BIOS Settings Thinkpad E560

1. Main
2. Config
    a. Network
        i. Wake On Lan — Disabled
        ii. UEFI IPv4 Network Stack — Enabled
        iii. UEFI IPv6 Network Stack — Enabled
        iv. UEFI PXE Boot Priority — IPv4 First
    b. USB
        i. USB UEFI BIOS Support — Enabled
        ii. Always On USB — Enabled
            1. Charge in Battery Mode — Disabled
    c. Keyboard/Mouse
        i. Fn and Ctrl Key swap — Disabled
        ii. Fn Sticky Key — Disabled
        iii. F1-F12 as Primary Function — Disabled
    d. Display
        i. Boot Display Device — ThinkPad LCD
        ii. Total Graphics Memory — 256MB
        iii. Boot Time Extension — Disabled
    e. Power
        i. Intel ® Hyper-Threading Technology — Enabled
        ii. Intel ® SpeedStep technology — Enabled
            1. Mode for AC — Maximum Perf
            2. Mode for Battery — Battery Opti
        iii. CPU Power Management — Enabled
    f. CPU
        i. Core Multi-Processing — Enabled
3. Date/Time
4. Security
    a. Password
        i. Supervisor Password — Disabled
        ii. Lock UEFI BIOS Settings — Disabled
        iii. Password at Unattended Boot — Disabled
        iv. Password at Restart — Disabled
        v. Password at Boot Device List — Disabled
        vi. Password Count Exceeded Error — Enabled
        vii. Set Minimum Length — Disabled
        viii. Power-On Password — Disabled
        ix. Hard Disk1 Password — Disabled
    b. Security Chip
        i. Security Chip Selection — Intel PTT
        ii. Security Chip — Enabled
        iii. Clear Security Chip — Enter

- iv. Physical Presence for Provisioning — Disabled
- v. Physical Presence for Clear — Enabled

c. UEFI BIOS Update Option
- i. Flash Bios Updating by End-Users — Enabled
- ii. Secure RollBack Prevention — Enabled

d. Memory Protection
- i. Execution Prevention — Disabled

e. Virtualization
- i. Intel ® Virtualization Technology — Enabled
- ii. Intel ® VT-d Feature — Enabled

f. I/O Port Access
- i. Ethernet LAN — Enabled
- ii. Wireless LAN — Enabled
- iii. Bluetooth — Enabled
- iv. USB Port — Enabled
- v. Optical Drive — Enabled
- vi. Memory Card Slot — Enabled
- vii. Integrated Camera — Enabled
- viii. Microphone — Enabled
- ix. Fingerprint Reader — Disabled

g. Internal Device Access
- i. Internal Storage Tamper Detection — Disabled

h. Anti-Theft
- i. Computrance
  1. Computrance Module Activation
     a. Current Setting — Disabled
     b. Current State — Not Activated

i. Secure Boot Configuration
- i. Secure Boot — Disabled
- ii. Platform Mode — User Mode
- iii. Secure Boot Mode — Standard Mode
- iv. Reset to Secure Mode — Enter
- v. Restore Factory Keys — Enter
- vi. Clear All Secure Boot Keys — Enter

j. Intel ® SGX
- i. Intel ® SGX Control — Disabled
- ii. Change Owner EPOCH — Enter

5. Startup
   a. Boot
      - i. Boot Priority Order
        1. USB CD
        2. USB FDD
        3. ATA HDD0 TOSHIBA Q300
        4. ATAPI CD0 HL-DT-ST DVDRAM GUE0N
        5. USB HDD
        6. PCI LAN

        a. LAN (C85B7642AB5B) –Ipv4
        b. LAN (C85B7642AB5B) –Ipv6
    ii. Excluded from boot priority order
  b. Network Boot ATA HDD0 TOSHIB
  c. UEFI/Legacy Boot — Both
    i. UEFI/Legacy Boot Priority — UEFI First
    ii. CSM Support — Yes
  d. Boot Mode — Quick
  e. Option key Display — Enabled
  f. Boot device List F12 Option — Enabled
  g. Boot Order Lock — Disabled
6. Restart
  a. Exit Saving Changes
  b. Exit Discarding Changes
  c. Load Setup Defaults
    i. OS Optimized Defaults — Enabled
  d. Discard Changes
  e. Save Changes

Änderungen:

Security Chip Selection: Discrete T

Security Chip: Inactive

Secure RollBack Prevention: Disabled

- Intel (R) SGX Control: Software Controlled
- Current State: Disabled

Network Boot: PCI LAN

CSM Support: No