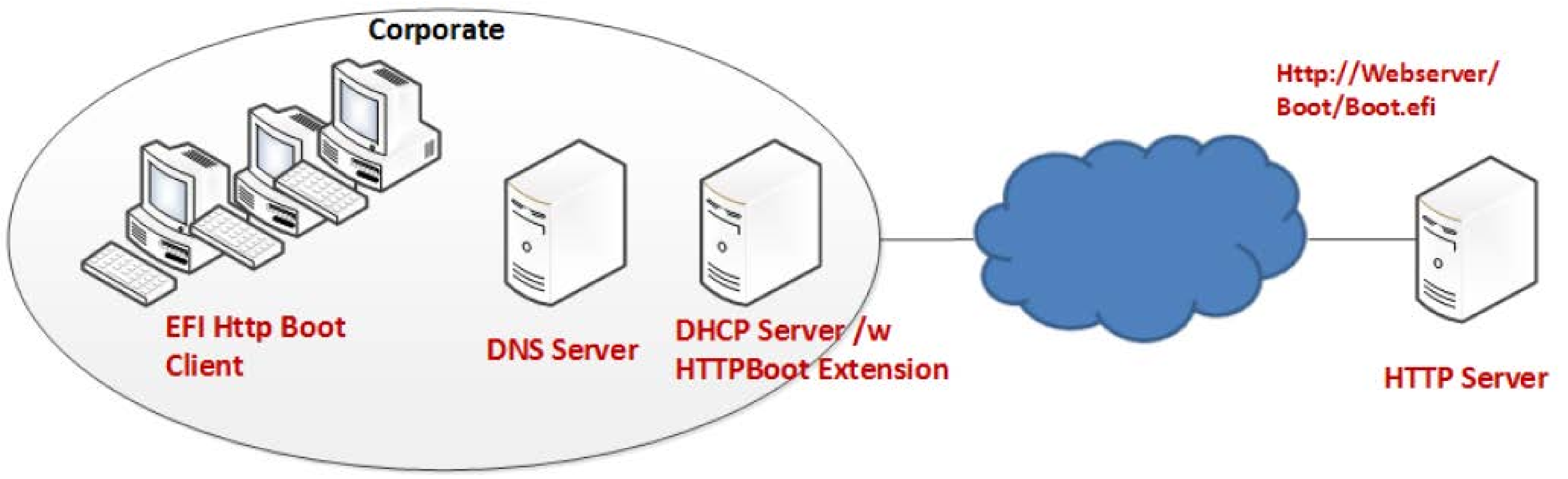
- Senior Principal Engineer – Intel Software and Services Group
- Chair of UEFI Network and security subteam

Deployment

- Trusted Execution Technology http://www.apress.com/9781430261483
- Today's PXE boot
- ISCSI
- IPV4 and IPV6
- HTTP Boot
  - TLS for HTTP-S
- RAM Disk Protocol
- HII Registry http://www.uefi.org/registry
- chipsec https://github.com/chipsec/chipsec






Corporate
EFI Http Boot Client
DNS Server
DHCP Server /w HTTPBoot Extension
Http://Webserver/Boot/Boot.efi
HTTP Server