Bundesamt
für Sicherheit in der
Informationstechnik

SUSIv8

Sicherheitsanalyse der UEFI-Integration und „Secure Boot“- Implementierung von Windows 8

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5786
E-Mail: bsi-publikationen@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Dokumentenhistorie

Datum	Änderungszusammenfassung
13.08.2013	Erste Version des Zwischenberichtes zu Meilenstein I
20.08.2013	Tabelle „Übersicht über die Zertifikatsspeicher“ hinzugefügt
16.09.2013	– Umbenennung des Dokumentes zur „Vorabversion“ – Abschnitt „Shim“ eingefügt – Kapitel „Untersuchung der Installierbarkeit verschiedener Betriebssysteme (AP 5)“ eingefügt – Kapitel „Nutzung von „Secure Boot“ für vertrauenswürdige IT-Plattformen (AP 6)“ eingefügt
17.10.2013	– Überarbeitung von Kapitel 4 – Einfügen von Kapitel 5
25.10.2013	– Rechtschreib- und Grammatikkorrekturen
13.11.2013	– Fazit erweitert
21.11.2013	– Fazit ergänzt (Moderater Sicherheitsgewinn)
25.11.2013	– Fazit konkretisiert
02.12.2013	– Abschnitt über Fedora 19 aktualisiert

2 Einführung

Für den Boot-Vorgang eines Computers war in der Vergangenheit das PC-BIOS-System zuständig. Dieses übernahm die Grundfunktionen der Initialisierung des Systems und den Start des Betriebssystems. In vielen modernen Systemen wurde das PC-BIOS durch die UEFI-Firmware abgelöst. Das Unified-Extensible-Firmware-Interface unterstützt eine einfache Erweiterung der Firmware durch unterschiedlichste Module. Hierzu gehören zum Beispiel ein eingebettetes Netzwerkmodul für die Fernwartung, Module für Digital Rights Management und die BIOS-Emulation mit dem Compatibility Support Module (CSM). UEFI erlaubt auch die Nutzung eines Secure-Boot-Mechanismus, der den Boot-Vorgang auf einen signierten Bootloader beschränkt. Die Secure Boot Technologie prüft, ob der Bootloader mit einem kryptographischen Schlüssel signiert ist, der durch eine in der Firmware enthaltene Datenbank autorisiert ist. Durch die entsprechende Signaturverifikation des Bootloaders, des Kernels und möglicherweise weiteren Userspace-Codes wird die Ausführung unsignierter Software wirksam unterbunden.

Windows 8 der Firma Microsoft ist das erste Betriebssystem, welches diese Funktion nutzt. So kann durch eine Integritätsprüfung während des Bootvorgangs die Ausführung von Schadcode verhindert werden. Durch die Festlegung der erlaubten erwünschten Programme durch den Hardware-Hersteller wird die Entscheidungsfreiheit des Eigentümers bei der Wahl der installierfähigen Betriebssysteme eingeschränkt.

2.1 UEFI Secure Boot

UEFI Secure Boot validiert den Bootvorgang (Boot Path). Die UEFI Spezifikation 2.3 definiert die folgenden Komponenten und Verfahren:

- Eine Programmierschnittstelle für den Zugriff auf kryptographisch geschützte UEFI-Variablen in Flash-Speicher
- Ein Format zur Speicherung von X.509-Zertifikaten in UEFI-Variablen
- Ein Verfahren zur Validierung des Bootloaders und der Treiber mit Hilfe von AuthentiCode[1] Signaturen
- Einen Mechanismus für den Widerruf (Revocation) kompromittierter Zertifikate und Signaturen

UEFI Secure Boot unterscheidet die folgenden Schlüssel:

- Platform Key (PK)
- Nur ein einziger PK möglich
- Meist ein Schlüssel des Hardware Herstellers (OEM)
- PK erlaubt die Manipulation der KEK
- Key Exchange Key (KEK)
- Mehrere Zertifikate möglich
- Unterschiedliche Schlüssel für unterschiedliche OS-Anbieter möglich

1http://msdn.microsoft.com/en-us/library/ms537359\%28v=vs.85\%29.aspx

- Zum Beispiel: Microsoft KEK CA
- KEK erlaubt die Manipulation der db und dbx
- Autorisierte DB (db)
- Mehrere Zertifikate und Hashes möglich
- Zum Beispiel: Microsoft Windows Production CA
- Zur Identifizierung von vertrauenswürdigem Code
- Nicht autorisierte DB (dbx)
- Mehrere Zertifikate oder Hashes möglich
- Zur Identifizierung von kompromittiertem Code oder Schadcode

Des Weiteren beschreibt die Spezifikation zwei Modi in denen sich Secure Boot befinden kann. Zum einen ist dies der „Setup Mode“. Eine UEFI-Firmware, dessen Secure Boot-Implementierung im Setup Mode betrieben wird, stellt keinerlei Schutzmechanismen zur Manipulation der Zertifikatsspeicher bereit. Es ist insbesondere möglich, aus einem laufenden Betriebssystem heraus Zertifikate als auch Hashes in die UEFI-Zertifikatsspeicher einzufügen oder aus diesen zu entfernen. Dieser Modus dient primär zur Einrichtung von Secure Boot.

Ferner existiert der „User Mode“. Befindet sich eine Secure Boot-Implementierung im User Mode, so ist eine Manipulation der Zertifikatsspeicher nur sehr eingeschränkt möglich. Insbesondere sind Änderungen ohne Authentifizierung aus einem laufenden Betriebssystem nicht mehr durchführbar. Zur Veränderung des db- oder dbx-Zertifikatsspeichers ist eine Autorisierung mittels des privaten Schlüssels eines im KEK-Speicher hinterlegten Zertifikate nötig. Zur Änderung des KEK-und PK-Speichers bedarf es hingegen des privaten Schlüssels des hinterlegten Plattform-Key-Zertifikats.

Der Wechsel vom „User Mode“ in den „Setup Mode“ ist zum einen durch das Entfernen des Plattform Keys möglich. Dies setzt die Kenntnis des privaten Schlüssels des installierten Plattform Keys voraus. Alternativ kann mittels des UEFI-Setups in den Setup Mode gewechselt werden. Dies setzt einen physikalischen Zugang zur Hardware und gegebenenfalls die Kenntnis von Kennwörtern zur Nutzung des Setups voraus.

Diese Regeln sollen die unautorisierte Manipulation am Schlüsselmaterial für den Secure Boot-Vorgang verhindern und damit die Integrität des Bootvorgangs schützen.

UEFI Secure Boot verhindert nicht die Installation von Malware oder Modifikation des Bootloaders, sondern stellt dessen Vertrauenswürdigkeit während des Bootvorgangs sicher. Kann die Vertrauenswürdigkeit nicht festgestellt werden, so unterbindet Secure Boot den Bootvorgang. Das System bootet somit nicht mehr, wenn es zu einer unerlaubten Manipulation gekommen ist.

2.2 Secure Boot mit Microsoft Windows

Microsoft unterstützt Secure Boot ab Microsoft Windows 8. Jedoch ist Secure Boot keine zwingende Voraussetzung für die Funktionstüchtigkeit des Betriebssystems. Ältere Microsoft-Betriebssysteme können auf einem System mit aktiver Secure Boot-Funktion nicht eingesetzt werden, da Microsoft für diese noch keine signierten Bootloader bereitstellt.

Hardware-Hersteller, die ihre Systeme mit dem "Windows 8 Logo" ausstatten möchten, müssen jedoch UEFI Secure Boot unterstützen und diese Funktion im Auslieferungszustand aktivieren. Daher müssen diese Systeme auch über das notwendige Schlüsselmaterial in der UEFI-Firmware verfügen. Hierzu gehört mindestens das „Microsoft Windows Production PCA 2011“ Zertifikat, welches von Microsoft für die Signatur eigener Produkte genutzt wird. Die Hardwarehersteller dürfen weitere Microsoft Zertifikate, wie das „Microsoft Corporation UEFI CA 2011“ Zertifikat, und eigene Zertifikate in den UEFI-Speicher ablegen.

UEFI Secure Boot wird bisher hauptsächlich auf Client-Systemen eingesetzt. Zukünftige Microsoft Betriebssysteme werden diese Technologie jedoch wahrscheinlich auch auf Serversystemen zur Verfügung stellen oder deren Nutzung sogar erzwingen.

2.3 Secure Boot mit Linux

2.3.1 Third Party Signaturen

Um Secure Boot auch mit anderen Betriebssystemen nutzen zu können, stehen grundsätzlich drei Möglichkeiten zur Verfügung:

- Signierung der eigenen Bootloader durch Microsoft.
- Hinterlegung eines eigenen KEK-Schlüsselmaterials durch den Hardware-Hersteller. Offenbar verfügt jedoch kein weiterer Betriebssystemanbieter über die entsprechende politische Marktmacht, um die Hardware-Hersteller flächendeckend von der Installation weiteren KEK-Schlüsselmaterials überzeugen zu können.
- Erzeugung eines eigenen Platform Key (PK) und Hinterlegung (Enrollment) in der UEFI-Firmware. Durch den Austausch des Platform Keys wird ein Zugriff auf alle weiteren Zertifikatsspeicher möglich. Das Ersetzen eines fremden Platform Keys bedingt jedoch pyhsikalischen Zugang zum System.

Alle in diesem Projekt untersuchten Betriebssysteme, die Secure Boot unterstützen, schlagen den ersten Weg ein. Damit ist die Installation ihrer Bootloader auf einem System mit aktiven Secure Boot und installierten Microsoft Schlüsselmaterial möglich. Hierzu bietet Microsoft einen Signaturdienst an, der ursprünglich nur für die Signatur von UEFI-Treibern vorgesehen war. Dieser Dienst wurde auch auf alternative Bootloader von Drittanbietern erweitert. Hierzu sendet der authentifizierte Drittanbieter seinen Bootloader an Microsoft. Microsoft prüft den Bootloader und sendet ihn mit einer AuthentiCode-Signatur zurück an den Absender. Die Signatur verifiziert nicht den Urheber (pseudonymisiert), sondern lediglich die Unversehrtheit des Bootloaders.

Die Signatur erfolgt mit dem Zertifikat „Microsoft Corporation UEFI CA 2011“. Daher ist die Funktionsfähigkeit des Bootloaders nicht auf jeder Hardware garantiert, da dieses Zertifikat nach Microsoft

Spezifikation nicht installiert sein muss. Auch hier ist möglicherweise ein Enrollment eines weiteren Zertifikats erforderlich.

Durch die Signierung des Bootloaders durch Microsoft bestehen grundsätzlich zwei Gefahren bei dem Einsatz in der Produktion:

- Microsoft kann das Zertifikat widerrufen. Werden die Revocation-Lists im Rahmen von Software-Updates in der UEFI-Firmware hinterlegt, erlaubt die Firmware die Nutzung des entsprechenden Bootloaders nicht mehr.
- Die Signatur ist nur für eine bestimmte Zeit gültig. Die UEFI-Firmware kann den signierten Bootloader nach Ablauf der Signatur ablehnen und den Bootvorgang abbrechen. Erfolgt keine erneute Signierung, kann das System nicht mehr booten.

2.3.2 Shim

Zur Umsetzung von Secure Boot anhand des Signierdienstes von Microsoft wird typischerweise der Bootloader Shim eingesetzt. Bei Shim handelt es sich um einen einfach strukturierten Open-Source-Bootloader. Er ermöglicht es, Bootloader, die nicht von Microsoft signiert sind, indirekt zu starten. Shim kann somit als Bindeglied zwischen der von Microsoft geprägten Secure-Boot-Umgebung und Betriebssystemen Dritter eingesetzt werden.

Ermöglicht wird dies u.a. durch eine öffentlich zugängliche Shim Version die von Microsoft mittels des Zertifikats „Microsoft Corporation UEFI CA 2011“ (Seriennr.: 61:08:d3:c4:00:00:00:00:00:04) signiert ist. Aufgrund dieser Signierung kann Shim von allen in dieser Arbeit untersuchten Hardwareplattformen mittels des jeweiligen Standardschlüsselmaterials mit aktivierten Secure Boot gestartet werden. Ferner installieren einige Linux-Systeme, wie z.B. Ubuntu 13.04 oder Fedora 19, alternative Versionen von Shim, die ebenfalls von Microsoft signiert sind.

Shim überprüft die Signatur des als nächstes zu ladenden Bootloaders. Das Schlüsselmaterial für diese Verifizierung kann hierbei aus drei Quellen stammen:

- Die UEFI-Zertifikatsspeicher db und dbx
- Die Machine Owner Key List (MokList), ein Shim-eigener Zertifikatsspeicher
- Ein im Shim-Binary hinterlegtes Zertifikat oder hinterlegter Hash

Die MokList kann sowohl Zertifikate als auch Hashes speichern. Die Nutzung von Zertifikaten bedingt die Signierung des zweiten Bootloaders. Die MokList wird zwar ebenso wie die UEFI-spezifischen Zertifikatsspeicher im NVRAM der UEFI-Firmware gespeichert, sie ist jedoch zumindest während des Bootvorgangs typischerweise ohne Authentifizierung modifizierbar.

Durch die Möglichkeit Zertifikate direkt in der Binärdatei von Shim zu hinterlegen, kann der Verifizierungsvorgang unabhängig vom Inhalt der Zertifikatsspeicher gestaltet werden. Diesen Weg wählen die Linux-Distributionen Ubuntu 13.04 und Fedora 19.

Ist die Verifizierung des zweiten Bootloaders, typischerweise Grub2, erfolgreich, so wird dieser ausgeführt. Schlägt die Verifizierung dagegen fehl oder kann der zweite Bootloader aus einem anderen Grund nicht geladen werden, so wird die zu Shim gehörende Anwendung MokManager aufgerufen, sofern diese installiert ist. Der MokManager ermöglicht es dem Anwender, interaktiv Zertifikate oder Hashes in die MokList einzufügen und somit die Ausführung des zweiten Bootloaders zu erlauben.

3 Projektziele

Da die Secure-Boot-Technologie weitreichende Auswirkungen auf die Installation von alternativen Betriebssystemen in Stand-Alone und Dual-Boot-Umgebungen hat, soll dieses Projekt die Möglichkeiten und Probleme in diesen Umgebungen analysieren.

Erstes Ziel des Projektes ist daher die Analyse der in der UEFI-PreBoot-Umgebung hinterlegten Module, Schlüssel und Variablen und ihren Einfluss auf den Start des Betriebssystems. Betrachtungsgegenstand sind je eine 64-Bit x86-kompatible Plattform der Hersteller HP, Dell, Lenovo und Medion. Jeder Hersteller kann unterschiedliche Firmwaremodule und zusätzliches Schlüsselmaterial über die Anforderungen des „Windows 8 Logo“ hinaus installieren. Hierzu gehört auch die Problematik des optionalen Zertifikats „Microsoft Corporation UEFI CA 2011“. Die Verfügbarkeit bestimmter Firmwaremodule, z.B. ein Netzwerkmodul zur Fernwartung, erhöht möglicherweise gewisse Restrisiken im Einsatz in sensitiven Umgebungen.

Des Weiteren soll die Einflussmöglichkeit des Eigentümers einer Hardwareplattform auf das durch Secure Boot kontrollierte Bootverfahren untersucht werden. Hierbei stehen besonders die folgenden Fragen im Vordergrund:

- Kann der Anwender Secure Boot deaktivieren?
- Kann der Anwender alternatives Schlüsselmaterial in der UEFI-Firmware hinterlegen?
- Welche Möglichkeiten bietet der Hardware-Hersteller für die Modifikation des Schlüsselmaterials?

Darüber hinaus wird untersucht inwieweit sich die Betriebssysteme Windows 8 Pro, Red Hat Enterprise Linux 6.4, Ubuntu 13.04, Debian 7.1.0 und Fedora 19 bei aktivem Secure Boot installieren und nutzen lassen. Gegebenenfalls werden Anpassungsschritte erarbeitet, um eine Funktionstüchtigkeit des jeweiligen Betriebssystemes bei Nutzung von Secure Boot zu gewährleisten.

Anschließend wird der Einsatz von Secure Boot im Zusammenhang mit einer Dual-Boot-Umgebungen, bestehend aus Windows 8 Pro und Debian 7.1.0, untersucht. Hierbei wird u.a. untersucht, wie Änderungen an der Secure-Boot-Konfiguration durch ein Betriebssystem unterbunden werden können und somit eine entsprechende Beeinflussung der Funktionstüchtigkeit der Betriebssysteme untereinander ausgeschlossen werden kann.

Des Weiteren wird herausgearbeitet welche organisatorischen und technischen Maßnahmen ergriffen werden können, um Secure Boot zur effizienten Absicherung des Bootprozesses eines Linux-Systems nutzen zu können.

Abschließend wird eine Einschätzung der Anwendungsmöglichkeiten von Secure Boot gegeben.

4 Analyse verschiedener Hardwareplattformen

4.1 HP-Plattform

4.1.1 Systembeschreibung

Model: HP Spectre XT Pro Ultrabook (Touchsmart 15-4000eg)

Seriennr.: CND2510KS9

UEFI-Firmware: InsydeH20 Setup Utility Rev. 3.7

UEFI-Firmware-Hersteller: Insyde

UEFI-Firmware-Version: F.11

Secure Boot bei Auslieferung aktiv: Ja

Secure Boot deaktivierbar: Ja

4.1.2 Erfassung der vorhandenen Firmwaremodule (AP 2)

Neben dem Bootloader von Microsoft beinhaltet die EFI-Partition im Ordner /EFI/HP Anwendungen von HP. Dies ist ein Werkzeug zur Durchführung einer Diagnose des Gesamtsystems oder einzelner Systemkomponenten. Des Weiteren existiert eine Applikation zur Durchführung von UEFI-Firmware-Updates. Auch die zu installierenden Firmwareimages werden offenbar vor oder während der Installation auf der EFI-Partition hinterlegt. Darüber hinaus existiert eine Kopie des Windows-Bootmanagers. Eine vollständige Liste aller Dateien ist in Anhang 7.6 gegeben.

4.1.3 Analyse der Schlüsseldatenbank (AP 3)

Im Folgenden wird eine Übersicht über alle standardmäßig installierten Zertifikate und Hashe in den UEFI-Zertifikatsspeichern PK, KEK, db und dbx gegeben. Eine ausführliche Auflistung der Zertifikate ist in Anhang 7.2 enthalten.

PK:

Hewlett-Packard UEFI Secure Boot Platform Key (1b:6a:ef:49:8c:fb:7f:90:b6:81:32:1a:e8:9e:c2:ef)

KEK:

Microsoft Corporation KEK CA 2011 (61:0a:d1:88:00:00:00:00:00:03)

Hewlett-Packard UEFI Secure Boot Key Exchange Key (04:31:75:a3:b6:04:a1:75:71:55:ea:6e:37:52:6d:40)

db:

Microsoft Corporation UEFI CA 2011 (61:08:d3:c4:00:00:00:00:00:04)

Microsoft Windows Production PCA 2011 (61:07:76:56:00:00:00:00:00:08)

dbx:

Hash: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

4.1.4 Zugriffsmöglichkeiten auf die Schlüsseldatenbanken (AP 4)

UEFI-Setup:

Das UEFI-Setup bietet in der aktuellen Version keine Möglichkeit Zertifikate oder Hashes zu importieren oder zu exportieren. Das Setup bietet die Möglichkeit die Zertifikatsdatenbank neu mit den oben aufgeführten Schlüsseln zu initialisieren und dabei evtl. vorhandene Schlüssel zu ersetzen. Ferner können alle Schlüsseldatenbanken gelöscht werden. Letztere Option entfernt insbesondere den Plattform Key und versetzt den Rechner in den Setup Mode.

EFI-Keytool:

Mittels der EFI-Tools können alle Zertifikatsspeicher erfolgreich ausgelesen und deren Inhalt auf einen USB-Stick kopiert werden. Ferner ist das Ersetzen und gegebenenfalls das Hinzufügen von Zertifikaten im Setup Mode möglich. Auch ist das Hinzufügen und Entfernen von Hashes in db und dbx möglich.

4.1.5 Besonderheiten

Der in Gänze aus Null-Bits bestehende Hash in dem dbx-Speicher gehört sicherlich zu keinem real existierenden Bootloader. Ein Grund für die Aufnahme eines solchen Hashes ist nicht offensichtlich.

4.2 Dell-Plattform

4.2.1 Systembeschreibung

Model: Dell Latitude 3330

Seriennr.: GX44RT1

UEFI-Firmware-Version: A00

Secure Boot bei Auslieferung aktiv: Ja

Secure Boot deaktivierbar: Ja

4.2.2 Erfassung der vorhandenen Firmwaremodule (AP 2)

Der Microsoft Bootmanager ist nicht nur an der üblichen Stelle /EFI/Microsoft/Boot/en-US/bootmgr.efi.mui, sondern auch als /en-us/bootmgr.efi.mui zu finden. Eine vollständige Liste aller Dateien ist in Anhang 7.7 gegeben.

4.2.3 Analyse der Schlüsseldatenbank (AP 3)

Im Folgenden wird eine Übersicht über alle standardmäßig installierten Zertifikate und Hashe in den UEFI-Zertifikatsspeichern PK, KEK, db und dbx gegeben. Eine ausführliche Auflistung der Zertifikate ist in Anhang 7.3 enthalten.

PK:

Dell Inc. UEFI Platform Key (0x4ee77b3a)

KEK:

Microsoft Corporation KEK CA 2011 (61:0a:d1:88:00:00:00:00:00:03)

db:

Microsoft Corporation UEFI CA 2011 (61:08:d3:c4:00:00:00:00:00:04)

Microsoft Windows Production PCA 2011 (61:07:76:56:00:00:00:00:00:08)

dbx:

Microsoft Windows PCA 2010 (61:0c:6a:19:00:00:00:00:00:04)

4.2.4 Zugriffsmöglichkeiten auf die Schlüsseldatenbanken (AP 4)

UEFI-Setup:

Das UEFI-Setup bietet in der aktuellen Version die Möglichkeit Zertifikate oder Hashes von einem USB-Stick zu importieren oder auf einen solchen zu exportieren. Eine weitere Verarbeitung der ausgelesenen Zertifikate ist z.B. mit den EFI-Tools möglich. Das Setup bietet ferner die Möglichkeit, die Zertifikatsdatenbank neu mit den oben aufgeführten Schlüsseln zu initialisieren und dabei evtl. vorhandene Schlüssel zu ersetzen. Ferner können alle Schlüsseldatenbanken gelöscht werden. Letztere Option entfernt insbesondere den Plattform Key und versetzt den Rechner in den Setup Mode.

EFI-Keytool:

Mittels der EFI-Tools können alle Zertifikatsspeicher erfolgreich ausgelesen und deren Inhalt auf einen USB-Stick kopiert werden. Ferner ist das Ersetzen und gegebenenfalls das Hinzufügen von Zertifikaten im Setup Mode möglich. Auch ist das Hinzufügen und Entfernen von Hashes in db und dbx möglich.

4.2.5 Besonderheiten

Der standardmäßig hinterlegte Plattform Key ist laut den in dem Zertifikat hinterlegten Daten lediglich bis zum 17. Juli 2014 gültig. Das manuelle Setzen der Zeit auf einen Wert nach dem Gültigkeitsdatum führt jedoch zu keiner ersichtlichen Änderung im Secure-Boot-Prozess. Es ist daher zu mutmaßen, dass die entsprechende Angabe im Zertifikat seitens der UEFI-Firmware nicht ausgewertet wird.

4.3 Lenovo-Plattform

4.3.1 Systembeschreibung

Model: Lenovo Thinkpad Twist (N3C7WGE)

Seriennr.: MP3PL36

UEFI-Firmware: ThinkPad Setup

UEFI-Firmware-Version: GDET97WW (1.57)

Secure Boot bei Auslieferung aktiv: Ja

Secure Boot deaktivierbar: Ja

4.3.2 Erfassung der vorhandenen Firmwaremodule (AP 2)

Es sind neben dem Windows-Bootmanager standardmäßig keine weiteren Tools vorhanden. Eine vollständige Liste aller Dateien ist in Anhang 7.8 gegeben.

4.3.3 Analyse der Schlüsseldatenbank (AP 3)

Im Folgenden wird eine Übersicht über alle standardmäßig installierten Zertifikate und Hashe in den UEFI-Zertifikatsspeichern PK, KEK, db und dbx gegeben. Eine ausführliche Auflistung der Zertifikate ist in Anhang 7.4 enthalten.

PK:

Lenovo Ltd. PK CA 2012 (0xebb513d46bb1dc6e)

KEK:

Lenovo Ltd. KEK CA 2012 (0x955243828a5a652e)

Microsoft Corporation KEK CA 2011 (61:0a:d1:88:00:00:00:00:00:03)

db:

Microsoft Corporation UEFI CA 2011 (61:08:d3:c4:00:00:00:00:00:04)

Microsoft Windows Production PCA 2011 (61:07:76:56:00:00:00:00:00:08)

ThinkPad Product CA 2012 (09:45:63:7a:d8:c2:20:df:61:ea:52:44)

Hash: 14 e6 2a 49 05 e1 91 89 e7 08 28 98 31 65 93 9a fc 0a 33 1d 0b 41 5f 33 32 b0 e8 18 a8 27 f4 36

dbx:

Hash: 14 e6 2a 49 05 e1 91 89 e7 08 28 98 31 65 93 9a fc 0a 33 1d 0b 41 5f 33 32 b0 e8 18 a8 27 f4 36

4.3.4 Zugriffsmöglichkeiten auf die Schlüsseldatenbanken (AP 4)

UEFI-Setup:

Das UEFI-Setup bietet in der aktuellen Version keine Möglichkeit Zertifikate oder Hashes zu importieren oder zu exportieren. Das Setup bietet die Möglichkeit, die Zertifikatsdatenbank neu mit den oben aufgeführten Schlüsseln zu initialisieren und dabei evtl. vorhandene Schlüssel zu

ersetzen. Ferner existiert eine Option die Firmware explizit in den Setup Mode zu versetzen. Diese Funktion führt zur Löschung des Plattform Keys, lässt andere Zertifikatsspeicher aber unberührt.

EFI-Keytool:

Mittels der EFI-Tools können alle Zertifikatsspeicher erfolgreich ausgelesen und deren Inhalt auf einen USB-Stick kopiert werden. Ferner ist das Ersetzen und das Hinzufügen von Zertifikaten im Setup Mode zum Teil (siehe Abschnitt 4.3.5) möglich. Auch ist das Hinzufügen und Entfernen von Hashes in db und dbx möglich.

4.3.5 Besonderheiten

Wenngleich es möglich ist Hashes in die db einzutragen, so verweigert die UEFI-Firmware das Starten der zugehörigen Bootloader. Ein mit einem im db-Speicher enthaltenen Zertifikat signierter Bootloader wird jedoch anstandslos ausgeführt. Ebenso werden EFI-Applikationen, deren Hashes im dbx-Speicher enthalten sind, wie erwartet nicht gestartet.

Im Gegensatz zu den anderen drei UEFI-Plattformen beinhaltet das ThinkPad auch ein eigenes Zertifikat im db-Zertifikatsspeicher. Es ist Lenovo somit möglich, ohne Unterstützung durch Microsoft weitere Betriebssysteme und UEFI-Tools zu signieren und bei aktivem Secure Boot auszuführen.

Ferner ist ein und derselbe Hash sowohl in dem db- als auch im dbx-Speicher. Ein Grund für ein solches Vorgehen seitens Lenovo ist nicht offensichtlich.

4.4 Medion-Plattform

4.4.1 Systembeschreibung

Model: Medion AKOYA S4613 Ultrabook

Seriennr.: 12BPE3034742

UEFI-Firmware: Aptio Setup Utility

UEFI-Firmware-Hersteller: American Megatrands

UEFI-Firmware-Version: 507

Secure Boot bei Auslieferung aktiv: Ja

Secure Boot deaktivierbar: Ja

4.4.2 Erfassung der vorhandenen Firmwaremodule (AP 2)

Es sind neben dem Windows-Bootmanager standardmäßig keine weiteren Tools vorhanden. Eine vollständige Liste aller Dateien ist in Anhang 7.9 gegeben.

4.4.3 Analyse der Schlüsseldatenbank (AP 3)

Im Folgenden wird eine Übersicht über alle standardmäßig installierten Zertifikate und Hashe in den UEFI-Zertifikatsspeichern PK, KEK, db und dbx gegeben. Eine ausführliche Auflistung der Zertifikate ist in Anhang 7.5 enthalten.

PK:

MEDION Certificate ((Negative)78:bd:0b:37:19:a8:4b:5b:b0:cf:c2:0c:8d:7a:8c:59)

KEK:

Microsoft Corporation KEK CA 2011 (61:0a:d1:88:00:00:00:00:00:03)

db:

Microsoft Corporation UEFI CA 2011 (61:08:d3:c4:00:00:00:00:00:04)

Microsoft Windows Production PCA 2011 (61:07:76:56:00:00:00:00:00:08)

dbx:

Hash: e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

4.4.4 Zugriffsmöglichkeiten auf die Schlüsseldatenbanken (AP 4)

UEFI-Setup:

Das UEFI-Setup bietet in der aktuellen Version Menüeinträge zum Exportieren der Zertifikate aus der Firmware in eine Datei und zum Importieren von Zertifikaten aus einer Datei in die Firmware. Diese Optionen scheinen aber ohne Funktion. Es ist zumindest in den Tests auch durch Änderung anderer Setup-Einstellungen nicht gelungen, die erwartetete Reaktion der Firmware auszulösen. Das Setup bietet ferner die Möglichkeit, die Zertifikatsdatenbank neu mit den oben aufgeführten

Schlüsseln zu initialisieren und dabei evtl. vorhandene Schlüssel zu ersetzen. Ferner können alle Schlüsseldatenbanken unabhängig voneinander gelöscht werden. Das Leeren des PK-Speichers versetzt die Plattform in den Setup Mode.

EFI-Keytool:

Mittels der EFI-Tools können alle Zertifikatsspeicher erfolgreich ausgelesen und deren Inhalt auf einen USB-Stick kopiert werden. Ferner ist das Ersetzen und gegebenenfalls das Hinzufügen von Zertifikaten im Setup Mode möglich. Auch ist das Hinzufügen und Entfernen von Hashes in db und dbx möglich.

4.5 Zusammenfassung

Alle untersuchten Systeme ermöglichen die Veränderung der Zertifikatsspeicher, die dem Secure-Boot-Vorgang zugrunde liegen. Mittels des UEFI-Setups können bei allen Systemen die ursprünglich vom Hersteller ausgelieferten Schlüssel in den Zertifikatsspeicher geladen werden und so diese Systeme in den vom Hersteller definierten Ausgangszustand versetzt werden. Auch ermöglicht das UEFI-Setup in allen Fällen den Wechsel in den Setup-Mode und somit eine anschließende Modifizierung der Zertifikatsspeicher.

Das gezielte Einfügen oder Entfernen einzelner Zertifikate oder Hashes aus dem UEFI-Setup heraus ermöglichte jedoch nur das System von Dell. Bei allen Systemen ist es aber zumindest möglich, die Zertifikatsspeicher im Setup Mode mittels der EFI-Tools zu modifizieren.

Darüber hinaus bieten alle Systeme die Möglichkeit Secure Boot zu deaktivieren.

Ferner liefern alle Hersteller der untersuchten Systeme die durch die Windows Hardware Certification Requirements vorgeschriebenen Zertifikate einschließlich des optionalen Zertifikats „Microsoft Corporation UEFI CA 2011“ mit. Einige Hersteller installieren darüberhinaus eigene Zertifikate.

Die auf der EFI-Partition vorinstallierte Software beschränkt sich im Wesentlichen auf Diagnose-Software der Hersteller. Eine genauere Überprüfung der Funktionsweise dieser Software, z.B. durch Disassemblierung, wurde im Sinne der Aufgabenstellung dieses Projektes nicht durchgeführt.

Auf allen zur Verfügung gestellten Systemen ist der Anwender somit in der Lage, auf die Secure Boot Funktionalität Einfluss zu nehmen. Er kann Secure Boot deaktivieren, in den Setup Modus versetzen und eigenes Schlüsselmaterial laden. Hierzu kann er teilweise die Werkzeuge aus dem UEFI-Setup nutzen. In den meisten Fällen muss jedoch auf weitere Werkzeuge, wie zum Beispiel die EFI-Tools, zurückgegriffen werden.

	HP	Dell	Lenovo	Medion
PK	HP UEFI Secure Boot Platform Key	Dell Inc. UEFI Platform Key	Lenovo Ltd. PK CA 2012	MEDION Certificate
KEK	MS KEK CA 2011 HP UEFI Secure Boot Key Exchange Key	MS KEK CA 2011	MS KEK CA 2011 Lenovo Ltd. KEK CA 2012	MS KEK CA 2011
db	MS UEFI CA 2011 MS Windows Production PCA 2011	MS UEFI CA 2011 MS Windows Production PCA 2011	MS UEFI CA 2011 MS Windows Production PCA 2011 ThinkPad Product CA 2012 Hash: 14 e6 ... f4 36	MS UEFI CA 2011 MS Windows Production PCA 2011
dbx	Hash: 00 00 ... 00 00	MS Windows PCA 2010	Hash: 14 e6 ... f4 36	Hash: e3 b0 ... b8 55

Tabelle 1: Übersicht über die Zertifikatsspeicher (Namen und Hashes sind verkürzt dargestellt. Eine vollständige Darstellung ist in den Anhängen 7.2 bis 7.5 gegeben.)

5 Untersuchung der Installierbarkeit verschiedener Betriebssysteme (AP 5)

5.1 Einleitung

Im Folgenden wird untersucht inwieweit aktuelle Betriebssysteme unter Nutzung von Secure Boot auf den vorliegenden Hardwareplattformen betrieben werden können. Hierzu wird eine Testinstallation auf jeder der vier vorliegenden Hardwareplattformen durchgeführt und die hierzu notwendigen Schritte beschrieben. Es wird ferner überprüft, ob das System nach der Installation ordnungsgemäß startet und somit grundsätzlich funktionstüchtig ist. Eine vollständige Kompatibilitätsprüfung der Betriebssysteme mit allen Hardwarekomponenten wird nicht durchgeführt.

Sofern das jeweilige Betriebssystem Secure Boot unterstützt, wird dessen Umsetzung analysiert. Ist eine Unterstützung von Secure Boot nicht gegeben, so werden zusätzliche Schritte beschrieben, die das System bei aktivem Secure Boot einsetzbar machen. Hierbei steht die Funktionstüchtigkeit im Vordergrund. Eine mögliche Vorgehensweise zur Härtung im Zusammenhang mit Secure Boot wird am Beispiel des Betriebssystems Debian 7.1.0 in Abschnitt 6.3.1 erläutert.

Die getesteten Betriebssysteme sind:

- Microsoft Windows 8 Pro
- Red Hat Enterprise Linux 6.4
- Ubuntu 13.04
- Debian 7.1.0
- Fedora 19

5.2 Vorbereitungsschritte, Installation, Funktion von Microsoft Windows 8 Pro (AP 5.1)

5.2.1 Microsoft Windows 8 Pro

Windows 8 ist das, zum Zeitpunkt der Erstellung dieser Arbeit, aktuellste Betriebssystem von Microsoft. Eine der wesentlichen Neuerungen ist die Unterstützung von UEFI und Secure Boot.

Es existieren vier verschiedene Editionen von Windows 8:

- Windows 8: Ausgelegt für Heimanwender
- Windows 8 Pro: Erweiterter Funktionsumfang für Unternehmen
- Windows 8 Enterprise: Voller Funktionsumfang für Unternehmen
- Windows RT: Für ARM-Prozessoren ausgelegte Version

Alle Editionen, mit Ausnahme von Windows RT, sind für Intel-kompatible Prozessoren mit 32-Bit als auch mit 64-Bit erhältlich. Im Rahmen dieser Arbeit wird Windows 8 Pro auf einem 64-Bit-Prozessor verwendet.

5.2.2 Ausgangssituation

Die im Folgenden beschriebene Installation erfolgt, nachdem das jeweilige Gerät über das UEFI-Setup auf seine Defaultwerte zurückgesetzt und das Standardschlüsselmaterial installiert ist. Ferner wird sichergestellt, dass die UEFI-Firmware ausschließlich im EFI-Modus bootet. Auch werden vor der Installation alle evtl. bestehenden Festplattenpartitionen entfernt.

5.2.3 Vorbereitung

Für die Plattformen von HP und Dell müssen Treiber für die Intel Rapid-Storage-Technik[2] auf einem Wechseldatenträger für die Installation bereitgehalten werden, damit die Installationsroutine auf die Festplatte zugreifen kann. Selbstentpackende Archive, die den Treiber enthalten, sind auf den Webseiten des jeweiligen Herstellers[3] zu beziehen.

Weitere Vorbereitungsschritte sind nicht notwendig. Insbesondere ist Secure Boot während des Installationsvorgangs aktiviert.

5.2.4 Installation

Die Installation von Windows 8 Pro erfolgt auf der HP-, Lenovo- und der Dell-Plattform über ein offizielles DVD-Installationsmedium (de_windows_8_x64_dvd_915409.iso). Für die Medion-Plattform wird das von Medion mitgelieferte Windows 8-Installationsmedium genutzt, da notwendige Treiber nicht in anderer Form zur Verfügung stehen.

Sofern die jeweilige Hardwareplattform kein eingebautes DVD-Laufwerk besitzt, wird ein externes Laufwerk über USB genutzt.

2 http://www.intel.com/p/de_DE/support/highlights/sftwr-prod/imsm

3 Die Treiber stehen unter der URI http://h10025.www1.hp.com/ewfrf/wc/softwareDownloadIndex?softwareitem=ob-112529-1&cc=us&dlc=en&lc=en&os=4132&product=5375651&sw_lang= bzw. http://www.dell.com/support/drivers/de/de/dedhs1/DriverDetails/Product/latitude-3330-laptop?driverId=X50R1&osCode=W864&fileId=3176126447&languageCode=DE&categoryId=SA zur Verfügung.

Im Folgenden werden die Eingaben des jeweiligen Installationsschrittes aufgelistet.

- Windows Setup:
  - Installationssprache: Deutsch (Deutschland)
  - Uhrzeit und Währungsformat: Deutsch (Deutschland)
  - Tastatur oder Eingabemethode: Deutsch
- Lizenzbedingungen: „Ich akzeptiere die Lizenzbedingungen“ ausgewählt
- Wählen Sie eine Installationsart aus: „Benutzerdefiniert: nur Windows installieren (...)“ ausgewählt
- Wo möchten Sie Windows installieren: Erste Festplatte ausgewählt
  (Bei den Plattformen von HP und Dell ist hier ein Nachladen von SATA-Treibern von einem Wechselmedium erforderlich, um die Festplatte auswählen zu können)

Nach einem Neustart wird die Einrichtung des Systems wie folgt fortgesetzt:

- Anpassen: Name des PCs: win8
- Funk: „Später mit einem Funknetzwerk verbinden“ ausgewählt
- Einstellungen: „Express-Einstellungen verwenden“ ausgewählt
- Am PC anmelden: „Ohne Microsoft-Konto anmelden“ ausgewählt
- Am PC anmelden: „Lokales Konto“ ausgewählt
- Am PC anmelden:
  - Benutzernamen: user
  - Kennwort: kennwort
  - Kennwort erneut eingeben: kennwort
  - Kennworthinweis: trownnek

5.2.5 Funktionsweise

Grundlage des Betriebs von Windows 8 Pro bei aktiviertem Secure Boot ist die Signierung des Bootloaders, des Betriebssystemkerns sowie der Systemtreiber und Systemdateien.[4]

Die Verifikation weiterer Kernelkomponenten, wie z.B. Treibern, wird grundsätzlich im Zusammenspiel mit einem Anti-Malware-Produkt, wie z.B. dem mit Windows 8 Pro automatisch installierten Microsoft Defender, durchgeführt. Damit dieses Vorgehen effektiv sein kann, muss die Anti-Malware-Anwendung gestartet werden, bevor eine evtl. vorhandene Schadsoftware in den Kernel eingedrungen ist. Anderenfalls wäre es der Schadsoftware möglich, die korrekte Ausführung des Anti-Malware-Produktes zu verhindern und somit dessen Schutzfunktion zu unterwandern.

Um das Laden von schadhaftem Code vor Aktivierung des Anti-Malware-Produktes zu verhindern, hat Microsoft die „Early Launch Anti-Malware“-Technik (ELAM) in Windows 8 eingeführt. Diese stellt Herstellern von Anti-Malware-Produkten Schnittstellen bereit, mittels derer Treiber während des Bootvorgangs verifiziert werden können. Hierzu werden vom jeweiligen Softwarehersteller sogenannte ELAM-Treiber entwickelt. Diese werden während des Bootprozesses vor Treibern von Drittanbietern geladen und dienen dazu diese zu verifizieren. Somit ist den Herstellern von Anti-Malware-Produkten eine Möglichkeit gegeben, Code vor evtl. vorhandener Schadsoftware zur Ausführung zu bringen.

Die Effektivität dieser Lösung beruht somit auf der Identifizierung von Schadcode in einem sehr frühen Stadium des Bootvorgangs. Aufgrund dieses frühen Stadiums sind die dem ELAM-Treiber zur Verfügung

4 Quelle: http://technet.microsoft.com/en-us/windows/dn168167.aspx

stehenden Möglichkeiten stark begrenzt. Insbesondere ist der Zugriff auf das Dateisystem zur eingehenden Untersuchung des zu verifizierenden Treibers nicht möglich. Zur Verfügung stehen hingegen Informationen bzgl. einer evtl. vorhandenen Signierung des zu verifizierenden Treibers. Darüber hinaus ist der Name der Binärdatei des zu prüfenden Treibers sowie eines Hashes dieser Datei ermittelbar.

Um aufbauend auf diesen Informationen eine Beurteilung des zu verifizierenden Treibers durchführen zu können, hat der ELAM-Treiber eingeschränkte Zugriffsmöglichkeit auf die Windows-Registrierung. Diese kann somit als Datenbank genutzt werden um Erkenntnisse, die zuvor von der Anti-Malware-Lösung im Userspace gewonnen wurden, als Grundlage der Beurteilung zu nutzen. Beispielsweise kann das Anti-Malware-Produkt einen als Schädling erkannten Treiber entsprechend in der Registrierung vermerken und ihn durch den Hash der entsprechenden Binärdatei identifizierbar machen. Der zugehörige ELAM-Treiber kann bei nachfolgenden Bootvorgängen diesen somit erkennen und dessen Aktivierung verhindern.

ELAM-Treiber müssen zwingend von Microsoft signiert sein.

5.2.6 Zusammenfassung

Windows 8 Pro lässt sich auf allen untersuchten Hardwareplattformen installieren und betreiben. Bei den Plattformen von HP, Dell und Medion ist hierzu jedoch die Bereitstellung eines Treibers für den SATA-Controller notwendig. Dieser kann im Fall von HP und Dell auf deren Webseiten gefunden werden. Die Medion-Plattform kann durch das beigelegte Windows 8-Installationsmedium eingerichtet werden.

Die Verifikationskette bei Einsatz von Secure Boot umfasst laut Microsoft den Bootloader, den Kernel, grundlegend zum Betriebssystem gehörende und von Microsoft ausgelieferte System-Treiber und -Dateien als auch alle ELAM-Treiber.

Die Verifikation weiterer Treiber, die im Kernel ausgeführt werden sollen, erfolgt zusammen mit einem Anti-Malware-Produkt, z.B. dem vorinstallierten Microsoft Defender. Der Schutz des Kernels vor Kompromittierung hängt daher im besonderen Maße von dem Vorhandensein und der Qualität eines Anti-Malware-Produktes ab. Aufgrund der großen Anzahl verschiedener Produkte und deren zumeist sehr komplexen Funktionsweise ist eine Abschätzung der Effektivität des von Windows 8 Pro gebotenen Schutzes des Kernels vor Kompromittierung nicht ohne Weiteres möglich.

Auch ist eine Einschätzung der Sicherheitsaspekte der zu Grunde liegenden ELAM-Technik nicht trivial. Insbesondere die Tatsache, dass zur Identifizierung von Schadcode auf grundsätzlich nicht verifizierte Informationsquellen, wie z.B. die Windows-Registrierung, zurückgegriffen wird, ist kritisch zu sehen.

Abschließend lässt sich daher sagen, dass der Betrieb von Windows 8 Pro mit Secure Boot auf allen untersuchten Hardwareplattformen problemlos möglich ist. Die Effektivität der Schutzfunktionen vor Kompromittierung des Kernels hängt dabei im hohen Maße von dem eingesetzten Anti-Malware-Produkt ab. Eine abschließende Beurteilung über die Effektivität der eingesetzten Sicherheitsfunktionen bzgl. des Schutzes des Kernels vor Kompromittierung ist im Rahmen dieser Arbeit nicht möglich.

5.3 Vorbereitungsschritte, Installation, Funktion von Red Hat Enterprise Linux (AP 5.2)

5.3.1 Red Hat Enterprise Linux

Red Hat Enterprise Linux (RHEL) ist eine von der Firma Red Hat erstellte Linux-Distribution. Der primäre Fokus bei deren Entwicklung liegt auf dem professionellen Einsatz in Unternehmen. Red Hat garantiert u.a. innerhalb einer Dauer von bis zu zehn Jahren nach Erscheinen einer Version in unterschiedlichem Umfang die Bereitstellung von Updates. Enterprise Linux wird ausschließlich in Zusammenhang mit einem Supportvertrag vertrieben.

Die dieser Untersuchung zugrunde liegende und zum Zeitpunkt der Erstellung aktuelle Version von Red Hat Enterprise Linux ist 6.4. Wenngleich Red Hat eine zukünftige Unterstützung von Secure Boot vorsieht[5], so ist diese zur Zeit noch nicht gegeben. Dies bedeutet insbesondere, dass kein von Microsoft signierter Bootloader bereitgestellt wird.

Um Red Hat Enterprise Linux 6.4 dennoch mit aktiviertem Secure Boot, unter Nutzung des auf den untersuchten Hardwareplattformen standardmäßig ausgelieferten Schlüsselmaterials zu betreiben, sind daher einige Anpassungen notwendig. Den Kern dieser Anpassungen stellt der Bootloader Shim[6] in Version 0.2 dar. Eine kurze Einführung zu Shim gibt Abschnitt 2.3.2.

Im Folgenden wird u.a. festgehalten wie Shim installiert werden kann, damit Red Hat Enterprise Linux 6.4 bei aktivem Secure Boot einsatzfähig ist. Hierbei liegt der Fokus auf der Funktionsfähigkeit des Systems. Eine weitergehende Betrachtung bzgl. der Härtung eines Linux Systems in Zusammenhang mit Secure Boot wird in Kapitel 6.3.1 am Beispiel der Linux-Distribution Debian 7.1.0 durchgeführt.

5.3.2 Ausgangssituation

Die im Folgenden beschriebene Installation erfolgt, nachdem das jeweilige Gerät über das UEFI-Setup auf seine Defaultwerte zurückgesetzt und das Standardschlüsselmaterial installiert ist. Ferner wird sichergestellt, dass die UEFI-Firmware ausschließlich im EFI-Modus bootet. Auch werden vor der Installation alle evtl. bestehenden Festplattenpartitionen entfernt.

5.3.3 Vorbereitung

Da der Installationsprozess von Red Hat Enterprise Linux den Secure Boot nicht unterstützt und daher bei aktiviertem Secure Boot nicht ohne Weiteres ausgeführt werden kann, wird Secure Boot vor dem Beginn der Installation deaktiviert.

5.3.4 Installation

5.3.4.1 Installation von Red Hat Enterprise Linux

Die Installation von Red Hat Enterprise Linux 6.4 (Santiago) erfolgt über das offizielle DVD-Installationsmedium (rhel-server-6.4-x86_64-dvd.iso). Enterprise Linux wird in deutscher Sprache mit dem Softwarepaket „Desktop“ installiert. Die im Folgenden aufgeführten Installationsschritte beschreiben

5 http://www.redhat.com/about/news/archive/2012/6/uefi-secure-boot
6 http://www.codon.org.uk/~mjg59/shim-signed/

den Installationsprozess von Red Hat Enterprise Linux 6.4, der den weiteren Abschnitten zugrunde liegt. Sie entsprechen den typischen Schritten zur Installation von Red Hat Enterprise Linux 6.4 auf einem Desktop und beinhalten keinerlei spezifische Anpassung auf die jeweilige Hardwareplattform oder für den Einsatz mit Secure Boot. Sofern die jeweilige Hardwareplattform kein eingebautes DVD-Laufwerk besitzt, wird ein externes Laufwerk mittels USB genutzt.

Gestartet wird die Installation durch Auswahl des Eintrags „Red Hat Enterprise Linux 6.4“ im Bootmenü des Installationsmediums. Im Folgenden werden die Eingaben des jeweiligen Installationsschrittes aufgelistet.

- Disc Found: Media Test: Skip
- What language would you like to use during the installation process?: German/Deutsch
- Wählen Sie die passende Tastatur für Ihr System: Deutsch (latin1 ohne 'tote' Tasten/Akzente)
- Welche Gerätetypen umfasst Ihre Installation?: „Basis-Speichergeräte“ ausgewählt
- Bitte vergeben Sie einen Namen für den Computer:
  - Rechnername: rhel
- Bitte wählen Sie die nächstgelegene Stadt in Ihrer Zeitzone: Europa/Berlin
  - „System verwendet UTC (koordinierte Weltzeit)“ ausgewählt
- 'root' ist das Konto für die Systemverwaltung. Geben Sie ein Passwort für den Benutzer 'root' ein.:
  - root-Passwort: kennwort
  - Bestätigen: kennwort
- Schwaches Kennwort: Dennoch verwenden
- Welche Art von Installation bevorzugen Sie?:
  - „Gesamten Platz verwenden“ ausgewählt
  - „System verschlüsseln“ nicht ausgewählt
  - „Partitions-Layout noch einmal überprüfen und ändern“: nicht ausgewählt
- Schreibe Partitionierung auf die Festplatte: Änderungen auf Festplatte schreiben
- Die Standard-Installation von Red Hat Enterprise Linux ist eine grundlegende Server-Installation.
  - Sie können jetzt optional ein anderes Software-Set wählen: „Desktop“ ausgewählt
  - Bitte wählen Sie alle zusätzlichen Repositories, die Sie für die Softwareinstallation verwenden möchten: „Red Hat Enterprise Linux“ ausgewählt, alle anderen Unterpunkte nicht ausgewählt
  - Sie können die Software-Auswahl jetzt weiter anpassen oder nach Fertigstellung der Installation via Software-Verwaltung-Anwendung: „Später anpassen“ ausgewählt

Nachdem die eigentliche Installation abgeschlossen ist, wird das System neu gestartet und dessen Einrichtung im Zuge des „First Boot“-Vorgangs fortgesetzt.

- Lizenz-Informationen: Ja, ich stimme der Lizenzerklärung zu
- Benutzer erstellen:
  - Benutzername: user
  - Vollständiger Name: user
  - Passwort: kennwort
  - Passwort bestätigen: kennwort

- Datum und Uhrzeit: Aktuelles Datum und aktuelle Zeit
- Kdump:
  - „Kdump aktivieren?“ ausgewählt
  - Kdump-Speicher (MB): 128
  - Advanced kdump configuration: unverändert beibehalten
  - Die abschließende Abfrage bzgl. eines Neustarts des Systems mit ja beantwortet

Abschließend wird das Software-Repository, welches sich auf der Installations-DVD befindet, eingebunden. Hierzu wird die folgende Zeile an die Datei /etc/fstab angehängt:

```
/dev/scd0 /media/dvd udf,iso9660 user,noauto 0 0
```

Ferner wird die Datei /etc/yum.repos.d/rhel-dvd.repo mit folgendem Inhalt erzeugt:

```
[rhel-dvd]
name=Red Hat Enterprise Linux $releasever - $basearch - DVD
baseurl=file:///media/dvd
enabled=1
gpgcheck=0
```

Nach dem Erstellen des Verzeichnisses /media/dvd durch den Aufruf von „mkdir /media/dvd“ und dem Einhängen der Installations-DVD durch den Befehl „mount /media/dvd“ steht das Repository für Softwareinstallationen zur Verfügung.

Die Installation von Red Hat Enterprise Linux 6.4 ist auf allen vier untersuchten Hardwareplattformen bei deaktiviertem Secure Boot durchführbar.[7]

5.3.4.2 Installation von Shim und des Secure-Boot-Preloaders

Zur Installation von Shim muss schreibend auf die EFI-Partition des Systems zugegriffen werden. Aus diesem Grund müssen die nachfolgenden Schritte mit Root-Rechten durchgeführt werden. Die EFI-Partition wird von Red Hat Enterprise Linux 6.4 standardmäßig im Verzeichnis /boot/efi eingebunden.

Nach dem Herunterladen des Archivs shim-signed.tgz[8] und dessen Extraktion werden die beiden enthaltenen Dateien, shim.efi und MokManager.efi in das zu erstellende Verzeichnis /boot/efi/EFI/redhat/shim kopiert. Die Datei shim.efi enthält den eigentlichen Bootloader Shim und ist von Microsoft mittels des Zertifikats „Microsoft Corporation UEFI CA 2011“ (Seriennr.: 61:08:d3:c4:00:00:00:00:00:04) signiert. Shim startet nach dessen Verifizierung durch die UEFI-Firmware einen weiteren Bootloader. Problematisch an dieser Verifizierung ist, dass bei einer Änderung der Binärdatei des zweiten Bootloaders, z.B. im Rahmen eines Updates, dessen Signatur bzw. Hash ungültig und der Bootvorgang somit funktionsuntüchtig wird.

Aus diesem Grund empfiehlt es sich, nicht direkt den durch die Installation des Betriebssystems konfigurierten Bootloader, sondern einen weiteren auf Grub2 basierenden Bootloader, im Folgenden Secure-Boot-Preloader genannt, zu starten.[9] Dieser ruft, ohne eine weitere Verifizierung, den eigentlichen Bootloader des Systems auf. Hiermit sind Änderungen sowohl der Konfiguration als auch der Binärdateien des von Red Hat Enterprise Linux installierten und verwalteten Bootloaders möglich, ohne die

7 Die Touch-Funktion des Bildschirms steht jedoch auf der HP- wie auch auf der Lenovo-Plattform, mutmaßlich aufgrund fehlender Treiber im Kernel nicht zur Verfügung. Ferner funktioniert das Mousepad während der Installation nicht. Im Betrieb ist es funktionstüchtig.

8 http://www.codon.org.uk/~mjg59/shim-signed/shim-signed.tgz

9 Ein weiterer Grund für die Nutzung eines vorgelagerten Bootloaders, ist der Umstand, dass sich der bei der Betriebssysteminstallation eingerichtete Bootloader nicht zuverlässig entsprechend den UEFI-Vorgaben signieren oder hashen lässt. Der Grund hierfür ist mutmaßlich eine fehlerhafte Erstellung der Binärdatei.

ordnungsgemäße Ausführung des Bootvorganges zu verhindern. Die Erstellung des Secure-Boot-Preloaders erfolgt hierbei anhand des Quellcodes von Grub2.

Damit Shim von der UEFI-Firmware gestartet wird, wird ein entsprechender UEFI-Booteintrag erstellt. Dies kann z.B. durch die Anwendung efibootmgr erfolgen. Nach der Erstellung eines solchen Eintrags kann Shim durch die UEFI-Firmware gestartet werden und führt seinerseits unverzüglich den Secure-Boot-Preloader aus. Im Fehlerfall, z.B. auf Grund einer fehlgeschlagenen Verifizierung des Secure-Boot-Preloaders durch Shim, wird statt dessen der MokManager gestartet. Der MokManager ist in der Datei MokManager.efi enthalten und dient zum interaktiven Hinzufügen von Zertifikaten oder Hashes in die MokList während des Bootprozesses.

Die im Folgenden aufgeführte Liste beinhaltet die notwendigen Befehle zur Nutzung von Secure Boot. Alle Befehle sind durch den Benutzer root in seiner Login-Shell auszuführen. Ferner wird davon ausgegangen, dass das System wie im vorherigen Abschnitt beschrieben, installiert ist.

```
# Übersetzen von Grub2 und Erstellen des Secure-Boot-Preloaders.
cd /root
yum -y install automake make gcc bison flex
wget ftp://ftp.gnu.org/gnu/grub/grub-2.00.tar.gz
tar xzf grub-2.00.tar.gz
cd grub-2.00
./configure -with-platform=efi -target=amd64-pe
make
cat <<EOF > conf
echo "Secure-Boot-Preloader: starting grub2"
chainloader /EFI/redhat/grub.efi
boot
EOF
mkdir /boot/efi/EFI/redhat/shim
./grub-mkimage --format x86_64-efi --config conf --output
/boot/efi/EFI/redhat/shim/grubx64.efi normal echo fat part_gpt chain

# Installieren von Shim
cd /root
wget http://www.codon.org.uk/~mjg59/shim-signed/shim-signed.tgz
tar xzf shim-signed.tgz
cp shim-signed/shim.efi shim-signed/MokManager.efi /boot/efi/EFI/redhat/shim

# Eintragen von Shim ins UEFI-Bootmenü als höchstpriorisierten Eintrag
efibootmgr --create --label rhel-secure-boot --loader
\\EFI\\redhat\\shim\\shim.efi --disk /dev/sda --part 1
```

Soll der Bootvorgang anhand von Hashes durchgeführt werden, so wird der abschließende Einrichtungsschritt über den MokManager vollzogen. Hierzu wird das System neu gebootet und über das UEFI-Setup Secure Boot aktiviert. Daraufhin startet Shim und versucht seinerseits den Secure-Boot-Preloader zu verifizieren. Da die MokList jedoch keinen dazu geeigneten Eintrag enthält und die Verifizierung fehlschlägt, startet Shim den MokManager. Dort wird über den Menüeintrag „Enroll hash from disk“ die Datei grubx64.efi im Verzeichnis /EFI/redhat/shim ausgewählt. Hierdurch erstellt Shim einen Hash des Secure-Boot-Preloaders und fügt diesen in die MokList hinzu. In einem erneuten Bootvorgang[10] kann der Secure-Boot-Preloader nun erfolgreich durch Shim geladen und somit das Linux-System gebootet werden. Die nachfolgenden Schritte zur Signierung der Bootloader-Datei können bei Nutzung eines Hashes entfallen.

10 Hierbei ist zu beachten das die Auswahl des Menüpunkt „Continue Boot“ nicht zum Ziel führt. Der Bootprozess ist gänzlich neu zu initialisieren, z.B. durch Drücken der Tastenkombination Ctrl-Alt-Del.

5.3.4.3 Installation der sbsigntools

Soll eine Verifizierung des Secure-Boot-Preloaders nicht anhand eines Hashes sondern durch ein Zertifikat erfolgen, so muss die Binärdatei des Bootloaders signiert werden. Dies kann durch die Werkzeugsammlung sbsigntools[11] erfolgen, welche jedoch nicht Bestandteil von Red Hat Enterprise Linux 6.4 ist.

Die im Folgenden aufgeführte Liste beinhaltet die notwendigen Befehle zur Installation der sbsigntools aus deren Sourcecode. Alle Befehle sind durch den Benutzer root in seiner Login-Shell auszuführen. Ferner wird davon ausgegangen, dass das System, wie im vorherigen Abschnitt beschrieben, installiert ist.

```
yum –y install automake make gcc binutils-devel openssl-devel libuuid-devel git

# Download, Übersetzung und Installation von help2man
cd /root
wget 'http://ftp.gnu.org/gnu/help2man/help2man-1.43.3.tar.gz'
tar xzf help2man-1.43.3.tar.gz
cd help2man-1.43.3
./configure && make && make install

cd /root
git clone git://kernel.ubuntu.com/jk/sbsigntool
cd sbsigntool
# Mit dem folgenden optionalen Befehl kann die Version der sbigntools geladen
# werden, die diesem Dokument zu Grunde liegt.
#git checkout 951ee95a301674c046f55330cd7460e1314deff2

# Entfernen unnötiger Bestandteile der sbsigntools
sed –i 's/^man1_MANS.*/man1_MANS = sbsign.1 sbverify.1 sbattach.1/'
docs/Makefile.am
sed –i 's/^bin_PROGRAMS.*/bin_PROGRAMS = sbsign sbverify sbattach/'
src/Makefile.am

./autogen.sh && ./configure && make && make install
```

5.3.4.4 Signierung des Bootloaders

Voraussetzung für die Signierung mittels der sbsigntools ist das Vorliegen eines X509-Zertifikats im PEM-Format und des dazugehörigen privaten Schlüssels.

Durch die Anwendung sbsign, die Teil der sbsigntools ist, kann der Secure-Boot-Preloader, der in der Datei /boot/efi/EFI/redhat/shim/grubx64.efi gespeichert ist, signiert werden. Für den Import des Zertifikats in die MokList durch den MokManager muss dieses Zertifikat im DER-Format auf der EFI-Partition vorliegen.

Im Folgenden wird gezeigt wie die Signierung durch ein selbstsigniertes Zertifikat erfolgt. Hierbei ist zu beachten, dass das gezeigte Vorgehen ausschließlich Demonstrations- und Testzwecken dient. Es wird insbesondere darauf hingewiesen, dass die Speicherung des privaten Schlüssels auf dem betroffenen System erhebliche Sicherheitsrisiken birgt. Verfügt ein Angreifer oder eine Schadsoftware über die notwendigen Rechte um den Bootloader auszutauschen, so hat sie i.d.R. ebenfalls die Rechte einen lokal gespeicherten Schlüssel auszulesen und mit ihm eine Signierung eines kompromittierten Bootloaders durchzuführen und somit den Secure Boot-Mechanismus zu unterwandern. Auch kann das hier aufgeführte Vorgehen zur Erstellung von selbstsignierten Zertifikaten keineswegs die für den Aufbau einer sicheren Public-Key-Infrastruktur (PKI) notwendigen Prozesse ersetzen.

Alle Befehle sind durch den Benutzer root in seiner Login-Shell auszuführen. Ferner wird davon ausgegangen, dass das System, wie im vorherigen Abschnitt beschrieben, installiert ist und die Schritte des Abschnitts 5.3.4.3 durchgeführt sind.

11 https://launchpad.net/ubuntu/+source/sbsigntool

```
mkdir /root/cert
cd /root/cert

# Erstellen eines selbstsignierten Zertifikats. Die sbsigntools benötigen das
# Zertifikat im PEM-Format. Daten bzgl. des Zertifikats werden interaktiv
# abgefragt.
openssl req -new -x509 -newkey rsa:2048 -keyout signing.key -out signing.pem.crt
-outform pem -days 365 -nodes -sha256

# Signieren der Bootloader-Datei.
sbsign --key signing.key --cert signing.pem.crt --output
/boot/efi/EFI/redhat/grubx64.efi /boot/efi/EFI/redhat/grubx64.efi
# Optionale Überprüfung des Signierungsvorgangs
sbverify --cert signing.pem.crt /boot/efi/EFI/redhat/grubx64.efi

# Konvertieren des Zertifikats, da der MokManager dieses im DER-Format benötigt.
openssl x509 -in signing.pem.crt -inform pem -out signing.der.crt -outform der
# Kopieren des Zertifikats auf die EFI-Partition, damit dieses vom MokManager
# ausgelesen werden kann
cp signing.der.crt /boot/efi
```

Im Anschluss hieran wird das System neu gebootet und über das UEFI-Setup Secure Boot aktiviert. Da Shim die Verifizierung des Secure-Boot-Preloaders aufgrund einer leeren MokList misslingt, startet es den MokManager. Hier kann nun über den Menüpunkt „Enroll key from disk“ das zuvor auf die EFI-Partition kopierte Zertifikat ausgelesen und in die MokList aufgenommen werden. Hiernach ist Shim in der Lage, die Binärdatei des Secure-Boot-Preloader während des Bootvorgangs zu verifizieren. Somit ist der Bootvorgang funktionstüchtig.

5.3.5 Funktionsweise

Das hier gezeigte Vorgehen ermöglicht den Betrieb von Red Hat Enterprise Linux 6.4 bei aktiviertem Secure Boot durch die nachträgliche Installation des Bootloader Shim. Dieser wird in einer durch Microsoft mittels des Zertifikats „Microsoft Corporation UEFI CA 2011“ (Seriennr.: 61:08:d3:c4:00:00:00:00:00:04) signierten Form nach dem Installationsvorgang des Betriebssystems installiert. Shim startet seinerseits den Secure-Boot-Preloader, ein manuell eingerichteter monolithischer Bootloader basierend auf Grub2. Dieser dient als Zwischenglied zwischen Shim und dem eigentlichen Bootloader des Systems, mit dem Zweck letzteren nicht signieren oder hashen zu müssen. Somit kann der Bootloader des Betriebssystems modifiziert werden, ohne dass der Bootvorgang funktionsuntüchtig wird. Der Secure-Boot-Preloader wird wahlweise durch einen Hash oder eine Signatur von Shim verifiziert und startet seinerseits den eigentlichen Bootloader des Systems ohne Verifizierung.

Die Verifikationskette der aufgeführten Methode umfasst somit lediglich den ersten Bootloader Shim und den Secure-Boot-Preloader. Eine Verifikation des Kernels, ebenso wie eine Überprüfung der Kernelmodule erfolgt nicht. Einem Angreifer ist es somit grundsätzlich möglich, Kernelmodule zur Laufzeit nachzuladen und somit beliebigen Code in den Kernel einzuschleusen, sofern er Root-Rechte besitzt. Code, der in Kernelmodulen enthalten ist, ist gleichberechtigt mit dem regulären Kernel-Code. Somit ist eine uneingeschränkte Kompromittierung des Kernels auf diesem Wege möglich.

5.3.6 Zusammenfassung

Red Hat Enterprise Linux 6.4 unterstützt Secure Boot nicht und kann ohne Modifikationen bei aktiviertem Secure Boot weder installiert noch betrieben werden. Sofern Secure Boot deaktiviert ist, lässt sich Red Hat Enterprise Linux 6.4 jedoch auf allen untersuchten Hardwareplattformen problemlos installieren und betreiben.

Ferner lässt sich Red Hat Enterprise Linux 6.4 mittels der nachträglichen Installation von Shim auch unter Einsatz von Secure Boot mit dem jeweiligen Standardschlüsselmaterial der untersuchten Hardwareplattformen betreiben. Das hierzu aufgezeigte Vorgehen umfasst jedoch nicht die Verifizierung des Betriebssystemkerns.

Abschließend lässt sich daher sagen, dass der Betrieb von Red Hat Enterprise Linux 6.4 mit Secure Boot auf allen untersuchten Hardwareplattformen mit relativ geringem Aufwand möglich ist. Die Nutzung von Secure Boot im Rahmen des aufgezeigten Vorgehens führt jedoch zu keinem signifikanten Sicherheitsgewinn.

5.4 Vorbereitungsschritte, Installation, Funktion von Ubuntu (AP 5.3)

5.4.1 Ubuntu

Ubuntu ist eine von der Ubuntu Foundation, primär unterstützt durch das Unternehmen Canonical[12], erstellte Linux-Distribution. Sie basiert auf der Linux-Distribution Debian und wird ihrerseits wiederum als Basis einer Reihe anderer Distributionen genutzt.

Der Einsatzbereich von Ubuntu umfasst sowohl die Nutzung als Desktop- als auch als Serversystem. Üblicherweise werden für Ubuntu für ca. ein Jahr nach Erscheinen der jeweiligen Version Patches bereitgestellt. Darüber hinaus werden in regelmäßigen Abständen Versionen veröffentlicht, für die eine Unterstützung durch Patches für mindestens fünf Jahre zugesagt wird.

Die dieser Untersuchung zugrunde liegende und zum Zeitpunkt der Erstellung aktuelle Version von Ubuntu ist 13.04 (Raring Ringtail). Ubuntu 13.04 unterstützt Secure Boot.

5.4.2 Ausgangssituation

Die im Folgenden beschriebene Installation erfolgt, nachdem das jeweilige Gerät über das UEFI-Setup auf seine Defaultwerte zurückgesetzt und das Standardschlüsselmaterial installiert ist. Ferner wird sichergestellt, dass die UEFI-Firmware ausschließlich im EFI-Modus bootet. Auch werden vor der Installation alle evtl. bestehenden Festplattenpartitionen entfernt.

5.4.3 Vorbereitung

Vorbereitungsschritte sind nicht notwendig. Insbesondere ist Secure Boot während des Installationsvorgangs aktiviert.

5.4.4 Installation

Die Installation von Ubuntu 13.04 erfolgt von einem USB-Stick, der mit der Desktopinstallationsversion von Ubuntu (ubuntu-13.04-desktop-amd64.iso[13]) bespielt ist.

Die im Folgenden aufgeführten Installationsschritte beschreiben den Installationsprozess von Ubuntu 13.04, der den weiteren Abschnitten zugrunde liegt. Hierbei wird das Installationsprogramm über das Live-Ubuntu-System des Installationsmediums gestartet.[14] Dieses wird über den Bootmenüeintrag „Try Ubuntu without installing“ gebootet. Im Anschluss wird das Installationsprogramm mittels des Icons „Install Ubuntu 13.04“ gestartet.

Alle weiteren Schritte entsprechen den typischen Schritten zur Installation von Ubuntu 13.04 und beinhalten keinerlei spezifische Anpassung auf die jeweilige Hardwareplattform oder für den Einsatz mit Secure Boot. Im Folgenden werden die gemachten Eingaben im jeweiligen Installationsschritt aufgelistet.

- Willkommen: Deutsch
- Installation von Ubuntu wird vorbereitet:

12 http://www.canonical.com

13 http://www.ubuntu.com/start-download?distro=desktop&bits=64&release=latest

14 Die Installation nicht direkt über das Bootmenü, sondern über das Live-System zu starten hat den Vorteil der einfacheren Analyse evtl. auftretender Fehler. Eine Installation direkt aus dem Bootmenü sollte analog zu den hier aufgeführten Schritten möglich sein.

    - Aktualisierungen während der Installation herunterladen: ausgewählt
    - Software von Drittanbeitern installieren: nicht ausgewählt
- Installationsart:
    - Festplatte löschen und Ubuntu installieren: ausgewählt
    - Die neue Ubuntu-Installation zur Sicherheit verschlüsseln: nicht ausgewählt
    - LVM für die neue Ubuntu-Installation benutzen: nicht ausgewählt
- Wo befinden Sie sich?: Berlin
- Tastaturbelegung: Deutsch/Deutsch
- Wer sind Sie?:
    - Ihr Name: user
    - Name Ihres Rechners: ubuntu
    - Wählen Sie einen Benutzernamen: user
    - Wählen Sie ein Passwort: kennwort
    - Passwort wiederholen: kennwort
    - Passwort zum Anmelden abfragen: ausgewählt
    - Meine persönlichen Dateien verschlüsseln: nicht ausgewählt

Die beschriebene Installation von Ubuntu 13.04 ist auf allen vier untersuchten Hardwareplattformen problemlos und ohne Besonderheiten durchführbar. Insbesondere kann sowohl die Installation als auch der Betrieb des Systems mit dem jeweiligen Standardschlüsselmaterial bei aktiviertem Secure Boot durchgeführt werden.

5.4.5 Funktionsweise

Ermöglicht wird der Betrieb von Ubuntu 13.04 bei aktiviertem Secure Boot durch den Bootloader Shim. Dieser wird, in einer durch Microsoft mittels des Zertifikats „Microsoft Corporation UEFI CA 2011“ (Seriennr.: 61:08:d3:c4:00:00:00:00:00:04) signierten Form, automatisch während des Installationsprozesses installiert. Als zweiter Bootloader wird Grub2 genutzt. Die Verifizierung von Grub2 durch Shim erfolgt mittels des fest in die Binärdatei von Shim integrierten Zertifikats „Canonical Ltd. Master Certificate Authority“ (Seriennr.: 13348991040521802343)[15].

Da Grub2, sofern Secure Boot aktiviert ist, von Ubuntu 13.04 in monolithischer Form installiert wird, entfällt die Verifizierung von Grub2-Modulen. Ferner wird bei aktiviertem Secure Boot ein Nachladen von Grub2-Modulen durch eine Quellcodeänderung an Grub2 im Rahmen des Ubuntu-Projektes verhindert.

Die Verifizierung des Kernels erfolgt mit demselbem Zertifikat. Hierzu delegiert Grub2 die Verifizierung zurück an Shim. Diese Delegation wird durch Modifikationen am Quelltext von Grub2 für den Einsatz mit Ubuntu ermöglicht.

Die Verifikation von Kernelmodulen wird durch den Kernel jedoch nur bedingt durchgeführt. Zwar wird beim Kompilieren des Kernels und seiner Module ein privater Schlüssel und ein zugehöriges Zertifikat erzeugt und genutzt, um die Module zu signieren. Auch werden diese Signaturen beim Laden von Modulen durch den Kernel mittels des in ihm eingebetteten Zertifikats überprüft und gegebenenfalls das Laden des Moduls verweigert. Der Kernel verhindert jedoch das Laden von unsignierten Modulen nicht.

15 Das vollständige Zertifikat ist in Anhang 7.10 aufgeführt.

Somit ist ein Nachladen von beliebigem Code in den Kernel zur Laufzeit möglich, sofern der durchführende Benutzer Root-Rechte besitzt.[16]

5.4.6 Zusammenfassung

Ubuntu 13.04 lässt sich ohne Probleme und ohne Vorbereitungsschritte auf allen untersuchten Hardwareplattformen installieren und betreiben. Sowohl die Installation als auch der Betrieb können bei aktiviertem Secure Boot mit dem jeweiligen Standardschlüsselmaterial durchgeführt werden.

Die Verifikationskette umfasst hierbei den ersten Bootloader Shim, den zweiten Bootloader Grub2 und den Linux-Kernel. Wenngleich eine Verifikation von Grub2 durch Shim, als auch des Linux-Kernels durch Grub2 erfolgt, so fehlt eine effektive Verifizierung von Kernelmodulen gegenüber dem Kernel. Somit ist es einem Angreifer mit Root-Rechten möglich, mittels des Standardladevorgangs für Kernelmodule beliebigen Code in den Kernel einzuschleusen und das System hierdurch zu kompromittieren.

Abschließend lässt sich daher sagen, dass der Betrieb von Ubuntu 13.04 mit Secure Boot auf allen untersuchten Hardwareplattformen problemlos möglich ist. Die Nutzung von Secure Boot führt jedoch ohne weitere Anpassungen des Betriebssystems zu keinem signifikanten Sicherheitsgewinn.

16 Das Laden von unsignierten Modulen kann durch das Setzen der Bootoption module.sig_enforce oder durch die Kompilieroption CONFIG_MODULE_SIG_FORCE verhindert werden. Die erste Möglichkeit bedingt eine Änderung der Konfiguration von Grub. Da die entsprechende Konfigurationsdatei jedoch nicht durch Secure Boot geschützt wird ist es einem Angreifer mit Root-Rechten möglich diese zurückzusetzen und durch einen Neustart des Systems die Verifikation unsignierter Module wieder zu deaktivieren. Die zweite Möglichkeit bedingt eine erneute Übersetzung des Kernels und damit auch eine erneute Signierung.

5.5 Vorbereitungsschritte, Installation, Funktion von Debian (AP 5.4)

5.5.1 Debian

Debian ist eine durch das Debian-Projekt gemeinschaftlich entwickelte Linux-Distribution. Besonderes Merkmal hierbei ist die konsequente Verpflichtung zur Nutzung freier Software durch die „Richtlinien für freie Software“ des Debian-Projektes[17]. Debian dient als Grundlage einer Reihe weiterer Linux-Distributionen, wie z.B. für Ubuntu.

Die dieser Untersuchung zugrunde liegende und zum Zeitpunkt der Erstellung aktuelle Version von Debian ist 7.1.0 (Wheezy). Aufgrund von Konflikten des Secure Boot-Mechanismus mit den „Richtlinien für freie Software“ wird Secure Boot nicht unterstützt. Dies bedeutet insbesondere, dass Debian keinen von Microsoft signierten Bootloader bereitstellt. Ebenso ist eine zukünftige Bereitstellung unwahrscheinlich.

Um Debian 7.1.0 dennoch mit aktiviertem Secure Boot, unter Nutzung des auf den untersuchten Hardwareplattformen standardmäßig ausgelieferten Schlüsselmaterials zu betreiben, sind daher einige Anpassungen notwendig. Den Kern dieser Anpassungen stellt der Bootloader Shim[18] in Version 0.2 dar. Eine kurze Einführung zu Shim gibt Abschnitt 2.3.2.

Im Folgenden wird u.a. festgehalten wie Shim installiert werden kann, damit Debian 7.1.0 bei aktivem Secure Boot einsatzfähig ist. Hierbei liegt der Fokus auf der Funktionsfähigkeit des Systems. Eine weitergehende Betrachtung bzgl. der Härtung des Systems in Zusammenhang mit Secure Boot wird in Kapitel 6.3.1 durchgeführt.

5.5.2 Ausgangssituation

Die im Folgenden beschriebene Installation erfolgt, nachdem das jeweilige Gerät über das UEFI-Setup auf seine Defaultwerte zurückgesetzt und das Standardschlüsselmaterial installiert ist. Ferner wird sichergestellt, dass die UEFI-Firmware ausschließlich im EFI-Modus bootet. Auch werden vor der Installation alle evtl. bestehenden Festplattenpartitionen entfernt.

5.5.3 Vorbereitung

Da der Installationsprozess von Debian 7.1.0 bei aktivem Secure Boot auf Grund fehlender Unterstützung nicht ohne Weiteres ausgeführt werden kann, wird Secure Boot vor dem Beginn der Installation deaktiviert.

5.5.4 Installation

5.5.4.1 Installation von Debian

Die Installation von Debian 7.1.0 erfolgt von einem USB-Stick, der mit der Netzwerkinstallationsversion von Debian (debian-7.1.0-amd64-netinst.iso) bespielt ist.

Es wird eine Standardinstallation von Debian 7.1.0 in deutscher Sprache durchgeführt. Die installierten Softwarepakete sind: Debian desktop environment, Laptop, Standard-Systemwerkzeuge.

17 http://www.debian.org/social_contract.de.html#guidelines
18 http://www.codon.org.uk/~mjg59/shim-signed/

Die im Folgenden aufgeführten Installationsschritte beschreiben den Installationsprozess von Debian 7.1.0, der den weiteren Abschnitten zugrunde liegt. Sie entsprechen den typischen Schritten zur Installation von Debian 7.1.0 und beinhalten keinerlei spezifische Anpassung auf die jeweilige Hardwareplattform oder für den Einsatz mit Secure Boot.

- Im Bootmenü den Menüpunkt „Install“ ausgewählt
- Select a language: German
- Auswahl des Standortes: Deutschland
- Tastatur konfigurieren: Deutsch
- Netzwerk-Hardware erkennen - Fehlende Firmware von Wechseldatenträger laden?: Nein
- Netzwerk einrichten: „DNS-Server-Adresse eingegeben“: 8.8.8.8
- Netzwerk einrichten - Rechnername: debian
- Netzwerk einrichten - Domain-Name: *leergelassen*
- Benutzer und Passwörter einrichten - Root-Passwort: kennwort
- Benutzer und Passwörter einrichten - Bestätigung: kennwort
- Benutzer und Passwörter einrichten - Vollständiger Name des Benutzers: user
- Benutzer und Passwörter einrichten - Benutzername für Ihr Konto: user
- Benutzer und Passwörter einrichten - Passwort: kennwort
- Benutzer und Passwörter einrichten - Bestätigung: kennwort
- Festplatte partitionieren - Partitionsmethode: Geführt – vollständige Festplatte verwenden
- Festplatte partitionieren - zu partitionierende Festplatte: Auswahl der (ersten) Festplatte
- Festplatte partitionieren - Partitionsschema: Alle Dateien auf eine Partition [...]
- Festplatte partitionieren: Partitionierung beenden und Änderungen übernehmen
- Festplatte partitionieren - Änderungen auf Festplatte schreiben?: Ja
- Paketmanager konfigurieren - Land des Debian-Archiv-Spiegelservers: Deutschland
- Paketmanager konfigurieren - Debian-Archiv-Spiegelserver: ftp.de.debian.org
- Paketmanager konfigurieren - HTTP-Proxy-Daten: *leergelassen*
- Konfiguration popularity-contest - An der Paketverwaltung teilnehmen?: Nein
- Softwareauswahl - Welche Software soll installiert werden?: Debian desktop environment, Laptop, Standard-Systemwerkzeuge
- Installation abschließen - Installation abgeschlossen: Weiter

Die Installation von Debian 7.1.0 ist auf allen vier untersuchten Hardwareplattformen bei deaktiviertem Secure Boot problemlos und ohne Besonderheiten durchführbar.

5.5.4.2 Installation von Shim und des Secure-Boot-Preloaders

Zur Installation von Shim muss schreibend auf die EFI-Partition des Systems zugegriffen werden. Aus diesem Grund müssen die nachfolgenden Schritte mit Root-Rechten durchgeführt werden. Die EFI-Partition wird von Debian 7.1.0 standardmäßig im Verzeichnis /boot/efi eingebunden.

Nach dem Herunterladen des Archivs shim-signed.tgz[19] und dessen Extraktion werden die beiden enthaltenen Dateien, shim.efi und MokManager.efi in das zu erstellende Verzeichnis /boot/efi/EFI/debian/shim kopiert. Die Datei shim.efi enthält den Bootloader Shim und ist von Microsoft mittels des Zertifikats „Microsoft Corporation UEFI CA 2011“ (Seriennr.: 61:08:d3:c4:00:00:00:00:00:04) signiert. Shim startet nach dessen Verifizierung durch die UEFI-Firmware einen weiteren Bootloader. Problematisch an dieser Verifizierung ist, dass bei einer Änderung der Binärdatei des zweiten Bootloaders, z.B. im Rahmen eines Updates, dessen Signatur bzw. Hash ungültig und der Bootvorgang somit funktionsuntüchtig wird.

Aus diesem Grund empfiehlt es sich, nicht direkt den durch die Installation des Betriebssystems konfigurierten Bootloader, sondern einen weiteren auf Grub2 basierenden Bootloader, im Folgenden Secure-Boot-Preloader genannt, zu starten. Dieser ruft, ohne eine Verifizierung, den eigentlichen Bootloader des Systems auf. Hiermit sind Änderungen sowohl der Konfiguration als auch der Binärdateien des von Debian installierten und verwalteten Bootloaders möglich, ohne die ordnungsgemäße Ausführung des Bootvorganges zu verhindern.

Damit Shim von der UEFI-Firmware gestartet wird, wird ein entsprechender UEFI-Booteintrag erstellt. Dies kann z.B. durch die Anwendung efibootmgr erfolgen. Nach der Erstellung eines solchen Eintrags kann Shim durch die UEFI-Firmware gestartet werden und führt seinerseits unverzüglich den Secure-Boot-Preloader aus. Im Fehlerfall, z.B. auf Grund einer fehlgeschlagenen Verifizierung des Secure-Boot-Preloaders durch Shim, wird statt dessen der MokManager gestartet. Der MokManager ist in der Datei MokManager.efi enthalten und dient zum interaktiven Hinzufügen von Zertifikaten oder Hashes in die MokList während des Bootprozesses.

Die im Folgenden aufgeführte Liste beinhaltet die notwendigen Befehle zur Nutzung von Secure Boot. Alle Befehle sind durch den Benutzer root in seiner Login-Shell auszuführen. Ferner wird davon ausgegangen, dass das System wie im vorherigen Abschnitt beschrieben, installiert ist.

```
cd /root
# Herunterladen und installieren von Shim
wget http://www.codon.org.uk/~mjg59/shim-signed/shim-signed.tgz
tar xzf shim-signed.tgz
mkdir /boot/efi/EFI/debian/shim
cp shim-signed/shim.efi shim-signed/MokManager.efi /boot/efi/EFI/debian/shim

# Erstellen des monolithischen Secure-Boot-Preloaders, der von Shim gestartet
# wird
cat <<EOF > /tmp/conf
echo „Secure-Boot-Preloader: starting grub2“
chainloader /EFI/debian/grubx64.efi
boot
EOF
grub-mkimage --format x86_64-efi --config /tmp/conf --output
/boot/efi/EFI/debian/shim/grubx64.efi normal echo fat part_gpt chain

# Eintragen von Shim ins UEFI-Bootmenü als höchstpriorisierten Eintrag
efibootmgr --create --label debian-secure-boot --loader
\\EFI\\debian\\shim\\shim.efi --disk /dev/sda --part 1
```

Soll der Bootvorgang anhand von Hashes durchgeführt werden, so wird der abschließende Einrichtungsschritt über den MokManager vollzogen. Hierzu wird das System neu gebootet und über das UEFI-Setup Secure Boot aktiviert. Daraufhin startet Shim und versucht seinerseits den Secure-Boot-Preloader zu verifizieren. Da die MokList jedoch keinen dazu geeigneten Eintrag enthält und die Verifizierung daher fehlschlägt, startet Shim den MokManager. Dort wird über den Menüeintrag „Enroll hash from disk“ die Datei grubx64.efi im Verzeichnis /EFI/debian/shim ausgewählt. Hierdurch erstellt Shim einen Hash des Secure-Boot-Preloaders und fügt diesen in die MokList hinzu. In einem erneuten

19 http://www.codon.org.uk/~mjg59/shim-signed/shim-signed.tgz

Bootvorgang[20] kann der Secure-Boot-Preloader nun erfolgreich durch Shim geladen und somit das Debian-System gebootet werden. Die nachfolgenden Schritte zur Signierung der Bootloader-Datei können bei Nutzung eines Hashes entfallen.

5.5.4.3 Installation der sbsigntools

Soll eine Verifizierung des Secure-Boot-Preloaders nicht anhand eines Hashes, sondern durch ein Zertifikat erfolgen, so muss die Binärdatei des Bootloaders signiert werden. Dies kann durch die Werkzeugsammlung sbsigntools[21] erfolgen, welche jedoch nicht Bestandteil von Debian 7.1.0 ist.

Die im Folgenden aufgeführte Liste beinhaltet die notwendigen Befehle zur Installation der sbsigntools aus deren Quellcode. Alle Befehle sind durch den Benutzer root in seiner Login-Shell auszuführen. Ferner wird davon ausgegangen, dass das System, wie im vorherigen Abschnitt beschrieben, installiert ist.

```
aptitude install git
git clone git://kernel.ubuntu.com/jk/sbsigntool
cd sbsigntool
# Mit dem folgenden optionalen Befehl kann die Version der sbigntools geladen
# werden, die diesem Dokuent zu Grunde liegt.
#git checkout 951ee95a301674c046f55330cd7460e1314deff2
aptitude install automake make gcc binutils-dev libssl-dev pkg-config help2man
uuid-dev gnu-efi
./autogen.sh && ./configure && make && make install
```

5.5.4.4 Signierung des Bootloaders

Durch die Anwendung sbsign, die Teil der sbsigntools ist, kann der Secure-Boot-Preloader, der in der Datei /boot/efi/EFI/debian/shim/grubx64.efi gespeichert ist, signiert werden. Voraussetzung für die Signierung mittels der sbsigntools ist das Vorliegen eines X509-Zertifikats im PEM-Format und des dazugehörigen privaten Schlüssel. Für den Import des Zertifikats in die MokList durch den MokManager muss dieses Zertifikat im DER-Format auf der EFI-Partition vorliegen.

Im Folgenden wird gezeigt, wie die Signierung durch ein selbstsigniertes Zertifikat erfolgt. Hierbei ist zu beachten, dass das gezeigte Vorgehen ausschließlich Demonstrations- und Testzwecken dient. Es wird insbesondere darauf hingewiesen, dass die Speicherung des privaten Schlüssels auf dem betroffenen System erhebliche Sicherheitsrisiken birgt. Verfügt ein Angreifer oder eine Schadsoftware über die notwendigen Rechte um den Bootloader auszutauschen, so hat sie i.d.R. ebenfalls die Rechte einen lokal gespeicherten Schlüssel auszulesen und mit ihm eine Signierung eines kompromittierten Bootloaders durchzuführen und somit den Secure Boot-Mechanismus zu unterwandern. Auch kann das hier aufgeführte Vorgehen zur Erstellung von selbstsignierten Zertifikaten keineswegs die für den Aufbau einer sicheren Public-Key-Infrastruktur (PKI) notwendigen Prozesse ersetzen.

Alle Befehle sind durch den Benutzer root in seiner Login-Shell auszuführen. Ferner wird davon ausgegangen, dass das System, wie im vorherigen Abschnitt beschrieben, installiert ist und die Schritte des Abschnitts 5.5.4.3 durchgeführt sind.

```
mkdir /root/cert
cd /root/cert

# Erstellen eines selbstsignierten Zertifikats. Die sbsigntools benötigen das
# Zertifikat im PEM-Format. Daten bzgl. des Zertifikats werden interaktiv
# abgefragt.
openssl req -new -x509 -newkey rsa:2048 -keyout signing.key -out signing.pem.crt
-outform pem -days 365 -nodes -sha256
```

20 Hierbei ist zu beachten, dass die Auswahl des Menüpunkt „Continue Boot“ nicht zum Ziel führt. Der Bootprozess ist gänzlich neu zu initialisieren, z.B. durch Drücken der Tastenkombination Ctrl-Alt-Del.

21 https://launchpad.net/ubuntu/+source/sbsigntool

```
# Signieren der Bootloader-Datei.
sbsign --key signing.key --cert signing.pem.crt --output
/boot/efi/EFI/debian/shim/grubx64.efi /boot/efi/EFI/debian/shim/grubx64.efi
# Optionale Überprüfung des Signierungsvorgangs
sbverify --cert signing.pem.crt /boot/efi/EFI/debian/shim/grubx64.efi

# Konvertieren des Zertifikats, da der MokManager dieses im DER-Format
# benötigt.
openssl x509 -in signing.pem.crt -inform pem -out signing.der.crt -outform der
# Kopieren des Zertifikats auf die EFI-Partition, damit dieses vom MokManager
# ausgelesen werden kann
cp signing.der.crt /boot/efi
```

Im Anschluss hieran wird das System neu gebootet und über das UEFI-Setup Secure Boot aktiviert. Da Shim die Verifizierung des Secure-Boot-Preloaders aufgrund einer leeren MokList misslingt, startet es den MokManager. Hier kann nun über den Menüpunkt „Enroll key from disk“ das zuvor auf die EFI-Partition kopierte Zertifikat ausgelesen und in die MokList aufgenommen werden. Hiernach ist Shim in der Lage, die Binärdatei des Secure-Boot-Preloader während des Bootvorgangs zu verifizieren. Somit ist der Bootvorgang funktionstüchtig.

5.5.5 Funktionsweise

Das hier gezeigt Vorgehen ermöglicht den Betrieb von Debian 7.1.0 bei aktiviertem Secure Boot durch die nachträgliche Installation des Bootloader Shim. Dieser wird in einer durch Microsoft mittels des Zertifikats „Microsoft Corporation UEFI CA 2011“ (Seriennr.: 61:08:d3:c4:00:00:00:00:00:04) signierten Form nach dem Installationsvorgang des Betriebssystems installiert. Shim startet seinerseits den Secure-Boot-Preloader, ein manuell eingerichteter monolithischer Bootloader basierend auf Grub2. Dieser dient als Zwischenglied zwischen Shim und dem eigentlichen Bootloader des Systems, mit dem Zweck, letzteren nicht signieren oder hashen zu müssen. Somit kann der Bootloader des Betriebssystems modifiziert werden, ohne dass der Bootvorgang funktionsuntüchtig wird. Der Secure-Boot-Preloader wird wahlweise durch einen Hash oder eine Signatur von Shim verifiziert und startet seinerseits den eigentlichen Bootloader des Systems ohne Verifizierung.

Die Verifikationskette der aufgeführten Methode umfasst somit lediglich den ersten Bootloader Shim und den Secure-Boot-Preloader. Eine Verifikation des Kernels, ebenso wie eine Überprüfung der Kernelmodule, erfolgt nicht. Einem Angreifer ist es somit grundsätzlich möglich Kernelmodule zur Laufzeit nachzuladen und somit beliebigen Code in den Kernel einzuschleusen, sofern dieser Root-Rechte besitzt. Da Code, der in Form von Kernelmodulen ausgeführt wird, gleichberechtigt ist mit dem der im Kernel selbst enthalten ist, ist eine uneingeschränkte Kompromittierung des Kernels auf diesem Wege möglich.

5.5.6 Zusammenfassung

Debian 7.1.0 unterstützt Secure Boot nicht und kann ohne Modifikationen bei aktiviertem Secure Boot weder installiert noch betrieben werden. Sofern Secure Boot deaktiviert ist, lässt sich Debian 7.1.0 jedoch auf allen untersuchten Hardwareplattformen problemlos installieren und betreiben.

Ferner lässt sich Debian 7.1.0 mittels der nachträglichen Installation von Shim auch unter Einsatz von Secure Boot mit dem jeweiligen Standardschlüsselmaterial der untersuchten Hardwareplattformen betreiben. Das hierzu aufgezeigte Vorgehen umfasst jedoch nicht die Verifizierung des Betriebssystemkerns.

Abschließend lässt sich daher sagen, dass der Betrieb von Debian 7.1.0 mit Secure Boot auf allen untersuchten Hardwareplattformen mit relativ geringem Aufwand möglich ist. Die Nutzung von Secure Boot im Rahmen des aufgezeigten Vorgehens führt jedoch zu keinem signifikanten Sicherheitsgewinn.

5.6 Vorbereitungsschritte, Installation, Funktion von Fedora

5.6.1 Fedora

Fedora ist eine aus dem ehemaligen Red Hat Linux hervorgegangene Linux-Distribution. Die Entwicklung wird sowohl durch das Unternehmen Red Hat, als auch durch die Community, vorangetrieben.

Ein wesentliches Ziel bei der Entwicklung von Fedora ist die möglichst rasche Integration technologischer Neuerungen. Dies ist einer der Hauptgründe für das Erscheinen neuer Versionen in relativ kurzen Intervallen. So wird ca. alle 6 Monate eine neue Version veröffentlicht, welche dann für ca. ein Jahr gepflegt wird.

Die dieser Untersuchung zugrunde liegende und zum Zeitpunkt der Erstellung aktuelle Version von Fedora ist 19 (Schrödinger's Cat). Fedora 19 unterstützt Secure Boot.[22]

5.6.2 Ausgangssituation

Die im Folgenden beschriebene Installation erfolgt, nachdem das jeweilige Gerät über das UEFI-Setup auf seine Defaultwerte zurückgesetzt und das Standardschlüsselmaterial installiert ist. Ferner wird sichergestellt, dass die UEFI-Firmware ausschließlich im EFI-Modus bootet. Auch werden vor der Installation alle evtl. bestehenden Festplattenpartitionen entfernt.

5.6.3 Vorbereitung

Vorbereitungsschritte sind nicht notwendig. Insbesondere ist Secure Boot während des Installationsvorgangs aktiviert.

5.6.4 Installation

Die Installation von Red Hat Fedora 19 (Schrödinger's Cat) erfolgt von einem USB-Stick, auf dem die Desktopinstallationsversion von Fedora (Fedora-Live-Desktop-x86_64-19-1.iso) eingerichtet ist.

Die im Folgenden aufgeführten Installationsschritte beschreiben den Installationsprozess von Red Hat Fedora 19, der den weiteren Abschnitten zugrunde liegt. Hierbei wird das Installationsprogramm durch Auswahl des Menüeintrags „Fedora-Live-Desktop-x86_64-19-1“ des Bootloaders des Installationsmediums gestartet. Alle Schritte entsprechen den typischen Schritten zur Installation von Red Hat Fedora 19 und beinhalten keinerlei spezifische Anpassung auf die jeweilige Hardwareplattform oder für den Einsatz mit Secure Boot. Im Folgenden werden die gemachten Eingaben im jeweiligen Installationsschritt aufgelistet.

- Welcome to Fedora: Install to Hard Drive
- Willkommen bei FEDORA 19. Welche Sprache möchten Sie während des Installationsvorgangs verwenden?:
  - Auswahl: Deutsch (Deutschland)
  - "Tastatur mit der Standardbelegung der gewählten Sprache einrichten" ausgewählt
- Zusammenfassung der Installation: „Installationsziel“ anklicken
- Installationsziel: Erste Festplatte auswählen

22 Dokumentation zu Secure Boot für Fedora 18, auch für Fedora 19 gültig: http://docs.fedoraproject.org/en-US/Fedora/18/html/UEFI_Secure_Boot_Guide/index.html

- Installationsoptionen:
  - "Konfiguriere automatisch meine Fedora-Installation auf die von mir gewählte(n) Festplatte(n) und kehre zum Hauptmenü zurück" ausgewählt
  - Partitionierungsschema: LVM
  - "Meine Daten verschlüsseln, Passphrase später setzen." nicht ausgewählt
- "Installation starten" anklicken
- „ROOT-Passwort“ anklicken
- Root-Passwort:
  - Root-Passwort: kennwort
  - Bestätigen: kennwort

Nach einem Neustart und dem ersten Startvorgang des Systems wird die Einrichtung fortgeführt.

- Willkommen: Auswahl unverändert lassen
- Eingabemethode: Deutsch
- Netzwerk: Keines der Listenelemente ausgewählt
- Anmelden:
  - Vollständiger Name: user
  - Benutzername: user
  - Passwort: kennwort
  - Passwort bestätigen: kennwort
- Standort: Standort: Berlin
- Online-Konten: Keine Eingaben gemacht
- Vielen Dank: „GNOME 3 starten“ anklicken

Die Installation von Red Hat Fedora 19 ist auf allen vier untersuchten Hardwareplattformen problemlos und ohne Besonderheiten durchführbar. Insbesondere kann sowohl die Installation als auch der Betrieb des Systems mit dem jeweiligen Standardschlüsselmaterial bei aktiviertem Secure Boot durchgeführt werden.

5.6.5 Funktionsweise

Ermöglicht wird der Betrieb von Fedora 19 bei aktiviertem Secure Boot durch den Bootloader Shim. Dieser wird in einer durch Microsoft mittels des Zertifikats „Microsoft Corporation UEFI CA 2011“ (Seriennr.: 61:08:d3:c4:00:00:00:00:00:04) signierten Form automatisch während des Installationsprozesses installiert. Als zweiter Bootloader wird Grub2 genutzt. Die Verifizierung von Grub2 durch Shim erfolgt mittels des fest in die Binärdatei von Shim integrierten Zertifikats „Fedora Secure Boot CA“ (Seriennr.: 2574709492)[23].

Da Grub2, sofern Secure Boot aktiviert ist, von Fedora 19 in monolithischer Form installiert wird, entfällt die Verifizierung von Grub2-Modulen. Ferner wird bei aktiviertem Secure Boot ein Nachladen von Grub2-Modulen durch eine Quellcodeänderung an Grub2 im Rahmen des Fedora-Projektes verhindert.

Die Verifizierung des Kernels erfolgt mit dem selbem Zertifikat. Hierzu delegiert Grub2 die Verifizierung zurück an Shim. Diese Delegation wird durch Modifikationen am Quelltext von Grub2 für den Einsatz mit Fedora ermöglicht. Der Kernel verifiziert seinerseits die zu ladenden Kernelmodule. Dies wird durch die

23 Das vollständige Zertifikat ist in Anhang 7.11 aufgeführt.

Signierung der Module bei deren Kompilation ermöglicht. Das entsprechende Zertifikat wird bei diesem Übersetzungsvorgang in den Kernel eingebettet.

Somit findet eine lückenlose Verifikation der Bootloader, des Kernels und seiner Module statt.

5.6.6 Zusammenfassung

Fedora lässt sich ohne Probleme und ohne Vorbereitungsschritte auf allen untersuchten Hardwareplattformen installieren und betreiben. Sowohl die Installation als auch der Betrieb können bei aktiviertem Secure Boot mit dem jeweiligen Standardschlüsselmaterial durchgeführt werden.

Die Verifikationskette umfasst hierbei den ersten Bootloader Shim, den zweiten Bootloader Grub2, den Linux-Kernel und dessen Module. Somit ist Fedora 19 die einzige, in dieser Arbeit untersuchte Linux-Distribution die Secure Boot nutzt, um einer Kompromittierung des Kernels durch Einbringung von Schadcode entgegen zu wirken. Das hierfür gewählte Verfahren ist jedoch nicht fehlerfrei und ermöglicht es somit trotz aktivem Secure Boot Schadcode einzuschleusen.

In diesem Zusammenhang ist auch zu betonen, dass das gesamte genutzte Schlüsselmaterial, mit Ausnahme der in der Hardware installierten UEFI-Zertifikate, durch das Fedora Projekt verwaltet wird. Durch eine Kompromittierung dieses Schlüsselmaterials könnte auch nachträglich Schadcode signiert und, trotz Secure Boot, zur Ausführung gebracht werden.

Abschließend lässt sich daher sagen, dass der Betrieb von Fedora 19 mit Secure Boot auf den untersuchten Hardwareplattformen problemlos möglich ist. Da die Verifikationskette den gesamten Bootvorgang inkl. des Kernels und seiner Module umfasst, ist, je nach Anwendungsgebiet und Bedrohungslage, durchaus ein Sicherheitsgewinn durch den Einsatz von Secure Boot möglich.

5.7 Ergebnisse

Trotz der relativ neuen Technik und der umfangreichen Spezifikation arbeitet Secure Boot auf allen untersuchten Plattformen mit den eingesetzten Betriebssystemen zusammen. Das Starten einer signierten UEFI-Anwendung, wie z.B. eines Bootloaders funktioniert, sofern das entsprechende Zertifikat in dem db-Zertifikatsspeicher der UEFI-Firmware enthalten ist. Auch wird der Start einer solchen Anwendung verweigert, sofern kein passendes Zertifikat in diesem Zertifikatsspeicher vorhanden ist. Ebenso funktioniert die Verifikation von UEFI-Anwendungen anhand von Hashes problemlos.

Ferner ist die Installation und der Betrieb der Betriebssysteme Windows 8 Pro, Ubuntu 13.04 und Fedora 19 bei aktiviertem Secure Boot möglich. Die ebenfalls untersuchten Betriebssysteme Red Hat Enterprise Linux 6.4 und Debian 7.1.0 unterstützen Secure Boot nicht und werden daher bei deaktiviertem Secure Boot installiert. Sie lassen sich jedoch mit relativ geringem Aufwand so modifizieren, dass diese auch bei aktivem Secure Boot betrieben werden können.

Bei der Integration von Secure Boot in die untersuchten Betriebssysteme und dem daraus resultierenden Gewinn an Sicherheit gibt es jedoch gravierende Unterschiede. Der Gewinn an Sicherheit durch die beschriebenen Modifikation bei Debian und Red Hat Enterprise Linux ist auch bei aktiviertem Secure Boot nicht signifikant. Ebenso ist der Sicherheitsgewinn bei dem Einsatz von Ubuntu 13.04 als nicht signifikant einzuschätzen. Zwar werden die Bootloader verifiziert, eine effektive Überprüfung des Kernels samt seiner Module findet jedoch nicht statt.

Im Gegensatz hierzu findet bei Fedora 19 nicht nur eine Verifikation der Bootloader, sondern auch des Kernels und seiner Module statt. Das Einschleusen von Code in den Kernel während des Bootprozesses kann somit prinzipiell erkannt und verhindert werden.

Wenngleich Windows 8 Pro ebenfalls eine Überprüfung des Bootloaders und des Kernels durchführt, ist eine Beurteilung der Effektivität der Schutzmaßnahmen erheblich schwieriger als bei den untersuchten Linux-Systemen. Grund ist hierfür hauptsächlich das komplexe Vorgehen zur Verifikation von nachträglich zu ladenden Kernelkomponenten, wie z.B. Treibern. Microsoft setzt hier zur Erkennung von Schadsoftware auf eine Zusammenarbeit des Kernels mit Anti-Malware-Produkten. Die Effektivität der Schutzfunktionen hängt daher ganz erheblich von der Qualität des eingesetzten Produktes ab. Auch wird die von Microsoft neu eingeführte ELAM-Technik im Rahmen dieser Arbeit auf Grund seiner Komplexität nicht bewertet. Auf eine abschließende Beurteilung des Sicherheitsgewinns von Windows 8 Pro durch Nutzung von Secure Boot wird daher verzichtet.

Die Ergebnisse dieses Kapitels sind in Tabelle 2 zusammengefasst.

	Windows 8 Pro	Red Hat Enterprise Linux 6.4	Debian 7.1.0	Ubuntu 13.04	Fedora 19
WirdSecure Boot im Betrieb unterstützt?	Ja	Nein	Nein	Ja	Ja
Wird Secure Boot bei der Installation unterstützt?	Ja	Nein	Nein	Ja	Ja
Ist ggf. eine nachträgliche Unterstützung durch Shim möglich?	-	Ja	Ja	-	-
Effektiver Umfang der Verifikationskette[24]	Bootloader, Kernel (bedingt)[25]	Shim[26]	Shim[27]	Shim, Grub2[28]	Shim, Grub2, Kernel, Kernelmodule
Unterstützte Hardwareplattformen[29]	HP, Lenovo, Dell, Medion	HP, Lenovo, Dell, Medion	HP, Lenovo, Dell, Medion	HP, Lenovo, Dell, Medion	HP, Lenovo, Dell, Medion

Tabelle 2: Unterstützung von Secure Boot der untersuchten Betriebssysteme

24 Der Umfang der Verifikationskette beschreibt die effektiv validierten Teile des Bootprozesses nach der Installation des jeweiligen Betriebssystems bzw. nach deren wie in den vorhergehenden Abschnitten beschrieben Anpassungen.

25 Die Effektivität der Verifizierung hängt im hohen Maße sowohl von dem eingesetzten Anti-Malware-Produkt, als auch von der ELAM-Technik ab. Beide Aspekte stehen nicht im Fokus dieser Arbeit und werden daher nicht in einem Umfang untersucht, der es ermöglicht ein abschließendes Urteil zu bilden. Daher ist die gemachte Beurteilung nicht als abschließend anzusehen.

26 Zwar wird auch der Kern von Grub2 überprüft, diese Verifizierung ist jedoch nicht effektiv, da Grub2-Module ohne Verifizierung nachgeladen werden können.

27 Zwar wird auch der Kern von Grub2 überprüft, diese Verifizierung ist jedoch nicht effektiv, da Grub2-Module ohne Verifizierung nachgeladen werden können.

28 Wenngleich im Bootprozess von Ubuntu 13.04 auch der Linux-Kernel überprüft wird, so ist diese Verifizierung nicht effektiv, da Kernelmodule ohne Verifizierung nachgeladen werden können.

29 Hardwareplattformen auf denen das entsprechende Betriebssystem installiert und wie in diesem Kapitel beschrieben mit aktiviertem Secure Boot betrieben werden kann. Die vollständige Kompatibilität aller Hardwarekomponenten der Plattform mit dem jeweiligen Betriebssystem wird nicht garantiert.

6 Nutzung von „Secure Boot“ für vertrauenswürdige IT-Plattformen (AP 6)

6.1 Einleitung

Die folgende Betrachtung der Nutzung von Secure Boot als Bestandteil einer vertrauenswürdigen IT-Plattform ist in drei Teile gegliedert. Der erste Teil beschäftigt sich mit der Einrichtung von Windows 8 Pro und Debian 7.1.0 im Dual-Boot-Betrieb unter Nutzung von Secure Boot. Im Anschluss wird das grundsätzliche Vorgehen zur Härtung eines Linux-Systems am Beispiel von Debian 7.1.0 aufgezeigt. Ziel ist es hierbei, Manipulationen des Kernels während des Bootvorgangs zuverlässig zu erkennen und die Ausführung von kompromittiertem Code zu unterbinden. Abschließend wird eine Betrachtung möglicher Angriffswege zur Kompromittierung eines solchen Systems, als auch die technischen und organisatorischen Herausforderungen bei dessen Einführung durchgeführt.

6.2 Dual-Secure-Boot-Umgebung

6.2.1 Beschreibung der Konfiguration (AP 6.1)

Im Folgenden wird aufgezeigt, wie Debian 7.1.0 in einer Dual-Secure-Boot-Umgebung neben Windows 8 Pro installiert und konfiguriert werden kann. Das Debian-System soll hierbei unabhängig von den Zertifikaten der Firma Microsoft bei aktivem Secure Boot betriebsfähig sein. Die Betriebsfähigkeit von Windows 8 Pro soll hierdurch nicht beeinträchtigt werden. Keines der beiden Systeme soll die UEFI-Zertifikatsspeicher modifizieren können.

Die in den folgenden Abschnitten beschriebene Umsetzung besteht hierbei aus drei Schritten. Der erste Schritt beschreibt die Installation der beiden Betriebssysteme in Form einer Dual-Boot-Umgebung. Da Debian 7.1.0 Secure Boot nicht unterstützt, wird dessen Installation bei deaktiviertem Secure Boot durchgeführt.

Im zweiten Schritt werden die UEFI-Zertifikatsspeicher modifiziert. Somit wird sichergestellt, dass die Entscheidung bzgl. der Ausführbarkeit von Code während des Bootprozesses ausschließlich beim Inhaber des installierten Schlüsselmaterials liegt. Insbesondere wird hierdurch verhindert, dass die Distributoren der beiden Betriebssysteme die Ausführung des anderen Systems durch entsprechende Änderungen des db- oder dbx-Zertifikatsspeichers im Rahmen eines Updates unterbinden. Des Weiteren wird eigenes Schlüsselmaterial in den db-Zertifikatsspeicher eingebracht. Der Besitzer dieses Schlüsselmaterials wird hierdurch befähigt UEFI-Anwendungen mit einer validen Signatur zu versehen und somit deren Start zu ermöglichen. Sofern im abschließenden Arbeitsschritt nicht mit Zertifikaten gearbeitet werden soll, sondern lediglich Hashes zur Verifikation eingesetzt werden, kann die Manipulation des db-Zertifikatsspeicher unterbleiben. Vorausgesetzt wird, dass Schlüsselmaterial zur Einbringung in den PK-, den KEK- und optional den db-Zertifikatsspeicher vorliegt. Ebenso wird vorausgesetzt, dass das Zertifikat „Microsoft Windows Production PCA 2011“ (Seriennr.: 61:07:76:56:00:00:00:00:00:08) der Firma Microsoft bereit steht.[30]

Im dritten Arbeitsschritt wird der Bootloader des Debian-Systems signiert oder alternativ ein Hash erstellt und dieser in den db-Zertifikatsspeicher eingefügt.

30 Das Microsoft-Zertifikat kann z.B. durch die EFI-Tools aus der UEFI-Firmware ausgelesen werden.

6.2.2 Installations- und Konfigurationsschritte (AP 6.2)

6.2.2.1 Installation von Windows 8 Pro und Debian 7.1.0

Die Installation von Windows 8 Pro wird wie in Abschnitt 5.2.4 durchgeführt. Insbesondere erfolgt diese bei aktiviertem Secure Boot. Im Anschluss wird der von Windows reservierte Festplattenspeicherplatz verringert, um Speicherplatz für die Installation von Debian 7.1.0 zu schaffen.

Hierzu wird Windows regulär gestartet und es werden aus Windows heraus folgende Schritte abgearbeitet:

- Öffnen der Ausführen-Dialogbox druch Drücken der Tastenkombination Win-R
- Öffnen der Datenträgerverwaltung durch Aufruf von „diskmgmt.msc“.
- Öffnen des Dialogs „Verkleinern von Laufwerk C:“ durch Rechtsklick auf Laufwerk C und Linksklick auf den Menüpunkt „Volume verkleinern“.
- Verkleinern der Partition um 30GB[31] durch Eingabe des Wertes 30000 in das Feld „zu verkleinernder Speicherplatz in MB:“ und anschließendes Bestätigen durch Linksklick auf die Schaltfläche „Verkleinern“.

Sofern diese Schritte erfolgreich abgearbeitet sind, steht ausreichend Speicherplatz für die Installation von Debian 7.1.0 zur Verfügung. Diese wird, wie in Abschnitt 5.5.4.1 beschrieben, durchgeführt. Hierbei ist zu beachten, Secure Boot, wie beschrieben, vor dem Beginn der Installation zu deaktivieren. Ferner sind während der Installation folgende Abweichungen von dem in Abschnitt 5.5.4.1 beschriebenen Installationsverfahren durchzuführen:

- Als Partitionsmethode im Installationsschritt „Festplatte partitionieren“ wird statt „Geführt – vollständige Festplatte verwenden“ der Punkt „Geführt – den größten freien Speicherplatz verwenden“ ausgewählt.
- Bei der nachfolgenden Übersicht über die vorhandenen und anzulegenden Partitionen wird die von Windows angelegte EFI-Partition, welche im Auswahlmenü mit „EFIBoot“ beschriftet wird, ausgewählt. Im sich öffnenden Dialog wird im Feld „Benutzen als“ der Wert „EFI-Boot-Partition“ ausgewählt. Diese Angabe wird durch Auswahl der Schaltfläche „Anlegen der Partition beenden“ bestätigt. Im Anschluss wird durch Auswahl der Schaltfläche „Partitionierung beenden und Änderungen übernehmen“ die Partitionierung beendet.

Nach erfolgreicher Installation wird das Debian-System gestartet. Dies geschieht, indem das EFI-Bootmenü nach einem Neustart der Plattform aufgerufen wird. Die Taste oder Tastenkombination mit der dies geschieht ist hardwarespezifisch und ist ggfs. im Handbuch der Plattform nachzuschlagen. Im EFI-Bootmenü wird der Eintrag „debian“ ausgewählt. Dies bewirkt, dass der Bootloader Grub2 gestartet wird. Durch Auswahl des Menüeintrags „Debian GNU/Linux, mit Linux 3.2.0-4-amd64“ wird Debian gebootet.

6.2.2.2 Installation des Secure-Boot-Preloaders

Sofern die Installation beider Betriebssysteme erfolgreich abgeschlossen ist, muss der Bootloader des Debian-Systems signiert oder alternativ dessen Hash in den db-Zertifikatsspeicher eingetragen werden. Wenngleich dies für den im Rahmen der Systeminstallation eingerichteten Bootloader durchgeführt werden kann, so hat dies einen wesentlichen Nachteil. Kommt es zu einem Update des Bootloaders oder einer anderweitig ausgelösten Modifikation dessen Binärdatei, so wird die Signatur bzw. der Hash ungültig. Hierdurch würden nachfolgende Bootvorgänge bei der Verifizierung des Bootloaders scheitern und somit das Betriebssystem nicht mehr starten.

31 Der für Debian 7.1.0 mindestens benötigte Speicherplatz beträgt tatsächlich deutlich weniger als die hier angegebenen 30GB. Eine Reduzierung dieses Wertes ist daher möglich.

Aus diesem Grund wird analog zu Abschnitt 5.5.4.2 ein Secure-Boot-Preloader genutzt, der durch die folgenden Befehle installiert wird.

```
# Erstellen der Konfigurationdatei des Secure-Boot-Preloaders
cat <<EOF > /tmp/conf
echo „Secure-Boot-Preloader: starting grub2“
chainloader /EFI/debian/grubx64.efi
boot
EOF

# Erstellen des Secure-Boot-Preloaders als monolithische Grub2-Version
grub-mkimage --format x86_64-efi --config /tmp/conf --output
/boot/efi/EFI/debian/secure-boot-preloader.efi normal echo fat part_gpt chain

# Erstellen eines Eintrag in der UEFI-Firmware um den Secure-Boot-Loader zu
# booten
efibootmgr --create --label debian-secure-boot --loader
\\EFI\\debian\\secure-boot-preloader.efi --disk /dev/sda --part 1
```

6.2.2.3 Signierung des Bootloaders

Im Anschluss hieran wird der Secure-Boot-Loader signiert. Umgesetzt wird dies mit dem Werkzeug sbsign, welches zu der Werkzeugsammlung sbsigntools[32] gehört. Eine Installationsanleitung für dieses Werkzeug ist in Abschnitt 5.5.4.2 zu finden. Durch Ausführung des Befehls „sbsign --key db.key --cert db.pem.crt /boot/efi/EFI/debian/secure-boot-preloader.efi“ wird der Secure-Boot-Loader signiert. Hierbei wird davon ausgegangen, dass der private Schlüssel, der zur Signierung von UEFI-Anwendungen verwendet werden soll, in der Datei db.key und, dass das zugehörige Zertifikat in der Datei db.pem.crt vorliegt. Der Signierungsschritt sollte hierbei zur Sicherheit des privaten Schlüssels nicht auf dem betroffenen System selbst, sondern in einer sicheren Arbeitsumgebung stattfinden.

6.2.2.4 Modifikation der Zertifikatsspeicher

Nach erfolgreicher Einrichtung des Bootloaders, werden die Zertifikatsspeicher der UEFI-Firmware modifiziert.

Die Modifikation wird mithilfe der EFI-Tools durchgeführt. Hierzu wird das zugehörige USB-Image, z.B. mit dem Werkzeug dd, auf einen USB-Stick übertragen. Im Anschluss hieran wird sowohl das Zertifikat „Microsoft Windows Production PCA 2011“ (Seriennr.: 61:07:76:56:00:00:00:00:00:08) als auch die zum eigenen Schlüsselmaterial zugehörigen Schlüssel (PK, KEK, db) in ein Format umgewandelt, welches von der UEFI-Firmware verarbeitet werden kann. Dies erfolgt mittels der Anwendung cert-to-efi-sig-list, welche Bestandteil der EFI-Tools ist.

Nun wird das Secure-Boot-System der zu konfigurierenden Plattform über das UEFI-Setup in den Setup-Mode versetzt, um die Modifikationen der Zertifikatsspeicher durchführen zu können. Das genaue Vorgehen hierzu ist plattformspezifisch.

Hiernach wird von dem vorbereiteten USB-Stick gebootet. Mittels der sich öffnenden UEFI-Shell wird durch Eingabe der folgenden Befehle das Werkzeug „keytool“ gestartet. Dieses stellt eine rudimentäre textbasierte Oberfläche zur Modifikation der UEFI-Zertifikatsspeicher zur Verfügung.

```
fs0:
cd EFI
cd BOOT
KEYTOOL.EFI
```

32 https://launchpad.net/ubuntu/+source/sbsigntool

Über den Menüpunkt „Edit Keys“ wird ein Untermenü geöffnet, welches es ermöglicht die Zertifikatsspeicher PK, KEK, db, dbx und MokList wie folgt zu modifizieren:

- MokList
  - Alle evtl. vorhandenen Zertifikate und Hashes entfernen
- db
  - Alle evtl. vorhandenen Zertifikate und Hashes entfernen
  - Zertifikat „Microsoft Windows Production PCA 2011“ (Seriennr.: 61:07:76:56:00:00:00:00:00:08) einfügen
  - Eigenes Zertifikat zur Signierung von UEFI-Anwendungen einfügen. Alternativ kann auch ein Hash des Bootloaders eingefügt werden.
- dbx
  - Keine Änderungen notwendig
- KEK:
  - Alle evtl. vorhandenen Zertifikate und Hashes entfernen
  - Eigenes Zertifikat des KEK einfügen
- PK
  - Zertifikat des eigenen Plattform-Keys einsetzen

Hierbei ist zu beachten, dass die Modifikation des PK-Zertifikatsspeicher als letzter Arbeitsschritt durchgeführt wird, da durch das Einbringen eines Plattform Keys der Setup Mode verlassen und in den User Mode gewechselt wird. Eine nachträgliche Manipulation der Zertifikatsspeicher ist dann nur noch über signierte Updates oder durch Löschen des Plattform Keys mit Hilfe des UEFI-Setups möglich.

6.3 Härtung eines Linux-Systems

6.3.1 Allgemeines

Die Nutzung von Secure Boot mit dem Ziel einen tatsächlichen Sicherheitsgewinn zu erzielen, bedarf technischer Anpassungen und organisatorischer Prozesse, die über das in den vorhergehenden Abschnitten aufgezeigten Vorgehen hinausgehen. Aus diesem Grund gehen die folgenden Abschnitte auf die wesentlichen technischen wie organisatorischen Voraussetzungen zur Nutzung von Secure Boot mit dem Ziel der Absicherung des jeweiligen Systems ein. Hierbei wird darauf hingewiesen, dass diese Betrachtung keineswegs erschöpfend ist und aufgrund der Notwendigkeit eine konkrete Umsetzung auf die jeweilige Bedrohungslage hin anzupassen, dies auch nicht zum Ziel hat.

Ziel ist die Darstellung typischer Schritte zur Absicherung eines Linux-Betriebssystems, welches Secure Boot standardmäßig nicht unterstützt. Hierzu wird auf Debian 7.1.0, welches wie in Abschnitt 5.5.4.1 installiert ist, zurückgegriffen.

Im Anschluss hieran werden einige Risiken und Herausforderungen im Zusammenhang mit der Härtung des Systems durch Nutzung von Secure Boot betrachtet.

Abschließend werden die möglichen Betriebsarten von Secure Boot zusammengefasst und der mit ihnen verbundene Realisierungsaufwand und der zu erzielende Sicherheitsgewinn gegenüber gestellt.

6.3.2 Signierungs- und Installationsprozess

Wesentlich bei Nutzung von Secure Boot zur Absicherung des Bootprozesses ist die Tatsache, dass die Installation von signierter und damit verifizierbarer Software auf einer Hardwareplattform kein einmaliger Vorgang ist. Ferner muss die eingesetzte Software, insbesondere der Kernel, regelmäßig aktualisiert werden. Somit bedarf es eines Prozesses, der die hierzu notwendigen Arbeitsschritte beschreibt und unter Beachtung der jeweiligen Bedrohungslage deren Integrität sicherstellt. Ein solcher Prozess muss zumindest die folgenden Schritte umfassen:

1. Bezug und ggf. Kompilierung der zu signierenden Software
2. Verifikation der zu signierenden Software
3. Durchführung der Signierung
4. Paketierung der signierten Software und ggf. Signierung der Softwarepakete
5. Bereitstellung der Softwarepakete
6. Installation der Softwarepakete
7. Verteilung der Zertifikate
8. Deinstallation fehlerhafter oder nicht mehr benötigter Softwarepakete

Punkt 1 umfasst alle Schritte die die Beschaffung der zu signierenden Software und ggf. deren Kompilierung zum Gegenstand haben. Da der Bezug der Software typischerweise über das Internet erfolgt, besteht hier eine besondere Gefahr einer Kompromittierung der übermittelten Software als auch des ausführenden Systems.

Das Vorgehen zur Verifikation der Software und damit alle Maßnahmen, um eine evtl. Kompromittierung zu erkennen, beinhaltet der in Punkt 2 festgehaltene Arbeitsschritt. Da eine vollständige Analyse des Quellcodes, aufgrund des damit verbundenen Aufwands, nur in Ausnahmefällen sinnvoll ist, ist in diesem Zusammenhang zu klären, anhand welcher Kriterien die Integrität der Software in ausreichendem Maße sichergestellt werden kann.

Die anschließende Signierung der Software, welche in Punkt 3 beschrieben wird, benötigt Zugriff auf den privaten Schlüssel, welcher der Verifizierung während des Secure-Boot-Vorgangs zugrunde liegt. Die Herausforderung hierbei besteht u.a. darin, Software, wie in Zusammenhang mit Punkt 1 beschrieben, über das Internet zu beziehen ohne die Vertraulichkeit des eingesetzten Schlüssels zu gefährden.

Da die Software, neben den signierten Bestandteilen typischerweise weitere Komponenten, wie z.B. Hilfsprogramme zur Konfiguration oder Installationsroutinen, umfasst ist i.d.R. eine Paketierung erforderlich. Da eine Kompromittierung der genannten Bestandteile eine erhebliche Gefährdung für das Zielsystem darstellt, ist eine Signierung des Pakets typischerweise notwendig.

Punkt 5 umfasst das notwendige Vorgehen zur Bereitstellung der Softwarepakete, wie es z.B. in Form eines Softwarerepositoriums durchgeführt werden kann. Sofern die Softwarepakete signiert sind und somit deren Integrität automatisiert feststellbar ist, ist die Gefahr des Einschleusens von kompromittiertem Code über den Weg der Softwarebereitstellung eher gering. Allerdings kann eine Störung der Verfügbarkeit dazu führen, dass Software nicht installiert und somit Sicherheitslücken nicht geschlossen werden. Aus diesem Grund sind geeignete Maßnahmen zu Sicherstellung der Verfügbarkeit zu ergreifen. Des Weiteren ist zu überprüfen, wie Software vom signierenden System auf das System, das diese bereitstellt, übertragen wird, ohne dass die Vertraulichkeit des Schlüsselmaterials gefährdet wird.

Punkt 6 hat die Installation der bereitgestellten Software auf den jeweiligen Systemen zum Gegenstand. Hierzu bedarf es typischerweise einiger Modifikationen an diesen Systemen. So muss i.d.R., um eine Kompromittierung des zu installierenden Paketes auf dem bereitstellenden System oder aber während der Datenübertragung auszuschließen, eine Integritätsprüfung durchgeführt werden. Hierzu benötigt das jeweilige System entsprechende Schlüssel. Insbesondere wenn die Anzahl der Systeme, auf denen die

signierte Software installiert werden soll, groß ist, kann die Schlüsselverteilung und -verwaltung als auch deren Widerruf mit einem nicht unerheblichen Aufwand verbunden sein.

Des Weiteren muss entsprechendes Schlüsselmaterial in die UEFI-Zertifikatsspeicher eingetragen werden, was zumindest einen einmaligen physikalischen Zugriff auf das System bedingt.

Abschließend ist zu spezifizieren, wie die Nutzung von fehlerhafter oder nicht mehr benötigter aber gültig signierter Software verhindert wird. Zwar unterbindet das Löschen z.B. eines signierten Kernels von einem System dort dessen unmittelbare Ausführung. Einem Angreifer ist es jedoch u.U. möglich diesen erneut zu installieren und, sofern die Signatur nicht widerrufen ist, diesen somit auszuführen. Sofern der entsprechende Kernel Sicherheitslücken beinhaltet, können diese durch den Angreifer ausgenutzt und das System, trotz aktivem Secure Boot und dem Einspielen eines entsprechenden Updates, kompromittiert werden. Es ist aus diesem Grund für einen sicheren Einsatz von Secure Boot notwendig, den Start entsprechender Software, trotz durchgeführter Signierung, zu unterbinden.

Im Zusammenhang mit Secure Boot ist ein solcher Widerruf auf zwei verschiedenen Wegen umsetzbar. Zum einen kann das zur Signierung genutzte Schlüsselmaterial aus dem db-Zertifikatsspeicher entfernt werden. Hierbei ist jedoch zu beachten, dass somit jegliche Software deren Ausführung auf dem entfernten Schlüsselmaterial basiert, nicht mehr funktionstüchtig ist und ggf. erneut signiert, verteilt und installiert werden muss. Ein alternativer Ansatz ist die Aufnahme eines Hashes der unerwünschten Software in den dbx-Zertifikatsspeicher, um somit gezielt die Ausführung eines bestimmten Binärprogramms zu verbieten. Problematisch an diesem Ansatz ist jedoch, dass die UEFI-Spezifikation in der aktuellen Version 2.4 keinerlei Angabe zu der Anzahl der zu speichernden Hashes in dem dbx-Zertifikatsspeicher macht. Es besteht somit die Gefahr eines „Volllaufens“ des Zertifikatsspeichers, womit das Verhindern der Ausführung von fehlerhafter Software erschwert würde. Beide Ansätze bedingen eine automatische Modifikation des db- bzw. dbx-Zertifikatspeichers und somit zusätzlichen Aufwand zur Signierung entsprechender Updates mittels des UEFI Key Exchange Keys.

6.3.3 Einrichten des Bootloaders

Der erste Schritt zur Härtung eines Linux-Systems ist die Installation eines Secure-Boot-kompatiblen Bootloaders. Grundsätzlich sind hier mehrere Arten der Implementierung möglich.

Zum Einen kann ein einzelner signierter Bootloader eingesetzt werden, der als Bindeglied zwischen der UEFI-Firmware und dem zu ladenden Kernel dient. Dieser muss Secure Boot unterstützten, also insbesondere die Verifikation des Kernels im Sinne von Secure Boot durchführen. Der Vorteil des ersten Ansatzes ist seine Ähnlichkeit zum klassischen Bootvorgang und damit verbunden eine zumindest theoretisch gleichartige Einrichtung. Praktisch ist dieser Ansatz zum Zeitpunkt der Erstellung dieser Arbeit jedoch nur mit erheblichem Aufwand umsetzbar. Grund hierfür ist die Tatsache, dass keiner der verbreiteten Bootloader, wie z.B. Grub2 diesen Ansatz unterstützt. Insbesondere fehlt die Funktion, auf die UEFI-Zertifikatsspeicher zuzugreifen und eine kryptographisch sichere Verifizierung von zu ladendem Binärcode durchzuführen.

Ein weiterer Ansatz ist es, den Kernel, sofern er in Form einer EFI-Applikation vorliegt, direkt von der UEFI-Firmware verifizieren und starten zu lassen. Dies hat den Vorteil, dass durch den Verzicht auf einen Bootloader der Bootvorgang vereinfacht werden kann. Zu diesem Zweck definiert die UEFI-Spezifikation Schnittstellen zur Registrierung von EFI-Anwendungen gegenüber der Firmware. Auch schreibt der Standard die Unterstützung für ein Bootmenü, durch das der Benutzer das zu bootende System auswählen kann, vor. Die konkrete Gestaltung und das Vorgehen zum Aufruf dieses Menüs, wird jedoch nicht vorgegeben. Somit bedingt dieser Lösungsansatz plattformabhängige Unterschiede des Bootprozesses. Auch schränkt die Möglichkeit von Implementierungsfehlern der jeweiligen Plattformhersteller und die Tatsache, dass evtl. notwendige komplexe Initialisierungsschritte nicht unterstützt werden, die Einsatzfähigkeit dieser Lösung ein.

Einen dritten Lösungsansatz stellt die Nutzung mehrerer, aufeinander aufbauender Bootloader, die den Secure-Boot-Mechanismus kooperativ umsetzen, dar. Dies ist die zumindest prinzipiell komplexeste

Umsetzungsmöglichkeit. Sie bedingt, dass mehrere Bootloader verifiziert, d.h. üblicherweise signiert werden müssen. Auch bedingt dieser Lösungsweg die Kooperation dieser Bootloader und somit entsprechende Anpassungen. In der Praxis wird dieser Ansatz jedoch von vielen Linux-Distributionen, die Secure Boot unterstützen, mittels der Bootloader Shim und Grub2 umgesetzt.

Aufgrund der Tatsache, dass sich der letzte Ansatz in der Praxis bewährt hat, und die beiden anderen Ansätze einen hohen Arbeitsaufwand bzw. ein hohes Risiko plattformspezifischer Einschränkungen bedingen, wird im Folgenden der Einsatz von Shim zusammen mit Grub2 beschrieben. Hierbei übernimmt Grub2 alle Aufgaben eines typischen Bootloaders, mit Ausnahme der Verifizierung des zu ladenden Kernels. Hierfür greift Grub2 auf Shim zurück. Diese Arbeitsteilung ermöglicht es, insbesondere mit nur geringen Anpassungen am Quellcode von Grub2, eine Verifikation im Sinne von Secure Boot durchzuführen. Shim wird hierbei in einer ausschließlich durch eigenes Schlüsselmaterial signierten Form verwendet.

Debian 7.1.0 nutzt Grub2 als Bootloader und installiert diesen in der Version 1.99. Diese Version unterstützt zwar grundsätzlich das Booten in einer UEFI-Umgebung, nicht jedoch Secure Boot und die damit verbundenen Anforderungen zur Verifizierung des zu ladenden Linux-Kernels. Aus diesem Grund wird Grub2 1.99 durch die aktuellere Version 2.00 ersetzt werden. Um diesen Vorgang minimal invasiv zu gestalten, kann auf das Debian-Repository sid, welches bereits eine entsprechende Version von Grub2 beinhaltet, zurückgegriffen werden.

Diese Version enthält insbesondere einen Patch zur Verifikation eines zu ladenden Kernels durch Rückgriff auf Shim. Jedoch ist auch diese nicht ohne Weiteres für den oben beschriebenen Zweck nutzbar. Hierzu müssen drei Modifikation vorgenommen werden.

Die erste Modifikation ist nötig, da Grub2 grundsätzlich modular aufgebaut ist und durch Debian in modularer Form installiert wird. Eine Verifikation der Module beim Nachladen wird jedoch nicht unterstützt. Um der Gefahr der Kompromittierung des Bootloaders durch modifizierte Module zu begegnen, unterbindet Grub2 das Nachladen von Modulen bei aktiviertem Secure Boot grundsätzlich. Dies führt dazu, dass Grub2 in der im sid-Repository vorliegenden Form bei Einsatz von Secure Boot nicht funktionsfähig ist. Um dem Bootloader dennoch die zum Boot des Systems notwendigen Komponenten zur Verfügung zu stellen, ohne dessen Kompromittierung zu ermöglichen, muss dieser in eine monolithische Form überführt werden (s. Abschnitt 5.5.4.2).

Die zweite notwendige Anpassung des Bootloaders besteht darin, Module, die einen Bootvorgang ohne Verifikation im Sinne des Secure-Boot-Mechanismus ermöglichen, zu entfernen. Notwendig ist dies, da Grub2 eine Reihe unterschiedlicher Vorgehensweisen, in Form von Modulen, unterstützt, um verschiedenartige Betriebssystemkerne sowie weitere Bootloader zu starten. Ein Großteil dieser Verfahren unterstützt Secure Boot nicht und führt daher keine entsprechenden Verfizierungsschritte durch. Das Vorhandensein eines solchen Moduls böte daher die Möglichkeit, die Verifikationskette vorzeitig zu unterbrechen und den Secure-Boot-Vorgang somit zu unterwandern.

Der dritte Modifikationsschritt besteht aus der Signierung des Bootloaders mit dem entsprechenden Schlüsselmaterial.

6.3.4 Einrichten des Kernels

Ungeachtet der konkreten Funktionsweise des Bootloaders gibt es mehrere Anforderungen an den Linux-Kernel, um diesen auf sichere Weise in eine Secure Boot-Umgebung zu integrieren. Zum einen ist zu beachten, dass dieser im Rahmen seiner Kompilierung als EFI-kompatible Anwendung erstellt wird.[33] Ferner muss die Verifikation des Kernels während des Bootprozesses ermöglicht werden. Dies erfolgt typischerweise analog zum Bootloader durch Signierung der entsprechenden Binärdatei mit dem privaten Schlüssel des im UEFI-Zertifikatsspeicher hinterlegten Schlüsselmaterials. Ferner muss der Kernel in die Lage versetzt werden, zu ladende Kernelmodule zu verifizieren, sofern solche genutzt werden. Ansonsten kann eine Kompromittierung des Kernels durch das Laden von Schadcode in Form von Kernelmodulen

33 Hierzu müssen u.a. die Kernelübersetzungsoptionen CONFIG_EFI und CONFIG_EFI_STUB aktiviert sein.

erfolgen. Der Linux-Kernel unterstützt eine solche Verifizierung anhand asymetrischer Schlüssel. Hierzu wird während des Übersetzungsvorgangs des Kernels ein Zertifikat in diesen eingebettet. Mit dem zugehörigen privaten Schlüssel werden die Binärdateien der Kernelmodule signiert. Der Verifizierungsvorgang von Kernelmodulen ist somit unabhängig von dem, im Rahmen von Secure Boot eingesetzten, UEFI-Zertifikatsspeichern.

Wenngleich der zu Debian 7.1.0 gehörige Kernel in Form einer EFI-Anwendung ausgeliefert wird und somit eine Signierung unmittelbar möglich ist, so ist dieser dennoch nicht direkt zur Umsetzung des beschriebenen Ziels einsetzbar. Grund hierfür ist die Tatsache, dass der ausgelieferte Kernel modular aufgebaut ist und keine Verifizierung der mitgelieferten Kernelmodule durchführt. Um dies zu ändern kann der Kernel anhand des zugehörigen Debian-Quellcode-Pakets neu übersetzt werden und dessen Module in diesem Zuge signiert werden.[34]

Alternativ ist auch eine Übersetzung des Kernels in monolithischer Form denkbar. Die Notwendigkeit, Kernelmodule zu verifizieren, würde somit entfallen. Allerdings wäre ein solcher monolithischer Kernel aufgrund der konkreten Auswahl an eingebundenen Treibern und Funktionen sehr hardwarespezifisch. Dies würde die Nutzung auf verschiedenartigen Hardwareplattformen, so wie es der unveränderte Debian-Kernel ermöglicht, verhindern. Dieses Vorgehen ist daher nur in Ausnahmefällen sinnvoll.

Im Zusammenhang mit der Signierung von Kernelmodulen stellt sich ferner die Frage, welches Schlüsselmaterial hierzu zu nutzen ist und insbesondere, ob für jede Kernelversion unterschiedliches Schlüsselmaterial verwendet wird. Die Nutzung von gleichbleibenden Schlüsselmaterial zur Signierung von Modulen unterschiedlicher Kernelversionen hat den Vorteil, dass die Anzahl an verwendeten Schlüsseln und somit der Aufwand zu deren sicheren Verwahrung und Verwaltung minimiert wird. Dies ist insbesondere dann der Fall, wenn das Schlüsselmaterial, dass die Grundlage für den sonstigen Teil des Secure-Boot-Vorgang bildet, verwendet wird.

Dieser Ansatz bedingt jedoch ein signifikantes Sicherheitsrisiko. Beinhaltet ein Kernelmodul eine Schwachstelle, mittels derer der zugehörige Kernel kompromittiert werden kann, so wird dieser Gefahr i.d.R. dadurch begegnet, den Kernel samt seiner Module durch eine korrigierte Version auszutauschen. Wird jedoch zur Signierung der Kernelmodule des neuen Kernels das gleiche Schlüsselmaterial genutzt, das auch vormals für die Signierung des kompromittierbaren Kernelmoduls eingesetzt wurde, so wird der Verifizierungsvorgang des neuen Kernels das Laden des kompromitierbaren Kernelmoduls nicht unterbinden. Somit wäre es einem Angreifer u.U. möglich ein solches Kernelmodul zu verwenden, um eine eigentlich behobene Sicherheitslücke erneut zu nutzen und den Kernel hierüber zu kompromittieren. Dies ist insbesondere möglich, da der Kernel keine Möglichkeit bereitstellt die Signatur von Kernelmodulen zu widerrufen und somit einem solchen Angriff vorzubeugen. Hieraus resultiert, dass die Verwendung von gleichem Schlüsselmaterial für verschiedene Kernelversionen aus sicherheitstechnischen Gründen zu vermeiden ist.

Ein alternativer Ansatz besteht daher in der Nutzung von versionsspezifischen Schlüsseln. Durch die Verwendung des Schlüsselmaterials im Zusammenhang mit nur einer einzigen Kernelversion kann sichergestellt werden, dass eine Nutzung von Kernelmodulen über Versionsgrenzen hinweg vom Kernel erkannt und unterbunden wird. Nachteilig hierbei stellt sich im Allgemeinen die schnell wachsende Menge an zu verwaltender und sicher aufzubewahrender Schlüsseln und der damit verbundene Aufwand heraus.

Ein möglicher Lösungsansatz besteht darin, das jeweilige Schlüsselmaterial während des Übersetzungsprozesses zu erzeugen und den privaten Schlüssel nach der Signierung der Kernelmodule und der Einbettung des entsprechenden Zertifikats in dem Kernel zu löschen. Somit ist kein weiteres Schlüsselmaterial aufzubewahren. Ebenso wird sichergestellt, dass der Kernel nur diejenigen Module lädt, welche im Rahmen seines Übersetzungsprozesses erstellt wurden. Auch wird die Kompromittierung des verwendeten Schlüsselmaterials erschwert, da der zugehörige private Schlüssel nur für kurze Zeit während des Übersetzungsvorgangs existiert. Nachteilig ist jedoch, dass eine nachträgliche Signierung von

34 Wenngleich eine nachträgliche Signierung der Kernelmodule und die Einbettung des entsprechenden Zertifikats in den Kernel technisch denkbar sind, so existieren hierzu zur Zeit der Erstellung dieser Arbeit keine öffentlich verfügbaren Werkzeuge oder Anleitungen.

Kernelmodulen, aufgrund des fehlenden privaten Schlüssels, nicht möglich ist. Eine nachträgliche Erstellung von ladbaren Kernelmodulen, z.B. von Gerätetreiben von Drittanbietern, wird somit verhindert.

Abschließend ist daher die Nutzung von Schlüsselmaterial, welches nur für eine spezifische Kernelversion verwendet und nach dem Signierungsvorgang gelöscht wird, zu empfehlen, sofern auf eine nachträgliche Erstellung von Kernelmodulen verzichtet werden kann.

6.4 Risiken und Herausforderungen

6.4.1 Risiken

6.4.1.1 Kompromittierung kryptografischer Verfahren

Ein grundsätzliches Risiko beim Einsatz von Secure Boot ist die Kompromittierung der zugrundeliegenden kryptographischen Verfahren. Zwar hat sich RSA, welches typischerweise zur Signierung im Zusammenhang mit Secure Boot eingesetzt wird, in der Vergangenheit bei hinreichender Schlüssellänge als robust gegen Angriffe herausgestellt. Für einige der von Secure Boot unterstützen Hash-Verfahren sind jedoch Kollisionsangriffe bekannt, die zum Teil auch praktisch durchführbar sind. Insbesondere sind in diesem Zusammenhang die Verfahren md5 und sha1 zu nennen. Es ist somit bei Verwendung von Secure Boot insbesondere auf die kryptografische Stärke der gewählten Verfahren zu achten.

6.4.1.2 Kompromittierung einer Zertifikatsstelle

Wesentlich für die Sicherheit von Secure Boot ist die Vertraulichkeit der verwendeten privaten Schlüssel. Werden diese kompromittiert, so ist es einem Angreifer u.U. möglich, Schadcode zu signieren und trotz aktivem Secure Boot zur Ausführung zu bringen. Aus diesem Grund sind umfangreiche organisatorische und technische Maßnahmen vom Betreiber der Zertifikatsstelle zu ergreifen, um diese unter Berücksichtigung der jeweiligen Bedrohungslage zu sichern.

Insbesondere wenn die Verifizierung während des Secure-Boot-Vorgangs in Teilen oder in Gänze auf fremdem Schlüsselmaterial basiert, hängt die Sicherheit des Prozesses in erheblichem Maße von dem signierenden Drittanbieter ab. Eine solche Abhängigkeit besteht z.B. beim Einsatz von Microsoft Windows 8 Pro und Fedora 19, sofern die entsprechenden Systemkomponenten nicht vollständig und ausschließlich mittels eigenem Schlüsselmaterial signiert werden. Eine Kompromittierung des Schlüsselmaterials bei einem Drittanbieter ist hierbei sowohl durch einen gesetzwidrigen Angriff, als auch im Zusammenhang mit rechtlichen Rahmenbedingungen durch staatliche Stellen denkbar. Letzteres ist insbesondere von Bedeutung, sofern das genutzte Schlüsselmaterial im Ausland gespeichert wird.

Auch ist beim Einsatz von Secure Boot die Planung des Rückrufs eines kompromittierten Zertifikats unabdingbar. Insbesondere ergeben sich je nach Verwendungsart des kompromittierten Schlüsselmaterials sehr unterschiedliche Anforderungen an die Durchführung des Rückrufs. Ebenfalls ist zu klären, inwieweit eine notwendig gewordene Modifikation der Zertifikatsspeicher automatisiert werden kann oder ob im Falle einer Kompromittierung ein physikalischer Zugriff auf die betroffenen Systeme notwendig ist.

Des Weiteren ist zu beachten, dass Secure Boot die Einbindung mehrerer Zertifikatsstellen, durch Installation mehrerer Schlüssel im KEK-Zertifikatsspeicher erlaubt. Die Kompromittierung einer einzelnen Zertifikatsstelle genügt in einem solchen Fall prinzipiell zur Kompromittierung des Secure-Boot-Vorgangs.

6.4.1.3 Kompromittierung des Kernels zur Laufzeit

Wenngleich es im Rahmen von Secure Boot möglich ist die Integrität von Kernelmodulen zu verifizieren und somit eine unmittelbare Kompromittierung des Kernels zu verhindern, so besteht weiterhin die Möglichkeit durch Ausnutzung von Schwachstellen Schadcode in den Kernel einzubringen. Eine solche Art der Kompromittierung wird durch Secure Boot weder verhindert, noch signifikant erschwert. Härtungsmaßnahmen und das Einspielen von Sicherheitsupdates des Systems und insbesondere des Kernels kann Secure Boot daher nicht ersetzen.

6.4.1.4 Kompromittierung des Userspaces

Secure Boot schützt lediglich den Kernel, nicht jedoch Programme die im User-Space arbeiten. Wenngleich die Kompromittierung des Kernel einem Angreifer oder einer Schadsoftware die umfangreichsten Möglichkeiten bietet und somit üblicherweise das Worst-Case-Szenario darstellen, so hat die Kompromittierung eines User-Space-Programmes u.U. eine ähnlich verheerende Wirkung auf die Integrität des Systems. Eine besondere Gefährdung geht hierbei von Anwendungen aus, die mit besonders hohen Privilegien ausgeführt werden.

Im Zusammenhang mit Linux-Systemen ist hier der init-Prozess, der grundsätzlich mit Root-Rechten gestartet und wesentlichen Einfluss auf das Systemverhalten und die Ausführung weiterer Anwendungen hat, erwähnt. Auch besteht ein Schutz einer initialen Ramdisk typischerweise nur insofern, als das die enthaltenen Kernelmodule durch den Kernel während des Ladevorgangs verifiziert werden. Secure Boot bedingt jedoch nicht die Überprüfung von User-Space-Programmen die auf einer Ramdisk gespeichert sind.

Secure Boot kann daher entsprechende Schutzmaßnahmen zum Schutz des User-Spaces, wie z.B. Virenscanner, nicht ersetzen.

6.4.1.5 Umgehen von Secure Boot durch physikalischen Zugang

Da die UEFI-Firmware eine Deaktivierung von Secure Boot über das UEFI-Setup ermöglicht, besteht grundsätzlich die Gefahr, dass ein Benutzer des Systems, der physikalischen Zugang zu diesem hat, Secure Boot deaktiviert oder anderweitig dessen Konfiguration ändert. Somit wäre er im Stande das Betriebssystem unerlaubt zu modifizieren oder ein alternatives Betriebssystem zu starten. Ziel hierbei kann die gezielte Durchführung unerlaubter Handlungen sein, welche von dem installierten Betriebssystem andernfalls unterbunden würden. Beispiele hierfür sind das Kopieren von Daten auf einen Wechseldatenträger oder die Installation von Schadsoftware. Das Setzen eines Kennwortes zum Aufruf des UEFI-Setups kann diesbezüglich prinzipiell Abhilfe schaffen.

6.4.1.6 Kompromittierung der UEFI-Firmware

Eine Voraussetzung für den zuverlässigen Einsatz von Secure Boot im konkreten und die Integrität des Systems im Allgemeinen, ist die Korrektheit, Vertrauenswürdigkeit und Integrität der UEFI-Firmware. Arbeitet die Firmware die Arbeitsschritte des Secure-Boot-Vorgangs, insbesondere die Verifizierung der zu startenden EFI-Anwendungen nicht spezifikationsgemäß ab, so ist u.U. eine Kompromittierung des Bootprozesses möglich und somit dessen Sicherheit nicht gegeben. Mögliche Ursachen können Fehler bei der Programmierung der Firmware als auch beabsichtigte Abweichungen von der Spezifikation, z.B. um eine Schwächung des Bootprozesses zu bewirken, sein.

Ein weiterer Grund für eine nicht korrekte Durchführung von Secure Boot ist die Kompromittierung der UEFI-Firmware durch einen Angreifer oder durch Schadsoftware. Diese Gefahr besteht insbesondere aufgrund der umfangreichen UEFI-Spezifikation und der damit einhergehenden Komplexität der Firmware-Software. Insbesondere ist zu mutmaßen, dass der, gegenüber dem klassischem PC-BIOS, erweiterte Funktionsumfang der UEFI-Firmware, dieses in Zukunft zu einem lohnenswerten Angriffsziel

für Schadsoftware macht. In diesem Zusammenhang ist z.B. die Netzwerkunterstützung zu nennen. Auch ist zu mutmaßen, dass durch die Standardisierung der entsprechenden Firmware-Schnittstellen die Entwicklung von Schadsoftware, die die Firmware angreift, vereinheitlicht werden kann und diese somit vereinfacht.

6.4.1.7 Kompromittierung des Signierungsprozesses

Soll Software, die während des Secure-Boot-Vorgangs ausgeführt wird, unabhängig vom Distributor der jeweiligen Software signiert werden, so bedarf es eines entsprechenden Signierungsprozesses, der alle Vorgänge zur Durchführung einer Softwaresignierung beschreibt. Ferner bedarf es einer Signierungsplattform mittels derer die Signierung im Rahmen des Signierungsprozesses durchgeführt wird.

Von besonderer Bedeutung ist hierbei die Gestaltung dieses Prozesses hinsichtlich sicherheitstechnischer Aspekte. Um die, aus Sicherheitsgründen zwingend notwendige Einhaltung des Prozesses zu gewährleisten, ist dieser ebenfalls möglichst „alltagstauglich“ zu entwerfen. Ebenso ist die Integrität der zur Signierung genutzten Hardwareplattformen und IT-Infrastruktur zwingend notwendig.

Wird der Signierungsprozess fehlerhaft oder unvollständig durchgeführt oder sind die genutzten IT-Systeme kompromittiert, so ist die Sicherheit des Secure-Boot-Vorgangs nicht gewährleistet.

Besonders kritisch ist in diesem Zusammenhang die Beschaffung der zu signierenden Software, deren Prüfung und deren Signierung ohne die Vertraulichkeit des Schlüsselmaterials zu gefährden. Insbesondere ist zu beachten, dass die zu signierende Software typischerweise über das Internet bezogen wird und das der Signierungsprozess aufgrund von Sicherheitsupdates dieser Softwarekomponenten regelmäßig ausgeführt werden muss. So ist u.a. sicherzustellen, dass eine bei der Übermittlung der Software durchgeführte Kompromittierung verhindert oder erkannt wird. Auch ist das zur Signierung verwendete Schlüsselmaterial, unter Berücksichtigung der Anforderungen Software aus dem Internet zu beziehen und den Prozess effizient zu gestalten, zu schützen. Ferner stellt sich die Frage, nach welchen Kriterien und in welchem Umfang die zu signierende Software untersucht wird. Des Weiteren ist die Gefährdung des signierenden Systems durch die Verteilung der signierten Software möglichst zu minimieren.

6.4.1.8 Kompromittierung des Software-Repositoriums

Eine weitere Schwachstelle kann das Software-Repositorium, welche zur Verteilung der signierten Software genutzt wird, sein. Da die das Secure-Boot-Verfahren nutzenden Plattformen ihre Software und Updates von diesem beziehen, stellt es ein u.U. lohnenswertes Ziel für einen Angreifer dar. Daher bedarf dieses System eines erhöhten Schutzes. Zur weitergehenden Sicherung des Softwareverteilungsprozesses ist es sinnvoll, die bereitgestellten Pakete, unabhängig von der Signierung der enthaltenden Software ebenfalls zu signieren. Somit kann sichergestellt werden, dass das Zielsystem eine Manipulation auch an Nebenbestandteilen der Softwarepakete, wie z.B. an Installationsskripten erkennt und eine Kompromittierung dieser Systeme somit verhindert werden kann. Notwendig ist hierfür zumindest eine einmalige Schlüsselverteilung auf alle Zielsysteme, um eine Verifizierung der Softwarepakete zu ermöglichen.

6.4.1.9 Kompromittierung durch veraltete Software

Neben der Möglichkeit den Kern eines Betriebssystems während des Bootvorgangs zu kompromittieren, ist es möglich, dies nach Abschluss des Bootvorgang durchzuführen. Oftmals basieren solche Angriffe auf Fehlern im Kernel, welche sich zur Einschleusung von Schadcode ausnutzen lassen. Eine derartige Sicherheitslücke wird durch ein entsprechendes Update, also das Ersetzen der fehlerhaften Software durch eine korrigierte Version, geschlossen. Findet ein solches Update auf einem durch Secure Boot geschütztem System statt, so ist zu beachten, dass die fehlerhafte Version aufgrund ihrer Signierung weiterhin bootfähig

ist. Sofern ein Angreifer auf eine solche vormals benutzte Version Zugriff hat, kann er diese trotz aktiviertem Secure Boot zur Ausführung bringen und die vorhandene Sicherheitslücke ausnutzen.

Es ist daher sicherzustellen, dass veraltete Betriebssystemkomponenten trotz valider Signierung nicht mehr ausgeführt werden. In der Regel wird dies durch Erstellung eines entsprechenden Eintrags in dem dbx-Zertifikatsspeicher erfolgen. Hierbei muss jedoch sichergestellt werden, dass dies auf allen Systemen, die die Signierung der veralteten Software als valide ansehen, durchgeführt wird. Auch ist zu beachten, dass die Verifizierung von Betriebssystemkomponenten nicht ausschließlich auf den UEFI-Zertifikatsspeichern basiert. Beispielsweise überprüft der Linux-Kernel die zu ladenden Kernelmodule unabhängig von den UEFI-Zertifikatsspeichern und besitzt keinen Mechanismus zur Verhinderung des Ladens von Modulen mit valider Signatur.

6.4.2 Herausforderungen

6.4.2.1 Unbeabsichtigtes Signieren von kompromittiertem Code

Da die Integrität der im Rahmen des Bootvorgangs zu ladenden Komponenten im Linux-Umfeld i.d.R. ausschließlich auf Grund der Überprüfung von Signaturen sichergestellt wird, ist besondere Sorgfalt bei der Signierung zwingend notwendig.

In der Praxis stellt sich hier insbesondere die Frage, wie die Integrität des zu signierenden Binärcodes sicherzustellen ist. Da Komponenten wie der Linux-Kernel komplexe Gebilde sind, ist eine manuelle Überprüfung des zugrundeliegenden Codes i.d.R. ausgeschlossen.

Hier bleibt dem Anwender u.U. nur die Möglichkeit darauf zu vertrauen, dass der Distributor des jeweiligen Betriebssystems eine sorgfältige Überprüfung des von ihm ausgelieferten Codes durchführt. Dieser Ansatz kann auch deshalb einen sinnvollen Kompromiss zwischen Sicherheit und Arbeitsaufwand darstellen, da auch andere Leistungen, die von dem Distributor in Anspruch genommen werden, wie z.B. das Bereitstellen von Benutzeranwendungen oder Sicherheitsupdates, ein starkes Vertrauensverhältnis bedingen. Im Falle einer solchen Signierung auf Vertrauensbasis ist jedoch sicherzustellen, dass Dritte den Quell- oder Binärcode nicht vor der Signierung modifizieren können. Insbesondere ist hier auf eine sichere Datenübermittlung zwischen Distributor und CA, als auch auf die Integrität des signierenden Systems zu achten.

6.4.2.2 Absichtliches Signieren von kompromittiertem Code

Neben der Gefahr des unbeabsichtigten Signierens von kompromittiertem Code besteht ebenso die Gefahr, dass schadhafter Code absichtlich signiert wird, um den Schutz durch Secure Boot zu unterwandern. Ein solcher Angriff durch einen Innentäter mit Zugang zum entsprechenden Schlüsselmaterial stellt, aufgrund seiner besonderen Kenntnissen der IT-Umgebung, eine erhebliche Gefahr dar. Auch ist zu beachten das i.d.R. eine erhöhte Wahrscheinlichkeit besteht, dass ein solcher Angriff unentdeckt bleibt.

In diesem Zusammenhang stellt sich die Frage, welche und wie viele Personen die Möglichkeit haben, Code zu signieren. Mit steigender Größe dieses Personenkreises entsteht zumindest eine statistische Erhöhung des Missbrauchsrisikos. So sollte eine Anforderung an die Umsetzung einer durch Secure Boot gesicherten Umgebung der möglichst restriktive Zugang zu Schlüsselmaterial für eine möglichst kleine Anzahl an Personen sein. Dem gegenüber stehen jedoch zumeist eine Reihe an Anforderungen aus dem Arbeitsalltag. Beispielsweise stellt sich die Frage, inwieweit Secure Boot administrative Arbeiten, wie z.B. Diagnosemaßnahmen behindert. Gleiches gilt für den Einsatz eines Betriebssystemkerns, der speziell für den Einsatz auf einer einzelnen Hardwareplattform angepasst werden muss. Eine solche Individualisierung des Betriebssystems kann z.B. bei Konflikten mit neuer Hardware oder fehlenden Treibern notwendig sein.

Auf Grund dieser Konfliktsituation zwischen Sicherheits- und Effizienzanforderungen besteht die Gefahr, dass sich evtl. auch entgegen der Bestimmungen von Unternehmens- oder Behördenrichtlinien der

Personenkreis mit Zugang zu entsprechenden Schlüsselmaterial vergrößert und eine Zugriffskontrolle nicht mehr effektiv durchgeführt wird und sich somit das Risiko eines Angriffs durch einen Innentäter vergrößert.

6.4.2.3 Installieren von nicht signierter Software

Wenngleich es das Ziel von Secure Boot ist, die Ausführung von Schadcode während des Bootvorgangs zu verhindern, so kann Secure Boot jedoch nicht zwischen bösartigem und gutartigem, aber nicht signiertem Code, unterscheiden.

Wird somit ein autorisiertes, jedoch nicht korrekt signiertes Update eingespielt, so bootet das System nach einem Neustart nicht mehr. Gleiches gilt für die Modifikation signierter Software, z.B. im Zuge von Wartungsarbeiten.

In diesem Zusammenhang stellt sich die Frage, wie ein System, das einmal in einen solchen Zustand geraten ist, wieder repariert wird. Insbesondere wenn sich ein solcher Vorfall durch das automatische Einspielen eines fehlerhaften Updates auf einer großen Anzahl von Systemen ereignet, kann eine effizient durchführbare Behebungsmaßnahme sowohl für die Aufrechterhaltung des Betriebs, als auch für die Akzeptanz von Secure Boot, von großer Bedeutung sein.

6.4.2.4 Unerlaubtes Deaktivieren von Secure Boot

Aus der schon in Abschnitt 6.4.2.2 beschriebenen Konfliktsituation zwischen Sicherheits- und Effizienzanforderungen besteht ebenso die Gefahr, dass Secure Boot zeitweise evtl. aber auch dauerhaft auf Systemen unerlaubt und unkoordiniert deaktiviert wird. Hierbei ist insbesondere problematisch, dass die für Sicherheit zuständigen Stellen bei fehlendem Wissen über diese Deaktivierung weiterhin einen entsprechenden Schutz des jeweiligen Systems annehmen. Somit besteht nicht nur ein erhöhtes Risiko der Kompromittierung des Systems durch die Deaktivierung der Schutzmaßnahmen, sondern auch ein evtl. zu geringes Risikobewusstsein bei den für IT-Sicherheit zuständigen Personen.

Technische Schutzmaßnahmen, die eine unerlaubte Deaktivierung von Secure Boot verhindern, sind nur bedingt verfügbar. Zwar ist es möglich, das UEFI-Setup mit einem Kennwort zu schützen und somit den Personenkreis, die eine Deaktivierung durchführen können, prinzipiell zu beschränken. Hier stellt sich jedoch die Frage, wie effektiv ein solcher Passwortschutz in der Praxis ist und inwieweit der Personenkreis mit Wissen dieses Kennwortes, insbesondere vor dem Hintergrund, dass der Zugriff auf das UEFI-Setup auch für eine Reihe anderer administrativer Arbeiten notwendig ist, ausreichend eingeschränkt werden kann.

6.4.2.5 Überschätzung des Schutzumfangs von Secure Boot

Ein weiteres Risiko besteht in einer möglichen Fehleinschätzung des Schutzumfanges von Secure Boot seitens der für IT-Sicherheit verantwortlichen Stellen. Fehlendes Wissen über die Tatsache, dass Secure Boot lediglich die Integrität des Betriebssystemkerns während des Boot-Vorgangs sicherstellen soll, und sich der Schutzumfang daher nicht auf das gesamte System bezieht und auch nur zeitlich begrenzt ist, kann zu einer Überschätzung der Schutzfähigkeit von Secure Boot führen. Der Sachverhalt, dass der tatsächliche Schutzumfang, der von verschiedenen Betriebssystemen mittels Secure Boot umgesetzt wird, sich signifikant unterscheidet, kann diesen Effekt noch einmal verschärfen. So erzielt z.B. Ubuntu 13.04 durch Nutzung von Secure Boot keinen signifikanten Sicherheitsgewinn. Auch ist diesbezüglich eine präzise Einschätzung von Windows 8 Pro auf Grund des komplexen Zusammenspiels von Kernel- und User-Space-Komponenten nur mit erheblichem Aufwand möglich. Insbesondere ist hier zu berücksichtigen, dass Windows 8 Pro Treiber von Drittanbietern standardmäßig auch dann lädt, wenn deren Integrität nicht verifiziert werden konnte.

Die Überschätzung der Schutzfähigkeit birgt eine erhöhte Gefahr eines unzureichenden Risikobewusstseins und somit auch die Gefahr andere adäquate Schutzmaßnahmen zu vernachlässigen.

6.4.2.6 Zurückhalten von Sicherheitsupdates

Die Verifizierung von Software im Rahmen des Secure-Boot-Vorgangs bedingt die vorherige Überprüfung der Integrität und ggf. dessen Signierung. Wenngleich die entsprechenden Arbeitsschritte bei einer geplanten Einführung eines neuen Betriebssystems oder einer neuen Betriebssystemversion von langer Hand geplant und somit effizient in den Arbeitsablauf eingebettet werden können, so ist der Zeitpunkt für das notwendige Einspielen von Updates weit weniger vorhersagbar. Erschwerend kommt hinzu, dass der Arbeitsaufwand aufgrund der hohen Sicherheitsanforderung an den Signierungsvorgang u.U. nicht unerheblich ist. Hierzu gegensätzlich ist die Anforderung Sicherheitsupdates, insbesondere von so sicherheitskritischen Systemkomponenten wie dem Betriebssystemkern, zeitnah einzuspielen.

Es besteht daher die Gefahr, dass es zu einem „Verschleppen“ der Signierung sicherheitskritischer Updates und somit zu einer verspäteten Verteilung kommt. Dies hätte zur Folge, dass Schwachstellen länger als notwendig unbehoben bleiben und somit das Risiko einer Kompromittierung der entsprechenden Systeme steigt.

6.4.2.7 Fehlende Kompatibilität zur Anwendungsprogrammen

Um einen effektiven Schutz der Kernels zu gewährleisten, kann der Funktionsumfang des Betriebssystems, gegenüber einer Version die nicht mittels Secure Boot gestartet wird, eingeschränkt sein. Der Linux-Kernel unterstützt beispielsweise, sofern er mit aktivem Secure Boot gestartet wurde, keinen direkten Zugriff auf den Hauptspeicher mittels der Datei /dev/mem. Solche Funktionseinschränkungen können u.U. inkompatibel zu Anwendungsprogrammen, insbesondere solche die hardwarenahe Aufgaben ausführen, sein

6.5 Zusammenfassung

Im Folgenden werden die möglichen Betriebsarten von Secure Boot zusammengefasst und deren Realisierungsaufwand und der mögliche Sicherheitsgewinn gegenüber gestellt. Hierbei ist zu beachten, dass die Abschätzung des konkret erzielbaren Sicherheitsgewinns und somit die Abwägung des Einsatzes von Secure Boot letztendlich nur unter Berücksichtigung einer genauen Bedrohungsanalyse des jeweiligen Systems sinnvoll ist.

Zum einen kann Secure Boot gänzlich deaktiviert werden. Natürlicherweise entfaltet Secure Boot in diesem Modus keine Schutzfunktion. Ein solcher Einsatz ist für Systeme denkbar, die nur einen eingeschränkten Schutz benötigen oder aber deren Betriebssystem schon aufgrund anderer organisatorischer und technischer Schutzmaßnahmen in ausreichendem Maße gesichert ist. Auch kann dieser Betriebsmodus notwendig sein, sofern das eingesetzte Betriebssystem Secure Boot nicht unterstützt und eine entsprechende Anpassung nicht möglich oder nicht sinnvoll ist. Ebenso kann die Deaktivierung von Secure Boot notwendig sein, falls ein Betrieb mit Fremdschlüsseln z.B. von Microsoft nicht in Betracht kommt und die Verwendung von eigenem Schlüsselmaterial aufgrund des damit verbundenen hohen Aufwands nicht zu rechtfertigen ist.

Des Weiteren kann Secure Boot mittels Fremdschlüsseln, also Schlüsseln die von Dritten erstellt und verwaltet werden und auf dessen privaten Schlüsselteil kein Zugriff besteht, betrieben werden. Typischerweise wird das entsprechende Schlüsselmaterial vom Hersteller oder Distributor des Betriebssystems verwaltet, welcher auch die Prüfung und Signierung der Software übernimmt. In der Praxis sind in diesem Zusammenhang insbesondere die von Microsoft erstellten und auf von Microsoft zertifizierten Hardwareplattformen vorzufindenden Schlüssel relevant. Darüber hinaus nutzen auch

Linux-Distributionen wie Ubuntu 13.04 und Fedora 19, für einige der am Bootvorgang beteiligten Anwendungen, eigenes Schlüsselmaterial.

Der Sicherheitsgewinn, der mit einer solchen Lösung erzielt werden kann, ist hierbei u.a. vom Umfang der Signierung abhängig. Für die Absicherung des Bootloaders genügt die Verwendung eines signierten Bootloaders. Um weitergehende unerlaubte Modifikationen des Betriebssystemkerns zu verhindern, bedarf es einer lückenlosen Verifizierung sowohl der eingesetzten Bootloader, des Kerns als auch evtl. vorhandener Kernelmodule, wie z.B. Treiber. Findet eine solche lückenlose Überprüfung nicht statt, so kann dies von einem Angreifer oder einer Schadsoftware genutzt werden, um in Folge in den Bootprozess einzugreifen und das System zu kompromittieren. Hieraus folgt, dass ein maximaler Sicherheitsgewinn i.d.R. nur dann zu erzielen ist, sofern eine solch lückenlose Verifizierung und somit eine Signierung aller erwähnten Systemkomponenten durchgeführt wird.

Ferner ist der mögliche Sicherheitsgewinn bei Nutzung von Fremdschlüsseln in erheblichem Maße vom Besitzer des Schlüsselmaterials abhängig. Insbesondere können die vom Schlüsselbesitzer umgesetzten Sicherheitsvorkehrungen i.d.R. weder überprüft oder der eigenen Bedrohungslage angepasst werden. Hierdurch ergibt sich die Gefahr einer u.U. auch unentdeckten Kompromittierung des Schlüsselmaterials und somit die Möglichkeit Secure Boot zu unterwandern. Eine solche Kompromittierung ist, neben der Möglichkeit eines ungesetzlichen Angriffs, auch auf Basis gesetzlicher Rahmenbedingungen durch staatliche Organisationen denkbar.

Um die zuletzt genannten Probleme zu vermeiden, kann ferner ausschließlich eigenes Schlüsselmaterial verwendet werden. Ein solches Vorgehen bedingt jedoch, sowohl bei der Einführung als auch durch die regelmäßig notwendige Wartung der betroffenen Systeme, einen erheblichen Arbeitsaufwand. Auf Grund des hohen Aufwandes ist eine solche Nutzung von Secure Boot daher typischerweise nur für Systeme sinnvoll, welche einen besonders hohen Schutzbedarf aufweisen. Hier ist alleine durch die Nutzung von eigenem Schlüsselmaterial eine erhöhte Kontrolle über die installierten Bootloader und Betriebssysteme gegeben. Eine Maximierung der Sicherheit ist, wie bei der Nutzung von Fremdschlüsseln auch, nur gegeben, sofern eine lückenlose Verifizierung aller oben genannter Systemkomponenten möglich ist. Sofern letzteres gegeben ist, stellt Secure Boot eine effektive Möglichkeit dar, nicht nur den Bootprozess sondern auch weitere Komponenten des Systems an sich abzusichern.

In Tabelle 3 wird der Aufwand und der erzielbare Sicherheitsgewinn bei Nutzung von Secure Boot mit fremdem und eigenem Schlüsselmaterial gegenüber gestellt. Hierbei ist zu beachten, dass diese Darstellung lediglich eine grobe Einschätzung des Regelfalles darstellt und bei Berücksichtigung einer konkreten Bedrohungslage durchaus Abweichungen denkbar sind.

	Fremdes Schlüsselmaterial		**Eigenes Schlüsselmaterial**	
Nur Bootloader	Aufwand: Sicherheitsgewinn:	keiner niedrig	Aufwand: Sicherheitsgewinn:	mittel moderat
Bootloader, Kernel und Kernelmodule	Aufwand: Sicherheitsgewinn:	keiner moderat	Aufwand: Sicherheitsgewinn:	hoch hoch

Tabelle 3: Nutzung und möglicher Sicherheitsgewinn

7 Anhang

7.1 Patches für die EFI-Tools

Die folgenden Patches sind Fehlerbeseitigungen der EFI-Tools und notwendig um auf den untersuchten Plattformen unter Linux mit den EFI-Tools arbeiten zu können. Sie wurden dem Autor der EFI-Tools James Bottomley übersendet. Eine Antwort seinerseits steht bislang aus. Die Patches basieren in der hier dargestellten Reihenfolge auf dem git commit f5d338c8758df209b32d2ed66bc3228f3c3c5ae4.

```
From 9e674e1bfce61d3ae7d6892907d60f0b07250f0f Mon Sep 17 00:00:00 2001
From: Hendrik Schwartke <hendrik@os-t.de>
Date: Thu, 25 Jul 2013 13:43:32 +0000
Subject: [PATCH 1/4] Fixed bug that causes the efitools to overlook the
 efivarfs mount point

---
 lib/kernel_efivars.c |    2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)

diff --git a/lib/kernel_efivars.c b/lib/kernel_efivars.c
index 3c5852c..86ac522 100644
--- a/lib/kernel_efivars.c
+++ b/lib/kernel_efivars.c
@@ -38,7 +38,7 @@ kernel_variable_init(void)
      if (kernel_efi_path)
            return;
      mktemp(fname);
-     snprintf(cmdline, sizeof(cmdline), "mount -l > %s", fname);
+     snprintf(cmdline, sizeof(cmdline), "mount > %s", fname);
      ret = system(cmdline);
      if (WEXITSTATUS(ret) != 0)
            /* hopefully stderr said what was wrong */
--
1.7.10.4

From 0049bc9da66e0fecc1f5f032bc7c760c2b08a287 Mon Sep 17 00:00:00 2001
From: Hendrik Schwartke <hendrik@os-t.de>
Date: Thu, 25 Jul 2013 14:26:01 +0000
Subject: [PATCH 2/4] Fixed bug causes efitolls to overlook the efivarfs mount
 point.

---
 lib/kernel_efivars.c |    4 ++--
 1 file changed, 2 insertions(+), 2 deletions(-)

diff --git a/lib/kernel_efivars.c b/lib/kernel_efivars.c
index 86ac522..1e7681d 100644
--- a/lib/kernel_efivars.c
+++ b/lib/kernel_efivars.c
@@ -68,8 +68,8 @@ kernel_variable_init(void)

            sscanf(ptr, "%*s on %s type %s %*s\n%n", path, type, &count);
            ptr += count;
-           if (strcmp(type, "efivarfs") != 0)
-                 continue;
+           if (strcmp(type, "efivarfs") == 0)
+                 break;
      }
```

```
      if (strcmp(type, "efivarfs") != 0) {
            fprintf(stderr, "No efivarfs filesystem is mounted\n");
--
1.7.10.4

From 382f8728a466f51f16936673afcd292d57368cc6 Mon Sep 17 00:00:00 2001
From: Hendrik Schwartke <hendrik@os-t.de>
Date: Fri, 26 Jul 2013 10:10:02 +0200
Subject: [PATCH 3/4] Fixed bug in get_variable that causes efi-readvar to
 print negative cerificate lengths

---
 lib/kernel_efivars.c |    4 ++++
 1 file changed, 4 insertions(+)

diff --git a/lib/kernel_efivars.c b/lib/kernel_efivars.c
index 1e7681d..41d1cf2 100644
--- a/lib/kernel_efivars.c
+++ b/lib/kernel_efivars.c
@@ -101,6 +101,10 @@ get_variable(const char *var, EFI_GUID *guid, uint32_t
*attributes,

      if (fstat(fd, &st) < 0)
            return errno;
+     if (st.st_size == 0) {
+           *size = 0;
+           return 0;
+     }
      if (size)
            *size = st.st_size - sizeof(attr);

--
1.7.10.4

From 8f15815a9e7551361544399526c74b2ec6555223 Mon Sep 17 00:00:00 2001
From: Hendrik Schwartke <hendrik@os-t.de>
Date: Fri, 26 Jul 2013 14:56:01 +0200
Subject: [PATCH 4/4] Inserting a Certificate to the PK certificate store is
 now possible on setup mode

---
 efi-updatevar.c |    4 ++--
 1 file changed, 2 insertions(+), 2 deletions(-)

diff --git a/efi-updatevar.c b/efi-updatevar.c
index 62a8175..be56cb1 100644
--- a/efi-updatevar.c
+++ b/efi-updatevar.c
@@ -274,9 +274,9 @@ main(int argc, char *argv[])
            st.st_size = len;
      }

-     if (esl_mode && (!variable_is_setupmode() || strcmp(variables[i], "PK") ==
0)) {
+     if (esl_mode && !variable_is_setupmode()) {
            if (!key_file) {
-                 fprintf(stderr, "Can't update variable%s without a key\n",
variable_is_setupmode() ? "" : " in User Mode");
+                 fprintf(stderr, "Can't update variable without a key\n");
                  exit(1);
            }
            BIO *key = BIO_new_file(key_file, "r");
```

```
--
1.7.10.4
```

7.2 Zertifikate der HP-Plattform

7.2.1 PK

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1b:6a:ef:49:8c:fb:7f:90:b6:81:32:1a:e8:9e:c2:ef
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Hewlett-Packard Company, CN=Hewlett-Packard Printing
Device Infrastructure CA
        Validity
            Not Before: Aug  8 00:00:00 2012 GMT
            Not After : Aug  8 23:59:59 2032 GMT
        Subject: O=Hewlett-Packard Company, OU=Long Lived CodeSigning
Certificate, CN=Hewlett-Packard UEFI Secure Boot Platform Key
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e9:b8:62:b8:59:d9:e0:45:50:64:54:a0:0d:60:
                    5b:b2:59:89:25:38:a1:37:ce:65:a8:a2:95:4b:f4:
                    0c:e6:3d:89:ee:30:c7:96:64:8e:5f:e4:c8:0f:51:
                    4b:f3:4f:ec:7a:7e:b7:0d:31:89:b8:26:21:55:51:
                    f0:64:0d:3d:b1:76:c6:d9:55:12:4f:8b:dc:b5:32:
                    c8:6f:d2:16:f8:c9:ac:6f:9d:1e:e7:72:b1:e8:e2:
                    dd:40:b7:c9:b0:e3:5c:cf:87:56:82:67:82:24:8e:
                    6e:cc:03:4a:d7:29:29:57:28:8a:40:bb:52:9f:bb:
                    cb:22:7a:ae:ca:3d:b4:56:cb:2c:e8:16:8b:a6:8f:
                    09:52:4e:e7:97:29:84:af:f1:94:23:0a:df:b4:90:
                    ac:62:38:09:da:50:a0:a6:bc:b6:6f:19:47:1e:ad:
                    12:75:5c:77:43:b1:c9:2d:73:30:3d:6f:78:08:f1:
                    44:09:7b:cd:58:6c:d9:3c:7a:6c:e7:f4:99:8b:73:
                    8c:8d:2b:23:4d:6b:bb:06:2f:da:4b:6d:2a:76:68:
                    68:62:e2:d3:e9:64:f8:19:fa:6b:3c:34:98:e4:55:
                    9b:76:72:0b:54:da:2e:94:15:63:aa:a8:2e:c2:96:
                    c4:8f:fb:a1:88:2e:e8:8a:3e:bf:fb:47:31:a7:e9:
                    d8:99
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 CRL Distribution Points:

                Full Name:

URI:http://onsitecrl.verisign.com/HewlettPackardCompanyDeSPrintingDeviceCSIDTemp
/LatestCRL.crl

            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.11.4.4.1.1
                  User Notice:
```

```
                    Explicit Text: Hewlett Packard Company, 2, Authority to bind
Hewlett-Packard Company does not correspond with use or possession of this
certificate. Issued to facilitate communication with HP.

            Authority Information Access:
                OCSP - URI:http://onsite-ocsp.verisign.com

            X509v3 Subject Key Identifier:
                60:D1:25:41:E6:76:3C:5E:CD:94:4F:3A:A3:D1:A7:C3:AA:2E:DE:1A
            X509v3 Authority Key Identifier:

keyid:B8:A1:0C:BD:06:5F:46:11:E9:80:DB:F7:99:BD:1D:F4:FD:EA:0D:C6

            X509v3 Extended Key Usage: critical
                Code Signing
    Signature Algorithm: sha256WithRSAEncryption
         6d:b2:73:08:e6:c1:e2:c9:23:c4:c2:16:40:0a:f0:3e:0d:df:
         b3:91:1b:ce:1b:07:92:68:04:61:cf:26:a9:a0:53:8d:12:a0:
         e1:48:8a:6c:c4:93:22:72:97:b1:46:14:70:02:16:d9:69:bb:
         d9:d5:8d:2e:51:81:ca:ef:32:e2:98:a1:ec:36:62:f2:0e:c4:
         67:b7:31:f1:d1:c8:c7:6b:b7:2e:5d:27:7d:a3:11:2a:d4:c0:
         20:60:e8:26:9f:db:f1:6f:94:93:d7:f8:60:e1:07:9f:5b:bf:
         15:4b:d7:9a:32:4c:d2:f7:2d:52:c7:15:d2:90:82:29:e9:f7:
         b2:41:21:fa:2a:20:7d:ce:2c:70:b3:eb:a9:7f:15:56:3c:98:
         18:f3:4d:3f:52:58:a3:91:1b:3b:4a:54:4d:6c:78:31:18:0e:
         89:7b:03:64:17:c5:06:55:0a:86:62:b6:c4:37:b5:4c:a0:3a:
         62:19:b6:fb:13:da:52:1b:fc:36:77:59:4c:e3:eb:f4:d7:8d:
         8e:6b:b8:b8:c4:c2:cd:86:39:87:14:b2:7a:a9:e9:b6:81:29:
         d3:62:17:82:82:6a:98:4c:88:92:44:b9:7e:41:c4:b4:57:ce:
         8e:f7:61:8b:12:c1:47:ec:e3:80:62:58:35:dc:a4:6a:ff:7f:
         0a:fd:23:0f
-----BEGIN CERTIFICATE-----
MIIFhzCCBG+gAwIBAgIQG2rvSYz7f5C2gTIa6J7C7zANBgkqhkiG9w0BAQsFADBr
MQswCQYDVQQGEwJVUzEgMB4GA1UEChMXSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkx
OjA4BgNVBAMTMUhld2xldHQtUGFja2FyZCBQcmludGluZyBEZXZpY2UgSW5mcmFz
dHJ1Y3R1cmUgQ0EwHhcNMTIwODA4MDAwMDAwWhcNMzIwODA4MjM1OTU5WjCBhzEg
MB4GA1UEChMXSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkxKzApBgNVBAsUIkxvbmcg
TGl2ZWQgQ29kZVNpZ25pbmcgQ2VydGlmaWNhdGUxNjA0BgNVBAMULUhld2xldHQt
UGFja2FyZCBVRUZJIFNlY3VyZSBCb290IFBsYXRmb3JtIEtleTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAOm4YrhZ2eBFUGRUoA1gW7JZiSU4oTfOZaii
lUv0DOY9ie4wx5Zkjl/kyA9RS/NP7Hp+tw0xibgmIVVR8GQNPbF2xtlVEk+L3LUy
yG/SFvjJrG+dHudyseji3UC3ybDjXM+HVoJngiSObswDStcpKVcoikC7Up+7yyJ6
rso9tFbLLOgWi6aPCVJO55cphK/xlCMK37SQrGI4CdpQoKa8tm8ZRx6tEnVcd0Ox
yS1zMD1veAjxRAl7zVhs2Tx6bOf0mYtzjI0rI01ruwYv2kttKnZoaGLi0+lk+Bn6
azw0mORVm3ZyC1TaLpQVY6qoLsKWxI/7oYgu6Io+v/tHMafp2JkCAwEAAaOCAggw
ggIEMAwGA1UdEwEB/wQCMAAwawYDVR0fBGQwYjBgoF6gXIZaaHR0cDovL29uc2l0
ZWNybC52ZXJpc2lnbi5jb20vSGV3bGV0dFBhY2thcmRDb21wYW55RGVTUHJpbnRp
bmdEZXZpY2VDU0lEVGVtcC9MYXRlc3RDUkwuY3JsMA4GA1UdDwEB/wQEAwIHgDCB
4QYDVR0gBIHZMIHWMIHTBgorBgEEAQsEBAEBMIHEMIHBBggrBgEFBQcCAjCBtBqB
sUhld2xldHQgUGFja2FyZCBDb21wYW55LCAyLCBBdXRob3JpdHkgdG8gYmluZCBI
ZXdsZXR0LVBhY2thcmQgQ29tcGFueSBkb2VzIG5vdCBjb3JyZXNwb25kIHdpdGgg
dXNlIG9yIHBvc3Nlc3Npb24gb2YgdGhpcyBjZXJ0aWZpY2F0ZS4gSXNzdWVkIHRv
IGZhY2lsaXRhdGUgY29tbXVuaWNhdGlvbiB3aXRoIEhQLjA7BggrBgEFBQcBAQQv
MC0wKwYIKwYBBQUHMAGGH2h0dHA6Ly9vbnNpdGUtb2NzcC52ZXJpc2lnbi5jb20w
HQYDVR0OBBYEFGDRJUHmdjxezZRPOqPRp8OqLt4aMB8GA1UdIwQYMBaAFLihDL0G
X0YR6YDb95m9HfT96g3GMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMDMA0GCSqGSIb3
DQEBCwUAA4IBAQBtsnMI5sHiySPEwhZACvA+Dd+zkRvOGweSaARhzyapoFONEqDh
SIpsxJMicpexRhRwAhbZabvZ1Y0uUYHK7zLimKHsNmLyDsRntzHx0cjHa7cuXSd9
oxEq1MAgYOgmn9vxb5ST1/hg4QefW78VS9eaMkzS9y1SxxXSkIIp6feyQSH6KiB9
zixws+upfxVWPJgY800/UlijkRs7SlRNbHgxGA6JewNkF8UGVQqGYrbEN7VMoDpi
Gbb7E9pSG/w2d1lM4+v0142Oa7i4xMLNhjmHFLJ6qem2gSnTYheCgmqYTIiSRLl+
QcS0V86O92GLEsFH7OOAYlg13KRq/38K/SMP
```

```
-----END CERTIFICATE-----
```

7.2.2 KEK

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:0a:d1:88:00:00:00:00:00:03
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation Third Party Marketplace Root
        Validity
            Not Before: Jun 24 20:41:29 2011 GMT
            Not After : Jun 24 20:51:29 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation KEK CA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:e8:b5:8a:bf:ad:57:26:b0:26:c3:ea:e7:fb:
                    57:7a:44:02:5d:07:0d:da:4a:e5:74:2a:e6:b0:0f:
                    ec:6d:eb:ec:7f:b9:e3:5a:63:32:7c:11:17:4f:0e:
                    e3:0b:a7:38:15:93:8e:c6:f5:e0:84:b1:9a:9b:2c:
                    e7:f5:b7:91:d6:09:e1:e2:c0:04:a8:ac:30:1c:df:
                    48:f3:06:50:9a:64:a7:51:7f:c8:85:4f:8f:20:86:
                    ce:fe:2f:e1:9f:ff:82:c0:ed:e9:cd:ce:f4:53:6a:
                    62:3a:0b:43:b9:e2:25:fd:fe:05:f9:d4:c4:14:ab:
                    11:e2:23:89:8d:70:b7:a4:1d:4d:ec:ae:e5:9c:fa:
                    16:c2:d7:c1:cb:d4:e8:c4:2f:e5:99:ee:24:8b:03:
                    ec:8d:f2:8b:ea:c3:4a:fb:43:11:12:0b:7e:b5:47:
                    92:6c:dc:e6:04:89:eb:f5:33:04:eb:10:01:2a:71:
                    e5:f9:83:13:3c:ff:25:09:2f:68:76:46:ff:ba:4f:
                    be:dc:ad:71:2a:58:aa:fb:0e:d2:79:3d:e4:9b:65:
                    3b:cc:29:2a:9f:fc:72:59:a2:eb:ae:92:ef:f6:35:
                    13:80:c6:02:ec:e4:5f:cc:9d:76:cd:ef:63:92:c1:
                    af:79:40:84:79:87:7f:e3:52:a8:e8:9d:7b:07:69:
                    8f:15
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 Subject Key Identifier:
                62:FC:43:CD:A0:3E:A4:CB:67:12:D2:5B:D9:55:AC:7B:CC:B6:8A:5F
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:45:66:52:43:E1:7E:58:11:BF:D6:4E:9E:23:55:08:3B:3A:22:6A:A8

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicCorThiParMarRoo_2010-10-05.crl
```

```
            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt

    Signature Algorithm: sha256WithRSAEncryption
         d4:84:88:f5:14:94:18:02:ca:2a:3c:fb:2a:92:1c:0c:d7:a0:
         d1:f1:e8:52:66:a8:ee:a2:b5:75:7a:90:00:aa:2d:a4:76:5a:
         ea:79:b7:b9:37:6a:51:7b:10:64:f6:e1:64:f2:02:67:be:f7:
         a8:1b:78:bd:ba:ce:88:58:64:0c:d6:57:c8:19:a3:5f:05:d6:
         db:c6:d0:69:ce:48:4b:32:b7:eb:5d:d2:30:f5:c0:f5:b8:ba:
         78:07:a3:2b:fe:9b:db:34:56:84:ec:82:ca:ae:41:25:70:9c:
         6b:e9:fe:90:0f:d7:96:1f:e5:e7:94:1f:b2:2a:0c:8d:4b:ff:
         28:29:10:7b:f7:d7:7c:a5:d1:76:b9:05:c8:79:ed:0f:90:92:
         9c:c2:fe:df:6f:7e:6c:0f:7b:d4:c1:45:dd:34:51:96:39:0f:
         e5:5e:56:d8:18:05:96:f4:07:a6:42:b3:a0:77:fd:08:19:f2:
         71:56:cc:9f:86:23:a4:87:cb:a6:fd:58:7e:d4:69:67:15:91:
         7e:81:f2:7f:13:e5:0d:8b:8a:3c:87:84:eb:e3:ce:bd:43:e5:
         ad:2d:84:93:8e:6a:2b:5a:7c:44:fa:52:aa:81:c8:2d:1c:bb:
         e0:52:df:00:11:f8:9a:3d:c1:60:b0:e1:33:b5:a3:88:d1:65:
         19:0a:1a:e7:ac:7c:a4:c1:82:87:4e:38:b1:2f:0d:c5:14:87:
         6f:fd:8d:2e:bc:39:b6:e7:e6:c3:e0:e4:cd:27:84:ef:94:42:
         ef:29:8b:90:46:41:3b:81:1b:67:d8:f9:43:59:65:cb:0d:bc:
         fd:00:92:4f:f4:75:3b:a7:a9:24:fc:50:41:40:79:e0:2d:4f:
         0a:6a:27:76:6e:52:ed:96:69:7b:af:0f:f7:87:05:d0:45:c2:
         ad:53:14:81:1f:fb:30:04:aa:37:36:61:da:4a:69:1b:34:d8:
         68:ed:d6:02:cf:6c:94:0c:d3:cf:6c:22:79:ad:b1:f0:bc:03:
         a2:46:60:a9:c4:07:c2:21:82:f1:fd:f2:e8:79:32:60:bf:d8:
         ac:a5:22:14:4b:ca:c1:d8:4b:eb:7d:3f:57:35:b2:e6:4f:75:
         b4:b0:60:03:22:53:ae:91:79:1d:d6:9b:41:1f:15:86:54:70:
         b2:de:0d:35:0f:7c:b0:34:72:ba:97:60:3b:f0:79:eb:a2:b2:
         1c:5d:a2:16:b8:87:c5:e9:1b:f6:b5:97:25:6f:38:9f:e3:91:
         fa:8a:79:98:c3:69:0e:b7:a3:1c:20:05:97:f8:ca:14:ae:00:
         d7:c4:f3:c0:14:10:75:6b:34:a0:1b:b5:99:60:f3:5c:b0:c5:
         57:4e:36:d2:32:84:bf:9e
-----BEGIN CERTIFICATE-----
MIIF6DCCA9CgAwIBAgIKYQrRiAAAAAAAAzANBgkqhkiG9w0BAQsFADCBkTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE7MDkGA1UEAxMyTWljcm9z
b2Z0IENvcnBvcmF0aW9uIFRoaXJkIFBhcnR5IE1hcmtldHBsYWNlIFJvb3QwHhcN
MTEwNjI0MjA0MTI5WhcNMjYwNjI0MjA1MTI5WjCBgDELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1p
Y3Jvc29mdCBDb3Jwb3JhdGlvbjEqMCgGA1UEAxMhTWljcm9zb2Z0IENvcnBvcmF0
aW9uIEtFSyBDQSAyMDExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
xOi1ir+tVyawJsPq5/tXekQCXQcN2krldCrmsA/sbevsf7njWmMyfBEXTw7jC6c4
FZOOxvXghLGamyzn9beR1gnh4sAEqKwwHN9I8wZQmmSnUX/IhU+PIIbO/i/hn/+C
wO3pzc70U2piOgtDueIl/f4F+dTEFKsR4iOJjXC3pB1N7K7lnPoWwtfBy9ToxC/l
me4kiwPsjfKL6sNK+0MREgt+tUeSbNzmBInr9TME6xABKnHl+YMTPP8lCS9odkb/
uk++3K1xKliq+w7SeT3km2U7zCkqn/xyWaLrrpLv9jUTgMYC7ORfzJ12ze9jksGv
eUCEeYd/41Ko6J17B2mPFQIDAQABo4IBTzCCAUswEAYJKwYBBAGCNxUBBAMCAQAw
HQYDVR0OBBYEFGL8Q82gPqTLZxLSW9lVrHvMtopfMBkGCSsGAQQBgjcUAgQMHgoA
UwB1AGIAQwBBMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQY
MBaAFEVmUkPhflgRv9ZOniNVCDs6ImqoMFwGA1UdHwRVMFMwUaBPoE2GS2h0dHA6
Ly9jcmwubWljcm9zb2Z0LmNvbS9wa2kvY3JsL3Byb2R1Y3RzL01pY0NvclRoaVBh
ck1hclJvb18yMDEwLTEwLTA1LmNybDBgBggrBgEFBQcBAQRUMFIwUAYIKwYBBQUH
MAKGRGh0dHA6Ly93d3cubWljcm9zb2Z0LmNvbS9wa2kvY2VydHMvTWljQ29yVGhp
UGFyTWFyUm9vXzIwMTAtMTAtMDUuY3J0MA0GCSqGSIb3DQEBCwUAA4ICAQDUhIj1
FJQYAsoqPPsqkhwM16DR8ehSZqjuorV1epAAqi2kdlrqebe5N2pRexBk9uFk8gJn
vveoG3i9us6IWGQM1lfIGaNfBdbbxtBpzkhLMrfrXdIw9cD1uLp4B6Mr/pvbNFaE
7ILKrkElcJxr6f6QD9eWH+XnlB+yKgyNS/8oKRB799d8pdF2uQXIee0PkJKcwv7f
b35sD3vUwUXdNFGWOQ/lXlbYGAWW9AemQrOgd/0IGfJxVsyfhiOkh8um/Vh+1Gln
FZF+gfJ/E+UNi4o8h4Tr4869Q+WtLYSTjmorWnxE+lKqgcgtHLvgUt8AEfiaPcFg
```

```
sOEztaOI0WUZChrnrHykwYKHTjixLw3FFIdv/Y0uvDm25+bD4OTNJ4TvlELvKYuQ
RkE7gRtn2PlDWWXLDbz9AJJP9HU7p6kk/FBBQHngLU8Kaid2blLtlml7rw/3hwXQ
RcKtUxSBH/swBKo3NmHaSmkbNNho7dYCz2yUDNPPbCJ5rbHwvAOiRmCpxAfCIYLx
/fLoeTJgv9ispSIUS8rB2EvrfT9XNbLmT3W0sGADIlOukXkd1ptBHxWGVHCy3g01
D3ywNHK6l2A78HnrorIcXaIWuIfF6Rv2tZclbzif45H6inmYw2kOt6McIAWX+MoU
rgDXxPPAFBB1azSgG7WZYPNcsMVXTjbSMoS/ng==
-----END CERTIFICATE-----

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:31:75:a3:b6:04:a1:75:71:55:ea:6e:37:52:6d:40
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Hewlett-Packard Company, CN=Hewlett-Packard Printing
Device Infrastructure CA
        Validity
            Not Before: Aug  8 00:00:00 2012 GMT
            Not After : Aug  8 23:59:59 2032 GMT
        Subject: O=Hewlett-Packard Company, OU=Long Lived CodeSigning
Certificate, CN=Hewlett-Packard UEFI Secure Boot Key Exchange Key
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:a2:14:69:90:ea:34:c3:6a:f2:0e:60:5e:dd:
                    c7:d6:09:50:a2:24:09:dc:b5:43:b9:4c:d3:7e:89:
                    1b:8a:14:29:27:2c:59:3f:c9:d5:ff:3a:75:4a:d1:
                    00:f8:7f:29:0e:79:fc:6b:5b:be:c1:01:17:e7:d5:
                    de:99:07:a6:89:3c:98:e4:6a:bc:ae:c5:9d:de:fd:
                    aa:c4:2c:10:95:ae:bc:36:39:da:e7:7c:75:5c:bc:
                    20:84:5f:aa:0f:c6:c6:d5:17:c0:de:43:bf:ed:4b:
                    b3:25:73:88:95:06:aa:d7:f9:78:5f:6d:b9:c0:6d:
                    0d:d4:d6:10:e6:7f:1c:63:02:31:87:17:28:4f:41:
                    13:a9:0c:09:9d:c2:2b:bd:b6:35:f9:f8:92:15:03:
                    25:ca:be:81:1c:b1:cf:4f:f7:93:cf:48:02:1c:58:
                    25:d7:eb:e5:88:de:30:95:d4:7b:39:50:82:ab:80:
                    c8:48:f3:7e:e8:3b:cb:39:63:d5:cb:0a:1f:a3:5d:
                    06:04:8f:f3:27:04:52:95:d3:c7:ab:c6:72:98:be:
                    fb:cb:0b:8e:c9:ec:81:45:9a:c9:a9:7a:02:1b:53:
                    d4:b8:92:b7:e1:ab:98:bd:b2:9a:ca:60:f8:c4:63:
                    87:b3:93:b4:93:8c:b8:59:c0:06:8c:c7:d2:58:dd:
                    b3:e1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 CRL Distribution Points:

                Full Name:

URI:http://onsitecrl.verisign.com/HewlettPackardCompanyDeSPrintingDeviceCSIDTemp
/LatestCRL.crl

            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.11.4.4.1.1
                  User Notice:
                    Explicit Text: Hewlett Packard Company, 2, Authority to bind
Hewlett-Packard Company does not correspond with use or possession of this
certificate. Issued to facilitate communication with HP.
```

```
            Authority Information Access:
                OCSP - URI:http://onsite-ocsp.verisign.com

            X509v3 Subject Key Identifier:
                D0:C8:09:A2:EA:7A:D7:94:89:46:DC:1D:71:68:CB:07:23:7C:01:0F
            X509v3 Authority Key Identifier:

keyid:B8:A1:0C:BD:06:5F:46:11:E9:80:DB:F7:99:BD:1D:F4:FD:EA:0D:C6

            X509v3 Extended Key Usage: critical
                Code Signing
    Signature Algorithm: sha256WithRSAEncryption
         2c:4f:ad:16:c7:fd:99:69:86:b3:b2:2c:dd:6d:90:0e:e4:39:
         7c:6e:2b:41:5a:76:2e:4e:34:0b:9f:d4:fd:fa:d6:05:f6:8d:
         db:3a:af:55:89:63:3f:b4:66:29:46:50:15:c8:d1:92:b2:b9:
         f6:d2:de:58:47:90:48:ee:c3:ff:8b:cb:ab:b9:10:21:31:1e:
         fd:0a:44:86:95:d8:49:05:8c:8d:95:f9:b7:ac:f4:60:03:25:
         0a:27:c6:3b:35:bc:08:ce:62:0d:4c:23:80:4c:28:6b:10:28:
         88:5d:4c:33:49:53:7f:ad:5a:ef:ea:6c:2e:ce:1f:e5:14:52:
         f3:2d:3b:11:32:3e:49:ad:c4:f7:00:be:ed:80:a7:2f:c2:a1:
         84:34:27:ac:3f:52:2c:9b:a9:99:79:ec:14:b7:7e:67:e9:b3:
         12:cc:94:cf:64:d3:b0:e6:06:40:80:e0:aa:90:14:aa:51:b6:
         0b:07:8d:b2:af:b2:48:53:fc:e2:49:f8:51:5c:1c:1b:66:85:
         1c:2c:57:41:cc:ac:6f:db:c0:66:03:68:cc:15:9d:29:b9:23:
         c1:c7:d8:21:17:0e:6f:c9:b6:b1:2d:9a:58:5b:f1:be:30:bb:
         a1:9a:9a:bb:3b:c3:49:47:a4:fc:f0:66:5c:4a:6a:f1:b8:ac:
         41:ec:84:c8
-----BEGIN CERTIFICATE-----
MIIFizCCBHOgAwIBAgIQBDF1o7YEoXVxVepuN1JtQDANBgkqhkiG9w0BAQsFADBr
MQswCQYDVQQGEwJVUzEgMB4GA1UEChMXSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkx
OjA4BgNVBAMTMUhld2xldHQtUGFja2FyZCBQcmludGluZyBEZXZpY2UgSW5mcmFz
dHJ1Y3R1cmUgQ0EwHhcNMTIwODA4MDAwMDAwWhcNMzIwODA4MjM1OTU5WjCBizEg
MB4GA1UEChMXSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkxKzApBgNVBAsUIkxvbmcg
TGl2ZWQgQ29kZVNpZ25pbmcgQ2VydGlmaWNhdGUxOjA4BgNVBAMUMUhld2xldHQt
UGFja2FyZCBVRUZJIFNlY3VyZSBCb290IEtleSBFeGNoYW5nZSBLZXkwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvohRpkOo0w2ryDmBe3cfWCVCiJAnc
tUO5TNN+iRuKFCknLFk/ydX/OnVK0QD4fykOefxrW77BARfn1d6ZB6aJPJjkaryu
xZ3e/arELBCVrrw2OdrnfHVcvCCEX6oPxsbVF8DeQ7/tS7Mlc4iVBqrX+XhfbbnA
bQ3U1hDmfxxjAjGHFyhPQROpDAmdwiu9tjX5+JIVAyXKvoEcsc9P95PPSAIcWCXX
6+WI3jCV1Hs5UIKrgMhI837oO8s5Y9XLCh+jXQYEj/MnBFKV08erxnKYvvvLC47J
7IFFmsmpegIbU9S4krfhq5i9sprKYPjEY4ezk7STjLhZwAaMx9JY3bPhAgMBAAGj
ggIIMIICBDAMBgNVHRMBAf8EAjAAMGsGA1UdHwRkMGIwYKBeoFyGWmh0dHA6Ly9v
bnNpdGVjcmwudmVyaXNpZ24uY29tL0hld2xldHRQYWNrYXJkQ29tcGFueURlU1By
aW50aW5nRGV2aWNlQ1NJRFRlbXAvTGF0ZXN0Q1JMLmNybDAOBgNVHQ8BAf8EBAMC
B4AwgeEGA1UdIASB2TCB1jCB0wYKKwYBBAELBAQBATCBxDCBwQYIKwYBBQUHAgIw
gbQagbFIZXdsZXR0IFBhY2thcmQgQ29tcGFueSwgMiwgQXV0aG9yaXR5IHRvIGJp
bmQgSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkgZG9lcyBub3QgY29ycmVzcG9uZCB3
aXRoIHVzZSBvciBwb3NzZXNzaW9uIG9mIHRoaXMgY2VydGlmaWNhdGUuIElzc3Vl
ZCB0byBmYWNpbGl0YXRlIGNvbW11bmljYXRpb24gd2l0aCBIUC4wOwYIKwYBBQUH
AQEELzAtMCsGCCsGAQUFBzABhh9odHRwOi8vb25zaXRlLW9jc3AudmVyaXNpZ24u
Y29tMB0GA1UdDgQWBBTQyAmi6nrXlIlG3B1xaMsHI3wBDzAfBgNVHSMEGDAWgBS4
oQy9Bl9GEemA2/eZvR30/eoNxjAWBgNVHSUBAf8EDDAKBggrBgEFBQcDAzANBgkq
hkiG9w0BAQsFAAOCAQEALE+tFsf9mWmGs7Is3W2QDuQ5fG4rQVp2Lk40C5/U/frW
BfaN2zqvVYljP7RmKUZQFcjRkrK59tLeWEeQSO7D/4vLq7kQITEe/QpEhpXYSQWM
jZX5t6z0YAMlCifGOzW8CM5iDUwjgEwoaxAoiF1MM0lTf61a7+psLs4f5RRS8y07
ETI+Sa3E9wC+7YCnL8KhhDQnrD9SLJupmXnsFLd+Z+mzEsyUz2TTsOYGQIDgqpAU
qlG2CweNsq+ySFP84kn4UVwcG2aFHCxXQcysb9vAZgNozBWdKbkjwcfYIRcOb8m2
sS2aWFvxvjC7oZqauzvDSUek/PBmXEpq8bisQeyEyA==
-----END CERTIFICATE-----
```

7.2.3 db

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:08:d3:c4:00:00:00:00:00:04
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation Third Party Marketplace Root
        Validity
            Not Before: Jun 27 21:22:45 2011 GMT
            Not After : Jun 27 21:32:45 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation UEFI CA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a5:08:6c:4c:c7:45:09:6a:4b:0c:a4:c0:87:7f:
                    06:75:0c:43:01:54:64:e0:16:7f:07:ed:92:7d:0b:
                    b2:73:bf:0c:0a:c6:4a:45:61:a0:c5:16:2d:96:d3:
                    f5:2b:a0:fb:4d:49:9b:41:80:90:3c:b9:54:fd:e6:
                    bc:d1:9d:c4:a4:18:8a:7f:41:8a:5c:59:83:68:32:
                    bb:8c:47:c9:ee:71:bc:21:4f:9a:8a:7c:ff:44:3f:
                    8d:8f:32:b2:26:48:ae:75:b5:ee:c9:4c:1e:4a:19:
                    7e:e4:82:9a:1d:78:77:4d:0c:b0:bd:f6:0f:d3:16:
                    d3:bc:fa:2b:a5:51:38:5d:f5:fb:ba:db:78:02:db:
                    ff:ec:0a:1b:96:d5:83:b8:19:13:e9:b6:c0:7b:40:
                    7b:e1:1f:28:27:c9:fa:ef:56:5e:1c:e6:7e:94:7e:
                    c0:f0:44:b2:79:39:e5:da:b2:62:8b:4d:bf:38:70:
                    e2:68:24:14:c9:33:a4:08:37:d5:58:69:5e:d3:7c:
                    ed:c1:04:53:08:e7:4e:b0:2a:87:63:08:61:6f:63:
                    15:59:ea:b2:2b:79:d7:0c:61:67:8a:5b:fd:5e:ad:
                    87:7f:ba:86:67:4f:71:58:12:22:04:22:22:ce:8b:
                    ef:54:71:00:ce:50:35:58:76:95:08:ee:6a:b1:a2:
                    01:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                .....
            1.3.6.1.4.1.311.21.2:
                ....k..wSJ.%7.N.&{. p.
            X509v3 Subject Key Identifier:
                13:AD:BF:43:09:BD:82:70:9C:8C:D5:4F:31:6E:D5:22:98:8A:1B:D4
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:45:66:52:43:E1:7E:58:11:BF:D6:4E:9E:23:55:08:3B:3A:22:6A:A8

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicCorThiParMarRoo_2010-10-05.crl
```

```
            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt

    Signature Algorithm: sha256WithRSAEncryption
         35:08:42:ff:30:cc:ce:f7:76:0c:ad:10:68:58:35:29:46:32:
         76:27:7c:ef:12:41:27:42:1b:4a:aa:6d:81:38:48:59:13:55:
         f3:e9:58:34:a6:16:0b:82:aa:5d:ad:82:da:80:83:41:06:8f:
         b4:1d:f2:03:b9:f3:1a:5d:1b:f1:50:90:f9:b3:55:84:42:28:
         1c:20:bd:b2:ae:51:14:c5:c0:ac:97:95:21:1c:90:db:0f:fc:
         77:9e:95:73:91:88:ca:bd:bd:52:b9:05:50:0d:df:57:9e:a0:
         61:ed:0d:e5:6d:25:d9:40:0f:17:40:c8:ce:a3:4a:c2:4d:af:
         9a:12:1d:08:54:8f:bd:c7:bc:b9:2b:3d:49:2b:1f:32:fc:6a:
         21:69:4f:9b:c8:7e:42:34:fc:36:06:17:8b:8f:20:40:c0:b3:
         9a:25:75:27:cd:c9:03:a3:f6:5d:d1:e7:36:54:7a:b9:50:b5:
         d3:12:d1:07:bf:bb:74:df:dc:1e:8f:80:d5:ed:18:f4:2f:14:
         16:6b:2f:de:66:8c:b0:23:e5:c7:84:d8:ed:ea:c1:33:82:ad:
         56:4b:18:2d:f1:68:95:07:cd:cf:f0:72:f0:ae:bb:dd:86:85:
         98:2c:21:4c:33:2b:f0:0f:4a:f0:68:87:b5:92:55:32:75:a1:
         6a:82:6a:3c:a3:25:11:a4:ed:ad:d7:04:ae:cb:d8:40:59:a0:
         84:d1:95:4c:62:91:22:1a:74:1d:8c:3d:47:0e:44:a6:e4:b0:
         9b:34:35:b1:fa:b6:53:a8:2c:81:ec:a4:05:71:c8:9d:b8:ba:
         e8:1b:44:66:e4:47:54:0e:8e:56:7f:b3:9f:16:98:b2:86:d0:
         68:3e:90:23:b5:2f:5e:8f:50:85:8d:c6:8d:82:5f:41:a1:f4:
         2e:0d:e0:99:d2:6c:75:e4:b6:69:b5:21:86:fa:07:d1:f6:e2:
         4d:d1:da:ad:2c:77:53:1e:25:32:37:c7:6c:52:72:95:86:b0:
         f1:35:61:6a:19:f5:b2:3b:81:50:56:a6:32:2d:fe:a2:89:f9:
         42:86:27:18:55:a1:82:ca:5a:9b:f8:30:98:54:14:a6:47:96:
         25:2f:c8:26:e4:41:94:1a:5c:02:3f:e5:96:e3:85:5b:3c:3e:
         3f:bb:47:16:72:55:e2:25:22:b1:d9:7b:e7:03:06:2a:a3:f7:
         1e:90:46:c3:00:0d:d6:19:89:e3:0e:35:27:62:03:71:15:a6:
         ef:d0:27:a0:a0:59:37:60:f8:38:94:b8:e0:78:70:f8:ba:4c:
         86:87:94:f6:e0:ae:02:45:ee:65:c2:b6:a3:7e:69:16:75:07:
         92:9b:f5:a6:bc:59:83:58
-----BEGIN CERTIFICATE-----
MIIGEDCCA/igAwIBAgIKYQjTxAAAAAAABDANBgkqhkiG9w0BAQsFADCBkTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE7MDkGA1UEAxMyTWljcm9z
b2Z0IENvcnBvcmF0aW9uIFRoaXJkIFBhcnR5IE1hcmtldHBsYWNlIFJvb3QwHhcN
MTEwNjI3MjEyMjQ1WhcNMjYwNjI3MjEzMjQ1WjCBgTELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1p
Y3Jvc29mdCBDb3Jwb3JhdGlvbjErMCkGA1UEAxMiTWljcm9zb2Z0IENvcnBvcmF0
aW9uIFVFRkkgQ0EgMjAxMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AKUIbEzHRQlqSwykwId/BnUMQwFUZOAWfwftkn0LsnO/DArGSkVhoMUWLZbT9Sug
+01Jm0GAkDy5VP3mvNGdxKQYin9BilxZg2gyu4xHye5xvCFPmop8/0Q/jY8ysiZI
rnW17slMHkoZfuSCmh14d00MsL32D9MW07z6K6VROF31+7rbeALb/+wKG5bVg7gZ
E+m2wHtAe+EfKCfJ+u9WXhzmfpR+wPBEsnk55dqyYotNvzhw4mgkFMkzpAg31Vhp
XtN87cEEUwjnTrAqh2MIYW9jFVnqsit51wxhZ4pb/V6th3+6hmdPcVgSIgQiIs6L
71RxAM5QNVh2lQjuarGiAdUCAwEAAaOCAXYwggFyMBIGCSsGAQQBgjcVAQQFAgMB
AAEwIwYJKwYBBAGCNxUCBBYEFPjBa7d/d1NK8yU3HU6hJnsPIHCAMB0GA1UdDgQW
BBQTrb9DCb2CcJyM1U8xbtUimIob1DAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMA
QTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRFZlJD
4X5YEb/WTp4jVQg7OiJqqDBcBgNVHR8EVTBTMFGgT6BNhktodHRwOi8vY3JsLm1p
Y3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNDb3JUaGlQYXJNYXJSb29f
MjAxMC0xMC0wNS5jcmwwYAYIKwYBBQUHAQEEVDBSMFAGCCsGAQUFBzAChkRodHRw
Oi8vd3d3Lm1pY3Jvc29mdC5jb20vcGtpL2NlcnRzL01pY0NvclRoaVBhck1hclJv
b18yMDEwLTEwLTA1LmNydDANBgkqhkiG9w0BAQsFAAOCAgEANQhC/zDMzvd2DK0Q
aFg1KUYydid87xJBJ0IbSqptgThIWRNV8+lYNKYWC4KqXa2C2oCDQQaPtB3yA7nz
Gl0b8VCQ+bNVhEIoHCC9sq5RFMXArJeVIRyQ2w/8d56Vc5GIyr29UrkFUA3fV56g
Ye0N5W0l2UAPF0DIzqNKwk2vmhIdCFSPvce8uSs9SSsfMvxqIWlPm8h+QjT8NgYX
i48gQMCzmiV1J83JA6P2XdHnNlR6uVC10xLRB7+7dN/cHo+A1e0Y9C8UFmsv3maM
```

```
sCPlx4TY7erBM4KtVksYLfFolQfNz/By8K673YaFmCwhTDMr8A9K8GiHtZJVMnWh
aoJqPKMlEaTtrdcErsvYQFmghNGVTGKRIhp0HYw9Rw5EpuSwmzQ1sfq2U6gsgeyk
BXHInbi66BtEZuRHVA6OVn+znxaYsobQaD6QI7UvXo9QhY3GjYJfQaH0Lg3gmdJs
deS2abUhhvoH0fbiTdHarSx3Ux4lMjfHbFJylYaw8TVhahn1sjuBUFamMi3+oon5
QoYnGFWhgspam/gwmFQUpkeWJS/IJuRBlBpcAj/lluOFWzw+P7tHFnJV4iUisdl7
5wMGKqP3HpBGwwAN1hmJ4w41J2IDcRWm79AnoKBZN2D4OJS44Hhw+LpMhoeU9uCu
AkXuZcK2o35pFnUHkpv1prxZg1g=
-----END CERTIFICATE-----

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:07:76:56:00:00:00:00:00:08
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Root Certificate Authority 2010
        Validity
            Not Before: Oct 19 18:41:42 2011 GMT
            Not After : Oct 19 18:51:42 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Windows Production PCA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:dd:0c:bb:a2:e4:2e:09:e3:e7:c5:f7:96:69:bc:
                    00:21:bd:69:33:33:ef:ad:04:cb:54:80:ee:06:83:
                    bb:c5:20:84:d9:f7:d2:8b:f3:38:b0:ab:a4:ad:2d:
                    7c:62:79:05:ff:e3:4a:3f:04:35:20:70:e3:c4:e7:
                    6b:e0:9c:c0:36:75:e9:8a:31:dd:8d:70:e5:dc:37:
                    b5:74:46:96:28:5b:87:60:23:2c:bf:dc:47:a5:67:
                    f7:51:27:9e:72:eb:07:a6:c9:b9:1e:3b:53:35:7c:
                    e5:d3:ec:27:b9:87:1c:fe:b9:c9:23:09:6f:a8:46:
                    91:c1:6e:96:3c:41:d3:cb:a3:3f:5d:02:6a:4d:ec:
                    69:1f:25:28:5c:36:ff:fd:43:15:0a:94:e0:19:b4:
                    cf:df:c2:12:e2:c2:5b:27:ee:27:78:30:8b:5b:2a:
                    09:6b:22:89:53:60:16:2c:c0:68:1d:53:ba:ec:49:
                    f3:9d:61:8c:85:68:09:73:44:5d:7d:a2:54:2b:dd:
                    79:f7:15:cf:35:5d:6c:1c:2b:5c:ce:bc:9c:23:8b:
                    6f:6e:b5:26:d9:36:13:c3:4f:d6:27:ae:b9:32:3b:
                    41:92:2c:e1:c7:cd:77:e8:aa:54:4e:f7:5c:0b:04:
                    87:65:b4:43:18:a8:b2:e0:6d:19:77:ec:5a:24:fa:
                    48:03
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 Subject Key Identifier:
                A9:29:02:39:8E:16:C4:97:78:CD:90:F9:9E:4F:9A:E1:7C:55:AF:53
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:D5:F6:56:CB:8F:E8:A2:5C:62:68:D1:3D:94:90:5B:D7:CE:9A:18:C4

            X509v3 CRL Distribution Points:
```

```
                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt

    Signature Algorithm: sha256WithRSAEncryption
         14:fc:7c:71:51:a5:79:c2:6e:b2:ef:39:3e:bc:3c:52:0f:6e:
         2b:3f:10:13:73:fe:a8:68:d0:48:a6:34:4d:8a:96:05:26:ee:
         31:46:90:61:79:d6:ff:38:2e:45:6b:f4:c0:e5:28:b8:da:1d:
         8f:8a:db:09:d7:1a:c7:4c:0a:36:66:6a:8c:ec:1b:d7:04:90:
         a8:18:17:a4:9b:b9:e2:40:32:36:76:c4:c1:5a:c6:bf:e4:04:
         c0:ea:16:d3:ac:c3:68:ef:62:ac:dd:54:6c:50:30:58:a6:eb:
         7c:fe:94:a7:4e:8e:f4:ec:7c:86:73:57:c2:52:21:73:34:5a:
         f3:a3:8a:56:c8:04:da:07:09:ed:f8:8b:e3:ce:f4:7e:8e:ae:
         f0:f6:0b:8a:08:fb:3f:c9:1d:72:7f:53:b8:eb:be:63:e0:e3:
         3d:31:65:b0:81:e5:f2:ac:cd:16:a4:9f:3d:a8:b1:9b:c2:42:
         d0:90:84:5f:54:1d:ff:89:ea:ba:1d:47:90:6f:b0:73:4e:41:
         9f:40:9f:5f:e5:a1:2a:b2:11:91:73:8a:21:28:f0:ce:de:73:
         39:5f:3e:ab:5c:60:ec:df:03:10:a8:d3:09:e9:f4:f6:96:85:
         b6:7f:51:88:66:47:19:8d:a2:b0:12:3d:81:2a:68:05:77:bb:
         91:4c:62:7b:b6:c1:07:c7:ba:7a:87:34:03:0e:4b:62:7a:99:
         e9:ca:fc:ce:4a:37:c9:2d:a4:57:7c:1c:fe:3d:dc:b8:0f:5a:
         fa:d6:c4:b3:02:85:02:3a:ea:b3:d9:6e:e4:69:21:37:de:81:
         d1:f6:75:19:05:67:d3:93:57:5e:29:1b:39:c8:ee:2d:e1:cd:
         e4:45:73:5b:d0:d2:ce:7a:ab:16:19:82:46:58:d0:5e:9d:81:
         b3:67:af:6c:35:f2:bc:e5:3f:24:e2:35:a2:0a:75:06:f6:18:
         56:99:d4:78:2c:d1:05:1b:eb:d0:88:01:9d:aa:10:f1:05:df:
         ba:7e:2c:63:b7:06:9b:23:21:c4:f9:78:6c:e2:58:17:06:36:
         2b:91:12:03:cc:a4:d9:f2:2d:ba:f9:94:9d:40:ed:18:45:f1:
         ce:8a:5c:6b:3e:ab:03:d3:70:18:2a:0a:6a:e0:5f:47:d1:d5:
         63:0a:32:f2:af:d7:36:1f:2a:70:5a:e5:42:59:08:71:4b:57:
         ba:7e:83:81:f0:21:3c:f4:1c:c1:c5:b9:90:93:0e:88:45:93:
         86:e9:b1:20:99:be:98:cb:c5:95:a4:5d:62:d6:a0:63:08:20:
         bd:75:10:77:7d:3d:f3:45:b9:9f:97:9f:cb:57:80:6f:33:a9:
         04:cf:77:a4:62:1c:59:7e
-----BEGIN CERTIFICATE-----
MIIF1zCCA7+gAwIBAgIKYQd2VgAAAAAACDANBgkqhkiG9w0BAQsFADCBiDELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjEyMDAGA1UEAxMpTWljcm9z
b2Z0IFJvb3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IDIwMTAwHhcNMTExMDE5MTg0
MTQyWhcNMjYxMDE5MTg1MTQyWjCBhDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldh
c2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBD
b3Jwb3JhdGlvbjEuMCwGA1UEAxMlTWljcm9zb2Z0IFdpbmRvd3MgUHJvZHVjdGlv
biBQQ0EgMjAxMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN0Mu6Lk
Lgnj58X3lmm8ACG9aTMz760Ey1SA7gaDu8UghNn30ovzOLCrpK0tfGJ5Bf/jSj8E
NSBw48Tna+CcwDZ16Yox3Y1w5dw3tXRGlihbh2AjLL/cR6Vn91EnnnLrB6bJuR47
UzV85dPsJ7mHHP65ySMJb6hGkcFuljxB08ujP10Cak3saR8lKFw2//1DFQqU4Bm0
z9/CEuLCWyfuJ3gwi1sqCWsiiVNgFizAaB1TuuxJ851hjIVoCXNEXX2iVCvdefcV
zzVdbBwrXM68nCOLb261Jtk2E8NP1ieuuTI7QZIs4cfNd+iqVE73XAsEh2W0Qxio
suBtGXfsWiT6SAMCAwEAAaOCAUMwggE/MBAGCSsGAQQBgjcVAQQDAgEAMB0GA1Ud
DgQWBBSpKQI5jhbEl3jNkPmeT5rhfFWvUzAZBgkrBgEEAYI3FAIEDB4KAFMAdQBi
AEMAQTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBTV
9lbLj+iiXGJo0T2UkFvXzpoYxDBWBgNVHR8ETzBNMEugSaBHhkVodHRwOi8vY3Js
Lm1pY3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNSb29DZXJBdXRfMjAx
MC0wNi0yMy5jcmwwWgYIKwYBBQUHAQEETjBMMEoGCCsGAQUFBzAChj5odHRwOi8v
d3d3Lm1pY3Jvc29mdC5jb20vcGtpL2NlcnRzL01pY1Jvb0NlckF1dF8yMDEwLTA2
LTIzLmNydDANBgkqhkiG9w0BAQsFAAOCAgEAFPx8cVGlecJusu85Prw8Ug9uKz8Q
E3P+qGjQSKY0TYqWBSbuMUaQYXnW/zguRWv0wOUouNodj4rbCdcax0wKNmZqjOwb
```

```
1wSQqBgXpJu54kAyNnbEwVrGv+QEwOoW06zDaO9irN1UbFAwWKbrfP6Up06O9Ox8
hnNXwlIhczRa86OKVsgE2gcJ7fiL4870fo6u8PYLigj7P8kdcn9TuOu+Y+DjPTFl
sIHl8qzNFqSfPaixm8JC0JCEX1Qd/4nquh1HkG+wc05Bn0CfX+WhKrIRkXOKISjw
zt5zOV8+q1xg7N8DEKjTCen09paFtn9RiGZHGY2isBI9gSpoBXe7kUxie7bBB8e6
eoc0Aw5LYnqZ6cr8zko3yS2kV3wc/j3cuA9a+tbEswKFAjrqs9lu5GkhN96B0fZ1
GQVn05NXXikbOcjuLeHN5EVzW9DSznqrFhmCRljQXp2Bs2evbDXyvOU/JOI1ogp1
BvYYVpnUeCzRBRvr0IgBnaoQ8QXfun4sY7cGmyMhxPl4bOJYFwY2K5ESA8yk2fIt
uvmUnUDtGEXxzopcaz6rA9NwGCoKauBfR9HVYwoy8q/XNh8qcFrlQlkIcUtXun6D
gfAhPPQcwcW5kJMOiEWThumxIJm+mMvFlaRdYtagYwggvXUQd30980W5n5efy1eA
bzOpBM93pGIcWX4=
-----END CERTIFICATE-----
```

7.3 Zertifikate der Dell-Plattform

7.3.1 PK

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1323793210 (0x4ee77b3a)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=dell, CN=Configuration, CN=Services, CN=Public Key
Services, CN=AIA, CN=Dell Inc. Issuing CA 1
        Validity
            Not Before: Jul 17 00:51:45 2012 GMT
            Not After : Jul 17 01:21:45 2014 GMT
        Subject: DC=com, DC=dell, OU=1, OU=Signing, CN=Dell Inc. UEFI Platform
Key
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c5:26:35:3e:c1:96:01:ee:f6:c5:b2:5a:09:e5:
                    94:40:08:8a:d6:f7:14:2b:97:b9:db:f3:42:08:e3:
                    2b:ae:4a:e1:e2:d1:0b:51:fe:f1:58:74:e0:41:bb:
                    8d:95:2a:5b:98:e6:30:41:4f:7b:2b:20:50:c0:f5:
                    74:7e:55:4d:18:d2:23:6b:a0:76:aa:4a:c3:a7:c0:
                    ec:20:48:1e:de:60:06:6b:73:b4:22:bb:22:8c:e7:
                    ab:06:0a:76:21:b4:90:71:9f:c8:91:f9:49:24:2b:
                    66:6a:b7:f8:a8:5e:7c:13:51:e9:6e:f3:a5:8d:5b:
                    2e:9d:ed:f6:d5:45:52:50:42:0c:3f:15:0a:cd:3c:
                    70:bf:9f:f1:06:3b:e0:8f:0a:a5:89:86:a7:b0:78:
                    0a:29:03:9b:ae:53:6a:f2:45:31:33:6b:38:7b:62:
                    5e:36:96:54:15:41:2c:4d:93:8b:ba:41:0a:8a:b9:
                    45:0c:0c:a5:83:0d:51:3b:8f:16:f7:6b:d9:5e:95:
                    7c:ca:67:f5:b9:13:ed:c4:16:87:69:72:4a:78:ec:
                    6b:27:2f:8b:92:05:b1:3b:da:a5:4c:5c:c7:cb:2a:
                    08:e5:17:b0:ce:d9:28:5f:a3:84:cc:6c:ea:ed:62:
                    72:71:a9:89:0d:f5:e7:7e:13:6f:0c:b1:c4:95:0b:
                    97:b9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature
            X509v3 Extended Key Usage:
                Code Signing
            X509v3 CRL Distribution Points:
```

```
                Full Name:
                  URI:http://crl.dell.com/1/issuer.crl

                Full Name:
                  DirName: DC = com, DC = dell, CN = Configuration, CN =
Services, CN = Public Key Services, CN = AIA, CN = Dell Inc. Issuing CA 1, CN =
CRL1

            X509v3 Private Key Usage Period:
                Not Before: Jul 17 00:51:45 2012 GMT, Not After: Jul 17 01:21:45
2014 GMT
            X509v3 Authority Key Identifier:

keyid:88:96:5F:DA:89:F6:DD:70:51:44:14:00:92:00:55:8E:C3:2C:EC:64

            X509v3 Subject Key Identifier:
                1B:6B:AB:4F:11:F4:0E:46:64:F6:FE:7A:35:39:C4:E3:94:0E:93:BB
            X509v3 Basic Constraints:
                CA:FALSE
            1.2.840.113533.7.65.0:
                0
..V8.1....
    Signature Algorithm: sha256WithRSAEncryption
         25:94:c7:6e:34:44:e9:69:77:45:f0:73:25:54:5b:ba:44:cd:
         c9:94:94:95:3f:f9:ae:b1:31:58:ee:c1:b5:ac:74:63:14:2a:
         4d:2c:1e:f0:6c:b0:c0:03:38:7d:d1:b5:48:b1:4f:f5:cb:63:
         45:c9:25:19:42:67:ee:2c:d2:0b:9e:70:b7:89:7a:90:99:5d:
         a7:fd:9c:7e:72:b8:f3:7c:64:e8:be:c7:a2:8d:c0:2b:54:cf:
         cc:06:34:ef:f1:09:ac:d8:5f:a2:ce:07:97:4c:e5:7d:3e:5e:
         b3:b6:e9:ae:ab:7e:67:02:64:e6:81:d5:33:b4:13:13:38:1e:
         ab:c2:84:f6:59:c5:b0:7c:74:72:25:ab:48:a6:60:40:ab:5e:
         ff:2f:c8:f0:f9:9b:84:0e:a1:0f:66:2a:d5:85:f2:84:7a:8a:
         e2:b1:c7:fc:6e:51:99:ce:54:10:ee:72:c4:3a:70:45:5d:1d:
         72:f8:5e:e8:ab:03:76:a6:a2:b9:ab:fe:70:b1:69:51:7a:60:
         f5:c0:cf:88:b1:df:ce:45:2e:22:3a:03:b0:31:c1:fe:0d:60:
         b6:71:0f:26:9a:1e:ed:1c:5e:bd:03:51:a5:ef:e1:20:63:70:
         ee:bf:13:39:c3:10:5e:63:82:5e:02:e7:7b:e9:b5:d1:f0:19:
         98:b1:80:e2
-----BEGIN CERTIFICATE-----
MIIFQzCCBCugAwIBAgIETud7OjANBgkqhkiG9w0BAQsFADCBozETMBEGCgmSJomT
8ixkARkWA2NvbTEUMBIGCgmSJomT8ixkARkWBGRlbGwxFjAUBgNVBAMTDUNvbmZp
Z3VyYXRpb24xETAPBgNVBAMTCFNlcnZpY2VzMRwwGgYDVQQDExNQdWJsaWMgS2V5
IFNlcnZpY2VzMQwwCgYDVQQDEwNBSUExHzAdBgNVBAMTFkRlbGwgSW5jLiBJc3N1
aW5nIENBIDEwHhcNMTIwNzE3MDA1MTQ1WhcNMTQwNzE3MDEyMTQ1WjBvMRMwEQYK
CZImiZPyLGQBGRYDY29tMRQwEgYKCZImiZPyLGQBGRYEZGVsbDEKMAgGA1UECxMB
MTEQMA4GA1UECxMHU2lnbmluZzEkMCIGA1UEAxMbRGVsbCBJbmMuIFVFRkkgUGxh
dGZvcm0gS2V5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxSY1PsGW
Ae72xbJaCeWUQAiK1vcUK5e52/NCCOMrrkrh4tELUf7xWHTgQbuNlSpbmOYwQU97
KyBQwPV0flVNGNIja6B2qkrDp8DsIEge3mAGa3O0IrsijOerBgp2IbSQcZ/IkflJ
JCtmarf4qF58E1HpbvOljVsune321UVSUEIMPxUKzTxwv5/xBjvgjwqliYansHgK
KQObrlNq8kUxM2s4e2JeNpZUFUEsTZOLukEKirlFDAylgw1RO48W92vZXpV8ymf1
uRPtxBaHaXJKeOxrJy+LkgWxO9qlTFzHyyoI5RewztkoX6OEzGzq7WJycamJDfXn
fhNvDLHElQuXuQIDAQABo4IBsDCCAawwCwYDVR0PBAQDAgeAMBMGA1UdJQQMMAoG
CCsGAQUFBwMDMIH0BgNVHR8EgewwgekwJqAkoCKGIGh0dHA6Ly9jcmwuZGVsbC5j
b20vMS9pc3N1ZXIuY3JsMIG+oIG7oIG4pIG1MIGyMRMwEQYKCZImiZPyLGQBGRYD
Y29tMRQwEgYKCZImiZPyLGQBGRYEZGVsbDEWMBQGA1UEAxMNQ29uZmlndXJhdGlv
bjERMA8GA1UEAxMIU2VydmljZXMxHDAaBgNVBAMTE1B1YmxpYyBLZXkgU2Vydmlj
ZXMxDDAKBgNVBAMTA0FJQTEfMB0GA1UEAxMWRGVsbCBJbmMuIElzc3VpbmcgQ0Eg
MTENMAsGA1UEAxMEQ1JMMTArBgNVHRAEJDAigA8yMDEyMDcxNzAwNTE0NVqBDzIw
MTQwNzE3MDEyMTQ1WjAfBgNVHSMEGDAWgBSIll/aifbdcFFEFACSAFWOwyzsZDAd
BgNVHQ4EFgQUG2urTxH0DkZk9v56NTnE45QOk7swCQYDVR0TBAIwADAZBgkqhkiG
9n0HQQAEDDAKGwRWOC4xAwIDqDANBgkqhkiG9w0BAQsFAAOCAQEAJZTHbjRE6Wl3
```

```
RfBzJVRbukTNyZSUlT/5rrExWO7Btax0YxQqTSwe8GywwAM4fdG1SLFP9ctjRckl
GUJn7izSC55wt4l6kJldp/2cfnK483xk6L7Hoo3AK1TPzAY07/EJrNhfos4Hl0zl
fT5es7bprqt+ZwJk5oHVM7QTEzgeq8KE9lnFsHx0ciWrSKZgQKte/y/I8PmbhA6h
D2Yq1YXyhHqK4rHH/G5Rmc5UEO5yxDpwRV0dcvhe6KsDdqaiuav+cLFpUXpg9cDP
iLHfzkUuIjoDsDHB/g1gtnEPJpoe7RxevQNRpe/hIGNw7r8TOcMQXmOCXgLne+m1
0fAZmLGA4g==
-----END CERTIFICATE-----
```

7.3.2 KEK

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:0a:d1:88:00:00:00:00:00:03
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation Third Party Marketplace Root
        Validity
            Not Before: Jun 24 20:41:29 2011 GMT
            Not After : Jun 24 20:51:29 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation KEK CA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:e8:b5:8a:bf:ad:57:26:b0:26:c3:ea:e7:fb:
                    57:7a:44:02:5d:07:0d:da:4a:e5:74:2a:e6:b0:0f:
                    ec:6d:eb:ec:7f:b9:e3:5a:63:32:7c:11:17:4f:0e:
                    e3:0b:a7:38:15:93:8e:c6:f5:e0:84:b1:9a:9b:2c:
                    e7:f5:b7:91:d6:09:e1:e2:c0:04:a8:ac:30:1c:df:
                    48:f3:06:50:9a:64:a7:51:7f:c8:85:4f:8f:20:86:
                    ce:fe:2f:e1:9f:ff:82:c0:ed:e9:cd:ce:f4:53:6a:
                    62:3a:0b:43:b9:e2:25:fd:fe:05:f9:d4:c4:14:ab:
                    11:e2:23:89:8d:70:b7:a4:1d:4d:ec:ae:e5:9c:fa:
                    16:c2:d7:c1:cb:d4:e8:c4:2f:e5:99:ee:24:8b:03:
                    ec:8d:f2:8b:ea:c3:4a:fb:43:11:12:0b:7e:b5:47:
                    92:6c:dc:e6:04:89:eb:f5:33:04:eb:10:01:2a:71:
                    e5:f9:83:13:3c:ff:25:09:2f:68:76:46:ff:ba:4f:
                    be:dc:ad:71:2a:58:aa:fb:0e:d2:79:3d:e4:9b:65:
                    3b:cc:29:2a:9f:fc:72:59:a2:eb:ae:92:ef:f6:35:
                    13:80:c6:02:ec:e4:5f:cc:9d:76:cd:ef:63:92:c1:
                    af:79:40:84:79:87:7f:e3:52:a8:e8:9d:7b:07:69:
                    8f:15
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 Subject Key Identifier:
                62:FC:43:CD:A0:3E:A4:CB:67:12:D2:5B:D9:55:AC:7B:CC:B6:8A:5F
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:
```

```
keyid:45:66:52:43:E1:7E:58:11:BF:D6:4E:9E:23:55:08:3B:3A:22:6A:A8

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicCorThiParMarRoo_2010-10-05.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt

    Signature Algorithm: sha256WithRSAEncryption
         d4:84:88:f5:14:94:18:02:ca:2a:3c:fb:2a:92:1c:0c:d7:a0:
         d1:f1:e8:52:66:a8:ee:a2:b5:75:7a:90:00:aa:2d:a4:76:5a:
         ea:79:b7:b9:37:6a:51:7b:10:64:f6:e1:64:f2:02:67:be:f7:
         a8:1b:78:bd:ba:ce:88:58:64:0c:d6:57:c8:19:a3:5f:05:d6:
         db:c6:d0:69:ce:48:4b:32:b7:eb:5d:d2:30:f5:c0:f5:b8:ba:
         78:07:a3:2b:fe:9b:db:34:56:84:ec:82:ca:ae:41:25:70:9c:
         6b:e9:fe:90:0f:d7:96:1f:e5:e7:94:1f:b2:2a:0c:8d:4b:ff:
         28:29:10:7b:f7:d7:7c:a5:d1:76:b9:05:c8:79:ed:0f:90:92:
         9c:c2:fe:df:6f:7e:6c:0f:7b:d4:c1:45:dd:34:51:96:39:0f:
         e5:5e:56:d8:18:05:96:f4:07:a6:42:b3:a0:77:fd:08:19:f2:
         71:56:cc:9f:86:23:a4:87:cb:a6:fd:58:7e:d4:69:67:15:91:
         7e:81:f2:7f:13:e5:0d:8b:8a:3c:87:84:eb:e3:ce:bd:43:e5:
         ad:2d:84:93:8e:6a:2b:5a:7c:44:fa:52:aa:81:c8:2d:1c:bb:
         e0:52:df:00:11:f8:9a:3d:c1:60:b0:e1:33:b5:a3:88:d1:65:
         19:0a:1a:e7:ac:7c:a4:c1:82:87:4e:38:b1:2f:0d:c5:14:87:
         6f:fd:8d:2e:bc:39:b6:e7:e6:c3:e0:e4:cd:27:84:ef:94:42:
         ef:29:8b:90:46:41:3b:81:1b:67:d8:f9:43:59:65:cb:0d:bc:
         fd:00:92:4f:f4:75:3b:a7:a9:24:fc:50:41:40:79:e0:2d:4f:
         0a:6a:27:76:6e:52:ed:96:69:7b:af:0f:f7:87:05:d0:45:c2:
         ad:53:14:81:1f:fb:30:04:aa:37:36:61:da:4a:69:1b:34:d8:
         68:ed:d6:02:cf:6c:94:0c:d3:cf:6c:22:79:ad:b1:f0:bc:03:
         a2:46:60:a9:c4:07:c2:21:82:f1:fd:f2:e8:79:32:60:bf:d8:
         ac:a5:22:14:4b:ca:c1:d8:4b:eb:7d:3f:57:35:b2:e6:4f:75:
         b4:b0:60:03:22:53:ae:91:79:1d:d6:9b:41:1f:15:86:54:70:
         b2:de:0d:35:0f:7c:b0:34:72:ba:97:60:3b:f0:79:eb:a2:b2:
         1c:5d:a2:16:b8:87:c5:e9:1b:f6:b5:97:25:6f:38:9f:e3:91:
         fa:8a:79:98:c3:69:0e:b7:a3:1c:20:05:97:f8:ca:14:ae:00:
         d7:c4:f3:c0:14:10:75:6b:34:a0:1b:b5:99:60:f3:5c:b0:c5:
         57:4e:36:d2:32:84:bf:9e
-----BEGIN CERTIFICATE-----
MIIF6DCCA9CgAwIBAgIKYQrRiAAAAAAAAzANBgkqhkiG9w0BAQsFADCBkTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE7MDkGA1UEAxMyTWljcm9z
b2Z0IENvcnBvcmF0aW9uIFRoaXJkIFBhcnR5IE1hcmtldHBsYWNlIFJvb3QwHhcN
MTEwNjI0MjA0MTI5WhcNMjYwNjI0MjA1MTI5WjCBgDELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1p
Y3Jvc29mdCBDb3Jwb3JhdGlvbjEqMCgGA1UEAxMhTWljcm9zb2Z0IENvcnBvcmF0
aW9uIEtFSyBDQSAyMDExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
xOi1ir+tVyawJsPq5/tXekQCXQcN2krldCrmsA/sbevsf7njWmMyfBEXTw7jC6c4
FZOOxvXghLGamyzn9beR1gnh4sAEqKwwHN9I8wZQmmSnUX/IhU+PIIbO/i/hn/+C
wO3pzc70U2piOgtDueIl/f4F+dTEFKsR4iOJjXC3pB1N7K7lnPoWwtfBy9ToxC/l
me4kiwPsjfKL6sNK+0MREgt+tUeSbNzmBInr9TME6xABKnHl+YMTPP8lCS9odkb/
uk++3K1xKliq+w7SeT3km2U7zCkqn/xyWaLrrpLv9jUTgMYC7ORfzJ12ze9jksGv
eUCEeYd/41Ko6J17B2mPFQIDAQABo4IBTzCCAUswEAYJKwYBBAGCNxUBBAMCAQAw
HQYDVR0OBBYEFGL8Q82gPqTLZxLSW9lVrHvMtopfMBkGCSsGAQQBgjcUAgQMHgoA
UwB1AGIAQwBBMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQY
MBaAFEVmUkPhflgRv9ZOniNVCDs6ImqoMFwGA1UdHwRVMFMwUaBPoE2GS2h0dHA6
Ly9jcmwubWljcm9zb2Z0LmNvbS9wa2kvY3JsL3Byb2R1Y3RzL01pY0NvclRoaVBh
```

```
ck1hclJvb18yMDEwLTEwLTA1LmNybDBgBggrBgEFBQcBAQRUMFIwUAYIKwYBBQUH
MAKGRGh0dHA6Ly93d3cubWljcm9zb2Z0LmNvbS9wa2kvY2VydHMvTWljQ29yVGhp
UGFyTWFyUm9vXzIwMTAtMTAtMDUuY3J0MA0GCSqGSIb3DQEBCwUAA4ICAQDUhIj1
FJQYAsoqPPsqkhwM16DR8ehSZqjuorV1epAAqi2kdlrqebe5N2pRexBk9uFk8gJn
vveoG3i9us6IWGQM1lfIGaNfBdbbxtBpzkhLMrfrXdIw9cD1uLp4B6Mr/pvbNFaE
7ILKrkElcJxr6f6QD9eWH+XnlB+yKgyNS/8oKRB799d8pdF2uQXIee0PkJKcwv7f
b35sD3vUwUXdNFGWOQ/lXlbYGAWW9AemQrOgd/0IGfJxVsyfhiOkh8um/Vh+1Gln
FZF+gfJ/E+UNi4o8h4Tr4869Q+WtLYSTjmorWnxE+lKqgcgtHLvgUt8AEfiaPcFg
sOEztaOI0WUZChrnrHykwYKHTjixLw3FFIdv/Y0uvDm25+bD4OTNJ4TvlELvKYuQ
RkE7gRtn2PlDWWXLDbz9AJJP9HU7p6kk/FBBQHngLU8Kaid2blLtlml7rw/3hwXQ
RcKtUxSBH/swBKo3NmHaSmkbNNho7dYCz2yUDNPPbCJ5rbHwvAOiRmCpxAfCIYLx
/fLoeTJgv9ispSIUS8rB2EvrfT9XNbLmT3W0sGADIlOukXkd1ptBHxWGVHCy3g01
D3ywNHK6l2A78HnrorIcXaIWuIfF6Rv2tZclbzif45H6inmYw2kOt6McIAWX+MoU
rgDXxPPAFBB1azSgG7WZYPNcsMVXTjbSMoS/ng==
-----END CERTIFICATE-----
```

7.3.3 db

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:07:76:56:00:00:00:00:00:08
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Root Certificate Authority 2010
        Validity
            Not Before: Oct 19 18:41:42 2011 GMT
            Not After : Oct 19 18:51:42 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Windows Production PCA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:dd:0c:bb:a2:e4:2e:09:e3:e7:c5:f7:96:69:bc:
                    00:21:bd:69:33:33:ef:ad:04:cb:54:80:ee:06:83:
                    bb:c5:20:84:d9:f7:d2:8b:f3:38:b0:ab:a4:ad:2d:
                    7c:62:79:05:ff:e3:4a:3f:04:35:20:70:e3:c4:e7:
                    6b:e0:9c:c0:36:75:e9:8a:31:dd:8d:70:e5:dc:37:
                    b5:74:46:96:28:5b:87:60:23:2c:bf:dc:47:a5:67:
                    f7:51:27:9e:72:eb:07:a6:c9:b9:1e:3b:53:35:7c:
                    e5:d3:ec:27:b9:87:1c:fe:b9:c9:23:09:6f:a8:46:
                    91:c1:6e:96:3c:41:d3:cb:a3:3f:5d:02:6a:4d:ec:
                    69:1f:25:28:5c:36:ff:fd:43:15:0a:94:e0:19:b4:
                    cf:df:c2:12:e2:c2:5b:27:ee:27:78:30:8b:5b:2a:
                    09:6b:22:89:53:60:16:2c:c0:68:1d:53:ba:ec:49:
                    f3:9d:61:8c:85:68:09:73:44:5d:7d:a2:54:2b:dd:
                    79:f7:15:cf:35:5d:6c:1c:2b:5c:ce:bc:9c:23:8b:
                    6f:6e:b5:26:d9:36:13:c3:4f:d6:27:ae:b9:32:3b:
                    41:92:2c:e1:c7:cd:77:e8:aa:54:4e:f7:5c:0b:04:
                    87:65:b4:43:18:a8:b2:e0:6d:19:77:ec:5a:24:fa:
                    48:03
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 Subject Key Identifier:
                A9:29:02:39:8E:16:C4:97:78:CD:90:F9:9E:4F:9A:E1:7C:55:AF:53
            1.3.6.1.4.1.311.20.2:
```

```
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:D5:F6:56:CB:8F:E8:A2:5C:62:68:D1:3D:94:90:5B:D7:CE:9A:18:C4

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt

    Signature Algorithm: sha256WithRSAEncryption
         14:fc:7c:71:51:a5:79:c2:6e:b2:ef:39:3e:bc:3c:52:0f:6e:
         2b:3f:10:13:73:fe:a8:68:d0:48:a6:34:4d:8a:96:05:26:ee:
         31:46:90:61:79:d6:ff:38:2e:45:6b:f4:c0:e5:28:b8:da:1d:
         8f:8a:db:09:d7:1a:c7:4c:0a:36:66:6a:8c:ec:1b:d7:04:90:
         a8:18:17:a4:9b:b9:e2:40:32:36:76:c4:c1:5a:c6:bf:e4:04:
         c0:ea:16:d3:ac:c3:68:ef:62:ac:dd:54:6c:50:30:58:a6:eb:
         7c:fe:94:a7:4e:8e:f4:ec:7c:86:73:57:c2:52:21:73:34:5a:
         f3:a3:8a:56:c8:04:da:07:09:ed:f8:8b:e3:ce:f4:7e:8e:ae:
         f0:f6:0b:8a:08:fb:3f:c9:1d:72:7f:53:b8:eb:be:63:e0:e3:
         3d:31:65:b0:81:e5:f2:ac:cd:16:a4:9f:3d:a8:b1:9b:c2:42:
         d0:90:84:5f:54:1d:ff:89:ea:ba:1d:47:90:6f:b0:73:4e:41:
         9f:40:9f:5f:e5:a1:2a:b2:11:91:73:8a:21:28:f0:ce:de:73:
         39:5f:3e:ab:5c:60:ec:df:03:10:a8:d3:09:e9:f4:f6:96:85:
         b6:7f:51:88:66:47:19:8d:a2:b0:12:3d:81:2a:68:05:77:bb:
         91:4c:62:7b:b6:c1:07:c7:ba:7a:87:34:03:0e:4b:62:7a:99:
         e9:ca:fc:ce:4a:37:c9:2d:a4:57:7c:1c:fe:3d:dc:b8:0f:5a:
         fa:d6:c4:b3:02:85:02:3a:ea:b3:d9:6e:e4:69:21:37:de:81:
         d1:f6:75:19:05:67:d3:93:57:5e:29:1b:39:c8:ee:2d:e1:cd:
         e4:45:73:5b:d0:d2:ce:7a:ab:16:19:82:46:58:d0:5e:9d:81:
         b3:67:af:6c:35:f2:bc:e5:3f:24:e2:35:a2:0a:75:06:f6:18:
         56:99:d4:78:2c:d1:05:1b:eb:d0:88:01:9d:aa:10:f1:05:df:
         ba:7e:2c:63:b7:06:9b:23:21:c4:f9:78:6c:e2:58:17:06:36:
         2b:91:12:03:cc:a4:d9:f2:2d:ba:f9:94:9d:40:ed:18:45:f1:
         ce:8a:5c:6b:3e:ab:03:d3:70:18:2a:0a:6a:e0:5f:47:d1:d5:
         63:0a:32:f2:af:d7:36:1f:2a:70:5a:e5:42:59:08:71:4b:57:
         ba:7e:83:81:f0:21:3c:f4:1c:c1:c5:b9:90:93:0e:88:45:93:
         86:e9:b1:20:99:be:98:cb:c5:95:a4:5d:62:d6:a0:63:08:20:
         bd:75:10:77:7d:3d:f3:45:b9:9f:97:9f:cb:57:80:6f:33:a9:
         04:cf:77:a4:62:1c:59:7e
-----BEGIN CERTIFICATE-----
MIIF1zCCA7+gAwIBAgIKYQd2VgAAAAAACDANBgkqhkiG9w0BAQsFADCBiDELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjEyMDAGA1UEAxMpTWljcm9z
b2Z0IFJvb3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IDIwMTAwHhcNMTExMDE5MTg0
MTQyWhcNMjYxMDE5MTg1MTQyWjCBhDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldh
c2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBD
b3Jwb3JhdGlvbjEuMCwGA1UEAxMlTWljcm9zb2Z0IFdpbmRvd3MgUHJvZHVjdGlv
biBQQ0EgMjAxMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN0Mu6Lk
Lgnj58X3lmm8ACG9aTMz760Ey1SA7gaDu8UghNn30ovzOLCrpK0tfGJ5Bf/jSj8E
NSBw48Tna+CcwDZ16Yox3Y1w5dw3tXRGlihbh2AjLL/cR6Vn91EnnnLrB6bJuR47
UzV85dPsJ7mHHP65ySMJb6hGkcFuljxB08ujP10Cak3saR8lKFw2//1DFQqU4Bm0
```

```
z9/CEuLCWyfuJ3gwi1sqCWsiiVNgFizAaB1TuuxJ851hjIVoCXNEXX2iVCvdefcV
zzVdbBwrXM68nCOLb261Jtk2E8NP1ieuuTI7QZIs4cfNd+iqVE73XAsEh2W0Qxio
suBtGXfsWiT6SAMCAwEAAaOCAUMwggE/MBAGCSsGAQQBgjcVAQQDAgEAMB0GA1Ud
DgQWBBSpKQI5jhbEl3jNkPmeT5rhfFWvUzAZBgkrBgEEAYI3FAIEDB4KAFMAdQBi
AEMAQTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBTV
9lbLj+iiXGJo0T2UkFvXzpoYxDBWBgNVHR8ETzBNMEugSaBHhkVodHRwOi8vY3Js
Lm1pY3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNSb29DZXJBdXRfMjAx
MC0wNi0yMy5jcmwwWgYIKwYBBQUHAQEETjBMMEoGCCsGAQUFBzAChj5odHRwOi8v
d3d3Lm1pY3Jvc29mdC5jb20vcGtpL2NlcnRzL01pY1Jvb0NlckF1dF8yMDEwLTA2
LTIzLmNydDANBgkqhkiG9w0BAQsFAAOCAgEAFPx8cVGlecJusu85Prw8Ug9uKz8Q
E3P+qGjQSKY0TYqWBSbuMUaQYXnW/zguRWv0wOUouNodj4rbCdcax0wKNmZqjOwb
1wSQqBgXpJu54kAyNnbEwVrGv+QEwOoW06zDaO9irN1UbFAwWKbrfP6Up06O9Ox8
hnNXwlIhczRa86OKVsgE2gcJ7fiL4870fo6u8PYLigj7P8kdcn9TuOu+Y+DjPTFl
sIHl8qzNFqSfPaixm8JC0JCEX1Qd/4nquh1HkG+wc05Bn0CfX+WhKrIRkXOKISjw
zt5zOV8+q1xg7N8DEKjTCen09paFtn9RiGZHGY2isBI9gSpoBXe7kUxie7bBB8e6
eoc0Aw5LYnqZ6cr8zko3yS2kV3wc/j3cuA9a+tbEswKFAjrqs9lu5GkhN96B0fZ1
GQVn05NXXikbOcjuLeHN5EVzW9DSznqrFhmCRljQXp2Bs2evbDXyvOU/JOI1ogp1
BvYYVpnUeCzRBRvr0IgBnaoQ8QXfun4sY7cGmyMhxPl4bOJYFwY2K5ESA8yk2fIt
uvmUnUDtGEXxzopcaz6rA9NwGCoKauBfR9HVYwoy8q/XNh8qcFrlQlkIcUtXun6D
gfAhPPQcwcW5kJMOiEWThumxIJm+mMvFlaRdYtagYwggvXUQd30980W5n5efy1eA
bzOpBM93pGIcWX4=
-----END CERTIFICATE-----

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:08:d3:c4:00:00:00:00:00:04
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation Third Party Marketplace Root
        Validity
            Not Before: Jun 27 21:22:45 2011 GMT
            Not After : Jun 27 21:32:45 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation UEFI CA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a5:08:6c:4c:c7:45:09:6a:4b:0c:a4:c0:87:7f:
                    06:75:0c:43:01:54:64:e0:16:7f:07:ed:92:7d:0b:
                    b2:73:bf:0c:0a:c6:4a:45:61:a0:c5:16:2d:96:d3:
                    f5:2b:a0:fb:4d:49:9b:41:80:90:3c:b9:54:fd:e6:
                    bc:d1:9d:c4:a4:18:8a:7f:41:8a:5c:59:83:68:32:
                    bb:8c:47:c9:ee:71:bc:21:4f:9a:8a:7c:ff:44:3f:
                    8d:8f:32:b2:26:48:ae:75:b5:ee:c9:4c:1e:4a:19:
                    7e:e4:82:9a:1d:78:77:4d:0c:b0:bd:f6:0f:d3:16:
                    d3:bc:fa:2b:a5:51:38:5d:f5:fb:ba:db:78:02:db:
                    ff:ec:0a:1b:96:d5:83:b8:19:13:e9:b6:c0:7b:40:
                    7b:e1:1f:28:27:c9:fa:ef:56:5e:1c:e6:7e:94:7e:
                    c0:f0:44:b2:79:39:e5:da:b2:62:8b:4d:bf:38:70:
                    e2:68:24:14:c9:33:a4:08:37:d5:58:69:5e:d3:7c:
                    ed:c1:04:53:08:e7:4e:b0:2a:87:63:08:61:6f:63:
                    15:59:ea:b2:2b:79:d7:0c:61:67:8a:5b:fd:5e:ad:
                    87:7f:ba:86:67:4f:71:58:12:22:04:22:22:ce:8b:
                    ef:54:71:00:ce:50:35:58:76:95:08:ee:6a:b1:a2:
                    01:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                .....
```

```
            1.3.6.1.4.1.311.21.2:
                ....k..wSJ.%7.N.&{. p.
            X509v3 Subject Key Identifier:
                13:AD:BF:43:09:BD:82:70:9C:8C:D5:4F:31:6E:D5:22:98:8A:1B:D4
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:45:66:52:43:E1:7E:58:11:BF:D6:4E:9E:23:55:08:3B:3A:22:6A:A8

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicCorThiParMarRoo_2010-10-05.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt

    Signature Algorithm: sha256WithRSAEncryption
         35:08:42:ff:30:cc:ce:f7:76:0c:ad:10:68:58:35:29:46:32:
         76:27:7c:ef:12:41:27:42:1b:4a:aa:6d:81:38:48:59:13:55:
         f3:e9:58:34:a6:16:0b:82:aa:5d:ad:82:da:80:83:41:06:8f:
         b4:1d:f2:03:b9:f3:1a:5d:1b:f1:50:90:f9:b3:55:84:42:28:
         1c:20:bd:b2:ae:51:14:c5:c0:ac:97:95:21:1c:90:db:0f:fc:
         77:9e:95:73:91:88:ca:bd:bd:52:b9:05:50:0d:df:57:9e:a0:
         61:ed:0d:e5:6d:25:d9:40:0f:17:40:c8:ce:a3:4a:c2:4d:af:
         9a:12:1d:08:54:8f:bd:c7:bc:b9:2b:3d:49:2b:1f:32:fc:6a:
         21:69:4f:9b:c8:7e:42:34:fc:36:06:17:8b:8f:20:40:c0:b3:
         9a:25:75:27:cd:c9:03:a3:f6:5d:d1:e7:36:54:7a:b9:50:b5:
         d3:12:d1:07:bf:bb:74:df:dc:1e:8f:80:d5:ed:18:f4:2f:14:
         16:6b:2f:de:66:8c:b0:23:e5:c7:84:d8:ed:ea:c1:33:82:ad:
         56:4b:18:2d:f1:68:95:07:cd:cf:f0:72:f0:ae:bb:dd:86:85:
         98:2c:21:4c:33:2b:f0:0f:4a:f0:68:87:b5:92:55:32:75:a1:
         6a:82:6a:3c:a3:25:11:a4:ed:ad:d7:04:ae:cb:d8:40:59:a0:
         84:d1:95:4c:62:91:22:1a:74:1d:8c:3d:47:0e:44:a6:e4:b0:
         9b:34:35:b1:fa:b6:53:a8:2c:81:ec:a4:05:71:c8:9d:b8:ba:
         e8:1b:44:66:e4:47:54:0e:8e:56:7f:b3:9f:16:98:b2:86:d0:
         68:3e:90:23:b5:2f:5e:8f:50:85:8d:c6:8d:82:5f:41:a1:f4:
         2e:0d:e0:99:d2:6c:75:e4:b6:69:b5:21:86:fa:07:d1:f6:e2:
         4d:d1:da:ad:2c:77:53:1e:25:32:37:c7:6c:52:72:95:86:b0:
         f1:35:61:6a:19:f5:b2:3b:81:50:56:a6:32:2d:fe:a2:89:f9:
         42:86:27:18:55:a1:82:ca:5a:9b:f8:30:98:54:14:a6:47:96:
         25:2f:c8:26:e4:41:94:1a:5c:02:3f:e5:96:e3:85:5b:3c:3e:
         3f:bb:47:16:72:55:e2:25:22:b1:d9:7b:e7:03:06:2a:a3:f7:
         1e:90:46:c3:00:0d:d6:19:89:e3:0e:35:27:62:03:71:15:a6:
         ef:d0:27:a0:a0:59:37:60:f8:38:94:b8:e0:78:70:f8:ba:4c:
         86:87:94:f6:e0:ae:02:45:ee:65:c2:b6:a3:7e:69:16:75:07:
         92:9b:f5:a6:bc:59:83:58
-----BEGIN CERTIFICATE-----
MIIGEDCCA/igAwIBAgIKYQjTxAAAAAAABDANBgkqhkiG9w0BAQsFADCBkTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE7MDkGA1UEAxMyTWljcm9z
b2Z0IENvcnBvcmF0aW9uIFRoaXJkIFBhcnR5IE1hcmtldHBsYWNlIFJvb3QwHhcN
MTEwNjI3MjEyMjQ1WhcNMjYwNjI3MjEzMjQ1WjCBgTELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1p
```

```
Y3Jvc29mdCBDb3Jwb3JhdGlvbjErMCkGA1UEAxMiTWljcm9zb2Z0IENvcnBvcmF0
aW9uIFVFRkkgQ0EgMjAxMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AKUIbEzHRQlqSwykwId/BnUMQwFUZOAWfwftkn0LsnO/DArGSkVhoMUWLZbT9Sug
+01Jm0GAkDy5VP3mvNGdxKQYin9BilxZg2gyu4xHye5xvCFPmop8/0Q/jY8ysiZI
rnW17slMHkoZfuSCmh14d00MsL32D9MW07z6K6VROF31+7rbeALb/+wKG5bVg7gZ
E+m2wHtAe+EfKCfJ+u9WXhzmfpR+wPBEsnk55dqyYotNvzhw4mgkFMkzpAg31Vhp
XtN87cEEUwjnTrAqh2MIYW9jFVnqsit51wxhZ4pb/V6th3+6hmdPcVgSIgQiIs6L
71RxAM5QNVh2lQjuarGiAdUCAwEAAaOCAXYwggFyMBIGCSsGAQQBgjcVAQQFAgMB
AAEwIwYJKwYBBAGCNxUCBBYEFPjBa7d/d1NK8yU3HU6hJnsPIHCAMB0GA1UdDgQW
BBQTrb9DCb2CcJyM1U8xbtUimIob1DAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMA
QTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRFZlJD
4X5YEb/WTp4jVQg7OiJqqDBcBgNVHR8EVTBTMFGgT6BNhktodHRwOi8vY3JsLm1p
Y3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNDb3JUaGlQYXJNYXJSb29f
MjAxMC0xMC0wNS5jcmwwYAYIKwYBBQUHAQEEVDBSMFAGCCsGAQUFBzAChkRodHRw
Oi8vd3d3Lm1pY3Jvc29mdC5jb20vcGtpL2NlcnRzL01pY0NvclRoaVBhck1hclJv
b18yMDEwLTEwLTA1LmNydDANBgkqhkiG9w0BAQsFAAOCAgEANQhC/zDMzvd2DK0Q
aFg1KUYydid87xJBJ0IbSqptgThIWRNV8+lYNKYWC4KqXa2C2oCDQQaPtB3yA7nz
Gl0b8VCQ+bNVhEIoHCC9sq5RFMXArJeVIRyQ2w/8d56Vc5GIyr29UrkFUA3fV56g
Ye0N5W0l2UAPF0DIzqNKwk2vmhIdCFSPvce8uSs9SSsfMvxqIWlPm8h+QjT8NgYX
i48gQMCzmiV1J83JA6P2XdHnNlR6uVC10xLRB7+7dN/cHo+A1e0Y9C8UFmsv3maM
sCPlx4TY7erBM4KtVksYLfFolQfNz/By8K673YaFmCwhTDMr8A9K8GiHtZJVMnWh
aoJqPKMlEaTtrdcErsvYQFmghNGVTGKRIhp0HYw9Rw5EpuSwmzQ1sfq2U6gsgeyk
BXHInbi66BtEZuRHVA6OVn+znxaYsobQaD6QI7UvXo9QhY3GjYJfQaH0Lg3gmdJs
deS2abUhhvoH0fbiTdHarSx3Ux4lMjfHbFJylYaw8TVhahn1sjuBUFamMi3+oon5
QoYnGFWhgspam/gwmFQUpkeWJS/IJuRBlBpcAj/lluOFWzw+P7tHFnJV4iUisdl7
5wMGKqP3HpBGwwAN1hmJ4w41J2IDcRWm79AnoKBZN2D4OJS44Hhw+LpMhoeU9uCu
AkXuZcK2o35pFnUHkpv1prxZg1g=
-----END CERTIFICATE-----
```

7.3.4 dbx

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:0c:6a:19:00:00:00:00:00:04
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Root Certificate Authority 2010
        Validity
            Not Before: Jul  6 20:40:23 2010 GMT
            Not After : Jul  6 20:50:23 2025 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Windows PCA 2010
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c0:79:bb:3a:b1:f0:0f:84:b8:ad:64:2a:75:16:
                    73:d0:bb:07:f6:3e:0d:9d:14:e4:b1:9f:c1:c8:94:
                    b0:38:7c:1f:d0:33:55:f5:ba:23:66:f5:2e:28:48:
                    53:c7:16:83:ba:f5:51:ac:7e:ac:e0:26:7f:0f:74:
                    fc:59:95:dc:c9:c6:a2:f7:52:70:5a:2c:1d:94:ab:
                    19:bf:af:95:7d:af:66:a1:6f:9b:62:6e:6d:4b:bc:
                    2f:35:6c:de:a4:6a:63:5a:5f:fb:f3:0d:4d:61:cc:
                    0a:7e:31:eb:6c:0a:d0:4d:97:0f:fd:7f:38:46:e6:
                    8a:c7:73:69:76:55:69:96:4c:e4:d8:f0:34:eb:ba:
                    b1:1f:ce:29:7e:c4:4f:9d:13:15:ab:13:1b:72:58:
                    62:56:6c:8a:81:a3:64:77:98:46:65:29:9d:83:14:
                    a5:4c:08:a0:83:d7:23:1f:f3:5f:df:6f:2c:cf:da:
```

```
                    16:d8:0e:72:04:28:d8:6b:3e:f8:13:b1:7c:a2:17:
                    79:4f:7e:dc:3a:e4:9d:70:27:6b:bf:db:fc:1e:c7:
                    07:d8:c0:be:0b:93:1e:28:e0:73:6d:d2:54:e9:28:
                    4c:bf:6b:5d:9f:ff:5d:33:12:37:95:25:61:34:6a:
                    42:cb:7c:9d:3a:bb:88:59:e1:a3:42:6d:3a:50:5b:
                    48:d1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 Subject Key Identifier:
                D1:4F:A9:8A:07:08:CE:F4:24:18:98:E5:00:FF:F3:D6:79:1D:37:BC
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:D5:F6:56:CB:8F:E8:A2:5C:62:68:D1:3D:94:90:5B:D7:CE:9A:18:C4

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.311.46.3
                  CPS: http://www.microsoft.com/PKI/docs/CPS/default.htm
                  User Notice:
                    Explicit Text:  #

    Signature Algorithm: sha256WithRSAEncryption
         2e:41:a6:86:b5:06:6f:f0:80:85:fa:3b:ca:17:e9:c9:fa:e4:
         39:c2:94:70:c3:64:94:c3:d8:56:a6:90:8e:fe:e4:9a:f4:6d:
         f5:6f:8e:53:8d:5a:a8:f3:ae:db:46:6c:be:7f:1d:54:56:1b:
         3c:1d:71:c4:51:15:54:7e:bf:ee:a5:95:42:33:fd:0d:90:24:
         24:e3:f9:dc:96:ca:fc:b8:ac:bf:f4:c2:39:56:b8:bb:ed:73:
         b3:17:dd:7e:86:50:23:8b:56:24:ca:bb:a6:1d:9a:87:2f:27:
         85:e7:a1:b6:0a:9c:0d:1b:8c:f3:00:62:41:ba:48:74:87:82:
         fd:50:c9:f4:87:29:c3:03:aa:2b:df:1a:29:79:e8:12:24:9a:
         86:ed:d0:2e:d3:40:81:f5:07:5f:33:06:54:5d:40:b5:f7:b1:
         62:fd:4d:48:f7:6e:41:47:52:1c:bb:1b:c2:57:3a:a8:99:56:
         93:d4:c6:de:26:a8:60:75:86:bb:ec:62:a6:f0:1d:04:45:df:
         3e:a7:84:d1:5b:44:23:63:25:36:77:6f:ae:5b:dc:22:d5:14:
         23:6a:41:7f:d0:42:a6:db:ef:25:7b:04:e3:d2:96:37:62:06:
         af:f8:1b:0f:8e:b3:39:9a:bb:89:f5:35:06:e5:a4:5b:c3:8c:
         9e:37:5f:53:d1:a3:37:fd:a4:4f:e8:1b:0e:6b:76:e4:b8:8f:
         b0:c2:ea:fd:75:f7:2c:41:b7:9c:a3:e1:1e:05:fe:97:92:cb:
         7f:59:03:6d:a8:4e:8d:4e:80:17:d4:d5:72:f6:56:e4:48:9f:
         a3:23:ba:06:a0:c0:8e:d1:88:4f:93:20:f2:70:5f:d8:6b:72:
         a3:20:49:fc:77:0c:5d:c5:c7:e1:02:0f:38:42:10:0e:db:02:
         ae:9a:37:1d:50:80:29:1e:a4:a7:d9:c6:9a:25:55:fd:40:ca:
         ad:64:10:e8:31:f9:12:54:79:1a:f2:0e:d8:d6:ab:1e:33:fe:
         02:e7:26:6d:61:49:8f:f1:25:c2:8b:74:99:df:f9:93:1a:90:
```

```
          1c:ee:dd:94:33:0e:42:50:db:7f:50:f8:9f:62:82:ec:a6:82:
          16:7c:66:bc:ec:99:b0:c1:58:5d:a8:b0:9a:61:14:91:d1:99:
          2f:49:e4:3e:81:99:d6:e6:ef:ca:e3:fd:3e:ee:ec:09:86:03:
          07:0d:1b:0d:7c:eb:f4:5a:c9:95:cf:87:12:0a:5d:ec:c5:02:
          92:cd:05:99:72:ca:7d:f1:2a:10:18:38:e4:31:a3:28:b4:e6:
          4c:c5:52:a3:9c:6a:c7:7d:c0:71:09:04:0d:70:de:02:3f:87:
          ee:56:a1:ec:eb:b5:4c:85
-----BEGIN CERTIFICATE-----
MIIGazCCBFOgAwIBAgIKYQxqGQAAAAAABDANBgkqhkiG9w0BAQsFADCBiDELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjEyMDAGA1UEAxMpTWljcm9z
b2Z0IFJvb3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IDIwMTAwHhcNMTAwNzA2MjA0
MDIzWhcNMjUwNzA2MjA1MDIzWjB5MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2Fz
aGluZ3RvbjEQMA4GA1UEBxMHUmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENv
cnBvcmF0aW9uMSMwIQYDVQQDExpNaWNyb3NvZnQgV2luZG93cyBQQ0EgMjAxMDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMB5uzqx8A+EuK1kKnUWc9C7
B/Y+DZ0U5LGfwciUsDh8H9AzVfW6I2b1LihIU8cWg7r1Uax+rOAmfw90/FmV3MnG
ovdScFosHZSrGb+vlX2vZqFvm2JubUu8LzVs3qRqY1pf+/MNTWHMCn4x62wK0E2X
D/1/OEbmisdzaXZVaZZM5NjwNOu6sR/OKX7ET50TFasTG3JYYlZsioGjZHeYRmUp
nYMUpUwIoIPXIx/zX99vLM/aFtgOcgQo2Gs++BOxfKIXeU9+3DrknXAna7/b/B7H
B9jAvguTHijgc23SVOkoTL9rXZ//XTMSN5UlYTRqQst8nTq7iFnho0JtOlBbSNEC
AwEAAaOCAeMwggHfMBAGCSsGAQQBgjcVAQQDAgEAMB0GA1UdDgQWBBTRT6mKBwjO
9CQYmOUA//PWeR03vDAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMAQTALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBTV9lbLj+iiXGJo0T2U
kFvXzpoYxDBWBgNVHR8ETzBNMEugSaBHhkVodHRwOi8vY3JsLm1pY3Jvc29mdC5j
b20vcGtpL2NybC9wcm9kdWN0cy9NaWNSb29DZXJBdXRfMjAxMC0wNi0yMy5jcmww
WgYIKwYBBQUHAQEETjBMMEoGCCsGAQUFBzAChj5odHRwOi8vd3d3Lm1pY3Jvc29m
dC5jb20vcGtpL2NlcnRzL01pY1Jvb0NlckF1dF8yMDEwLTA2LTIzLmNydDCBnQYD
VR0gBIGVMIGSMIGPBgkrBgEEAYI3LgMwgYEwPQYIKwYBBQUHAgEWMWh0dHA6Ly93
d3cubWljcm9zb2Z0LmNvbS9QS0kvZG9jcy9DUFMvZGVmYXVsdC5odG0wQAYIKwYB
BQUHAgIwNB4yIB0ATABlAGcAYQBsAF8AUABvAGwAaQBjAHkAXwBTAHQAYQB0AGUA
bQBlAG4AdAAuIB0wDQYJKoZIhvcNAQELBQADggIBAC5Bpoa1Bm/wgIX6O8oX6cn6
5DnClHDDZJTD2FamkI7+5Jr0bfVvjlONWqjzrttGbL5/HVRWGzwdccRRFVR+v+6l
lUIz/Q2QJCTj+dyWyvy4rL/0wjlWuLvtc7MX3X6GUCOLViTKu6YdmocvJ4XnobYK
nA0bjPMAYkG6SHSHgv1QyfSHKcMDqivfGil56BIkmobt0C7TQIH1B18zBlRdQLX3
sWL9TUj3bkFHUhy7G8JXOqiZVpPUxt4mqGB1hrvsYqbwHQRF3z6nhNFbRCNjJTZ3
b65b3CLVFCNqQX/QQqbb7yV7BOPSljdiBq/4Gw+Oszmau4n1NQblpFvDjJ43X1PR
ozf9pE/oGw5rduS4j7DC6v119yxBt5yj4R4F/peSy39ZA22oTo1OgBfU1XL2VuRI
n6MjugagwI7RiE+TIPJwX9hrcqMgSfx3DF3Fx+ECDzhCEA7bAq6aNx1QgCkepKfZ
xpolVf1Ayq1kEOgx+RJUeRryDtjWqx4z/gLnJm1hSY/xJcKLdJnf+ZMakBzu3ZQz
DkJQ239Q+J9iguymghZ8ZrzsmbDBWF2osJphFJHRmS9J5D6Bmdbm78rj/T7u7AmG
AwcNGw186/RayZXPhxIKXezFApLNBZlyyn3xKhAYOOQxoyi05kzFUqOcasd9wHEJ
BA1w3gI/h+5WoezrtUyF
-----END CERTIFICATE-----
```

7.4 Zertifikate der Lenovo-Plattform

7.4.1 PK

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 16984503372758506606 (0xebb513d46bb1dc6e)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=JP, ST=Kanagawa, L=Yokohama, O=Lenovo Ltd., CN=Lenovo Ltd. PK
CA 2012
        Validity
            Not Before: Jun 29 10:34:36 2012 GMT
            Not After : Jun 24 10:34:36 2032 GMT
        Subject: C=JP, ST=Kanagawa, L=Yokohama, O=Lenovo Ltd., CN=Lenovo Ltd. PK
CA 2012
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b6:9c:5d:62:63:d3:d1:77:52:66:99:5f:d8:22:
                    12:86:71:1b:1e:ae:14:3a:18:4b:ff:0c:54:fd:fb:
                    f2:be:5a:49:d4:a1:a7:52:1e:7f:6c:4b:c7:60:0a:
                    ce:c2:bc:7d:ab:13:b6:66:e9:12:c3:7c:75:f3:de:
                    c0:f3:32:19:b8:5e:f2:9c:cb:58:98:66:d9:73:14:
                    e8:9b:6f:2a:b2:64:34:16:3f:07:9b:b8:19:fa:2c:
                    c9:d6:06:55:4e:77:b5:21:e5:73:6c:02:a5:40:b1:
                    f4:b2:31:87:d3:53:24:f8:2c:aa:6d:42:aa:5c:b4:
                    bb:a5:ec:ce:05:29:c5:42:93:5a:1c:d4:e7:ab:df:
                    5e:83:70:87:77:a8:59:78:33:d4:ca:f1:46:6a:c0:
                    9e:9c:04:3f:03:9e:13:52:0f:0a:13:3c:db:94:6b:
                    5d:4c:14:09:73:17:1a:0b:3a:e6:ec:a1:45:1d:3a:
                    a5:aa:9a:f4:de:b4:b3:15:f1:07:c8:d6:fa:e0:a8:
                    30:99:b7:8e:a3:d0:ff:3b:f2:c9:f9:88:8b:31:b6:
                    a2:fd:0a:4d:f4:ff:28:ae:c5:b5:da:3e:42:93:26:
                    9a:9a:bd:aa:0e:54:58:fe:87:af:20:a0:77:cc:3d:
                    e1:96:52:f2:98:4e:32:14:2e:b2:e8:ed:3b:01:7a:
                    d8:93
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                FF:77:DF:4B:17:4C:71:8B:74:F9:17:9D:EC:34:3D:8D:19:0E:94:48
            X509v3 Authority Key Identifier:

keyid:FF:77:DF:4B:17:4C:71:8B:74:F9:17:9D:EC:34:3D:8D:19:0E:94:48

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         70:65:af:af:90:25:ad:55:d6:91:a5:e6:df:91:a0:89:ef:8f:
         32:4b:b5:ee:c6:d5:8e:bb:13:8e:43:5d:3d:72:4e:3a:4f:26:
         a6:67:b0:28:56:cf:6a:1c:ea:30:ee:08:61:2d:7d:42:8c:fa:
         de:d6:ee:d5:3b:94:0c:28:61:df:4f:4f:f0:fe:21:db:a6:cd:
         78:8a:0f:07:28:5f:d5:dd:b5:d7:93:72:98:c9:6e:65:88:f2:
         a5:b7:a9:c3:75:0e:65:12:bc:d5:32:d4:5d:ce:c2:d1:65:5e:
         b9:6c:4e:a8:00:07:ba:28:78:30:8a:0c:70:b5:54:58:50:b5:
         22:23:3e:df:61:4f:e0:91:ee:60:1b:47:84:72:f7:ea:69:a5:
         28:ca:4f:f5:3a:b7:18:0e:3e:bf:87:31:87:0a:10:d9:c5:34:
```

```
         ab:00:7d:10:07:e9:ba:c2:ed:41:a9:41:c0:bf:ea:9e:82:fb:
         54:9d:85:b9:81:36:5f:01:f1:9c:1a:b9:b8:5c:b1:16:c9:e9:
         4c:80:12:78:41:79:07:e8:f9:6d:11:ed:2c:88:8e:3d:0d:bd:
         6c:23:17:60:1c:d6:47:1b:f6:2b:51:b4:b6:82:51:7c:c9:5e:
         d2:60:25:59:3c:79:65:33:1f:3a:90:80:23:ca:c1:98:2e:6e:
         14:8e:91:76
-----BEGIN CERTIFICATE-----
MIIDpzCCAo+gAwIBAgIJAOu1E9RrsdxuMA0GCSqGSIb3DQEBCwUAMGoxCzAJBgNV
BAYTAkpQMREwDwYDVQQIDAhLYW5hZ2F3YTERMA8GA1UEBwwIWW9rb2hhbWExFDAS
BgNVBAoMC0xlbm92byBMdGQuMR8wHQYDVQQDDBZMZW5vdm8gTHRkLiBQSyBDQSAy
MDEyMB4XDTEyMDYyOTEwMzQzNloXDTMyMDYyNDEwMzQzNlowajELMAkGA1UEBhMC
SlAxETAPBgNVBAgMCEthbmFnYXdhMREwDwYDVQQHDAhZb2tvaGFtYTEUMBIGA1UE
CgwLTGVub3ZvIEx0ZC4xHzAdBgNVBAMMFkxlbm92byBMdGQuIFBLIENBIDIwMTIw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2nF1iY9PRd1JmmV/YIhKG
cRserhQ6GEv/DFT9+/K+WknUoadSHn9sS8dgCs7CvH2rE7Zm6RLDfHXz3sDzMhm4
XvKcy1iYZtlzFOibbyqyZDQWPwebuBn6LMnWBlVOd7Uh5XNsAqVAsfSyMYfTUyT4
LKptQqpctLul7M4FKcVCk1oc1Oer316DcId3qFl4M9TK8UZqwJ6cBD8DnhNSDwoT
PNuUa11MFAlzFxoLOubsoUUdOqWqmvTetLMV8QfI1vrgqDCZt46j0P878sn5iIsx
tqL9Ck30/yiuxbXaPkKTJpqavaoOVFj+h68goHfMPeGWUvKYTjIULrLo7TsBetiT
AgMBAAGjUDBOMB0GA1UdDgQWBBT/d99LF0xxi3T5F53sND2NGQ6USDAfBgNVHSME
GDAWgBT/d99LF0xxi3T5F53sND2NGQ6USDAMBgNVHRMEBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4IBAQBwZa+vkCWtVdaRpebfkaCJ748yS7XuxtWOuxOOQ109ck46Tyam
Z7AoVs9qHOow7ghhLX1CjPre1u7VO5QMKGHfT0/w/iHbps14ig8HKF/V3bXXk3KY
yW5liPKlt6nDdQ5lErzVMtRdzsLRZV65bE6oAAe6KHgwigxwtVRYULUiIz7fYU/g
ke5gG0eEcvfqaaUoyk/1OrcYDj6/hzGHChDZxTSrAH0QB+m6wu1BqUHAv+qegvtU
nYW5gTZfAfGcGrm4XLEWyelMgBJ4QXkH6PltEe0siI49Db1sIxdgHNZHG/YrUbS2
glF8yV7SYCVZPHllMx86kIAjysGYLm4UjpF2
-----END CERTIFICATE-----
```

7.4.2 KEK

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 10759736687687525678 (0x955243828a5a652e)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=JP, ST=Kanagawa, L=Yokohama, O=Lenovo Ltd., CN=Lenovo Ltd. KEK
CA 2012
        Validity
            Not Before: Jun 29 10:35:34 2012 GMT
            Not After : Jun 24 10:35:34 2032 GMT
        Subject: C=JP, ST=Kanagawa, L=Yokohama, O=Lenovo Ltd., CN=Lenovo Ltd.
KEK CA 2012
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e6:a5:3a:22:e6:3f:34:50:8c:4b:1a:eb:d7:45:
                    ef:6a:57:7b:0f:1e:3f:c2:24:fa:ba:b1:70:43:79:
                    db:ad:01:9e:2e:16:e1:e0:66:fb:8c:b5:81:0f:d7:
                    20:84:94:c7:3b:18:c2:6c:80:21:56:10:55:98:ae:
                    4e:91:34:60:37:98:41:79:0d:e9:4b:39:3c:b7:54:
                    c1:50:39:50:fe:07:cf:9d:22:c4:09:24:d2:37:6c:
                    64:c0:64:33:37:6e:87:d2:f0:62:1b:8e:b3:6b:30:
                    f8:c9:f6:cd:4d:a8:79:02:2c:ff:9e:a5:6c:fd:93:
                    85:73:6b:a0:42:19:6c:c7:eb:c7:b3:c4:41:ad:83:
                    94:8f:01:d7:0a:4e:ef:74:b1:06:21:4f:89:37:8d:
                    6a:ca:5b:92:fa:3c:5c:c3:c8:06:09:dd:c5:02:ce:
                    5f:77:51:6c:e9:6d:ff:86:8b:44:3d:07:96:d5:d3:
                    32:17:51:ad:4f:7c:83:b6:ad:e1:21:b3:a5:70:cf:
```

```
                    f7:d2:b7:ad:df:c6:a4:0b:c9:ce:ea:84:eb:ca:9f:
                    e1:5a:f9:d8:f9:68:d9:b1:e0:29:51:cd:90:a4:86:
                    e7:a0:e7:09:0c:d7:c4:a0:dd:8b:4c:bc:ef:89:3f:
                    8c:76:64:fe:28:15:61:50:07:8b:bf:46:eb:0a:61:
                    ba:65
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                80:8E:F9:C1:79:96:40:DE:41:46:C8:0E:7C:4B:B4:82:46:3E:7D:D4
            X509v3 Authority Key Identifier:

keyid:80:8E:F9:C1:79:96:40:DE:41:46:C8:0E:7C:4B:B4:82:46:3E:7D:D4

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         90:fc:18:1c:1b:6d:f0:02:3b:83:44:24:b8:69:ab:c8:df:2d:
         22:aa:55:da:a7:f0:88:5b:db:41:a1:03:4d:4a:9d:f9:72:2c:
         8d:1a:9d:ac:53:89:08:82:70:f4:f8:93:56:b7:68:ba:5f:2e:
         3e:e5:b8:84:4b:8d:b8:a4:86:a1:a8:7a:ab:fc:65:52:71:ae:
         02:66:49:d4:85:bb:ed:95:28:05:8d:3a:5c:bb:7f:40:13:d2:
         42:29:01:88:92:be:a2:0b:ba:6a:d3:34:af:3c:fb:6a:99:ff:
         2e:2f:be:06:7a:1b:8b:36:fc:1b:7b:08:ae:f6:02:82:2e:e4:
         83:38:7b:56:ba:23:52:fa:6f:f0:64:a5:0a:37:f2:5d:9f:22:
         09:5b:bf:5d:6c:80:fe:8b:73:7d:84:16:f3:6a:fb:1a:4a:5b:
         86:34:73:22:0a:a7:73:1e:28:4c:f8:76:10:c8:5c:8c:fd:6c:
         12:90:00:85:b1:e2:3a:66:ef:69:16:46:9e:12:45:7e:ec:0b:
         31:57:cc:3e:06:5f:de:4b:72:5e:74:cb:bc:de:e3:c5:aa:7a:
         a7:82:11:aa:b9:65:98:f2:40:ca:a7:74:54:6d:1a:a0:5c:49:
         26:84:df:2e:bd:a3:57:1d:13:51:8c:5f:bb:e6:1a:7c:82:a4:
         57:7c:8b:bf
-----BEGIN CERTIFICATE-----
MIIDqTCCApGgAwIBAgIJAJVSQ4KKWmUuMA0GCSqGSIb3DQEBCwUAMGsxCzAJBgNV
BAYTAkpQMREwDwYDVQQIDAhLYW5hZ2F3YTERMA8GA1UEBwwIWW9rb2hhbWExFDAS
BgNVBAoMC0xlbm92byBMdGQuMSAwHgYDVQQDDBdMZW5vdm8gTHRkLiBLRUsgQ0Eg
MjAxMjAeFw0xMjA2MjkxMDM1MzRaFw0zMjA2MjQxMDM1MzRaMGsxCzAJBgNVBAYT
AkpQMREwDwYDVQQIDAhLYW5hZ2F3YTERMA8GA1UEBwwIWW9rb2hhbWExFDASBgNV
BAoMC0xlbm92byBMdGQuMSAwHgYDVQQDDBdMZW5vdm8gTHRkLiBLRUsgQ0EgMjAx
MjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOalOiLmPzRQjEsa69dF
72pXew8eP8Ik+rqxcEN5260Bni4W4eBm+4y1gQ/XIISUxzsYwmyAIVYQVZiuTpE0
YDeYQXkN6Us5PLdUwVA5UP4Hz50ixAkk0jdsZMBkMzduh9LwYhuOs2sw+Mn2zU2o
eQIs/56lbP2ThXNroEIZbMfrx7PEQa2DlI8B1wpO73SxBiFPiTeNaspbkvo8XMPI
BgndxQLOX3dRbOlt/4aLRD0HltXTMhdRrU98g7at4SGzpXDP99K3rd/GpAvJzuqE
68qf4Vr52Plo2bHgKVHNkKSG56DnCQzXxKDdi0y874k/jHZk/igVYVAHi79G6wph
umUCAwEAAaNQME4wHQYDVR0OBBYEFICO+cF5lkDeQUbIDnxLtIJGPn3UMB8GA1Ud
IwQYMBaAFICO+cF5lkDeQUbIDnxLtIJGPn3UMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAJD8GBwbbfACO4NEJLhpq8jfLSKqVdqn8Ihb20GhA01Knfly
LI0anaxTiQiCcPT4k1a3aLpfLj7luIRLjbikhqGoeqv8ZVJxrgJmSdSFu+2VKAWN
Oly7f0AT0kIpAYiSvqILumrTNK88+2qZ/y4vvgZ6G4s2/Bt7CK72AoIu5IM4e1a6
I1L6b/BkpQo38l2fIglbv11sgP6Lc32EFvNq+xpKW4Y0cyIKp3MeKEz4dhDIXIz9
bBKQAIWx4jpm72kWRp4SRX7sCzFXzD4GX95Lcl50y7ze48WqeqeCEaq5ZZjyQMqn
dFRtGqBcSSaE3y69o1cdE1GMX7vmGnyCpFd8i78=
-----END CERTIFICATE-----

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:0a:d1:88:00:00:00:00:00:03
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation Third Party Marketplace Root
```

```
        Validity
            Not Before: Jun 24 20:41:29 2011 GMT
            Not After : Jun 24 20:51:29 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation KEK CA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:e8:b5:8a:bf:ad:57:26:b0:26:c3:ea:e7:fb:
                    57:7a:44:02:5d:07:0d:da:4a:e5:74:2a:e6:b0:0f:
                    ec:6d:eb:ec:7f:b9:e3:5a:63:32:7c:11:17:4f:0e:
                    e3:0b:a7:38:15:93:8e:c6:f5:e0:84:b1:9a:9b:2c:
                    e7:f5:b7:91:d6:09:e1:e2:c0:04:a8:ac:30:1c:df:
                    48:f3:06:50:9a:64:a7:51:7f:c8:85:4f:8f:20:86:
                    ce:fe:2f:e1:9f:ff:82:c0:ed:e9:cd:ce:f4:53:6a:
                    62:3a:0b:43:b9:e2:25:fd:fe:05:f9:d4:c4:14:ab:
                    11:e2:23:89:8d:70:b7:a4:1d:4d:ec:ae:e5:9c:fa:
                    16:c2:d7:c1:cb:d4:e8:c4:2f:e5:99:ee:24:8b:03:
                    ec:8d:f2:8b:ea:c3:4a:fb:43:11:12:0b:7e:b5:47:
                    92:6c:dc:e6:04:89:eb:f5:33:04:eb:10:01:2a:71:
                    e5:f9:83:13:3c:ff:25:09:2f:68:76:46:ff:ba:4f:
                    be:dc:ad:71:2a:58:aa:fb:0e:d2:79:3d:e4:9b:65:
                    3b:cc:29:2a:9f:fc:72:59:a2:eb:ae:92:ef:f6:35:
                    13:80:c6:02:ec:e4:5f:cc:9d:76:cd:ef:63:92:c1:
                    af:79:40:84:79:87:7f:e3:52:a8:e8:9d:7b:07:69:
                    8f:15
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 Subject Key Identifier:
                62:FC:43:CD:A0:3E:A4:CB:67:12:D2:5B:D9:55:AC:7B:CC:B6:8A:5F
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:45:66:52:43:E1:7E:58:11:BF:D6:4E:9E:23:55:08:3B:3A:22:6A:A8

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicCorThiParMarRoo_2010-10-05.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt

    Signature Algorithm: sha256WithRSAEncryption
         d4:84:88:f5:14:94:18:02:ca:2a:3c:fb:2a:92:1c:0c:d7:a0:
         d1:f1:e8:52:66:a8:ee:a2:b5:75:7a:90:00:aa:2d:a4:76:5a:
         ea:79:b7:b9:37:6a:51:7b:10:64:f6:e1:64:f2:02:67:be:f7:
         a8:1b:78:bd:ba:ce:88:58:64:0c:d6:57:c8:19:a3:5f:05:d6:
         db:c6:d0:69:ce:48:4b:32:b7:eb:5d:d2:30:f5:c0:f5:b8:ba:
         78:07:a3:2b:fe:9b:db:34:56:84:ec:82:ca:ae:41:25:70:9c:
         6b:e9:fe:90:0f:d7:96:1f:e5:e7:94:1f:b2:2a:0c:8d:4b:ff:
```

```
          28:29:10:7b:f7:d7:7c:a5:d1:76:b9:05:c8:79:ed:0f:90:92:
          9c:c2:fe:df:6f:7e:6c:0f:7b:d4:c1:45:dd:34:51:96:39:0f:
          e5:5e:56:d8:18:05:96:f4:07:a6:42:b3:a0:77:fd:08:19:f2:
          71:56:cc:9f:86:23:a4:87:cb:a6:fd:58:7e:d4:69:67:15:91:
          7e:81:f2:7f:13:e5:0d:8b:8a:3c:87:84:eb:e3:ce:bd:43:e5:
          ad:2d:84:93:8e:6a:2b:5a:7c:44:fa:52:aa:81:c8:2d:1c:bb:
          e0:52:df:00:11:f8:9a:3d:c1:60:b0:e1:33:b5:a3:88:d1:65:
          19:0a:1a:e7:ac:7c:a4:c1:82:87:4e:38:b1:2f:0d:c5:14:87:
          6f:fd:8d:2e:bc:39:b6:e7:e6:c3:e0:e4:cd:27:84:ef:94:42:
          ef:29:8b:90:46:41:3b:81:1b:67:d8:f9:43:59:65:cb:0d:bc:
          fd:00:92:4f:f4:75:3b:a7:a9:24:fc:50:41:40:79:e0:2d:4f:
          0a:6a:27:76:6e:52:ed:96:69:7b:af:0f:f7:87:05:d0:45:c2:
          ad:53:14:81:1f:fb:30:04:aa:37:36:61:da:4a:69:1b:34:d8:
          68:ed:d6:02:cf:6c:94:0c:d3:cf:6c:22:79:ad:b1:f0:bc:03:
          a2:46:60:a9:c4:07:c2:21:82:f1:fd:f2:e8:79:32:60:bf:d8:
          ac:a5:22:14:4b:ca:c1:d8:4b:eb:7d:3f:57:35:b2:e6:4f:75:
          b4:b0:60:03:22:53:ae:91:79:1d:d6:9b:41:1f:15:86:54:70:
          b2:de:0d:35:0f:7c:b0:34:72:ba:97:60:3b:f0:79:eb:a2:b2:
          1c:5d:a2:16:b8:87:c5:e9:1b:f6:b5:97:25:6f:38:9f:e3:91:
          fa:8a:79:98:c3:69:0e:b7:a3:1c:20:05:97:f8:ca:14:ae:00:
          d7:c4:f3:c0:14:10:75:6b:34:a0:1b:b5:99:60:f3:5c:b0:c5:
          57:4e:36:d2:32:84:bf:9e
-----BEGIN CERTIFICATE-----
MIIF6DCCA9CgAwIBAgIKYQrRiAAAAAAAAzANBgkqhkiG9w0BAQsFADCBkTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE7MDkGA1UEAxMyTWljcm9z
b2Z0IENvcnBvcmF0aW9uIFRoaXJkIFBhcnR5IE1hcmtldHBsYWNlIFJvb3QwHhcN
MTEwNjI0MjA0MTI5WhcNMjYwNjI0MjA1MTI5WjCBgDELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1p
Y3Jvc29mdCBDb3Jwb3JhdGlvbjEqMCgGA1UEAxMhTWljcm9zb2Z0IENvcnBvcmF0
aW9uIEtFSyBDQSAyMDExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
xOi1ir+tVyawJsPq5/tXekQCXQcN2krldCrmsA/sbevsf7njWmMyfBEXTw7jC6c4
FZOOxvXghLGamyzn9beR1gnh4sAEqKwwHN9I8wZQmmSnUX/IhU+PIIbO/i/hn/+C
wO3pzc70U2piOgtDueIl/f4F+dTEFKsR4iOJjXC3pB1N7K7lnPoWwtfBy9ToxC/l
me4kiwPsjfKL6sNK+0MREgt+tUeSbNzmBInr9TME6xABKnHl+YMTPP8lCS9odkb/
uk++3K1xKliq+w7SeT3km2U7zCkqn/xyWaLrrpLv9jUTgMYC7ORfzJ12ze9jksGv
eUCEeYd/41Ko6J17B2mPFQIDAQABo4IBTzCCAUswEAYJKwYBBAGCNxUBBAMCAQAw
HQYDVR0OBBYEFGL8Q82gPqTLZxLSW9lVrHvMtopfMBkGCSsGAQQBgjcUAgQMHgoA
UwB1AGIAQwBBMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQY
MBaAFEVmUkPhflgRv9ZOniNVCDs6ImqoMFwGA1UdHwRVMFMwUaBPoE2GS2h0dHA6
Ly9jcmwubWljcm9zb2Z0LmNvbS9wa2kvY3JsL3Byb2R1Y3RzL01pY0NvclRoaVBh
ck1hclJvb18yMDEwLTEwLTA1LmNybDBgBggrBgEFBQcBAQRUMFIwUAYIKwYBBQUH
MAKGRGh0dHA6Ly93d3cubWljcm9zb2Z0LmNvbS9wa2kvY2VydHMvTWljQ29yVGhp
UGFyTWFyUm9vXzIwMTAtMTAtMDUuY3J0MA0GCSqGSIb3DQEBCwUAA4ICAQDUhIj1
FJQYAsoqPPsqkhwM16DR8ehSZqjuorV1epAAqi2kdlrqebe5N2pRexBk9uFk8gJn
vveoG3i9us6IWGQM1lfIGaNfBdbbxtBpzkhLMrfrXdIw9cD1uLp4B6Mr/pvbNFaE
7ILKrkElcJxr6f6QD9eWH+XnlB+yKgyNS/8oKRB799d8pdF2uQXIee0PkJKcwv7f
b35sD3vUwUXdNFGWOQ/lXlbYGAWW9AemQrOgd/0IGfJxVsyfhiOkh8um/Vh+1Gln
FZF+gfJ/E+UNi4o8h4Tr4869Q+WtLYSTjmorWnxE+lKqgcgtHLvgUt8AEfiaPcFg
sOEztaOI0WUZChrnrHykwYKHTjixLw3FFIdv/Y0uvDm25+bD4OTNJ4TvlELvKYuQ
RkE7gRtn2PlDWWXLDbz9AJJP9HU7p6kk/FBBQHngLU8Kaid2blLtlml7rw/3hwXQ
RcKtUxSBH/swBKo3NmHaSmkbNNho7dYCz2yUDNPPbCJ5rbHwvAOiRmCpxAfCIYLx
/fLoeTJgv9ispSIUS8rB2EvrfT9XNbLmT3W0sGADIlOukXkd1ptBHxWGVHCy3g01
D3ywNHK6l2A78HnrorIcXaIWuIfF6Rv2tZclbzif45H6inmYw2kOt6McIAWX+MoU
rgDXxPPAFBB1azSgG7WZYPNcsMVXTjbSMoS/ng==
-----END CERTIFICATE-----
```

7.4.3 db

```
Certificate:
```

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:07:76:56:00:00:00:00:00:08
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Root Certificate Authority 2010
        Validity
            Not Before: Oct 19 18:41:42 2011 GMT
            Not After : Oct 19 18:51:42 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Windows Production PCA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:dd:0c:bb:a2:e4:2e:09:e3:e7:c5:f7:96:69:bc:
                    00:21:bd:69:33:33:ef:ad:04:cb:54:80:ee:06:83:
                    bb:c5:20:84:d9:f7:d2:8b:f3:38:b0:ab:a4:ad:2d:
                    7c:62:79:05:ff:e3:4a:3f:04:35:20:70:e3:c4:e7:
                    6b:e0:9c:c0:36:75:e9:8a:31:dd:8d:70:e5:dc:37:
                    b5:74:46:96:28:5b:87:60:23:2c:bf:dc:47:a5:67:
                    f7:51:27:9e:72:eb:07:a6:c9:b9:1e:3b:53:35:7c:
                    e5:d3:ec:27:b9:87:1c:fe:b9:c9:23:09:6f:a8:46:
                    91:c1:6e:96:3c:41:d3:cb:a3:3f:5d:02:6a:4d:ec:
                    69:1f:25:28:5c:36:ff:fd:43:15:0a:94:e0:19:b4:
                    cf:df:c2:12:e2:c2:5b:27:ee:27:78:30:8b:5b:2a:
                    09:6b:22:89:53:60:16:2c:c0:68:1d:53:ba:ec:49:
                    f3:9d:61:8c:85:68:09:73:44:5d:7d:a2:54:2b:dd:
                    79:f7:15:cf:35:5d:6c:1c:2b:5c:ce:bc:9c:23:8b:
                    6f:6e:b5:26:d9:36:13:c3:4f:d6:27:ae:b9:32:3b:
                    41:92:2c:e1:c7:cd:77:e8:aa:54:4e:f7:5c:0b:04:
                    87:65:b4:43:18:a8:b2:e0:6d:19:77:ec:5a:24:fa:
                    48:03
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 Subject Key Identifier:
                A9:29:02:39:8E:16:C4:97:78:CD:90:F9:9E:4F:9A:E1:7C:55:AF:53
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:D5:F6:56:CB:8F:E8:A2:5C:62:68:D1:3D:94:90:5B:D7:CE:9A:18:C4

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt

    Signature Algorithm: sha256WithRSAEncryption
```

```
          14:fc:7c:71:51:a5:79:c2:6e:b2:ef:39:3e:bc:3c:52:0f:6e:
          2b:3f:10:13:73:fe:a8:68:d0:48:a6:34:4d:8a:96:05:26:ee:
          31:46:90:61:79:d6:ff:38:2e:45:6b:f4:c0:e5:28:b8:da:1d:
          8f:8a:db:09:d7:1a:c7:4c:0a:36:66:6a:8c:ec:1b:d7:04:90:
          a8:18:17:a4:9b:b9:e2:40:32:36:76:c4:c1:5a:c6:bf:e4:04:
          c0:ea:16:d3:ac:c3:68:ef:62:ac:dd:54:6c:50:30:58:a6:eb:
          7c:fe:94:a7:4e:8e:f4:ec:7c:86:73:57:c2:52:21:73:34:5a:
          f3:a3:8a:56:c8:04:da:07:09:ed:f8:8b:e3:ce:f4:7e:8e:ae:
          f0:f6:0b:8a:08:fb:3f:c9:1d:72:7f:53:b8:eb:be:63:e0:e3:
          3d:31:65:b0:81:e5:f2:ac:cd:16:a4:9f:3d:a8:b1:9b:c2:42:
          d0:90:84:5f:54:1d:ff:89:ea:ba:1d:47:90:6f:b0:73:4e:41:
          9f:40:9f:5f:e5:a1:2a:b2:11:91:73:8a:21:28:f0:ce:de:73:
          39:5f:3e:ab:5c:60:ec:df:03:10:a8:d3:09:e9:f4:f6:96:85:
          b6:7f:51:88:66:47:19:8d:a2:b0:12:3d:81:2a:68:05:77:bb:
          91:4c:62:7b:b6:c1:07:c7:ba:7a:87:34:03:0e:4b:62:7a:99:
          e9:ca:fc:ce:4a:37:c9:2d:a4:57:7c:1c:fe:3d:dc:b8:0f:5a:
          fa:d6:c4:b3:02:85:02:3a:ea:b3:d9:6e:e4:69:21:37:de:81:
          d1:f6:75:19:05:67:d3:93:57:5e:29:1b:39:c8:ee:2d:e1:cd:
          e4:45:73:5b:d0:d2:ce:7a:ab:16:19:82:46:58:d0:5e:9d:81:
          b3:67:af:6c:35:f2:bc:e5:3f:24:e2:35:a2:0a:75:06:f6:18:
          56:99:d4:78:2c:d1:05:1b:eb:d0:88:01:9d:aa:10:f1:05:df:
          ba:7e:2c:63:b7:06:9b:23:21:c4:f9:78:6c:e2:58:17:06:36:
          2b:91:12:03:cc:a4:d9:f2:2d:ba:f9:94:9d:40:ed:18:45:f1:
          ce:8a:5c:6b:3e:ab:03:d3:70:18:2a:0a:6a:e0:5f:47:d1:d5:
          63:0a:32:f2:af:d7:36:1f:2a:70:5a:e5:42:59:08:71:4b:57:
          ba:7e:83:81:f0:21:3c:f4:1c:c1:c5:b9:90:93:0e:88:45:93:
          86:e9:b1:20:99:be:98:cb:c5:95:a4:5d:62:d6:a0:63:08:20:
          bd:75:10:77:7d:3d:f3:45:b9:9f:97:9f:cb:57:80:6f:33:a9:
          04:cf:77:a4:62:1c:59:7e
-----BEGIN CERTIFICATE-----
MIIF1zCCA7+gAwIBAgIKYQd2VgAAAAAACDANBgkqhkiG9w0BAQsFADCBiDELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjEyMDAGA1UEAxMpTWljcm9z
b2Z0IFJvb3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IDIwMTAwHhcNMTExMDE5MTg0
MTQyWhcNMjYxMDE5MTg1MTQyWjCBhDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldh
c2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBD
b3Jwb3JhdGlvbjEuMCwGA1UEAxMlTWljcm9zb2Z0IFdpbmRvd3MgUHJvZHVjdGlv
biBQQ0EgMjAxMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN0Mu6Lk
Lgnj58X3lmm8ACG9aTMz760Ey1SA7gaDu8UghNn30ovzOLCrpK0tfGJ5Bf/jSj8E
NSBw48Tna+CcwDZ16Yox3Y1w5dw3tXRGlihbh2AjLL/cR6Vn91EnnnLrB6bJuR47
UzV85dPsJ7mHHP65ySMJb6hGkcFuljxB08ujP10Cak3saR8lKFw2//1DFQqU4Bm0
z9/CEuLCWyfuJ3gwi1sqCWsiiVNgFizAaB1TuuxJ851hjIVoCXNEXX2iVCvdefcV
zzVdbBwrXM68nCOLb261Jtk2E8NP1ieuuTI7QZIs4cfNd+iqVE73XAsEh2W0Qxio
suBtGXfsWiT6SAMCAwEAAaOCAUMwggE/MBAGCSsGAQQBgjcVAQQDAgEAMB0GA1Ud
DgQWBBSpKQI5jhbEl3jNkPmeT5rhfFWvUzAZBgkrBgEEAYI3FAIEDB4KAFMAdQBi
AEMAQTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBTV
9lbLj+iiXGJo0T2UkFvXzpoYxDBWBgNVHR8ETzBNMEugSaBHhkVodHRwOi8vY3Js
Lm1pY3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNSb29DZXJBdXRfMjAx
MC0wNi0yMy5jcmwwWgYIKwYBBQUHAQEETjBMMEoGCCsGAQUFBzAChj5odHRwOi8v
d3d3Lm1pY3Jvc29mdC5jb20vcGtpL2NlcnRzL01pY1Jvb0NlckF1dF8yMDEwLTA2
LTIzLmNydDANBgkqhkiG9w0BAQsFAAOCAgEAFPx8cVGlecJusu85Prw8Ug9uKz8Q
E3P+qGjQSKY0TYqWBSbuMUaQYXnW/zguRWv0wOUouNodj4rbCdcax0wKNmZqjOwb
1wSQqBgXpJu54kAyNnbEwVrGv+QEwOoW06zDaO9irN1UbFAwWKbrfP6Up06O9Ox8
hnNXwlIhczRa86OKVsgE2gcJ7fiL4870fo6u8PYLigj7P8kdcn9TuOu+Y+DjPTFl
sIHl8qzNFqSfPaixm8JC0JCEX1Qd/4nquh1HkG+wc05Bn0CfX+WhKrIRkXOKISjw
zt5zOV8+q1xg7N8DEKjTCen09paFtn9RiGZHGY2isBI9gSpoBXe7kUxie7bBB8e6
eoc0Aw5LYnqZ6cr8zko3yS2kV3wc/j3cuA9a+tbEswKFAjrqs9lu5GkhN96B0fZ1
GQVn05NXXikbOcjuLeHN5EVzW9DSznqrFhmCRljQXp2Bs2evbDXyvOU/JOI1ogp1
BvYYVpnUeCzRBRvr0IgBnaoQ8QXfun4sY7cGmyMhxPl4bOJYFwY2K5ESA8yk2fIt
uvmUnUDtGEXxzopcaz6rA9NwGCoKauBfR9HVYwoy8q/XNh8qcFrlQlkIcUtXun6D
gfAhPPQcwcW5kJMOiEWThumxIJm+mMvFlaRdYtagYwggvXUQd30980W5n5efy1eA
bzOpBM93pGIcWX4=
```

```
-----END CERTIFICATE-----

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:08:d3:c4:00:00:00:00:00:04
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation Third Party Marketplace Root
        Validity
            Not Before: Jun 27 21:22:45 2011 GMT
            Not After : Jun 27 21:32:45 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation UEFI CA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a5:08:6c:4c:c7:45:09:6a:4b:0c:a4:c0:87:7f:
                    06:75:0c:43:01:54:64:e0:16:7f:07:ed:92:7d:0b:
                    b2:73:bf:0c:0a:c6:4a:45:61:a0:c5:16:2d:96:d3:
                    f5:2b:a0:fb:4d:49:9b:41:80:90:3c:b9:54:fd:e6:
                    bc:d1:9d:c4:a4:18:8a:7f:41:8a:5c:59:83:68:32:
                    bb:8c:47:c9:ee:71:bc:21:4f:9a:8a:7c:ff:44:3f:
                    8d:8f:32:b2:26:48:ae:75:b5:ee:c9:4c:1e:4a:19:
                    7e:e4:82:9a:1d:78:77:4d:0c:b0:bd:f6:0f:d3:16:
                    d3:bc:fa:2b:a5:51:38:5d:f5:fb:ba:db:78:02:db:
                    ff:ec:0a:1b:96:d5:83:b8:19:13:e9:b6:c0:7b:40:
                    7b:e1:1f:28:27:c9:fa:ef:56:5e:1c:e6:7e:94:7e:
                    c0:f0:44:b2:79:39:e5:da:b2:62:8b:4d:bf:38:70:
                    e2:68:24:14:c9:33:a4:08:37:d5:58:69:5e:d3:7c:
                    ed:c1:04:53:08:e7:4e:b0:2a:87:63:08:61:6f:63:
                    15:59:ea:b2:2b:79:d7:0c:61:67:8a:5b:fd:5e:ad:
                    87:7f:ba:86:67:4f:71:58:12:22:04:22:22:ce:8b:
                    ef:54:71:00:ce:50:35:58:76:95:08:ee:6a:b1:a2:
                    01:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                .....
            1.3.6.1.4.1.311.21.2:
                ....k..wSJ.%7.N.&{. p.
            X509v3 Subject Key Identifier:
                13:AD:BF:43:09:BD:82:70:9C:8C:D5:4F:31:6E:D5:22:98:8A:1B:D4
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:45:66:52:43:E1:7E:58:11:BF:D6:4E:9E:23:55:08:3B:3A:22:6A:A8

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicCorThiParMarRoo_2010-10-05.crl
```

```
            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt

    Signature Algorithm: sha256WithRSAEncryption
         35:08:42:ff:30:cc:ce:f7:76:0c:ad:10:68:58:35:29:46:32:
         76:27:7c:ef:12:41:27:42:1b:4a:aa:6d:81:38:48:59:13:55:
         f3:e9:58:34:a6:16:0b:82:aa:5d:ad:82:da:80:83:41:06:8f:
         b4:1d:f2:03:b9:f3:1a:5d:1b:f1:50:90:f9:b3:55:84:42:28:
         1c:20:bd:b2:ae:51:14:c5:c0:ac:97:95:21:1c:90:db:0f:fc:
         77:9e:95:73:91:88:ca:bd:bd:52:b9:05:50:0d:df:57:9e:a0:
         61:ed:0d:e5:6d:25:d9:40:0f:17:40:c8:ce:a3:4a:c2:4d:af:
         9a:12:1d:08:54:8f:bd:c7:bc:b9:2b:3d:49:2b:1f:32:fc:6a:
         21:69:4f:9b:c8:7e:42:34:fc:36:06:17:8b:8f:20:40:c0:b3:
         9a:25:75:27:cd:c9:03:a3:f6:5d:d1:e7:36:54:7a:b9:50:b5:
         d3:12:d1:07:bf:bb:74:df:dc:1e:8f:80:d5:ed:18:f4:2f:14:
         16:6b:2f:de:66:8c:b0:23:e5:c7:84:d8:ed:ea:c1:33:82:ad:
         56:4b:18:2d:f1:68:95:07:cd:cf:f0:72:f0:ae:bb:dd:86:85:
         98:2c:21:4c:33:2b:f0:0f:4a:f0:68:87:b5:92:55:32:75:a1:
         6a:82:6a:3c:a3:25:11:a4:ed:ad:d7:04:ae:cb:d8:40:59:a0:
         84:d1:95:4c:62:91:22:1a:74:1d:8c:3d:47:0e:44:a6:e4:b0:
         9b:34:35:b1:fa:b6:53:a8:2c:81:ec:a4:05:71:c8:9d:b8:ba:
         e8:1b:44:66:e4:47:54:0e:8e:56:7f:b3:9f:16:98:b2:86:d0:
         68:3e:90:23:b5:2f:5e:8f:50:85:8d:c6:8d:82:5f:41:a1:f4:
         2e:0d:e0:99:d2:6c:75:e4:b6:69:b5:21:86:fa:07:d1:f6:e2:
         4d:d1:da:ad:2c:77:53:1e:25:32:37:c7:6c:52:72:95:86:b0:
         f1:35:61:6a:19:f5:b2:3b:81:50:56:a6:32:2d:fe:a2:89:f9:
         42:86:27:18:55:a1:82:ca:5a:9b:f8:30:98:54:14:a6:47:96:
         25:2f:c8:26:e4:41:94:1a:5c:02:3f:e5:96:e3:85:5b:3c:3e:
         3f:bb:47:16:72:55:e2:25:22:b1:d9:7b:e7:03:06:2a:a3:f7:
         1e:90:46:c3:00:0d:d6:19:89:e3:0e:35:27:62:03:71:15:a6:
         ef:d0:27:a0:a0:59:37:60:f8:38:94:b8:e0:78:70:f8:ba:4c:
         86:87:94:f6:e0:ae:02:45:ee:65:c2:b6:a3:7e:69:16:75:07:
         92:9b:f5:a6:bc:59:83:58
-----BEGIN CERTIFICATE-----
MIIGEDCCA/igAwIBAgIKYQjTxAAAAAAABDANBgkqhkiG9w0BAQsFADCBkTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE7MDkGA1UEAxMyTWljcm9z
b2Z0IENvcnBvcmF0aW9uIFRoaXJkIFBhcnR5IE1hcmtldHBsYWNlIFJvb3QwHhcN
MTEwNjI3MjEyMjQ1WhcNMjYwNjI3MjEzMjQ1WjCBgTELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1p
Y3Jvc29mdCBDb3Jwb3JhdGlvbjErMCkGA1UEAxMiTWljcm9zb2Z0IENvcnBvcmF0
aW9uIFVFRkkgQ0EgMjAxMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AKUIbEzHRQlqSwykwId/BnUMQwFUZOAWfwftkn0LsnO/DArGSkVhoMUWLZbT9Sug
+01Jm0GAkDy5VP3mvNGdxKQYin9BilxZg2gyu4xHye5xvCFPmop8/0Q/jY8ysiZI
rnW17slMHkoZfuSCmh14d00MsL32D9MW07z6K6VROF31+7rbeALb/+wKG5bVg7gZ
E+m2wHtAe+EfKCfJ+u9WXhzmfpR+wPBEsnk55dqyYotNvzhw4mgkFMkzpAg31Vhp
XtN87cEEUwjnTrAqh2MIYW9jFVnqsit51wxhZ4pb/V6th3+6hmdPcVgSIgQiIs6L
71RxAM5QNVh2lQjuarGiAdUCAwEAAaOCAXYwggFyMBIGCSsGAQQBgjcVAQQFAgMB
AAEwIwYJKwYBBAGCNxUCBBYEFPjBa7d/d1NK8yU3HU6hJnsPIHCAMB0GA1UdDgQW
BBQTrb9DCb2CcJyM1U8xbtUimIob1DAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMA
QTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRFZlJD
4X5YEb/WTp4jVQg7OiJqqDBcBgNVHR8EVTBTMFGgT6BNhktodHRwOi8vY3JsLm1p
Y3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNDb3JUaGlQYXJNYXJSb29f
MjAxMC0xMC0wNS5jcmwwYAYIKwYBBQUHAQEEVDBSMFAGCCsGAQUFBzAChkRodHRw
Oi8vd3d3Lm1pY3Jvc29mdC5jb20vcGtpL2NlcnRzL01pY0NvclRoaVBhck1hclJv
b18yMDEwLTEwLTA1LmNydDANBgkqhkiG9w0BAQsFAAOCAgEANQhC/zDMzvd2DK0Q
aFg1KUYydid87xJBJ0IbSqptgThIWRNV8+lYNKYWC4KqXa2C2oCDQQaPtB3yA7nz
Gl0b8VCQ+bNVhEIoHCC9sq5RFMXArJeVIRyQ2w/8d56Vc5GIyr29UrkFUA3fV56g
Ye0N5W0l2UAPF0DIzqNKwk2vmhIdCFSPvce8uSs9SSsfMvxqIWlPm8h+QjT8NgYX
i48gQMCzmiV1J83JA6P2XdHnNlR6uVC10xLRB7+7dN/cHo+A1e0Y9C8UFmsv3maM
sCPlx4TY7erBM4KtVksYLfFolQfNz/By8K673YaFmCwhTDMr8A9K8GiHtZJVMnWh
```

```
aoJqPKMlEaTtrdcErsvYQFmghNGVTGKRIhp0HYw9Rw5EpuSwmzQ1sfq2U6gsgeyk
BXHInbi66BtEZuRHVA6OVn+znxaYsobQaD6QI7UvXo9QhY3GjYJfQaH0Lg3gmdJs
deS2abUhhvoH0fbiTdHarSx3Ux4lMjfHbFJylYaw8TVhahn1sjuBUFamMi3+oon5
QoYnGFWhgspam/gwmFQUpkeWJS/IJuRBlBpcAj/lluOFWzw+P7tHFnJV4iUisdl7
5wMGKqP3HpBGwwAN1hmJ4w41J2IDcRWm79AnoKBZN2D4OJS44Hhw+LpMhoeU9uCu
AkXuZcK2o35pFnUHkpv1prxZg1g=
-----END CERTIFICATE-----

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            09:45:63:7a:d8:c2:20:df:61:ea:52:44
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=JP, ST=Kanagawa, L=Yokohama, O=Lenovo Ltd., CN=Lenovo Ltd.
Root CA 2012
        Validity
            Not Before: Jun 29 10:47:31 2012 GMT
            Not After : Jun 24 10:47:31 2032 GMT
        Subject: C=JP, ST=Kanagawa, L=Yokohama, O=Lenovo Ltd., CN=ThinkPad
Product CA 2012
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d7:56:37:db:a8:c3:70:67:8e:5f:ee:64:67:7a:
                    16:04:71:4f:4c:c9:eb:89:2e:e9:24:3e:eb:c7:e4:
                    a4:74:57:ed:d2:5f:f3:a5:9f:92:8a:e3:9f:59:e3:
                    98:ae:66:b9:2d:01:fc:75:47:bb:b8:71:b0:b1:e6:
                    64:7f:1e:74:16:d6:0a:4c:1d:29:94:e1:61:41:37:
                    37:5e:17:d0:de:37:6a:4b:e4:30:79:62:33:cd:a0:
                    da:3e:b6:62:a0:69:43:27:1a:be:51:a1:73:61:13:
                    c7:b5:93:0b:7a:b9:25:1f:b8:0c:e3:fe:14:5b:05:
                    ff:84:58:a2:3b:c0:9e:e8:8a:26:49:b9:74:00:0f:
                    5f:1e:12:a3:6a:8b:73:de:59:35:a4:34:b3:62:70:
                    16:cd:73:87:7c:09:b0:77:87:91:e7:99:f7:e5:bc:
                    10:52:da:d7:57:27:05:54:7e:94:62:cc:33:52:1b:
                    5a:7b:37:10:14:47:44:2e:13:8a:d6:62:a5:22:e9:
                    32:54:66:02:6d:8d:5f:f3:82:cf:48:b0:21:5f:ca:
                    ca:88:4a:86:5a:f1:f6:2d:0b:c5:24:28:2a:49:90:
                    03:a0:c8:dc:39:8f:4d:41:d3:8f:cb:2b:b9:c5:cf:
                    8c:6e:f9:34:2c:13:1f:dc:c6:c1:db:f8:f8:b5:63:
                    ca:ff
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                83:8B:1F:54:C1:55:04:63:F4:5F:98:70:06:40:F1:10:69:26:59:49
            X509v3 Authority Key Identifier:

keyid:EF:81:91:F6:CD:17:16:41:0A:68:50:6E:54:7E:70:CD:92:05:61:6B

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         ab:e4:4e:ce:fa:c2:39:f5:e1:eb:3c:93:35:a8:a8:9c:95:36:
         18:c4:8e:98:be:47:fd:28:bf:42:28:8b:22:49:9b:38:23:43:
         a3:69:05:58:8b:fc:47:f7:81:c5:87:3c:25:f6:bb:db:08:24:
         b6:9f:cd:bf:6d:18:d7:22:14:40:01:18:73:5f:1f:79:44:cc:
         74:fd:c8:f9:a9:4b:5b:3b:a3:80:c4:28:e6:42:15:26:eb:a0:
         73:ec:cb:9a:83:c1:28:00:e9:27:ba:d0:e6:26:83:8a:41:2f:
         09:2d:f4:65:aa:8b:24:bf:d8:c0:8e:12:b8:01:77:61:f8:9b:
         61:30:00:78:90:5b:23:6c:26:b3:14:b3:24:af:4f:a6:a2:ae:
```

```
          43:54:8b:3c:d6:0c:5b:82:50:b2:73:27:70:27:4c:6b:40:58:
          d6:e7:24:6a:31:9e:53:0d:e8:58:50:42:60:df:b7:89:da:c9:
          31:00:e0:f3:0f:88:c6:d1:9c:f3:67:f1:c8:4b:36:17:da:04:
          c6:f8:c4:05:89:b3:8f:bf:0c:27:55:df:fc:da:d4:ab:34:9a:
          0e:2d:63:1a:e2:50:ad:c5:5c:51:ee:be:ac:d7:4a:7d:4d:dc:
          51:e1:25:4d:8e:cc:46:5c:71:d2:46:1b:f9:e2:d6:e0:50:64:
          8a:8e:40:c0
-----BEGIN CERTIFICATE-----
MIIDrjCCApagAwIBAgIMCUVjetjCIN9h6lJEMA0GCSqGSIb3DQEBCwUAMGwxCzAJ
BgNVBAYTAkpQMREwDwYDVQQIDAhLYW5hZ2F3YTERMA8GA1UEBwwIWW9rb2hhbWEx
FDASBgNVBAoMC0xlbm92byBMdGQuMSEwHwYDVQQDDBhMZW5vdm8gTHRkLiBSb290
IENBIDIwMTIwHhcNMTIwNjI5MTA0NzMxWhcNMzIwNjI0MTA0NzMxWjBsMQswCQYD
VQQGEwJKUDERMA8GA1UECAwIS2FuYWdhd2ExETAPBgNVBAcMCFlva29oYW1hMRQw
EgYDVQQKDAtMZW5vdm8gTHRkLjEhMB8GA1UEAwwYVGhpbmtQYWQgUHJvZHVjdCBD
QSAyMDEyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA11Y326jDcGeO
X+5kZ3oWBHFPTMnriS7pJD7rx+SkdFft0l/zpZ+SiuOfWeOYrma5LQH8dUe7uHGw
seZkfx50FtYKTB0plOFhQTc3XhfQ3jdqS+QweWIzzaDaPrZioGlDJxq+UaFzYRPH
tZMLerklH7gM4/4UWwX/hFiiO8Ce6IomSbl0AA9fHhKjaotz3lk1pDSzYnAWzXOH
fAmwd4eR55n35bwQUtrXVycFVH6UYswzUhtaezcQFEdELhOK1mKlIukyVGYCbY1f
84LPSLAhX8rKiEqGWvH2LQvFJCgqSZADoMjcOY9NQdOPyyu5xc+Mbvk0LBMf3MbB
2/j4tWPK/wIDAQABo1AwTjAdBgNVHQ4EFgQUg4sfVMFVBGP0X5hwBkDxEGkmWUkw
HwYDVR0jBBgwFoAU74GR9s0XFkEKaFBuVH5wzZIFYWswDAYDVR0TBAUwAwEB/zAN
BgkqhkiG9w0BAQsFAAOCAQEAq+ROzvrCOfXh6zyTNaionJU2GMSOmL5H/Si/QiiL
IkmbOCNDo2kFWIv8R/eBxYc8Jfa72wgktp/Nv20Y1yIUQAEYc18feUTMdP3I+alL
WzujgMQo5kIVJuugc+zLmoPBKADpJ7rQ5iaDikEvCS30ZaqLJL/YwI4SuAF3Yfib
YTAAeJBbI2wmsxSzJK9PpqKuQ1SLPNYMW4JQsnMncCdMa0BY1uckajGeUw3oWFBC
YN+3idrJMQDg8w+IxtGc82fxyEs2F9oExvjEBYmzj78MJ1Xf/NrUqzSaDi1jGuJQ
rcVcUe6+rNdKfU3cUeElTY7MRlxx0kYb+eLW4FBkio5AwA==
-----END CERTIFICATE-----
```

7.5 Zertifikate der Medion-Plattform

7.5.1 PK

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
             (Negative)78:bd:0b:37:19:a8:4b:5b:b0:cf:c2:0c:8d:7a:8c:59
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=MEDION Certificate
        Validity
            Not Before: Jul 20 08:41:12 2012 GMT
            Not After : Jul 20 08:41:11 2032 GMT
        Subject: CN=MEDION Certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ac:3c:6a:cb:12:04:37:74:3e:36:f0:2b:46:44:
                    8c:24:8b:f4:e3:ea:48:2f:3a:89:2b:24:e5:1f:7e:
                    f4:ea:f3:89:90:df:d1:63:0c:ff:6a:f9:f3:d3:96:
                    2b:e8:a1:c7:4a:d5:72:13:2d:d5:53:2a:6b:2a:70:
                    67:0b:aa:be:58:b2:17:e5:dd:6e:09:7b:20:77:4d:
                    b9:92:48:ff:46:18:5d:b5:26:9d:4f:f3:9b:0a:2a:
                    24:a4:23:18:e1:72:05:fc:b3:50:b5:36:91:38:68:
                    d9:1e:0c:90:4c:b3:ee:aa:19:78:ea:1a:ba:0a:d2:
                    b4:60:85:12:e9:1e:69:a1:3b:32:6e:47:b1:91:1f:
                    0b:e3:17:48:c2:e4:0c:47:81:cf:f9:41:2e:60:1c:
                    dc:75:b8:42:06:e7:7e:54:d8:56:5b:b2:ee:7b:8b:
                    76:b6:e0:74:d7:1c:5a:5a:0d:92:69:b8:c2:0a:93:
                    5a:a1:45:67:73:e4:05:33:63:cc:f7:cd:b5:8b:f7:
                    21:1d:7a:32:a1:7e:fd:4b:bd:17:6a:92:2e:6d:b9:
                    28:f0:7b:21:b8:42:b2:da:79:ef:08:b6:ce:2e:79:
                    80:c8:5d:0c:99:68:a0:f9:04:89:f5:7e:0d:0d:ca:
                    ba:c6:c3:50:7c:69:2a:41:da:7f:e4:ef:5b:7a:de:
                    d8:65
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            2.5.29.1:
                0E....0.#._...[.|t....0.1.0...U....MEDION
Certificate...B...W..O0=.r.s.
    Signature Algorithm: sha256WithRSAEncryption
         2e:29:3a:c0:5d:d6:b7:8b:1f:5a:0f:e7:5d:fe:be:85:a2:c3:
         9d:a7:dd:20:b4:f3:e1:30:9f:7a:15:21:21:68:a1:0f:67:0f:
         47:33:43:bf:cb:77:fc:c1:13:89:3c:da:65:10:cd:1d:80:79:
         64:20:05:11:c7:e5:a6:af:e9:d2:bc:02:cd:2d:e2:e5:9a:df:
         be:ae:68:a6:c8:60:77:e3:a7:52:73:45:65:3e:e1:8d:01:15:
         00:a9:3c:fc:3e:56:49:b5:bc:a5:54:df:0d:8d:80:6b:4b:7e:
         b9:cb:cd:96:65:f4:2b:76:0e:1f:96:84:a0:ed:e0:85:7a:86:
         8e:77:fe:50:ef:3f:dd:1b:0d:74:ff:cd:73:83:92:12:97:b3:
         74:ca:d2:eb:d3:8a:9d:9b:3a:e2:81:c8:d1:db:e1:77:e3:bd:
         8e:bb:6d:5d:68:97:7b:43:f9:34:ed:d3:87:e8:54:49:58:98:
         00:45:7f:9a:4b:6b:6c:65:81:c1:49:da:85:78:0c:8f:04:3d:
         ae:da:db:cb:46:e6:46:3b:f9:1d:7b:c1:a2:70:bd:0d:39:76:
         b7:24:44:20:15:ec:2a:64:70:70:70:22:31:59:35:6d:b2:52:
         87:40:2f:f2:49:d7:1c:21:42:de:0b:d5:35:e3:55:f1:ba:7e:
         85:55:c5:05
```

```
-----BEGIN CERTIFICATE-----
MIIDFjCCAf6gAwIBAgIQh0L0yOZXtKRPMD3zcoVzpzANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJNRURJT04gQ2VydGlmaWNhdGUwHhcNMTIwNzIwMDg0MTEyWhcN
MzIwNzIwMDg0MTExWjAdMRswGQYDVQQDExJNRURJT04gQ2VydGlmaWNhdGUwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCsPGrLEgQ3dD428CtGRIwki/Tj
6kgvOokrJOUffvTq84mQ39FjDP9q+fPTlivoocdK1XITLdVTKmsqcGcLqr5Yshfl
3W4JeyB3TbmSSP9GGF21Jp1P85sKKiSkIxjhcgX8s1C1NpE4aNkeDJBMs+6qGXjq
GroK0rRghRLpHmmhOzJuR7GRHwvjF0jC5AxHgc/5QS5gHNx1uEIG535U2FZbsu57
i3a24HTXHFpaDZJpuMIKk1qhRWdz5AUzY8z3zbWL9yEdejKhfv1LvRdqki5tuSjw
eyG4QrLaee8Its4ueYDIXQyZaKD5BIn1fg0NyrrGw1B8aSpB2n/k71t63thlAgMB
AAGjUjBQME4GA1UdAQRHMEWAEJXOMIMjhV/etMVbunx0B46hHzAdMRswGQYDVQQD
ExJNRURJT04gQ2VydGlmaWNhdGWCEIdC9MjmV7SkTzA983KFc6cwDQYJKoZIhvcN
AQELBQADggEBAC4pOsBd1reLH1oP513+voWiw52n3SC08+Ewn3oVISFooQ9nD0cz
Q7/Ld/zBE4k82mUQzR2AeWQgBRHH5aav6dK8As0t4uWa376uaKbIYHfjp1JzRWU+
4Y0BFQCpPPw+Vkm1vKVU3w2NgGtLfrnLzZZl9Ct2Dh+WhKDt4IV6ho53/lDvP90b
DXT/zXODkhKXs3TK0uvTip2bOuKByNHb4XfjvY67bV1ol3tD+TTt04foVElYmABF
f5pLa2xlgcFJ2oV4DI8EPa7a28tG5kY7+R17waJwvQ05drckRCAV7CpkcHBwIjFZ
NW2yUodAL/JJ1xwhQt4L1TXjVfG6foVVxQU=
-----END CERTIFICATE-----
```

7.5.2 KEK

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:0a:d1:88:00:00:00:00:00:03
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation Third Party Marketplace Root
        Validity
            Not Before: Jun 24 20:41:29 2011 GMT
            Not After : Jun 24 20:51:29 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation KEK CA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:e8:b5:8a:bf:ad:57:26:b0:26:c3:ea:e7:fb:
                    57:7a:44:02:5d:07:0d:da:4a:e5:74:2a:e6:b0:0f:
                    ec:6d:eb:ec:7f:b9:e3:5a:63:32:7c:11:17:4f:0e:
                    e3:0b:a7:38:15:93:8e:c6:f5:e0:84:b1:9a:9b:2c:
                    e7:f5:b7:91:d6:09:e1:e2:c0:04:a8:ac:30:1c:df:
                    48:f3:06:50:9a:64:a7:51:7f:c8:85:4f:8f:20:86:
                    ce:fe:2f:e1:9f:ff:82:c0:ed:e9:cd:ce:f4:53:6a:
                    62:3a:0b:43:b9:e2:25:fd:fe:05:f9:d4:c4:14:ab:
                    11:e2:23:89:8d:70:b7:a4:1d:4d:ec:ae:e5:9c:fa:
                    16:c2:d7:c1:cb:d4:e8:c4:2f:e5:99:ee:24:8b:03:
                    ec:8d:f2:8b:ea:c3:4a:fb:43:11:12:0b:7e:b5:47:
                    92:6c:dc:e6:04:89:eb:f5:33:04:eb:10:01:2a:71:
                    e5:f9:83:13:3c:ff:25:09:2f:68:76:46:ff:ba:4f:
                    be:dc:ad:71:2a:58:aa:fb:0e:d2:79:3d:e4:9b:65:
                    3b:cc:29:2a:9f:fc:72:59:a2:eb:ae:92:ef:f6:35:
                    13:80:c6:02:ec:e4:5f:cc:9d:76:cd:ef:63:92:c1:
                    af:79:40:84:79:87:7f:e3:52:a8:e8:9d:7b:07:69:
                    8f:15
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
```

```
                ...
            X509v3 Subject Key Identifier:
                62:FC:43:CD:A0:3E:A4:CB:67:12:D2:5B:D9:55:AC:7B:CC:B6:8A:5F
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:45:66:52:43:E1:7E:58:11:BF:D6:4E:9E:23:55:08:3B:3A:22:6A:A8

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicCorThiParMarRoo_2010-10-05.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt

    Signature Algorithm: sha256WithRSAEncryption
         d4:84:88:f5:14:94:18:02:ca:2a:3c:fb:2a:92:1c:0c:d7:a0:
         d1:f1:e8:52:66:a8:ee:a2:b5:75:7a:90:00:aa:2d:a4:76:5a:
         ea:79:b7:b9:37:6a:51:7b:10:64:f6:e1:64:f2:02:67:be:f7:
         a8:1b:78:bd:ba:ce:88:58:64:0c:d6:57:c8:19:a3:5f:05:d6:
         db:c6:d0:69:ce:48:4b:32:b7:eb:5d:d2:30:f5:c0:f5:b8:ba:
         78:07:a3:2b:fe:9b:db:34:56:84:ec:82:ca:ae:41:25:70:9c:
         6b:e9:fe:90:0f:d7:96:1f:e5:e7:94:1f:b2:2a:0c:8d:4b:ff:
         28:29:10:7b:f7:d7:7c:a5:d1:76:b9:05:c8:79:ed:0f:90:92:
         9c:c2:fe:df:6f:7e:6c:0f:7b:d4:c1:45:dd:34:51:96:39:0f:
         e5:5e:56:d8:18:05:96:f4:07:a6:42:b3:a0:77:fd:08:19:f2:
         71:56:cc:9f:86:23:a4:87:cb:a6:fd:58:7e:d4:69:67:15:91:
         7e:81:f2:7f:13:e5:0d:8b:8a:3c:87:84:eb:e3:ce:bd:43:e5:
         ad:2d:84:93:8e:6a:2b:5a:7c:44:fa:52:aa:81:c8:2d:1c:bb:
         e0:52:df:00:11:f8:9a:3d:c1:60:b0:e1:33:b5:a3:88:d1:65:
         19:0a:1a:e7:ac:7c:a4:c1:82:87:4e:38:b1:2f:0d:c5:14:87:
         6f:fd:8d:2e:bc:39:b6:e7:e6:c3:e0:e4:cd:27:84:ef:94:42:
         ef:29:8b:90:46:41:3b:81:1b:67:d8:f9:43:59:65:cb:0d:bc:
         fd:00:92:4f:f4:75:3b:a7:a9:24:fc:50:41:40:79:e0:2d:4f:
         0a:6a:27:76:6e:52:ed:96:69:7b:af:0f:f7:87:05:d0:45:c2:
         ad:53:14:81:1f:fb:30:04:aa:37:36:61:da:4a:69:1b:34:d8:
         68:ed:d6:02:cf:6c:94:0c:d3:cf:6c:22:79:ad:b1:f0:bc:03:
         a2:46:60:a9:c4:07:c2:21:82:f1:fd:f2:e8:79:32:60:bf:d8:
         ac:a5:22:14:4b:ca:c1:d8:4b:eb:7d:3f:57:35:b2:e6:4f:75:
         b4:b0:60:03:22:53:ae:91:79:1d:d6:9b:41:1f:15:86:54:70:
         b2:de:0d:35:0f:7c:b0:34:72:ba:97:60:3b:f0:79:eb:a2:b2:
         1c:5d:a2:16:b8:87:c5:e9:1b:f6:b5:97:25:6f:38:9f:e3:91:
         fa:8a:79:98:c3:69:0e:b7:a3:1c:20:05:97:f8:ca:14:ae:00:
         d7:c4:f3:c0:14:10:75:6b:34:a0:1b:b5:99:60:f3:5c:b0:c5:
         57:4e:36:d2:32:84:bf:9e
-----BEGIN CERTIFICATE-----
MIIF6DCCA9CgAwIBAgIKYQrRiAAAAAAAAzANBgkqhkiG9w0BAQsFADCBkTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE7MDkGA1UEAxMyTWljcm9z
b2Z0IENvcnBvcmF0aW9uIFRoaXJkIFBhcnR5IE1hcmtldHBsYWNlIFJvb3QwHhcN
MTEwNjI0MjA0MTI5WhcNMjYwNjI0MjA1MTI5WjCBgDELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1p
Y3Jvc29mdCBDb3Jwb3JhdGlvbjEqMCgGA1UEAxMhTWljcm9zb2Z0IENvcnBvcmF0
```

```
aW9uIEtFSyBDQSAyMDExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
xOi1ir+tVyawJsPq5/tXekQCXQcN2krldCrmsA/sbevsf7njWmMyfBEXTw7jC6c4
FZOOxvXghLGamyzn9beR1gnh4sAEqKwwHN9I8wZQmmSnUX/IhU+PIIbO/i/hn/+C
wO3pzc70U2piOgtDueIl/f4F+dTEFKsR4iOJjXC3pB1N7K7lnPoWwtfBy9ToxC/l
me4kiwPsjfKL6sNK+0MREgt+tUeSbNzmBInr9TME6xABKnHl+YMTPP8lCS9odkb/
uk++3K1xKliq+w7SeT3km2U7zCkqn/xyWaLrrpLv9jUTgMYC7ORfzJ12ze9jksGv
eUCEeYd/41Ko6J17B2mPFQIDAQABo4IBTzCCAUswEAYJKwYBBAGCNxUBBAMCAQAw
HQYDVR0OBBYEFGL8Q82gPqTLZxLSW9lVrHvMtopfMBkGCSsGAQQBgjcUAgQMHgoA
UwB1AGIAQwBBMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQY
MBaAFEVmUkPhflgRv9ZOniNVCDs6ImqoMFwGA1UdHwRVMFMwUaBPoE2GS2h0dHA6
Ly9jcmwubWljcm9zb2Z0LmNvbS9wa2kvY3JsL3Byb2R1Y3RzL01pY0NvclRoaVBh
ck1hclJvb18yMDEwLTEwLTA1LmNybDBgBggrBgEFBQcBAQRUMFIwUAYIKwYBBQUH
MAKGRGh0dHA6Ly93d3cubWljcm9zb2Z0LmNvbS9wa2kvY2VydHMvTWljQ29yVGhp
UGFyTWFyUm9vXzIwMTAtMTAtMDUuY3J0MA0GCSqGSIb3DQEBCwUAA4ICAQDUhIj1
FJQYAsoqPPsqkhwM16DR8ehSZqjuorV1epAAqi2kdlrqebe5N2pRexBk9uFk8gJn
vveoG3i9us6IWGQM1lfIGaNfBdbbxtBpzkhLMrfrXdIw9cD1uLp4B6Mr/pvbNFaE
7ILKrkElcJxr6f6QD9eWH+XnlB+yKgyNS/8oKRB799d8pdF2uQXIee0PkJKcwv7f
b35sD3vUwUXdNFGWOQ/lXlbYGAWW9AemQrOgd/0IGfJxVsyfhiOkh8um/Vh+1Gln
FZF+gfJ/E+UNi4o8h4Tr4869Q+WtLYSTjmorWnxE+lKqgcgtHLvgUt8AEfiaPcFg
sOEztaOI0WUZChrnrHykwYKHTjixLw3FFIdv/Y0uvDm25+bD4OTNJ4TvlELvKYuQ
RkE7gRtn2PlDWWXLDbz9AJJP9HU7p6kk/FBBQHngLU8Kaid2blLtlml7rw/3hwXQ
RcKtUxSBH/swBKo3NmHaSmkbNNho7dYCz2yUDNPPbCJ5rbHwvAOiRmCpxAfCIYLx
/fLoeTJgv9ispSIUS8rB2EvrfT9XNbLmT3W0sGADIlOukXkd1ptBHxWGVHCy3g01
D3ywNHK6l2A78HnrorIcXaIWuIfF6Rv2tZclbzif45H6inmYw2kOt6McIAWX+MoU
rgDXxPPAFBB1azSgG7WZYPNcsMVXTjbSMoS/ng==
-----END CERTIFICATE-----

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:31:75:a3:b6:04:a1:75:71:55:ea:6e:37:52:6d:40
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Hewlett-Packard Company, CN=Hewlett-Packard Printing
Device Infrastructure CA
        Validity
            Not Before: Aug  8 00:00:00 2012 GMT
            Not After : Aug  8 23:59:59 2032 GMT
        Subject: O=Hewlett-Packard Company, OU=Long Lived CodeSigning
Certificate, CN=Hewlett-Packard UEFI Secure Boot Key Exchange Key
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:a2:14:69:90:ea:34:c3:6a:f2:0e:60:5e:dd:
                    c7:d6:09:50:a2:24:09:dc:b5:43:b9:4c:d3:7e:89:
                    1b:8a:14:29:27:2c:59:3f:c9:d5:ff:3a:75:4a:d1:
                    00:f8:7f:29:0e:79:fc:6b:5b:be:c1:01:17:e7:d5:
                    de:99:07:a6:89:3c:98:e4:6a:bc:ae:c5:9d:de:fd:
                    aa:c4:2c:10:95:ae:bc:36:39:da:e7:7c:75:5c:bc:
                    20:84:5f:aa:0f:c6:c6:d5:17:c0:de:43:bf:ed:4b:
                    b3:25:73:88:95:06:aa:d7:f9:78:5f:6d:b9:c0:6d:
                    0d:d4:d6:10:e6:7f:1c:63:02:31:87:17:28:4f:41:
                    13:a9:0c:09:9d:c2:2b:bd:b6:35:f9:f8:92:15:03:
                    25:ca:be:81:1c:b1:cf:4f:f7:93:cf:48:02:1c:58:
                    25:d7:eb:e5:88:de:30:95:d4:7b:39:50:82:ab:80:
                    c8:48:f3:7e:e8:3b:cb:39:63:d5:cb:0a:1f:a3:5d:
                    06:04:8f:f3:27:04:52:95:d3:c7:ab:c6:72:98:be:
                    fb:cb:0b:8e:c9:ec:81:45:9a:c9:a9:7a:02:1b:53:
                    d4:b8:92:b7:e1:ab:98:bd:b2:9a:ca:60:f8:c4:63:
                    87:b3:93:b4:93:8c:b8:59:c0:06:8c:c7:d2:58:dd:
                    b3:e1
```

```
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 CRL Distribution Points:

                Full Name:

URI:http://onsitecrl.verisign.com/HewlettPackardCompanyDeSPrintingDeviceCSIDTemp
/LatestCRL.crl

            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.11.4.4.1.1
                  User Notice:
                    Explicit Text: Hewlett Packard Company, 2, Authority to bind
Hewlett-Packard Company does not correspond with use or possession of this
certificate. Issued to facilitate communication with HP.

            Authority Information Access:
                OCSP - URI:http://onsite-ocsp.verisign.com

            X509v3 Subject Key Identifier:
                D0:C8:09:A2:EA:7A:D7:94:89:46:DC:1D:71:68:CB:07:23:7C:01:0F
            X509v3 Authority Key Identifier:

keyid:B8:A1:0C:BD:06:5F:46:11:E9:80:DB:F7:99:BD:1D:F4:FD:EA:0D:C6

            X509v3 Extended Key Usage: critical
                Code Signing
    Signature Algorithm: sha256WithRSAEncryption
         2c:4f:ad:16:c7:fd:99:69:86:b3:b2:2c:dd:6d:90:0e:e4:39:
         7c:6e:2b:41:5a:76:2e:4e:34:0b:9f:d4:fd:fa:d6:05:f6:8d:
         db:3a:af:55:89:63:3f:b4:66:29:46:50:15:c8:d1:92:b2:b9:
         f6:d2:de:58:47:90:48:ee:c3:ff:8b:cb:ab:b9:10:21:31:1e:
         fd:0a:44:86:95:d8:49:05:8c:8d:95:f9:b7:ac:f4:60:03:25:
         0a:27:c6:3b:35:bc:08:ce:62:0d:4c:23:80:4c:28:6b:10:28:
         88:5d:4c:33:49:53:7f:ad:5a:ef:ea:6c:2e:ce:1f:e5:14:52:
         f3:2d:3b:11:32:3e:49:ad:c4:f7:00:be:ed:80:a7:2f:c2:a1:
         84:34:27:ac:3f:52:2c:9b:a9:99:79:ec:14:b7:7e:67:e9:b3:
         12:cc:94:cf:64:d3:b0:e6:06:40:80:e0:aa:90:14:aa:51:b6:
         0b:07:8d:b2:af:b2:48:53:fc:e2:49:f8:51:5c:1c:1b:66:85:
         1c:2c:57:41:cc:ac:6f:db:c0:66:03:68:cc:15:9d:29:b9:23:
         c1:c7:d8:21:17:0e:6f:c9:b6:b1:2d:9a:58:5b:f1:be:30:bb:
         a1:9a:9a:bb:3b:c3:49:47:a4:fc:f0:66:5c:4a:6a:f1:b8:ac:
         41:ec:84:c8
-----BEGIN CERTIFICATE-----
MIIFizCCBHOgAwIBAgIQBDF1o7YEoXVxVepuN1JtQDANBgkqhkiG9w0BAQsFADBr
MQswCQYDVQQGEwJVUzEgMB4GA1UEChMXSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkx
OjA4BgNVBAMTMUhld2xldHQtUGFja2FyZCBQcmludGluZyBEZXZpY2UgSW5mcmFz
dHJ1Y3R1cmUgQ0EwHhcNMTIwODA4MDAwMDAwWhcNMzIwODA4MjM1OTU5WjCBizEg
MB4GA1UEChMXSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkxKzApBgNVBAsUIkxvbmcg
TGl2ZWQgQ29kZVNpZ25pbmcgQ2VydGlmaWNhdGUxOjA4BgNVBAMUMUhld2xldHQt
UGFja2FyZCBVRUZJIFNlY3VyZSBCb290IEtleSBFeGNoYW5nZSBLZXkwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvohRpkOo0w2ryDmBe3cfWCVCiJAnc
tUO5TNN+iRuKFCknLFk/ydX/OnVK0QD4fykOefxrW77BARfn1d6ZB6aJPJjkaryu
xZ3e/arELBCVrrw2OdrnfHVcvCCEX6oPxsbVF8DeQ7/tS7Mlc4iVBqrX+XhfbbnA
bQ3U1hDmfxxjAjGHFyhPQROpDAmdwiu9tjX5+JIVAyXKvoEcsc9P95PPSAIcWCXX
6+WI3jCV1Hs5UIKrgMhI837oO8s5Y9XLCh+jXQYEj/MnBFKV08erxnKYvvvLC47J
7IFFmsmpegIbU9S4krfhq5i9sprKYPjEY4ezk7STjLhZwAaMx9JY3bPhAgMBAAGj
ggIIMIICBDAMBgNVHRMBAf8EAjAAMGsGA1UdHwRkMGIwYKBeoFyGWmh0dHA6Ly9v
```

```
bnNpdGVjcmwudmVyaXNpZ24uY29tL0hld2xldHRQYWNrYXJkQ29tcGFueURlU1By
aW50aW5nRGV2aWNlQ1NJRFRlbXAvTGF0ZXN0Q1JMLmNybDAOBgNVHQ8BAf8EBAMC
B4AwgeEGA1UdIASB2TCB1jCB0wYKKwYBBAELBAQBATCBxDCBwQYIKwYBBQUHAgIw
gbQagbFIZXdsZXR0IFBhY2thcmQgQ29tcGFueSwgMiwgQXV0aG9yaXR5IHRvIGJp
bmQgSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkgZG9lcyBub3QgY29ycmVzcG9uZCB3
aXRoIHVzZSBvciBwb3NzZXNzaW9uIG9mIHRoaXMgY2VydGlmaWNhdGUuIElzc3Vl
ZCB0byBmYWNpbGl0YXRlIGNvbW11bmljYXRpb24gd2l0aCBIUC4wOwYIKwYBBQUH
AQEELzAtMCsGCCsGAQUFBzABhh9odHRwOi8vb25zaXRlLW9jc3AudmVyaXNpZ24u
Y29tMB0GA1UdDgQWBBTQyAmi6nrXllIlG3B1xaMsHI3wBDzAfBgNVHSMEGDAWgBS4
oQy9Bl9GEemA2/eZvR30/eoNxjAWBgNVHSUBAf8EDDAKBggrBgEFBQcDAzANBgkq
hkiG9w0BAQsFAAOCAQEALE+tFsf9mWmGs7Is3W2QDuQ5fG4rQVp2Lk40C5/U/frW
BfaN2zqvVYljP7RmKUZQFcjRkrK59tLeWEeQSO7D/4vLq7kQITEe/QpEhpXYSQWM
jZX5t6z0YAMlCifGOzW8CM5iDUwjgEwoaxAoiF1MM0lTf61a7+psLs4f5RRS8y07
ETI+Sa3E9wC+7YCnL8KhhDQnrD9SLJupmXnsFLd+Z+mzEsyUz2TTsOYGQIDgqpAU
qlG2CweNsq+ySFP84kn4UVwcG2aFHCxXQcysb9vAZgNozBWdKbkjwcfYIRcOb8m2
sS2aWFvxvjC7oZqauzvDSUek/PBmXEpq8bisQeyEyA==
-----END CERTIFICATE-----
```

7.5.3 db

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:07:76:56:00:00:00:00:00:08
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Root Certificate Authority 2010
        Validity
            Not Before: Oct 19 18:41:42 2011 GMT
            Not After : Oct 19 18:51:42 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Windows Production PCA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:dd:0c:bb:a2:e4:2e:09:e3:e7:c5:f7:96:69:bc:
                    00:21:bd:69:33:33:ef:ad:04:cb:54:80:ee:06:83:
                    bb:c5:20:84:d9:f7:d2:8b:f3:38:b0:ab:a4:ad:2d:
                    7c:62:79:05:ff:e3:4a:3f:04:35:20:70:e3:c4:e7:
                    6b:e0:9c:c0:36:75:e9:8a:31:dd:8d:70:e5:dc:37:
                    b5:74:46:96:28:5b:87:60:23:2c:bf:dc:47:a5:67:
                    f7:51:27:9e:72:eb:07:a6:c9:b9:1e:3b:53:35:7c:
                    e5:d3:ec:27:b9:87:1c:fe:b9:c9:23:09:6f:a8:46:
                    91:c1:6e:96:3c:41:d3:cb:a3:3f:5d:02:6a:4d:ec:
                    69:1f:25:28:5c:36:ff:fd:43:15:0a:94:e0:19:b4:
                    cf:df:c2:12:e2:c2:5b:27:ee:27:78:30:8b:5b:2a:
                    09:6b:22:89:53:60:16:2c:c0:68:1d:53:ba:ec:49:
                    f3:9d:61:8c:85:68:09:73:44:5d:7d:a2:54:2b:dd:
                    79:f7:15:cf:35:5d:6c:1c:2b:5c:ce:bc:9c:23:8b:
                    6f:6e:b5:26:d9:36:13:c3:4f:d6:27:ae:b9:32:3b:
                    41:92:2c:e1:c7:cd:77:e8:aa:54:4e:f7:5c:0b:04:
                    87:65:b4:43:18:a8:b2:e0:6d:19:77:ec:5a:24:fa:
                    48:03
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 Subject Key Identifier:
```

```
                A9:29:02:39:8E:16:C4:97:78:CD:90:F9:9E:4F:9A:E1:7C:55:AF:53
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:D5:F6:56:CB:8F:E8:A2:5C:62:68:D1:3D:94:90:5B:D7:CE:9A:18:C4

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt

    Signature Algorithm: sha256WithRSAEncryption
         14:fc:7c:71:51:a5:79:c2:6e:b2:ef:39:3e:bc:3c:52:0f:6e:
         2b:3f:10:13:73:fe:a8:68:d0:48:a6:34:4d:8a:96:05:26:ee:
         31:46:90:61:79:d6:ff:38:2e:45:6b:f4:c0:e5:28:b8:da:1d:
         8f:8a:db:09:d7:1a:c7:4c:0a:36:66:6a:8c:ec:1b:d7:04:90:
         a8:18:17:a4:9b:b9:e2:40:32:36:76:c4:c1:5a:c6:bf:e4:04:
         c0:ea:16:d3:ac:c3:68:ef:62:ac:dd:54:6c:50:30:58:a6:eb:
         7c:fe:94:a7:4e:8e:f4:ec:7c:86:73:57:c2:52:21:73:34:5a:
         f3:a3:8a:56:c8:04:da:07:09:ed:f8:8b:e3:ce:f4:7e:8e:ae:
         f0:f6:0b:8a:08:fb:3f:c9:1d:72:7f:53:b8:eb:be:63:e0:e3:
         3d:31:65:b0:81:e5:f2:ac:cd:16:a4:9f:3d:a8:b1:9b:c2:42:
         d0:90:84:5f:54:1d:ff:89:ea:ba:1d:47:90:6f:b0:73:4e:41:
         9f:40:9f:5f:e5:a1:2a:b2:11:91:73:8a:21:28:f0:ce:de:73:
         39:5f:3e:ab:5c:60:ec:df:03:10:a8:d3:09:e9:f4:f6:96:85:
         b6:7f:51:88:66:47:19:8d:a2:b0:12:3d:81:2a:68:05:77:bb:
         91:4c:62:7b:b6:c1:07:c7:ba:7a:87:34:03:0e:4b:62:7a:99:
         e9:ca:fc:ce:4a:37:c9:2d:a4:57:7c:1c:fe:3d:dc:b8:0f:5a:
         fa:d6:c4:b3:02:85:02:3a:ea:b3:d9:6e:e4:69:21:37:de:81:
         d1:f6:75:19:05:67:d3:93:57:5e:29:1b:39:c8:ee:2d:e1:cd:
         e4:45:73:5b:d0:d2:ce:7a:ab:16:19:82:46:58:d0:5e:9d:81:
         b3:67:af:6c:35:f2:bc:e5:3f:24:e2:35:a2:0a:75:06:f6:18:
         56:99:d4:78:2c:d1:05:1b:eb:d0:88:01:9d:aa:10:f1:05:df:
         ba:7e:2c:63:b7:06:9b:23:21:c4:f9:78:6c:e2:58:17:06:36:
         2b:91:12:03:cc:a4:d9:f2:2d:ba:f9:94:9d:40:ed:18:45:f1:
         ce:8a:5c:6b:3e:ab:03:d3:70:18:2a:0a:6a:e0:5f:47:d1:d5:
         63:0a:32:f2:af:d7:36:1f:2a:70:5a:e5:42:59:08:71:4b:57:
         ba:7e:83:81:f0:21:3c:f4:1c:c1:c5:b9:90:93:0e:88:45:93:
         86:e9:b1:20:99:be:98:cb:c5:95:a4:5d:62:d6:a0:63:08:20:
         bd:75:10:77:7d:3d:f3:45:b9:9f:97:9f:cb:57:80:6f:33:a9:
         04:cf:77:a4:62:1c:59:7e
-----BEGIN CERTIFICATE-----
MIIF1zCCA7+gAwIBAgIKYQd2VgAAAAAACDANBgkqhkiG9w0BAQsFADCBiDELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjEyMDAGA1UEAxMpTWljcm9z
b2Z0IFJvb3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IDIwMTAwHhcNMTExMDE5MTg0
MTQyWhcNMjYxMDE5MTg1MTQyWjCBhDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldh
c2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBD
b3Jwb3JhdGlvbjEuMCwGA1UEAxMlTWljcm9zb2Z0IFdpbmRvd3MgUHJvZHVjdGlv
biBQQ0EgMjAxMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN0Mu6Lk
Lgnj58X3lmm8ACG9aTMz760Ey1SA7gaDu8UghNn30ovzOLCrpK0tfGJ5Bf/jSj8E
```

```
NSBw48Tna+CcwDZ16Yox3Y1w5dw3tXRGlihbh2AjLL/cR6Vn91EnnnLrB6bJuR47
UzV85dPsJ7mHHP65ySMJb6hGkcFuljxB08ujP10Cak3saR8lKFw2//1DFQqU4Bm0
z9/CEuLCWyfuJ3gwi1sqCWsiiVNgFizAaB1TuuxJ851hjIVoCXNEXX2iVCvdefcV
zzVdbBwrXM68nCOLb261Jtk2E8NP1ieuuTI7QZIs4cfNd+iqVE73XAsEh2W0Qxio
suBtGXfsWiT6SAMCAwEAAaOCAUMwggE/MBAGCSsGAQQBgjcVAQQDAgEAMB0GA1Ud
DgQWBBSpKQI5jhbEl3jNkPmeT5rhfFWvUzAZBgkrBgEEAYI3FAIEDB4KAFMAdQBi
AEMAQTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBTV
9lbLj+iiXGJo0T2UkFvXzpoYxDBWBgNVHR8ETzBNMEugSaBHhkVodHRwOi8vY3Js
Lm1pY3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNSb29DZXJBdXRfMjAx
MC0wNi0yMy5jcmwwWgYIKwYBBQUHAQEETjBMMEoGCCsGAQUFBzAChj5odHRwOi8v
d3d3Lm1pY3Jvc29mdC5jb20vcGtpL2NlcnRzL01pY1Jvb0NlckF1dF8yMDEwLTA2
LTIzLmNydDANBgkqhkiG9w0BAQsFAAOCAgEAFPx8cVGlecJusu85Prw8Ug9uKz8Q
E3P+qGjQSKY0TYqWBSbuMUaQYXnW/zguRWv0wOUouNodj4rbCdcax0wKNmZqjOwb
1wSQqBgXpJu54kAyNnbEwVrGv+QEwOoW06zDaO9irN1UbFAwWKbrfP6Up06O9Ox8
hnNXwlIhczRa86OKVsgE2gcJ7fiL4870fo6u8PYLigj7P8kdcn9TuOu+Y+DjPTFl
sIHl8qzNFqSfPaixm8JC0JCEX1Qd/4nquh1HkG+wc05Bn0CfX+WhKrIRkXOKISjw
zt5zOV8+q1xg7N8DEKjTCen09paFtn9RiGZHGY2isBI9gSpoBXe7kUxie7bBB8e6
eoc0Aw5LYnqZ6cr8zko3yS2kV3wc/j3cuA9a+tbEswKFAjrqs9lu5GkhN96B0fZ1
GQVn05NXXikbOcjuLeHN5EVzW9DSznqrFhmCRljQXp2Bs2evbDXyvOU/JOI1ogp1
BvYYVpnUeCzRBRvr0IgBnaoQ8QXfun4sY7cGmyMhxPl4bOJYFwY2K5ESA8yk2fIt
uvmUnUDtGEXxzopcaz6rA9NwGCoKauBfR9HVYwoy8q/XNh8qcFrlQlkIcUtXun6D
gfAhPPQcwcW5kJMOiEWThumxIJm+mMvFlaRdYtagYwggvXUQd30980W5n5efy1eA
bzOpBM93pGIcWX4=
-----END CERTIFICATE-----

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:08:d3:c4:00:00:00:00:00:04
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation Third Party Marketplace Root
        Validity
            Not Before: Jun 27 21:22:45 2011 GMT
            Not After : Jun 27 21:32:45 2026 GMT
        Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation UEFI CA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a5:08:6c:4c:c7:45:09:6a:4b:0c:a4:c0:87:7f:
                    06:75:0c:43:01:54:64:e0:16:7f:07:ed:92:7d:0b:
                    b2:73:bf:0c:0a:c6:4a:45:61:a0:c5:16:2d:96:d3:
                    f5:2b:a0:fb:4d:49:9b:41:80:90:3c:b9:54:fd:e6:
                    bc:d1:9d:c4:a4:18:8a:7f:41:8a:5c:59:83:68:32:
                    bb:8c:47:c9:ee:71:bc:21:4f:9a:8a:7c:ff:44:3f:
                    8d:8f:32:b2:26:48:ae:75:b5:ee:c9:4c:1e:4a:19:
                    7e:e4:82:9a:1d:78:77:4d:0c:b0:bd:f6:0f:d3:16:
                    d3:bc:fa:2b:a5:51:38:5d:f5:fb:ba:db:78:02:db:
                    ff:ec:0a:1b:96:d5:83:b8:19:13:e9:b6:c0:7b:40:
                    7b:e1:1f:28:27:c9:fa:ef:56:5e:1c:e6:7e:94:7e:
                    c0:f0:44:b2:79:39:e5:da:b2:62:8b:4d:bf:38:70:
                    e2:68:24:14:c9:33:a4:08:37:d5:58:69:5e:d3:7c:
                    ed:c1:04:53:08:e7:4e:b0:2a:87:63:08:61:6f:63:
                    15:59:ea:b2:2b:79:d7:0c:61:67:8a:5b:fd:5e:ad:
                    87:7f:ba:86:67:4f:71:58:12:22:04:22:22:ce:8b:
                    ef:54:71:00:ce:50:35:58:76:95:08:ee:6a:b1:a2:
                    01:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

```
            1.3.6.1.4.1.311.21.1:
                .....
            1.3.6.1.4.1.311.21.2:
                ....k..wSJ.%7.N.&{. p.
            X509v3 Subject Key Identifier:
                13:AD:BF:43:09:BD:82:70:9C:8C:D5:4F:31:6E:D5:22:98:8A:1B:D4
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:45:66:52:43:E1:7E:58:11:BF:D6:4E:9E:23:55:08:3B:3A:22:6A:A8

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.microsoft.com/pki/crl/products/MicCorThiParMarRoo_2010-10-05.crl

            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt

    Signature Algorithm: sha256WithRSAEncryption
         35:08:42:ff:30:cc:ce:f7:76:0c:ad:10:68:58:35:29:46:32:
         76:27:7c:ef:12:41:27:42:1b:4a:aa:6d:81:38:48:59:13:55:
         f3:e9:58:34:a6:16:0b:82:aa:5d:ad:82:da:80:83:41:06:8f:
         b4:1d:f2:03:b9:f3:1a:5d:1b:f1:50:90:f9:b3:55:84:42:28:
         1c:20:bd:b2:ae:51:14:c5:c0:ac:97:95:21:1c:90:db:0f:fc:
         77:9e:95:73:91:88:ca:bd:bd:52:b9:05:50:0d:df:57:9e:a0:
         61:ed:0d:e5:6d:25:d9:40:0f:17:40:c8:ce:a3:4a:c2:4d:af:
         9a:12:1d:08:54:8f:bd:c7:bc:b9:2b:3d:49:2b:1f:32:fc:6a:
         21:69:4f:9b:c8:7e:42:34:fc:36:06:17:8b:8f:20:40:c0:b3:
         9a:25:75:27:cd:c9:03:a3:f6:5d:d1:e7:36:54:7a:b9:50:b5:
         d3:12:d1:07:bf:bb:74:df:dc:1e:8f:80:d5:ed:18:f4:2f:14:
         16:6b:2f:de:66:8c:b0:23:e5:c7:84:d8:ed:ea:c1:33:82:ad:
         56:4b:18:2d:f1:68:95:07:cd:cf:f0:72:f0:ae:bb:dd:86:85:
         98:2c:21:4c:33:2b:f0:0f:4a:f0:68:87:b5:92:55:32:75:a1:
         6a:82:6a:3c:a3:25:11:a4:ed:ad:d7:04:ae:cb:d8:40:59:a0:
         84:d1:95:4c:62:91:22:1a:74:1d:8c:3d:47:0e:44:a6:e4:b0:
         9b:34:35:b1:fa:b6:53:a8:2c:81:ec:a4:05:71:c8:9d:b8:ba:
         e8:1b:44:66:e4:47:54:0e:8e:56:7f:b3:9f:16:98:b2:86:d0:
         68:3e:90:23:b5:2f:5e:8f:50:85:8d:c6:8d:82:5f:41:a1:f4:
         2e:0d:e0:99:d2:6c:75:e4:b6:69:b5:21:86:fa:07:d1:f6:e2:
         4d:d1:da:ad:2c:77:53:1e:25:32:37:c7:6c:52:72:95:86:b0:
         f1:35:61:6a:19:f5:b2:3b:81:50:56:a6:32:2d:fe:a2:89:f9:
         42:86:27:18:55:a1:82:ca:5a:9b:f8:30:98:54:14:a6:47:96:
         25:2f:c8:26:e4:41:94:1a:5c:02:3f:e5:96:e3:85:5b:3c:3e:
         3f:bb:47:16:72:55:e2:25:22:b1:d9:7b:e7:03:06:2a:a3:f7:
         1e:90:46:c3:00:0d:d6:19:89:e3:0e:35:27:62:03:71:15:a6:
         ef:d0:27:a0:a0:59:37:60:f8:38:94:b8:e0:78:70:f8:ba:4c:
         86:87:94:f6:e0:ae:02:45:ee:65:c2:b6:a3:7e:69:16:75:07:
         92:9b:f5:a6:bc:59:83:58
-----BEGIN CERTIFICATE-----
MIIGEDCCA/igAwIBAgIKYQjTxAAAAAAABDANBgkqhkiG9w0BAQsFADCBkTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE7MDkGA1UEAxMyTWljcm9z
b2Z0IENvcnBvcmF0aW9uIFRoaXJkIFBhcnR5IE1hcmtldHBsYWNlIFJvb3QwHhcN
```

```
MTEwNjI3MjEyMjQ1WhcNMjYwNjI3MjEzMjQ1WjCBgTELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1p
Y3Jvc29mdCBDb3Jwb3JhdGlvbjErMCkGA1UEAxMiTWljcm9zb2Z0IENvcnBvcmF0
aW9uIFVFRkkgQ0EgMjAxMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AKUIbEzHRQlqSwykwId/BnUMQwFUZOAWfwftkn0LsnO/DArGSkVhoMUWLZbT9Sug
+01Jm0GAkDy5VP3mvNGdxKQYin9BilxZg2gyu4xHye5xvCFPmop8/0Q/jY8ysiZI
rnW17slMHkoZfuSCmh14d00MsL32D9MW07z6K6VROF31+7rbeALb/+wKG5bVg7gZ
E+m2wHtAe+EfKCfJ+u9WXhzmfpR+wPBEsnk55dqyYotNvzhw4mgkFMkzpAg31Vhp
XtN87cEEUwjnTrAqh2MIYW9jFVnqsit51wxhZ4pb/V6th3+6hmdPcVgSIgQiIs6L
71RxAM5QNVh2lQjuarGiAdUCAwEAAaOCAXYwggFyMBIGCSsGAQQBgjcVAQQFAgMB
AAEwIwYJKwYBBAGCNxUCBBYEFPjBa7d/d1NK8yU3HU6hJnsPIHCAMB0GA1UdDgQW
BBQTrb9DCb2CcJyM1U8xbtUimIob1DAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMA
QTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRFZlJD
4X5YEb/WTp4jVQg7OiJqqDBcBgNVHR8EVTBTMFGgT6BNhktodHRwOi8vY3JsLm1p
Y3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNDb3JUaGlQYXJNYXJSb29f
MjAxMC0xMC0wNS5jcmwwYAYIKwYBBQUHAQEEVDBSMFAGCCsGAQUFBzAChkRodHRw
Oi8vd3d3Lm1pY3Jvc29mdC5jb20vcGtpL2NlcnRzL01pY0NvclRoaVBhck1hclJv
b18yMDEwLTEwLTA1LmNydDANBgkqhkiG9w0BAQsFAAOCAgEANQhC/zDMzvd2DK0Q
aFg1KUYydid87xJBJ0IbSqptgThIWRNV8+lYNKYWC4KqXa2C2oCDQQaPtB3yA7nz
Gl0b8VCQ+bNVhEIoHCC9sq5RFMXArJeVIRyQ2w/8d56Vc5GIyr29UrkFUA3fV56g
Ye0N5W0l2UAPF0DIzqNKwk2vmhIdCFSPvce8uSs9SSsfMvxqIWlPm8h+QjT8NgYX
i48gQMCzmiV1J83JA6P2XdHnNlR6uVC10xLRB7+7dN/cHo+A1e0Y9C8UFmsv3maM
sCPlx4TY7erBM4KtVksYLfFolQfNz/By8K673YaFmCwhTDMr8A9K8GiHtZJVMnWh
aoJqPKMlEaTtrdcErsvYQFmghNGVTGKRIhp0HYw9Rw5EpuSwmzQ1sfq2U6gsgeyk
BXHInbi66BtEZuRHVA6OVn+znxaYsobQaD6QI7UvXo9QhY3GjYJfQaH0Lg3gmdJs
deS2abUhhvoH0fbiTdHarSx3Ux4lMjfHbFJylYaw8TVhahn1sjuBUFamMi3+oon5
QoYnGFWhgspam/gwmFQUpkeWJS/IJuRBlBpcAj/lluOFWzw+P7tHFnJV4iUisdl7
5wMGKqP3HpBGwwAN1hmJ4w41J2IDcRWm79AnoKBZN2D4OJS44Hhw+LpMhoeU9uCu
AkXuZcK2o35pFnUHkpv1prxZg1g=
-----END CERTIFICATE-----
```

7.6 Auflistung aller Dateien der EFI-Partition der HP-Plattform

```
hp-EFI-Partition/:
total 20K
drwxr-xr-x 4 root root 4,0K Jan  1  1970 ./
drwxr-xr-x 9 root root 4,0K Jul 19 10:43 ../
drwxr-xr-x 2 root root 4,0K Dez 20  2012 boot/
drwxr-xr-x 5 root root 4,0K Jul 16 10:35 EFI/
-rwxr-xr-x 1 root root  200 Jul 15 11:03 GraphicsLib.Log*

hp-EFI-Partition/boot:
total 3,1M
drwxr-xr-x 2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 4 root root 4,0K Jan  1  1970 ../
-rwxr-xr-x 1 root root 3,1M Jun  2  2012 boot.sdi*

hp-EFI-Partition/EFI:
total 20K
drwxr-xr-x 5 root root 4,0K Jul 16 10:35 ./
drwxr-xr-x 4 root root 4,0K Jan  1  1970 ../
drwxr-xr-x 2 root root 4,0K Dez 20  2012 Boot/
drwxr-xr-x 7 root root 4,0K Jul 16 10:35 HP/
drwxr-xr-x 3 root root 4,0K Dez 20  2012 Microsoft/

hp-EFI-Partition/EFI/Boot:
total 1,4M
drwxr-xr-x 2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 5 root root 4,0K Jul 16 10:35 ../
-rwxr-xr-x 1 root root 1,3M Dez 20  2012 bootx64.efi*

hp-EFI-Partition/EFI/HP:
total 28K
drwxr-xr-x  7 root root 4,0K Jul 16 10:35 ./
drwxr-xr-x  5 root root 4,0K Jul 16 10:35 ../
drwxr-xr-x  5 root root 4,0K Jul 16 10:35 BIOS/
drwxr-xr-x  2 root root 4,0K Jul 16 10:35 BIOSUpdate/
drwxr-xr-x 39 root root 4,0K Dez 20  2012 boot/
drwxr-xr-x  4 root root 4,0K Dez 20  2012 EFI/
drwxr-xr-x  2 root root 4,0K Jul 15 11:03 SystemDiags/

hp-EFI-Partition/EFI/HP/BIOS:
total 20K
drwxr-xr-x 5 root root 4,0K Jul 16 10:35 ./
drwxr-xr-x 7 root root 4,0K Jul 16 10:35 ../
drwxr-xr-x 2 root root 4,0K Jul 16 10:35 Current/
drwxr-xr-x 2 root root 4,0K Jul 16 10:35 New/
drwxr-xr-x 2 root root 4,0K Jul 16 10:35 Previous/

hp-EFI-Partition/EFI/HP/BIOS/Current:
total 8,1M
drwxr-xr-x 2 root root 4,0K Jul 16 10:35 ./
drwxr-xr-x 5 root root 4,0K Jul 16 10:35 ../
-rwxr-xr-x 1 root root 8,0M Jul 16 10:35 01886.bin*
-rwxr-xr-x 1 root root  256 Dez 20  2012 01886.s12*
-rwxr-xr-x 1 root root  256 Jul 16 10:35 01886.sig*

hp-EFI-Partition/EFI/HP/BIOS/New:
total 12K
drwxr-xr-x 2 root root 4,0K Jul 16 10:35 ./
drwxr-xr-x 5 root root 4,0K Jul 16 10:35 ../
```

```
-rwxr-xr-x 1 root root  256 Jul 16 10:10 01886.s12*

hp-EFI-Partition/EFI/HP/BIOS/Previous:
total 8,1M
drwxr-xr-x 2 root root 4,0K Jul 16 10:35 ./
drwxr-xr-x 5 root root 4,0K Jul 16 10:35 ../
-rwxr-xr-x 1 root root 8,0M Jul 16 10:35 01886.bin*
-rwxr-xr-x 1 root root  256 Jul 16 10:35 01886.s12*
-rwxr-xr-x 1 root root  256 Jul 16 10:35 01886.sig*

hp-EFI-Partition/EFI/HP/BIOSUpdate:
total 2,4M
drwxr-xr-x 2 root root 4,0K Jul 16 10:35 ./
drwxr-xr-x 7 root root 4,0K Jul 16 10:35 ../
-rwxr-xr-x 1 root root 253K Nov  5  2012 CryptRSA32.efi*
-rwxr-xr-x 1 root root 434K Nov  5  2012 CryptRSA.efi*
-rwxr-xr-x 1 root root 799K Apr 18 08:58 HpBiosUpdate32.efi*
-rwxr-xr-x 1 root root  256 Apr 18 11:53 HpBiosUpdate32.s09*
-rwxr-xr-x 1 root root  256 Apr 18 11:53 HpBiosUpdate32.s12*
-rwxr-xr-x 1 root root  256 Apr 18 11:41 HpBiosUpdate32.sig*
-rwxr-xr-x 1 root root 828K Apr 18 08:58 HpBiosUpdate.efi*
-rwxr-xr-x 1 root root 3,4K Jul 16 10:35 HpBiosUpdate.log*
-rwxr-xr-x 1 root root  256 Apr 18 11:52 HpBiosUpdate.s09*
-rwxr-xr-x 1 root root  256 Apr 18 11:53 HpBiosUpdate.s12*
-rwxr-xr-x 1 root root  256 Apr 18 11:41 HpBiosUpdate.sig*

hp-EFI-Partition/EFI/HP/boot:
total 8,0M
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ./
drwxr-xr-x  7 root root 4,0K Jul 16 10:35 ../
-rwxr-xr-x  1 root root  12K Dez 20  2012 BCD*
-rwxr-xr-x  1 root root  12K Dez 20  2012 bcd.LOG*
drwxr-xr-x  2 root root 4,0K Dez 20  2012 bg-bg/
-rwxr-xr-x  1 root root 1,0K Jun  2  2012 bootfix.bin*
-rwxr-xr-x  1 root root 1,3M Dez 20  2012 bootmgfw.efi*
-rwxr-xr-x  1 root root 1,3M Dez 20  2012 bootmgr.efi*
-rwxr-xr-x  1 root root 3,1M Jun  2  2012 boot.sdi*
-rwxr-xr-x  1 root root 4,1K Jun 26  2012 boot.stl*
drwxr-xr-x  2 root root 4,0K Dez 20  2012 cs-cz/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 da-dk/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 de-de/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 el-gr/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 en-gb/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 en-us/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 es-es/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 et-ee/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 fi-fi/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 Fonts/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 fr-fr/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 hr-hr/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 hu-hu/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 it-it/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ja-jp/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ko-kr/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 lt-lt/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 lv-lv/
-rwxr-xr-x  1 root root 1,3M Jul 25  2012 memtest.efi*
-rwxr-xr-x  1 root root 954K Jul 26  2012 memtest.exe*
drwxr-xr-x  2 root root 4,0K Dez 20  2012 nb-no/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 nl-nl/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 pl-pl/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 pt-br/
```

```
drwxr-xr-x  2 root root 4,0K Dez 20  2012 pt-pt/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 qps-ploc/
drwxr-xr-x  4 root root 4,0K Dez 20  2012 Resources/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ro-ro/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ru-ru/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 sk-sk/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 sl-si/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 sr-latn-cs/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 sv-se/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 tr-tr/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 uk-ua/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 zh-cn/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 zh-hk/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 zh-tw/

hp-EFI-Partition/EFI/HP/boot/bg-bg:
total 236K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/cs-cz:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/da-dk:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/de-de:
total 344K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/el-gr:
total 344K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  78K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  78K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  78K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  46K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  46K Jul 26  2012 memtest.exe.mui*
```

```
hp-EFI-Partition/EFI/HP/boot/en-gb:
total 224K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/en-us:
total 320K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/es-es:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/et-ee:
total 236K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  73K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  73K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  73K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/fi-fi:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/Fonts:
total 13M
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root 3,6M Jun  2  2012 chs_boot.ttf*
-rwxr-xr-x  1 root root 3,7M Jun  2  2012 cht_boot.ttf*
-rwxr-xr-x  1 root root 1,9M Jun  2  2012 jpn_boot.ttf*
-rwxr-xr-x  1 root root 2,3M Jun  2  2012 kor_boot.ttf*
-rwxr-xr-x  1 root root 165K Jun  2  2012 malgun_boot.ttf*
-rwxr-xr-x  1 root root 162K Jun  2  2012 malgunn_boot.ttf*
-rwxr-xr-x  1 root root 132K Jun  2  2012 meiryo_boot.ttf*
-rwxr-xr-x  1 root root 130K Jun  2  2012 meiryon_boot.ttf*
-rwxr-xr-x  1 root root 152K Jun  2  2012 msjh_boot.ttf*
-rwxr-xr-x  1 root root 150K Jun  2  2012 msjhn_boot.ttf*
-rwxr-xr-x  1 root root 143K Jun  2  2012 msyh_boot.ttf*
```

```
-rwxr-xr-x  1 root root 139K Jun  2  2012 msyhn_boot.ttf*
-rwxr-xr-x  1 root root  36K Jun  2  2012 segmono_boot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoen_slboot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoe_slboot.ttf*
-rwxr-xr-x  1 root root  47K Jun  2  2012 wgl4_boot.ttf*

hp-EFI-Partition/EFI/HP/boot/fr-fr:
total 344K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/hr-hr:
total 236K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/hu-hu:
total 344K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/it-it:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/ja-jp:
total 300K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/ko-kr:
total 300K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*
```

```
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/lt-lt:
total 236K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/lv-lv:
total 236K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/nb-no:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/nl-nl:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/pl-pl:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/pt-br:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/pt-pt:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
```

```
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/qps-ploc:
total 200K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/boot/Resources:
total 36K
drwxr-xr-x  4 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  18K Jul 25  2012 bootres.dll*
drwxr-xr-x  2 root root 4,0K Dez 20  2012 de-DE/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 en-US/

hp-EFI-Partition/EFI/HP/boot/Resources/de-DE:
total 20K
drwxr-xr-x 2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 4 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x 1 root root  12K Okt 23  2012 bootres.dll.mui*

hp-EFI-Partition/EFI/HP/boot/Resources/en-US:
total 20K
drwxr-xr-x 2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 4 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x 1 root root  12K Jul 25  2012 bootres.dll.mui*

hp-EFI-Partition/EFI/HP/boot/ro-ro:
total 236K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/ru-ru:
total 324K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  44K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  44K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/sk-sk:
total 236K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/sl-si:
total 236K
```

```
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/sr-latn-cs:
total 236K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/sv-se:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/tr-tr:
total 332K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/uk-ua:
total 236K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.exe.mui*

hp-EFI-Partition/EFI/HP/boot/zh-cn:
total 288K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/boot/zh-hk:
total 288K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.exe.mui*
```

```
hp-EFI-Partition/EFI/HP/boot/zh-tw:
total 288K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgr.exe.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.exe.mui*

hp-EFI-Partition/EFI/HP/EFI:
total 16K
drwxr-xr-x  4 root root 4,0K Dez 20  2012 ./
drwxr-xr-x  7 root root 4,0K Jul 16 10:35 ../
drwxr-xr-x 36 root root 4,0K Okt 23  2012 Boot/
drwxr-xr-x  3 root root 4,0K Okt 23  2012 Microsoft/

hp-EFI-Partition/EFI/HP/EFI/Boot:
total 1,5M
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ./
drwxr-xr-x  4 root root 4,0K Dez 20  2012 ../
drwxr-xr-x  2 root root 4,0K Okt 23  2012 bg-bg/
-rwxr-xr-x  1 root root 1,3M Jul 26  2012 bootx64.efi*
drwxr-xr-x  2 root root 4,0K Okt 23  2012 cs-cz/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 da-dk/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 de-de/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 el-gr/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 en-gb/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 en-us/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 es-es/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 et-ee/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 fi-fi/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 fr-fr/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 hr-hr/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 hu-hu/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 it-it/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ja-jp/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ko-kr/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 lt-lt/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 lv-lv/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 nb-no/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 nl-nl/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 pl-pl/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 pt-br/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 pt-pt/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ro-ro/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ru-ru/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 sk-sk/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 sl-si/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 sr-latn-cs/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 sv-se/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 tr-tr/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 uk-ua/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 zh-cn/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 zh-hk/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 zh-tw/

hp-EFI-Partition/EFI/HP/EFI/Boot/bg-bg:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootx64.efi.mui*
```

```
hp-EFI-Partition/EFI/HP/EFI/Boot/cs-cz:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/da-dk:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/de-de:
total 88K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/el-gr:
total 88K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  78K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/en-gb:
total 80K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/en-us:
total 80K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/es-es:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/et-ee:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  73K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/fi-fi:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/fr-fr:
total 88K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/hr-hr:
```

```
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/hu-hu:
total 88K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/it-it:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/ja-jp:
total 76K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/ko-kr:
total 76K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/lt-lt:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/lv-lv:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/nb-no:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/nl-nl:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/pl-pl:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/pt-br:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
```

```
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/pt-pt:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/ro-ro:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/ru-ru:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/sk-sk:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/sl-si:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/sr-latn-cs:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/sv-se:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/tr-tr:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/uk-ua:
total 84K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/zh-cn:
total 72K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootx64.efi.mui*
```

```
hp-EFI-Partition/EFI/HP/EFI/Boot/zh-hk:
total 72K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Boot/zh-tw:
total 72K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 36 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootx64.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft:
total 12K
drwxr-xr-x  3 root root 4,0K Okt 23  2012 ./
drwxr-xr-x  4 root root 4,0K Dez 20  2012 ../
drwxr-xr-x 27 root root 4,0K Okt 23  2012 Boot/

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot:
total 1,6M
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ./
drwxr-xr-x  3 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root 256K Jun  2  2012 BCD*
drwxr-xr-x  2 root root 4,0K Okt 23  2012 cs-cz/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 da-dk/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 de-de/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 el-gr/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 en-us/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 es-es/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 fi-fi/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 Fonts/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 fr-fr/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 hu-hu/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 it-it/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ja-jp/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ko-kr/
-rwxr-xr-x  1 root root 1,3M Jul 26  2012 memtest.efi*
drwxr-xr-x  2 root root 4,0K Okt 23  2012 nb-no/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 nl-nl/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 pl-pl/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 pt-br/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 pt-pt/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 Resources/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ru-ru/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 sv-se/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 tr-tr/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 zh-cn/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 zh-hk/
drwxr-xr-x  2 root root 4,0K Okt 23  2012 zh-tw/

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/cs-cz:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/da-dk:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*
```

```
hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/de-de:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/el-gr:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  46K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/en-us:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/es-es:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/fi-fi:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/Fonts:
total 13M
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root 3,6M Jun  2  2012 chs_boot.ttf*
-rwxr-xr-x  1 root root 3,7M Jun  2  2012 cht_boot.ttf*
-rwxr-xr-x  1 root root 1,9M Jun  2  2012 jpn_boot.ttf*
-rwxr-xr-x  1 root root 2,3M Jun  2  2012 kor_boot.ttf*
-rwxr-xr-x  1 root root 165K Jun  2  2012 malgun_boot.ttf*
-rwxr-xr-x  1 root root 132K Jun  2  2012 meiryo_boot.ttf*
-rwxr-xr-x  1 root root 152K Jun  2  2012 msjh_boot.ttf*
-rwxr-xr-x  1 root root 143K Jun  2  2012 msyh_boot.ttf*
-rwxr-xr-x  1 root root  36K Jun  2  2012 segmono_boot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoe_slboot.ttf*
-rwxr-xr-x  1 root root  47K Jun  2  2012 wgl4_boot.ttf*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/fr-fr:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/hu-hu:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/it-it:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
```

```
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/ja-jp:
total 52K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/ko-kr:
total 52K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/nb-no:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/nl-nl:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/pl-pl:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/pt-br:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/pt-pt:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/Resources:
total 28K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  18K Jul 26  2012 bootres.dll*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/ru-ru:
total 52K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  44K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/sv-se:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*
```

```
hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/tr-tr:
total 56K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/zh-cn:
total 52K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/zh-hk:
total 52K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/EFI/Microsoft/Boot/zh-tw:
total 52K
drwxr-xr-x  2 root root 4,0K Okt 23  2012 ./
drwxr-xr-x 27 root root 4,0K Okt 23  2012 ../
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/HP/SystemDiags:
total 9,5M
drwxr-xr-x 2 root root 4,0K Jul 15 11:03 ./
drwxr-xr-x 7 root root 4,0K Jul 16 10:35 ../
-rwxr-xr-x 1 root root 101K Apr 18 08:57 CpuDiags32.udm*
-rwxr-xr-x 1 root root 114K Apr 18 08:57 CpuDiags.udm*
-rwxr-xr-x 1 root root 253K Nov  5  2012 CryptRSA32.efi*
-rwxr-xr-x 1 root root 434K Nov  5  2012 CryptRSA.efi*
-rwxr-xr-x 1 root root  90K Apr 18 08:58 FirewireDiags32.udm*
-rwxr-xr-x 1 root root  45K Apr 16 08:47 firewirediags.msg.xml*
-rwxr-xr-x 1 root root 109K Apr 18 08:57 FirewireDiags.udm*
-rwxr-xr-x 1 root root 224K Apr 18 08:58 OpticalDiags32.udm*
-rwxr-xr-x 1 root root  38K Dez 10  2012 opticaldiags.msg.xml*
-rwxr-xr-x 1 root root 254K Apr 18 08:58 OpticalDiags.udm*
-rwxr-xr-x 1 root root 3,3M Apr 18 11:33 SystemDiags32.efi*
-rwxr-xr-x 1 root root  256 Apr 18 11:51 SystemDiags32.s09*
-rwxr-xr-x 1 root root  256 Apr 18 11:52 SystemDiags32.s12*
-rwxr-xr-x 1 root root  256 Apr 18 11:41 SystemDiags32.sig*
-rwxr-xr-x 1 root root   62 Jul 15 11:03 SystemDiagsCeeHistory.log*
-rwxr-xr-x 1 root root 3,6M Apr 18 11:33 SystemDiags.efi*
-rwxr-xr-x 1 root root 4,2K Jul 15 11:03 SystemDiags.log*
-rwxr-xr-x 1 root root  256 Apr 18 11:50 SystemDiags.s09*
-rwxr-xr-x 1 root root  256 Apr 18 11:51 SystemDiags.s12*
-rwxr-xr-x 1 root root  256 Apr 18 11:41 SystemDiags.sig*
-rwxr-xr-x 1 root root 100K Apr 18 08:58 USBDiags32.udm*
-rwxr-xr-x 1 root root  98K Jan 24 16:28 usbdiags.msg.xml*
-rwxr-xr-x 1 root root 120K Apr 18 08:58 USBDiags.udm*
-rwxr-xr-x 1 root root 183K Apr 18 08:58 VideoDiags32.udm*
-rwxr-xr-x 1 root root 202K Apr 18 08:58 VideoDiags.udm*
-rwxr-xr-x 1 root root 140K Mär 11 14:18 VideoMem32.udm*
-rwxr-xr-x 1 root root 149K Mär 11 14:18 VideoMem.udm*

hp-EFI-Partition/EFI/Microsoft:
total 12K
drwxr-xr-x  3 root root 4,0K Dez 20  2012 ./
drwxr-xr-x  5 root root 4,0K Jul 16 10:35 ../
drwxr-xr-x 39 root root 4,0K Dez 20  2012 Boot/
```

```
hp-EFI-Partition/EFI/Microsoft/Boot:
total 4,1M
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ./
drwxr-xr-x  3 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  32K Jul 16 11:38 BCD*
-rwxr-xr-x  1 root root  28K Dez 20  2012 BCD.LOG*
-rwxr-xr-x  1 root root    0 Dez 20  2012 BCD.LOG1*
-rwxr-xr-x  1 root root    0 Dez 20  2012 BCD.LOG2*
drwxr-xr-x  2 root root 4,0K Dez 20  2012 bg-BG/
-rwxr-xr-x  1 root root 1,3M Dez 20  2012 bootmgfw.efi*
-rwxr-xr-x  1 root root 1,3M Dez 20  2012 bootmgr.efi*
-rwxr-xr-x  1 root root  64K Dez 20  2012 BOOTSTAT.DAT*
-rwxr-xr-x  1 root root 4,1K Jun 26  2012 boot.stl*
drwxr-xr-x  2 root root 4,0K Dez 20  2012 cs-CZ/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 da-DK/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 de-DE/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 el-GR/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 en-GB/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 en-US/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 es-ES/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 et-EE/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 fi-FI/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 Fonts/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 fr-FR/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 hr-HR/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 hu-HU/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 it-IT/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ja-JP/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ko-KR/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 lt-LT/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 lv-LV/
-rwxr-xr-x  1 root root 1,3M Jul 25  2012 memtest.efi*
drwxr-xr-x  2 root root 4,0K Dez 20  2012 nb-NO/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 nl-NL/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 pl-PL/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 pt-BR/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 pt-PT/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 qps-ploc/
drwxr-xr-x  4 root root 4,0K Dez 20  2012 Resources/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ro-RO/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ru-RU/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 sk-SK/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 sl-SI/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 sr-Latn-CS/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 sv-SE/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 tr-TR/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 uk-UA/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 zh-CN/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 zh-HK/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 zh-TW/

hp-EFI-Partition/EFI/Microsoft/Boot/bg-BG:
total 160K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/cs-CZ:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
```

```
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/da-DK:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/de-DE:
total 216K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/el-GR:
total 216K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  78K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  78K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  46K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/en-GB:
total 152K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/en-US:
total 200K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/es-ES:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/et-EE:
total 160K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  73K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  73K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/fi-FI:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
```

```
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/Fonts:
total 13M
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root 3,6M Jun  2  2012 chs_boot.ttf*
-rwxr-xr-x  1 root root 3,7M Jun  2  2012 cht_boot.ttf*
-rwxr-xr-x  1 root root 1,9M Jun  2  2012 jpn_boot.ttf*
-rwxr-xr-x  1 root root 2,3M Jun  2  2012 kor_boot.ttf*
-rwxr-xr-x  1 root root 165K Jun  2  2012 malgun_boot.ttf*
-rwxr-xr-x  1 root root 162K Jun  2  2012 malgunn_boot.ttf*
-rwxr-xr-x  1 root root 132K Jun  2  2012 meiryo_boot.ttf*
-rwxr-xr-x  1 root root 130K Jun  2  2012 meiryon_boot.ttf*
-rwxr-xr-x  1 root root 152K Jun  2  2012 msjh_boot.ttf*
-rwxr-xr-x  1 root root 150K Jun  2  2012 msjhn_boot.ttf*
-rwxr-xr-x  1 root root 143K Jun  2  2012 msyh_boot.ttf*
-rwxr-xr-x  1 root root 139K Jun  2  2012 msyhn_boot.ttf*
-rwxr-xr-x  1 root root  36K Jun  2  2012 segmono_boot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoen_slboot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoe_slboot.ttf*
-rwxr-xr-x  1 root root  47K Jun  2  2012 wgl4_boot.ttf*

hp-EFI-Partition/EFI/Microsoft/Boot/fr-FR:
total 216K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/hr-HR:
total 160K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/hu-HU:
total 216K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/it-IT:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/ja-JP:
total 188K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgfw.efi.mui*
```

```
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/ko-KR:
total 188K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/lt-LT:
total 160K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/lv-LV:
total 160K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/nb-NO:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/nl-NL:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/pl-PL:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/pt-BR:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/pt-PT:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
```

```
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/qps-ploc:
total 200K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/Resources:
total 36K
drwxr-xr-x  4 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  18K Jul 25  2012 bootres.dll*
drwxr-xr-x  2 root root 4,0K Dez 20  2012 de-DE/
drwxr-xr-x  2 root root 4,0K Dez 20  2012 en-US/

hp-EFI-Partition/EFI/Microsoft/Boot/Resources/de-DE:
total 20K
drwxr-xr-x 2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 4 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x 1 root root  12K Okt 23  2012 bootres.dll.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/Resources/en-US:
total 20K
drwxr-xr-x 2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 4 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x 1 root root  12K Jul 25  2012 bootres.dll.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/ro-RO:
total 160K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/ru-RU:
total 204K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  44K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/sk-SK:
total 160K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/sl-SI:
total 160K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/sr-Latn-CS:
total 160K
```

```
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/sv-SE:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/tr-TR:
total 208K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/uk-UA:
total 160K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/zh-CN:
total 180K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/zh-HK:
total 180K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

hp-EFI-Partition/EFI/Microsoft/Boot/zh-TW:
total 180K
drwxr-xr-x  2 root root 4,0K Dez 20  2012 ./
drwxr-xr-x 39 root root 4,0K Dez 20  2012 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*
```

7.7 Auflistung aller Dateien der EFI-Partition der Dell-Plattform

```
dell-EFI-Partition/:
total 16K
drwxr-xr-x 4 root root 4,0K Jan  1  1970 ./
drwxr-xr-x 9 root root 4,0K Jul 19 10:43 ../
drwxr-xr-x 4 root root 4,0K Apr 18 12:12 EFI/
drwxr-xr-x 2 root root 4,0K Mär  4 13:12 en-us/

dell-EFI-Partition/EFI:
total 16K
drwxr-xr-x 4 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 4 root root 4,0K Jan  1  1970 ../
drwxr-xr-x 2 root root 4,0K Apr 18 12:12 Boot/
drwxr-xr-x 3 root root 4,0K Apr 18 12:12 Microsoft/

dell-EFI-Partition/EFI/Boot:
total 1,4M
drwxr-xr-x 2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 4 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x 1 root root 1,3M Sep 20  2012 bootx64.efi*

dell-EFI-Partition/EFI/Microsoft:
total 12K
drwxr-xr-x  3 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x  4 root root 4,0K Apr 18 12:12 ../
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 Boot/

dell-EFI-Partition/EFI/Microsoft/Boot:
total 4,1M
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x  3 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  36K Jul 17 09:20 BCD*
-rwxr-xr-x  1 root root  32K Apr 18 12:12 BCD.LOG*
-rwxr-xr-x  1 root root    0 Apr 18 12:12 BCD.LOG1*
-rwxr-xr-x  1 root root    0 Apr 18 12:12 BCD.LOG2*
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 bg-BG/
-rwxr-xr-x  1 root root 1,3M Sep 20  2012 bootmgfw.efi*
-rwxr-xr-x  1 root root 1,3M Sep 20  2012 bootmgr.efi*
-rwxr-xr-x  1 root root  64K Apr 18 12:12 BOOTSTAT.DAT*
-rwxr-xr-x  1 root root 4,1K Jun 27  2012 boot.stl*
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 cs-CZ/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 da-DK/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 de-DE/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 el-GR/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 en-GB/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 en-US/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 es-ES/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 et-EE/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 fi-FI/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 Fonts/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 fr-FR/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 hr-HR/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 hu-HU/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 it-IT/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ja-JP/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ko-KR/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 lt-LT/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 lv-LV/
-rwxr-xr-x  1 root root 1,3M Jul 26  2012 memtest.efi*
```

```
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 nb-NO/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 nl-NL/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 pl-PL/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 pt-BR/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 pt-PT/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 qps-ploc/
drwxr-xr-x  3 root root 4,0K Apr 18 12:12 Resources/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ro-RO/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ru-RU/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 sk-SK/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 sl-SI/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 sr-Latn-CS/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 sv-SE/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 tr-TR/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 uk-UA/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 zh-CN/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 zh-HK/
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 zh-TW/

dell-EFI-Partition/EFI/Microsoft/Boot/bg-BG:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/cs-CZ:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/da-DK:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/de-DE:
total 216K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/el-GR:
total 216K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  78K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  78K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  46K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/en-GB:
total 152K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
```

```
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/en-US:
total 200K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/es-ES:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/et-EE:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  73K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  73K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/fi-FI:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/Fonts:
total 13M
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root 3,6M Jun  2  2012 chs_boot.ttf*
-rwxr-xr-x  1 root root 3,7M Jun  2  2012 cht_boot.ttf*
-rwxr-xr-x  1 root root 1,9M Jun  2  2012 jpn_boot.ttf*
-rwxr-xr-x  1 root root 2,3M Jun  2  2012 kor_boot.ttf*
-rwxr-xr-x  1 root root 165K Jun  2  2012 malgun_boot.ttf*
-rwxr-xr-x  1 root root 162K Jun  2  2012 malgunn_boot.ttf*
-rwxr-xr-x  1 root root 132K Jun  2  2012 meiryo_boot.ttf*
-rwxr-xr-x  1 root root 130K Jun  2  2012 meiryon_boot.ttf*
-rwxr-xr-x  1 root root 152K Jun  2  2012 msjh_boot.ttf*
-rwxr-xr-x  1 root root 150K Jun  2  2012 msjhn_boot.ttf*
-rwxr-xr-x  1 root root 143K Jun  2  2012 msyh_boot.ttf*
-rwxr-xr-x  1 root root 139K Jun  2  2012 msyhn_boot.ttf*
-rwxr-xr-x  1 root root  36K Jun  2  2012 segmono_boot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoen_slboot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoe_slboot.ttf*
-rwxr-xr-x  1 root root  47K Jun  2  2012 wgl4_boot.ttf*

dell-EFI-Partition/EFI/Microsoft/Boot/fr-FR:
total 216K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*
```

```
dell-EFI-Partition/EFI/Microsoft/Boot/hr-HR:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/hu-HU:
total 216K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/it-IT:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/ja-JP:
total 188K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/ko-KR:
total 188K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/lt-LT:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/lv-LV:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/nb-NO:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*
```

```
dell-EFI-Partition/EFI/Microsoft/Boot/nl-NL:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/pl-PL:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/pt-BR:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/pt-PT:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/qps-ploc:
total 200K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/Resources:
total 32K
drwxr-xr-x  3 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  18K Jul 25  2012 bootres.dll*
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 de-DE/

dell-EFI-Partition/EFI/Microsoft/Boot/Resources/de-DE:
total 20K
drwxr-xr-x 2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 3 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x 1 root root  12K Jul 26  2012 bootres.dll.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/ro-RO:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/ru-RU:
total 204K
```

```
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  44K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/sk-SK:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/sl-SI:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/sr-Latn-CS:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/sv-SE:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/tr-TR:
total 208K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/uk-UA:
total 160K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/zh-CN:
total 180K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/zh-HK:
total 180K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
```

```
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/EFI/Microsoft/Boot/zh-TW:
total 180K
drwxr-xr-x  2 root root 4,0K Apr 18 12:12 ./
drwxr-xr-x 39 root root 4,0K Apr 18 12:12 ../
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

dell-EFI-Partition/en-us:
total 80K
drwxr-xr-x 2 root root 4,0K Mär  4 13:12 ./
drwxr-xr-x 4 root root 4,0K Jan  1  1970 ../
-rwxr-xr-x 1 root root  72K Mär  4 13:04 bootmgr.efi.mui*
```

7.8 Auflistung aller Dateien der EFI-Partition der Lenovo-Plattform

```
lenovo-EFI-Partition/:
total 16K
drwxr-xr-x 4 root root 4,0K Jan  1  1970 ./
drwxr-xr-x 9 root root 4,0K Jul 19 10:43 ../
drwxr-xr-x 2 root root 4,0K Mai 22 23:41 BOOT/
drwxr-xr-x 5 root root 4,0K Mai 22 23:41 EFI/

lenovo-EFI-Partition/BOOT:
total 3,1M
drwxr-xr-x 2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 4 root root 4,0K Jan  1  1970 ../
-rwxr-xr-x 1 root root 3,1M Jun  2  2012 boot.sdi*

lenovo-EFI-Partition/EFI:
total 20K
drwxr-xr-x 5 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 4 root root 4,0K Jan  1  1970 ../
drwxr-xr-x 2 root root 4,0K Mai 22 23:41 Boot/
drwxr-xr-x 3 root root 4,0K Mai 23 00:24 Lenovo/
drwxr-xr-x 3 root root 4,0K Mai 22 23:41 Microsoft/

lenovo-EFI-Partition/EFI/Boot:
total 2,1M
drwxr-xr-x 2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 5 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x 1 root root 1,3M Sep 20  2012 bootx64.efi*
-rwxr-xr-x 1 root root 756K Aug  1  2012 LenovoBT.EFI*
-rwxr-xr-x 1 root root 1,5K Jun 18  2012 License.txt*
-rwxr-xr-x 1 root root   74 Aug  6  2012 ReadMe.txt*

lenovo-EFI-Partition/EFI/Lenovo:
total 12K
drwxr-xr-x  3 root root 4,0K Mai 23 00:24 ./
drwxr-xr-x  5 root root 4,0K Mai 22 23:41 ../
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 Boot/

lenovo-EFI-Partition/EFI/Lenovo/Boot:
total 4,1M
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x  3 root root 4,0K Mai 23 00:24 ../
-rwxr-xr-x  1 root root  40K Mai 23 00:24 BCD*
-rwxr-xr-x  1 root root  24K Mai 22 23:41 BCD.LOG*
-rwxr-xr-x  1 root root    0 Mai 22 23:41 BCD.LOG1*
-rwxr-xr-x  1 root root    0 Mai 22 23:41 BCD.LOG2*
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 bg-BG/
-rwxr-xr-x  1 root root 1,3M Sep 20  2012 bootmgfw.efi*
-rwxr-xr-x  1 root root 1,3M Sep 20  2012 bootmgr.efi*
-rwxr-xr-x  1 root root  64K Mai 22 23:41 BOOTSTAT.DAT*
-rwxr-xr-x  1 root root 4,1K Jun 26  2012 boot.stl*
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 cs-CZ/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 da-DK/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 de-DE/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 el-GR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 en-GB/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 en-US/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 es-ES/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 et-EE/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 fi-FI/
```

```
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 Fonts/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 fr-FR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 hr-HR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 hu-HU/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 it-IT/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ja-JP/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ko-KR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 lt-LT/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 lv-LV/
-rwxr-xr-x  1 root root 1,3M Jul 25  2012 memtest.efi*
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 nb-NO/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 nl-NL/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 pl-PL/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 pt-BR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 pt-PT/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 qps-ploc/
drwxr-xr-x  4 root root 4,0K Mai 22 23:41 Resources/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ro-RO/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ru-RU/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 sk-SK/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 sl-SI/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 sr-Latn-CS/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 sv-SE/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 tr-TR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 uk-UA/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 zh-CN/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 zh-HK/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 zh-TW/

lenovo-EFI-Partition/EFI/Lenovo/Boot/bg-BG:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/cs-CZ:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/da-DK:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/de-DE:
total 216K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/el-GR:
total 216K
```

```
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  78K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  78K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  46K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/en-GB:
total 152K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/en-US:
total 200K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/es-ES:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/et-EE:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  73K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  73K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/fi-FI:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/Fonts:
total 13M
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root 3,6M Jun  2  2012 chs_boot.ttf*
-rwxr-xr-x  1 root root 3,7M Jun  2  2012 cht_boot.ttf*
-rwxr-xr-x  1 root root 1,9M Jun  2  2012 jpn_boot.ttf*
-rwxr-xr-x  1 root root 2,3M Jun  2  2012 kor_boot.ttf*
-rwxr-xr-x  1 root root 165K Jun  2  2012 malgun_boot.ttf*
-rwxr-xr-x  1 root root 162K Jun  2  2012 malgunn_boot.ttf*
-rwxr-xr-x  1 root root 132K Jun  2  2012 meiryo_boot.ttf*
-rwxr-xr-x  1 root root 130K Jun  2  2012 meiryon_boot.ttf*
-rwxr-xr-x  1 root root 152K Jun  2  2012 msjh_boot.ttf*
-rwxr-xr-x  1 root root 150K Jun  2  2012 msjhn_boot.ttf*
-rwxr-xr-x  1 root root 143K Jun  2  2012 msyh_boot.ttf*
-rwxr-xr-x  1 root root 139K Jun  2  2012 msyhn_boot.ttf*
-rwxr-xr-x  1 root root  36K Jun  2  2012 segmono_boot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoen_slboot.ttf*
```

```
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoe_slboot.ttf*
-rwxr-xr-x  1 root root  47K Jun  2  2012 wgl4_boot.ttf*

lenovo-EFI-Partition/EFI/Lenovo/Boot/fr-FR:
total 216K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/hr-HR:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/hu-HU:
total 216K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/it-IT:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/ja-JP:
total 188K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/ko-KR:
total 188K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/lt-LT:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/lv-LV:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
```

```
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/nb-NO:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/nl-NL:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/pl-PL:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/pt-BR:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/pt-PT:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/qps-ploc:
total 200K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/Resources:
total 36K
drwxr-xr-x  4 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  18K Jul 25  2012 bootres.dll*
drwxr-xr-x  2 root root 4,0K Mai 22 23:58 de-DE/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 en-US/

lenovo-EFI-Partition/EFI/Lenovo/Boot/Resources/de-DE:
total 20K
drwxr-xr-x 2 root root 4,0K Mai 22 23:58 ./
drwxr-xr-x 4 root root 4,0K Mai 22 23:41 ../
```

```
-rwxr-xr-x 1 root root  12K Mai 22 23:57 bootres.dll.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/Resources/en-US:
total 20K
drwxr-xr-x 2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 4 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x 1 root root  12K Jul 25  2012 bootres.dll.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/ro-RO:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/ru-RU:
total 204K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  44K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/sk-SK:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/sl-SI:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/sr-Latn-CS:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/sv-SE:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/tr-TR:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/uk-UA:
total 160K
```

```
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/zh-CN:
total 180K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/zh-HK:
total 180K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Lenovo/Boot/zh-TW:
total 180K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft:
total 12K
drwxr-xr-x  3 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x  5 root root 4,0K Mai 22 23:41 ../
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 Boot/

lenovo-EFI-Partition/EFI/Microsoft/Boot:
total 4,1M
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x  3 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  40K Jul 16 15:16 BCD*
-rwxr-xr-x  1 root root  40K Mai 22 23:41 BCD.LOG*
-rwxr-xr-x  1 root root    0 Mai 22 23:41 BCD.LOG1*
-rwxr-xr-x  1 root root    0 Mai 22 23:41 BCD.LOG2*
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 bg-BG/
-rwxr-xr-x  1 root root 1,3M Sep 20  2012 bootmgfw.efi*
-rwxr-xr-x  1 root root 1,3M Sep 20  2012 bootmgr.efi*
-rwxr-xr-x  1 root root  64K Mai 22 23:41 BOOTSTAT.DAT*
-rwxr-xr-x  1 root root 4,1K Jun 26  2012 boot.stl*
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 cs-CZ/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 da-DK/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 de-DE/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 el-GR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 en-GB/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 en-US/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 es-ES/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 et-EE/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 fi-FI/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 Fonts/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 fr-FR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 hr-HR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 hu-HU/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 it-IT/
```

```
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ja-JP/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ko-KR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 lt-LT/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 lv-LV/
-rwxr-xr-x  1 root root 1,3M Jul 25  2012 memtest.efi*
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 nb-NO/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 nl-NL/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 pl-PL/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 pt-BR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 pt-PT/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 qps-ploc/
drwxr-xr-x  4 root root 4,0K Mai 22 23:41 Resources/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ro-RO/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ru-RU/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 sk-SK/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 sl-SI/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 sr-Latn-CS/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 sv-SE/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 tr-TR/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 uk-UA/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 zh-CN/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 zh-HK/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 zh-TW/

lenovo-EFI-Partition/EFI/Microsoft/Boot/bg-BG:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/cs-CZ:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/da-DK:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/de-DE:
total 216K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/el-GR:
total 216K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  78K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  78K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  46K Jul 25  2012 memtest.efi.mui*
```

```
lenovo-EFI-Partition/EFI/Microsoft/Boot/en-GB:
total 152K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/en-US:
total 200K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/es-ES:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/et-EE:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  73K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  73K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/fi-FI:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/Fonts:
total 13M
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root 3,6M Jun  2  2012 chs_boot.ttf*
-rwxr-xr-x  1 root root 3,7M Jun  2  2012 cht_boot.ttf*
-rwxr-xr-x  1 root root 1,9M Jun  2  2012 jpn_boot.ttf*
-rwxr-xr-x  1 root root 2,3M Jun  2  2012 kor_boot.ttf*
-rwxr-xr-x  1 root root 165K Jun  2  2012 malgun_boot.ttf*
-rwxr-xr-x  1 root root 162K Jun  2  2012 malgunn_boot.ttf*
-rwxr-xr-x  1 root root 132K Jun  2  2012 meiryo_boot.ttf*
-rwxr-xr-x  1 root root 130K Jun  2  2012 meiryon_boot.ttf*
-rwxr-xr-x  1 root root 152K Jun  2  2012 msjh_boot.ttf*
-rwxr-xr-x  1 root root 150K Jun  2  2012 msjhn_boot.ttf*
-rwxr-xr-x  1 root root 143K Jun  2  2012 msyh_boot.ttf*
-rwxr-xr-x  1 root root 139K Jun  2  2012 msyhn_boot.ttf*
-rwxr-xr-x  1 root root  36K Jun  2  2012 segmono_boot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoen_slboot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoe_slboot.ttf*
-rwxr-xr-x  1 root root  47K Jun  2  2012 wgl4_boot.ttf*

lenovo-EFI-Partition/EFI/Microsoft/Boot/fr-FR:
total 216K
```

```
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/hr-HR:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/hu-HU:
total 216K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/it-IT:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/ja-JP:
total 188K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/ko-KR:
total 188K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/lt-LT:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/lv-LV:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/nb-NO:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
```

```
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/nl-NL:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/pl-PL:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/pt-BR:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/pt-PT:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/qps-ploc:
total 200K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/Resources:
total 36K
drwxr-xr-x  4 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  18K Jul 25  2012 bootres.dll*
drwxr-xr-x  2 root root 4,0K Mai 22 23:58 de-DE/
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 en-US/

lenovo-EFI-Partition/EFI/Microsoft/Boot/Resources/de-DE:
total 20K
drwxr-xr-x 2 root root 4,0K Mai 22 23:58 ./
drwxr-xr-x 4 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x 1 root root  12K Mai 22 23:57 bootres.dll.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/Resources/en-US:
total 20K
drwxr-xr-x 2 root root 4,0K Mai 22 23:41 ./
```

```
drwxr-xr-x 4 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x 1 root root  12K Jul 25  2012 bootres.dll.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/ro-RO:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/ru-RU:
total 204K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  44K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/sk-SK:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/sl-SI:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/sr-Latn-CS:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/sv-SE:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/tr-TR:
total 208K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/uk-UA:
total 160K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 25  2012 bootmgr.efi.mui*
```

```
lenovo-EFI-Partition/EFI/Microsoft/Boot/zh-CN:
total 180K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/zh-HK:
total 180K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*

lenovo-EFI-Partition/EFI/Microsoft/Boot/zh-TW:
total 180K
drwxr-xr-x  2 root root 4,0K Mai 22 23:41 ./
drwxr-xr-x 39 root root 4,0K Mai 22 23:41 ../
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 25  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 25  2012 memtest.efi.mui*
```

7.9 Auflistung aller Dateien der EFI-Partition der Medion-Plattform

```
medion-EFI-Partition/:
total 6,0K
drwxr-xr-x 3 root root 1,0K Jan  1  1970 ./
drwxr-xr-x 9 root root 4,0K Jul 19 10:43 ../
drwxr-xr-x 4 root root 1,0K Sep 13  2012 EFI/

medion-EFI-Partition/EFI:
total 4,0K
drwxr-xr-x 4 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 3 root root 1,0K Jan  1  1970 ../
drwxr-xr-x 2 root root 1,0K Sep 13  2012 Boot/
drwxr-xr-x 3 root root 1,0K Sep 13  2012 Microsoft/

medion-EFI-Partition/EFI/Boot:
total 1,3M
drwxr-xr-x 2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 4 root root 1,0K Sep 13  2012 ../
-rwxr-xr-x 1 root root 1,3M Sep 20  2012 bootx64.efi*

medion-EFI-Partition/EFI/Microsoft:
total 5,0K
drwxr-xr-x  3 root root 1,0K Sep 13  2012 ./
drwxr-xr-x  4 root root 1,0K Sep 13  2012 ../
drwxr-xr-x 39 root root 3,0K Sep 13  2012 Boot/

medion-EFI-Partition/EFI/Microsoft/Boot:
total 4,0M
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ./
drwxr-xr-x  3 root root 1,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  36K Jul 16 14:48 BCD*
-rwxr-xr-x  1 root root  28K Sep 13  2012 BCD.LOG*
-rwxr-xr-x  1 root root    0 Sep 13  2012 BCD.LOG1*
-rwxr-xr-x  1 root root    0 Sep 13  2012 BCD.LOG2*
drwxr-xr-x  2 root root 1,0K Sep 13  2012 bg-BG/
-rwxr-xr-x  1 root root 1,3M Sep 20  2012 bootmgfw.efi*
-rwxr-xr-x  1 root root 1,3M Sep 20  2012 bootmgr.efi*
-rwxr-xr-x  1 root root  64K Sep 16  2012 BOOTSTAT.DAT*
-rwxr-xr-x  1 root root 4,1K Jun 27  2012 boot.stl*
drwxr-xr-x  2 root root 1,0K Sep 13  2012 cs-CZ/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 da-DK/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 de-DE/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 el-GR/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 en-GB/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 en-US/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 es-ES/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 et-EE/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 fi-FI/
drwxr-xr-x  2 root root 2,0K Sep 13  2012 Fonts/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 fr-FR/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 hr-HR/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 hu-HU/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 it-IT/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ja-JP/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ko-KR/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 lt-LT/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 lv-LV/
-rwxr-xr-x  1 root root 1,3M Jul 26  2012 memtest.efi*
drwxr-xr-x  2 root root 1,0K Sep 13  2012 nb-NO/
```

```
drwxr-xr-x  2 root root 1,0K Sep 13  2012 nl-NL/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 pl-PL/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 pt-BR/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 pt-PT/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 qps-ploc/
drwxr-xr-x  3 root root 1,0K Sep 13  2012 Resources/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ro-RO/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ru-RU/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 sk-SK/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 sl-SI/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 sr-Latn-CS/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 sv-SE/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 tr-TR/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 uk-UA/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 zh-CN/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 zh-HK/
drwxr-xr-x  2 root root 1,0K Sep 13  2012 zh-TW/

medion-EFI-Partition/EFI/Microsoft/Boot/bg-BG:
total 156K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/cs-CZ:
total 199K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/da-DK:
total 197K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/de-DE:
total 203K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/el-GR:
total 206K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  78K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  78K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  46K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/en-GB:
total 148K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgfw.efi.mui*
```

```
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/en-US:
total 193K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/es-ES:
total 201K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/et-EE:
total 150K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  73K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  73K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/fi-FI:
total 199K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/Fonts:
total 13M
drwxr-xr-x  2 root root 2,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root 3,6M Jun  2  2012 chs_boot.ttf*
-rwxr-xr-x  1 root root 3,7M Jun  2  2012 cht_boot.ttf*
-rwxr-xr-x  1 root root 1,9M Jun  2  2012 jpn_boot.ttf*
-rwxr-xr-x  1 root root 2,3M Jun  2  2012 kor_boot.ttf*
-rwxr-xr-x  1 root root 165K Jun  2  2012 malgun_boot.ttf*
-rwxr-xr-x  1 root root 162K Jun  2  2012 malgunn_boot.ttf*
-rwxr-xr-x  1 root root 132K Jun  2  2012 meiryo_boot.ttf*
-rwxr-xr-x  1 root root 130K Jun  2  2012 meiryon_boot.ttf*
-rwxr-xr-x  1 root root 152K Jun  2  2012 msjh_boot.ttf*
-rwxr-xr-x  1 root root 150K Jun  2  2012 msjhn_boot.ttf*
-rwxr-xr-x  1 root root 143K Jun  2  2012 msyh_boot.ttf*
-rwxr-xr-x  1 root root 139K Jun  2  2012 msyhn_boot.ttf*
-rwxr-xr-x  1 root root  36K Jun  2  2012 segmono_boot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoen_slboot.ttf*
-rwxr-xr-x  1 root root  76K Jun  2  2012 segoe_slboot.ttf*
-rwxr-xr-x  1 root root  47K Jun  2  2012 wgl4_boot.ttf*

medion-EFI-Partition/EFI/Microsoft/Boot/fr-FR:
total 203K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*
```

```
medion-EFI-Partition/EFI/Microsoft/Boot/hr-HR:
total 154K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/hu-HU:
total 203K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  77K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/it-IT:
total 199K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/ja-JP:
total 178K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/ko-KR:
total 178K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  66K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/lt-LT:
total 152K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/lv-LV:
total 152K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/nb-NO:
total 197K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/nl-NL:
```

```
total 201K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/pl-PL:
total 201K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  76K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/pt-BR:
total 199K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/pt-PT:
total 199K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/qps-ploc:
total 193K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  72K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/Resources:
total 23K
drwxr-xr-x  3 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  18K Jul 25  2012 bootres.dll*
drwxr-xr-x  2 root root 1,0K Sep 13  2012 en-US/

medion-EFI-Partition/EFI/Microsoft/Boot/Resources/en-US:
total 14K
drwxr-xr-x 2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 3 root root 1,0K Sep 13  2012 ../
-rwxr-xr-x 1 root root  12K Jul 25  2012 bootres.dll.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/ro-RO:
total 152K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/ru-RU:
total 198K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
```

```
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  44K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/sk-SK:
total 154K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/sl-SI:
total 154K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/sr-Latn-CS:
total 154K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/sv-SE:
total 199K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/tr-TR:
total 197K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  74K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  45K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/uk-UA:
total 154K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  75K Jul 26  2012 bootmgr.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/zh-CN:
total 172K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/zh-HK:
total 172K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgfw.efi.mui*
```

```
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*

medion-EFI-Partition/EFI/Microsoft/Boot/zh-TW:
total 172K
drwxr-xr-x  2 root root 1,0K Sep 13  2012 ./
drwxr-xr-x 39 root root 3,0K Sep 13  2012 ../
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgfw.efi.mui*
-rwxr-xr-x  1 root root  63K Jul 26  2012 bootmgr.efi.mui*
-rwxr-xr-x  1 root root  42K Jul 26  2012 memtest.efi.mui*
```

7.10 Shim Build-In-Zertifikat für Ubuntu

Das im Folgenden aufgeführte Zertifikat ist im Shim-Binary von Ubuntu 13.04 enthalten.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 13348991040521802343 (0xb94124a0182c9267)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Isle of Man, L=Douglas, O=Canonical Ltd., CN=Canonical
Ltd. Master Certificate Authority
        Validity
            Not Before: Apr 12 11:12:51 2012 GMT
            Not After : Apr 11 11:12:51 2042 GMT
        Subject: C=GB, ST=Isle of Man, L=Douglas, O=Canonical Ltd., CN=Canonical
Ltd. Master Certificate Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bf:5b:3a:16:74:ee:21:5d:ae:61:ed:9d:56:ac:
                    bd:de:de:72:f3:dd:7e:2d:4c:62:0f:ac:c0:6d:48:
                    08:11:cf:8d:8b:fb:61:1f:27:cc:11:6e:d9:55:3d:
                    39:54:eb:40:3b:b1:bb:e2:85:34:79:ca:f7:7b:bf:
                    ba:7a:c8:10:2d:19:7d:ad:59:cf:a6:d4:e9:4e:0f:
                    da:ae:52:ea:4c:9e:90:ce:c6:99:0d:4e:67:65:78:
                    5d:f9:d1:d5:38:4a:4a:7a:8f:93:9c:7f:1a:a3:85:
                    db:ce:fa:8b:f7:c2:a2:21:2d:9b:54:41:35:10:57:
                    13:8d:6c:bc:29:06:50:4a:7e:ea:99:a9:68:a7:3b:
                    c7:07:1b:32:9e:a0:19:87:0e:79:bb:68:99:2d:7e:
                    93:52:e5:f6:eb:c9:9b:f9:2b:ed:b8:68:49:bc:d9:
                    95:50:40:5b:c5:b2:71:aa:eb:5c:57:de:71:f9:40:
                    0a:dd:5b:ac:1e:84:2d:50:1a:52:d6:e1:f3:6b:6e:
                    90:64:4f:5b:b4:eb:20:e4:61:10:da:5a:f0:ea:e4:
                    42:d7:01:c4:fe:21:1f:d9:b9:c0:54:95:42:81:52:
                    72:1f:49:64:7a:c8:6c:24:f1:08:70:0b:4d:a5:a0:
                    32:d1:a0:1c:57:a8:4d:e3:af:a5:8e:05:05:3e:10:
                    43:a1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                AD:91:99:0B:C2:2A:B1:F5:17:04:8C:23:B6:65:5A:26:8E:34:5A:63
            X509v3 Authority Key Identifier:

keyid:AD:91:99:0B:C2:2A:B1:F5:17:04:8C:23:B6:65:5A:26:8E:34:5A:63

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
```

```
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://www.canonical.com/secure-boot-master-ca.crl

    Signature Algorithm: sha256WithRSAEncryption
         3f:7d:f6:76:a5:b3:83:b4:2b:7a:d0:6d:52:1a:03:83:c4:12:
         a7:50:9c:47:92:cc:c0:94:77:82:d2:ae:57:b3:99:04:f5:32:
         3a:c6:55:1d:07:db:12:a9:56:fa:d8:d4:76:20:eb:e4:c3:51:
         db:9a:5c:9c:92:3f:18:73:da:94:6a:a1:99:38:8c:a4:88:6d:
         c1:fc:39:71:d0:74:76:16:03:3e:56:23:35:d5:55:47:5b:1a:
         1d:41:c2:d3:12:4c:dc:ff:ae:0a:92:9c:62:0a:17:01:9c:73:
         e0:5e:b1:fd:bc:d6:b5:19:11:7a:7e:cd:3e:03:7e:66:db:5b:
         a8:c9:39:48:51:ff:53:e1:9c:31:53:91:1b:3b:10:75:03:17:
         ba:e6:81:02:80:94:70:4c:46:b7:94:b0:3d:15:cd:1f:8e:02:
         e0:68:02:8f:fb:f9:47:1d:7d:a2:01:c6:07:51:c4:9a:cc:ed:
         dd:cf:a3:5d:ed:92:bb:be:d1:fd:e6:ec:1f:33:51:73:04:be:
         3c:72:b0:7d:08:f8:01:ff:98:7d:cb:9c:e0:69:39:77:25:47:
         71:88:b1:8d:27:a5:2e:a8:f7:3f:5f:80:69:97:3e:a9:f4:99:
         14:db:ce:03:0e:0b:66:c4:1c:6d:bd:b8:27:77:c1:42:94:bd:
         fc:6a:0a:bc
-----BEGIN CERTIFICATE-----
MIIENDCCAxygAwIBAgIJALlBJKAYLJJnMA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
VQQGEwJHQjEUMBIGA1UECAwLSXNsZSBvZiBNYW4xEDAOBgNVBAcMB0RvdWdsYXMx
FzAVBgNVBAoMDkNhbm9uaWNhbCBMdGQuMTQwMgYDVQQDDCtDYW5vbmljYWwgTHRk
LiBNYXN0ZXIgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4XDTEyMDQxMjExMTI1MVoX
DTQyMDQxMTExMTI1MVowgYQxCzAJBgNVBAYTAkdCMRQwEgYDVQQIDAtJc2xlIG9m
IE1hbjEQMA4GA1UEBwwHRG91Z2xhczEXMBUGA1UECgwOQ2Fub25pY2FsIEx0ZC4x
NDAyBgNVBAMMK0Nhbm9uaWNhbCBMdGQuIE1hc3RlciBDZXJ0aWZpY2F0ZSBBdXRo
b3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC/WzoWdO4hXa5h
7Z1WrL3e3nLz3X4tTGIPrMBtSAgRz42L+2EfJ8wRbtlVPTlU60A7sbvihTR5yvd7
v7p6yBAtGX2tWc+m1OlOD9quUupMnpDOxpkNTmdleF350dU4Skp6j5OcfxqjhdvO
+ov3wqIhLZtUQTUQVxONbLwpBlBKfuqZqWinO8cHGzKeoBmHDnm7aJktfpNS5fbr
yZv5K+24aEm82ZVQQFvFsnGq61xX3nH5QArdW6wehC1QGlLW4fNrbpBkT1u06yDk
YRDaWvDq5ELXAcT+IR/ZucBUlUKBUnIfSWR6yGwk8QhwC02loDLRoBxXqE3jr6WO
BQU+EEOhAgMBAAGjgaYwgaMwHQYDVR0OBBYEFK2RmQvCKrH1FwSMI7ZlWiaONFpj
MB8GA1UdIwQYMBaAFK2RmQvCKrH1FwSMI7ZlWiaONFpjMA8GA1UdEwEB/wQFMAMB
Af8wCwYDVR0PBAQDAgGGMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly93d3cuY2Fu
b25pY2FsLmNvbS9zZWN1cmUtYm9vdC1tYXN0ZXItY2EuY3JsMA0GCSqGSIb3DQEB
CwUAA4IBAQA/ffZ2pbODtCt60G1SGgODxBKnUJxHkszAlHeC0q5Xs5kE9TI6xlUd
B9sSqVb62NR2IOvkw1Hbmlyckj8Yc9qUaqGZOIykiG3B/Dlx0HR2FgM+ViM11VVH
WxodQcLTEkzc/64KkpxiChcBnHPgXrH9vNa1GRF6fs0+A35m21uoyTlIUf9T4Zwx
U5EbOxB1Axe65oECgJRwTEa3lLA9Fc0fjgLgaAKP+/lHHX2iAcYHUcSazO3dz6Nd
7ZK7vtH95uwfM1FzBL48crB9CPgB/5h9y5zgaTl3JUdxiLGNJ6UuqPc/X4Bplz6p
9JkU284DDgtmxBxtvbgnd8FClL38agq8
-----END CERTIFICATE-----
```

7.11 Shim Build-In-Zertifikat für Fedora

Das im Folgenden aufgeführte Zertifikat ist im Shim-Binary von Red Hat Fedora 19 enthalten.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2574709492 (0x9976f2f4)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Fedora Secure Boot CA
        Validity
            Not Before: Dec  7 16:25:54 2012 GMT
            Not After : Dec  5 16:25:54 2022 GMT
        Subject: CN=Fedora Secure Boot CA
```

```
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ae:f5:f7:52:81:a9:5c:3e:2b:f7:1d:55:f4:5a:
                    68:84:2d:bc:8b:76:96:85:0d:27:b8:18:a5:cd:c1:
                    83:b2:8c:27:5d:23:0a:d1:12:0a:75:98:a2:e6:5d:
                    01:8a:f4:d9:9f:fc:70:bc:c3:c4:17:7b:02:b5:13:
                    c4:51:92:e0:c0:05:74:b9:2e:3d:24:78:a0:79:73:
                    94:c0:c2:2b:b2:82:a7:f4:ab:67:4a:22:f3:64:cd:
                    c3:f9:0c:26:01:bf:1b:d5:3d:39:bf:c9:fa:fb:5e:
                    52:b9:a4:48:fb:13:bf:87:29:0a:64:ef:21:7b:bc:
                    1e:16:7b:88:4f:f1:40:2b:d9:22:15:47:4e:84:f6:
                    24:1c:4d:53:16:5a:b1:29:bb:5e:7d:7f:c0:d4:e2:
                    d5:79:af:59:73:02:dc:b7:48:bf:ae:2b:70:c1:fa:
                    74:7f:79:f5:ee:23:d0:03:05:b1:79:18:4f:fd:4f:
                    2f:e2:63:19:4d:77:ba:c1:2c:8b:b3:d9:05:2e:d9:
                    d8:b6:51:13:bf:ce:36:67:97:e4:ad:58:56:07:ab:
                    d0:8c:66:12:49:dc:91:68:b4:c8:ea:dd:9c:c0:81:
                    c6:91:5b:db:12:78:db:ff:c1:af:08:16:fc:70:13:
                    97:5b:57:ad:6b:44:98:7e:1f:ec:ed:46:66:95:0f:
                    05:55
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                CA Issuers -
URI:https://fedoraproject.org/wiki/Features/SecureBoot

            X509v3 Authority Key Identifier:

keyid:FD:E3:25:99:C2:D6:1D:B1:BF:58:07:33:5D:7B:20:E4:CD:96:3B:42

            X509v3 Extended Key Usage:
                Code Signing
            X509v3 Subject Key Identifier:
                FD:E3:25:99:C2:D6:1D:B1:BF:58:07:33:5D:7B:20:E4:CD:96:3B:42
    Signature Algorithm: sha256WithRSAEncryption
         37:77:f0:3a:41:a2:1c:9f:71:3b:d6:9b:95:b5:15:df:4a:b6:
         f4:d1:51:ba:0d:04:da:9c:b2:23:f0:f3:34:59:8d:b8:d4:9a:
         75:74:65:80:17:61:3a:c1:96:7f:a7:c1:2b:d3:1a:d6:60:3c:
         71:3a:a4:c4:e3:39:03:02:15:12:08:1f:4e:cd:97:50:f8:ff:
         50:cc:b6:3e:03:7d:7a:e7:82:7a:c2:67:be:c9:0e:11:0f:16:
         2e:1e:a9:f2:6e:fe:04:bd:ea:9e:f4:a9:b3:d9:d4:61:57:08:
         87:c4:98:d8:a2:99:64:de:15:54:8d:57:79:14:1f:fa:0d:4d:
         6b:cd:98:35:f5:0c:06:bd:f3:31:d6:fe:05:1f:60:90:b6:1e:
         10:f7:24:e0:3c:f6:33:50:cd:44:c2:71:18:51:bd:18:31:81:
         1e:32:e1:e6:9f:f9:9c:02:53:b4:e5:6a:41:d6:65:b4:2e:f1:
         cf:b3:b8:82:b0:a3:96:e2:24:d8:83:ae:06:5b:b3:24:74:4d:
         d1:a4:0a:1d:0a:32:1b:75:a2:96:d1:0e:3e:e1:30:c3:18:e8:
         cb:53:c4:0b:00:ad:7e:ad:c8:49:41:ef:97:69:bd:13:5f:ef:
         ef:3c:da:60:05:d8:92:fc:da:6a:ea:48:3f:0e:3e:73:77:fd:
         a6:89:e9:3f
-----BEGIN CERTIFICATE-----
MIIDaDCCAlCgAwIBAgIFAJl28vQwDQYJKoZIhvcNAQELBQAwIDEeMBwGA1UEAxMV
RmVkb3JhIFNlY3VyZSBCb290IENBMB4XDTEyMTIwNzE2MjU1NFoXDTIyMTIwNTE2
MjU1NFowIDEeMBwGA1UEAxMVRmVkb3JhIFNlY3VyZSBCb290IENBMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArvX3UoGpXD4r9x1V9FpohC28i3aWhQ0n
uBilzcGDsownXSMK0RIKdZii5l0BivTZn/xwvMPEF3sCtRPEUZLgwAV0uS49JHig
eXOUwMIrsoKn9KtnSiLzZM3D+QwmAb8b1T05v8n6+15SuaRI+xO/hykKZO8he7we
FnuIT/FAK9kiFUdOhPYkHE1TFlqxKbtefX/A1OLVea9ZcwLct0i/ritwwfp0f3n1
7iPQAwWxeRhP/U8v4mMZTXe6wSyLs9kFLtnYtlETv842Z5fkrVhWB6vQjGYSSdyR
aLTI6t2cwIHGkVvbEnjb/8GvCBb8cBOXW1eta0SYfh/s7UZmlQ8FVQIDAQABo4Go
```

```
MIGlME4GCCsGAQUFBwEBBEIwQDA+BggrBgEFBQcwAoYyaHR0cHM6Ly9mZWRvcmFw
cm9qZWN0Lm9yZy93aWtpL0ZlYXR1cmVzL1NlY3VyZUJvb3QwHwYDVR0jBBgwFoAU
/eMlmcLWHbG/WAczXXsg5M2WO0IwEwYDVR0lBAwwCgYIKwYBBQUHAwMwHQYDVR0O
BBYEFP3jJZnC1h2xv1gHM117IOTNljtCMA0GCSqGSIb3DQEBCwUAA4IBAQA3d/A6
QaIcn3E71puVtRXfSrb00VG6DQTanLIj8PM0WY241Jp1dGWAF2E6wZZ/p8Er0xrW
YDxxOqTE4zkDAhUSCB9OzZdQ+P9QzLY+A31654J6wme+yQ4RDxYuHqnybv4Eveqe
9Kmz2dRhVwiHxJjYoplk3hVUjVd5FB/6DU1rzZg19QwGvfMx1v4FH2CQth4Q9yTg
PPYzUM1EwnEYUb0YMYEeMuHmn/mcAlO05WpB1mW0LvHPs7iCsKOW4iTYg64GW7Mk
dE3RpAodCjIbdaKW0Q4+4TDDGOjLU8QLAK1+rchJQe+Xab0TX+/vPNpgBdiS/Npq
6kg/Dj5zd/2miek/
-----END CERTIFICATE-----
```