presented by

Implementing Secure Boot:

A Refresher on Key & Database Configuration

UEFI PlugFest– March 18-22, 2013
Presented by Tim Lewis, CTO, Insyde Software

Agenda

- Securing the boot process
- Why we need Secure Boot
- The engineering of the secure boot feature
- Is my platform ready?

Much Progress in 2012

Window 8 and Windows Server 2012 Launched

“I would add that security improvements alone may justify the purchase for many enterprises. […] Like Windows 8, Windows Server 2012 has replaced the traditional ROM-BIOS with the new and improved industry boot standard known as UEFI using the security-hardened 2.3.1 version.”

Roger Grimes, infoworld.com

UEFI Versions of Fedora and Ubuntu Launched

“UEFI would provide a foundation for a chain of trust that would connect all the way up to the software layer, which could thwart attempts to install illicit, and harmful, software on [Linux] computers.”

Joab Jackson, pcworld.com

Ecosystem Ready for Secure Boot

System Firmware
OpRom Firmware

System Boards
Add-in Cards

Recovery Software
Operating Systems

Benefits of Secure Boot

- UEFI Boot inherently has lots of value
  - Support for large disk drives
  - Support for complex partition structures
  - Rich Network support including IPv6
  - Better PXE provisioning and boot from iSCSI
  - Better Error Reporting and Management Tools

- But UEFI Boot needs Secure Boot to lock down access to the critical boot files

Project Planning is Critical

– Benefits of a hardened system boot are clear, but…

– Secure products require selecting partners that prioritize security, starting in the firmware, and continuing throughout the boot process.

Partners can help you reach your security goals!

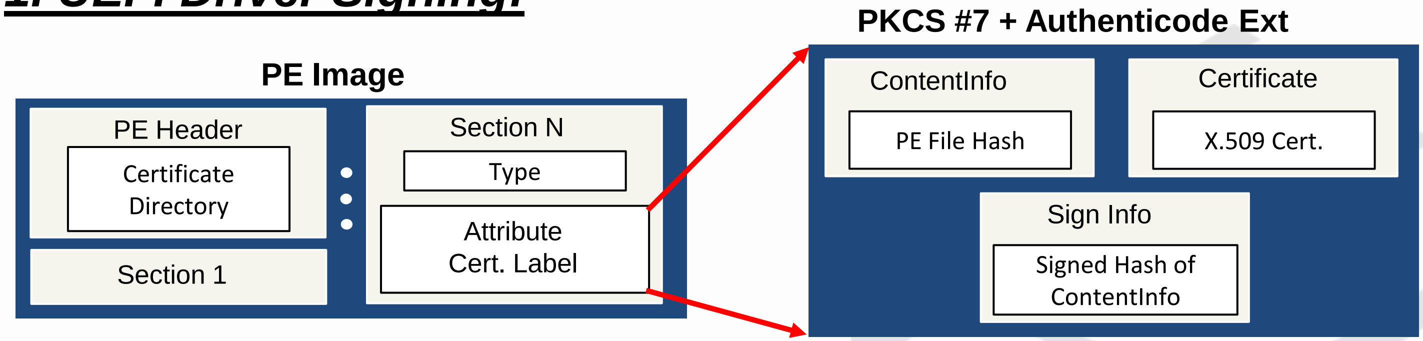
Quick Review – What is Secure Boot?

- UEFI Secure Boot is a technology to eliminate a major security hole during handoff from UEFI firmware to UEFI OS
- Option ROMs and OS boot loaders need to be signed by private key corresponding to a certificate in the systems Security Database
- Database is always provisioned at factory and maintained by OS if required for revocation.

UEFI Firmware
UEFI OS

Secure Boot – Step by Step

1. UEFI Driver Signing:



PKCS #7 + Authenticode Ext

ContentInfo

PE File Hash

Certificate

X.509 Cert.

Sign Info

Signed Hash of ContentInfo

PE Image

PE Header

Certificate Directory

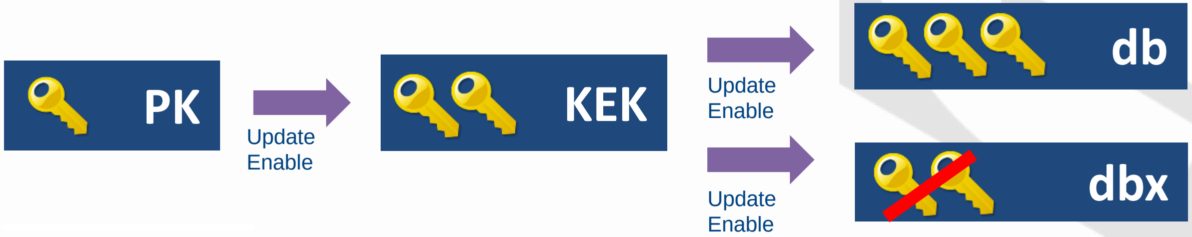
Section 1

Section N

Type

Attribute Cert. Label

2. UEFI Secure Boot Database:



PK

Update Enable

KEK

Update Enable

db

Update Enable

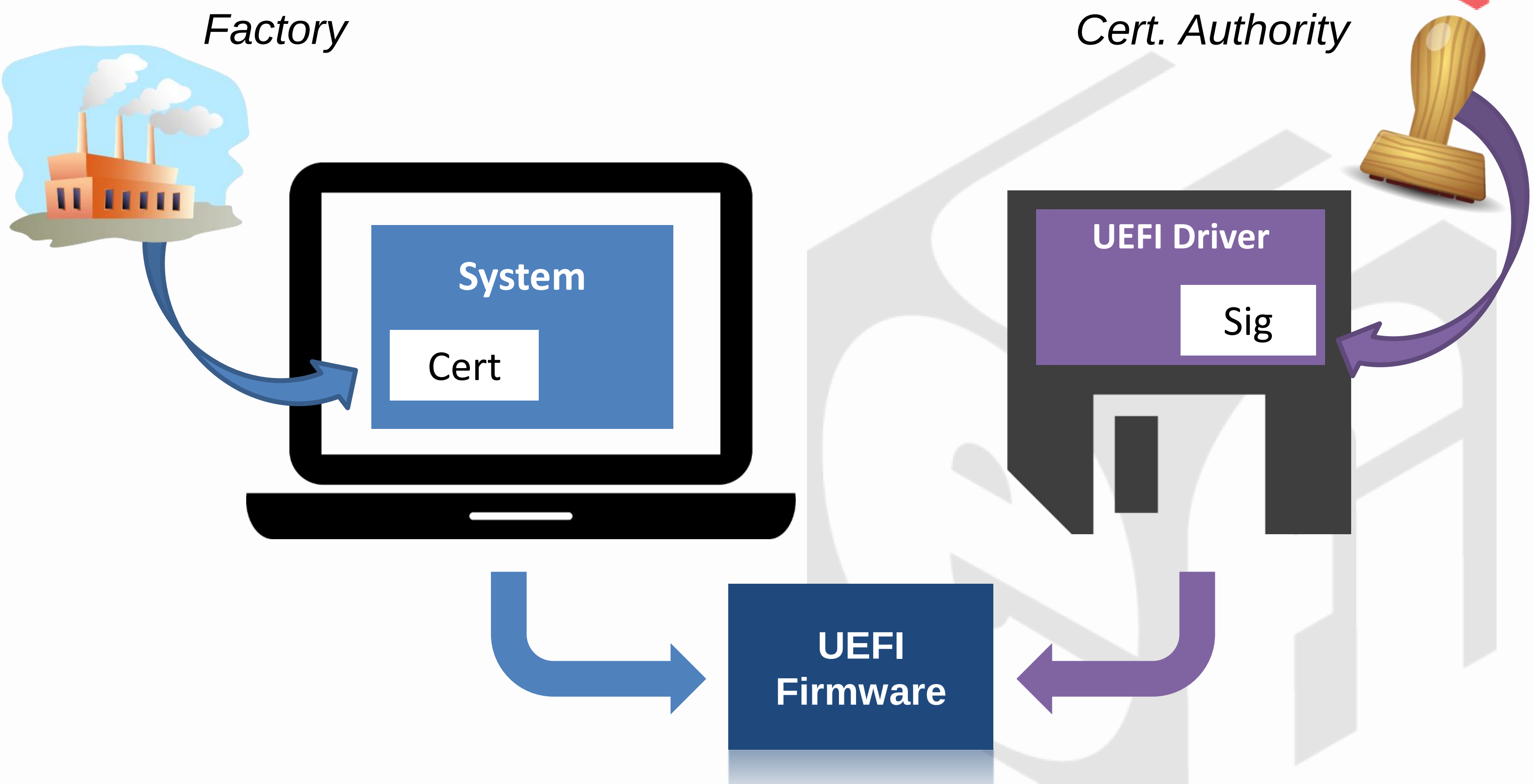
dbx

If Signed by key in db, driver or loader can Run!

If Signed by key in dbx, driver/loader forbidden!

Secure Boot – Step by Step

3. Platform does UEFI Driver Checking:



Firmware compares signature to database and if it matches, drivers are approved.

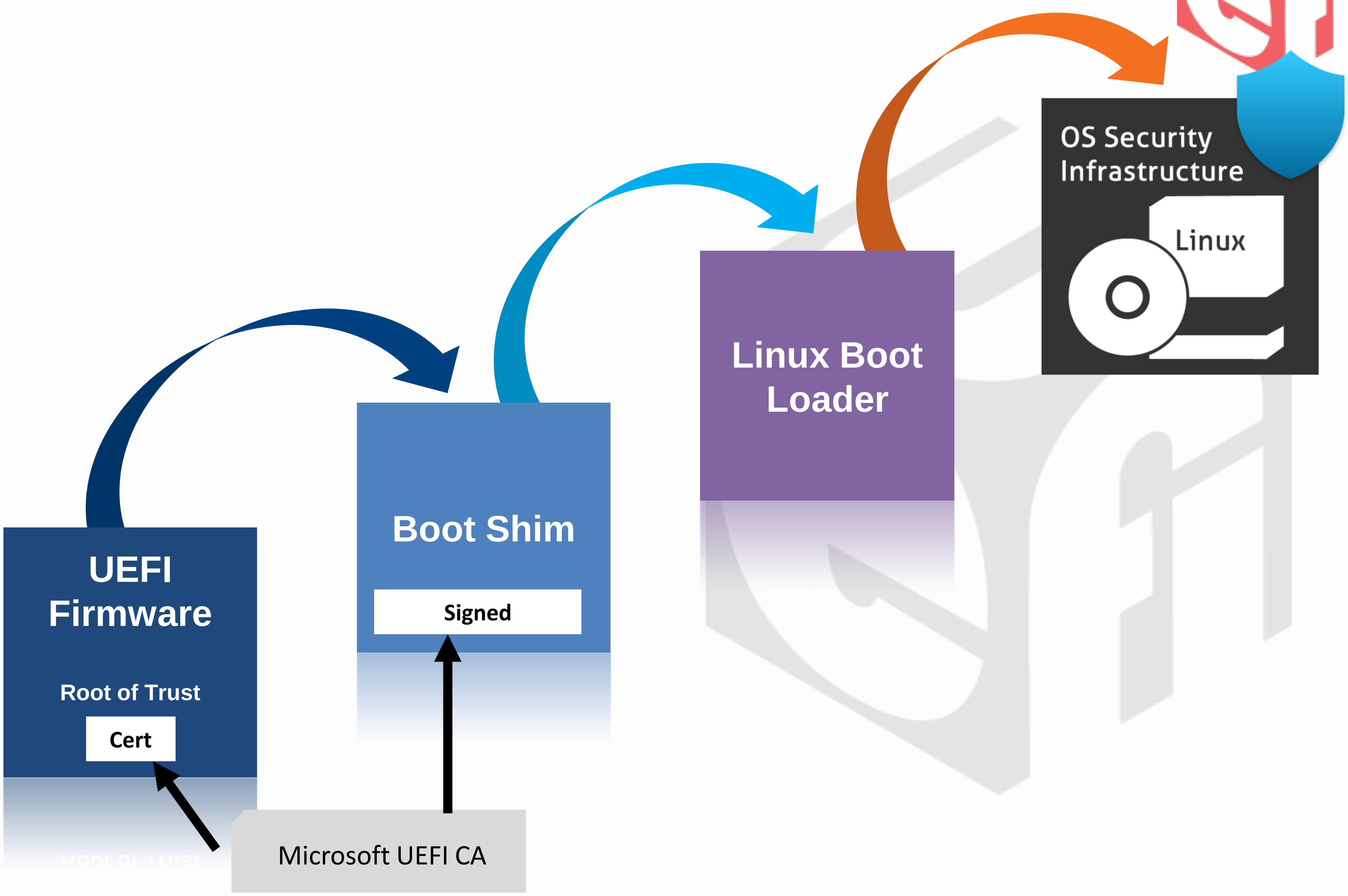
Microsoft CA

- UEFI Option ROMs need to be signed by a widely trusted Certificate Authority
- Microsoft has CA experience and volunteered to host the first all-industry UEFI CA
- Manufacturers are encouraged to put MS CA certificate into “Allowed” database
- Microsoft policies are non-discriminatory, for example Microsoft CA signed the Linux ‘Shim’ boot driver
- Could there emerge another trusted CA?

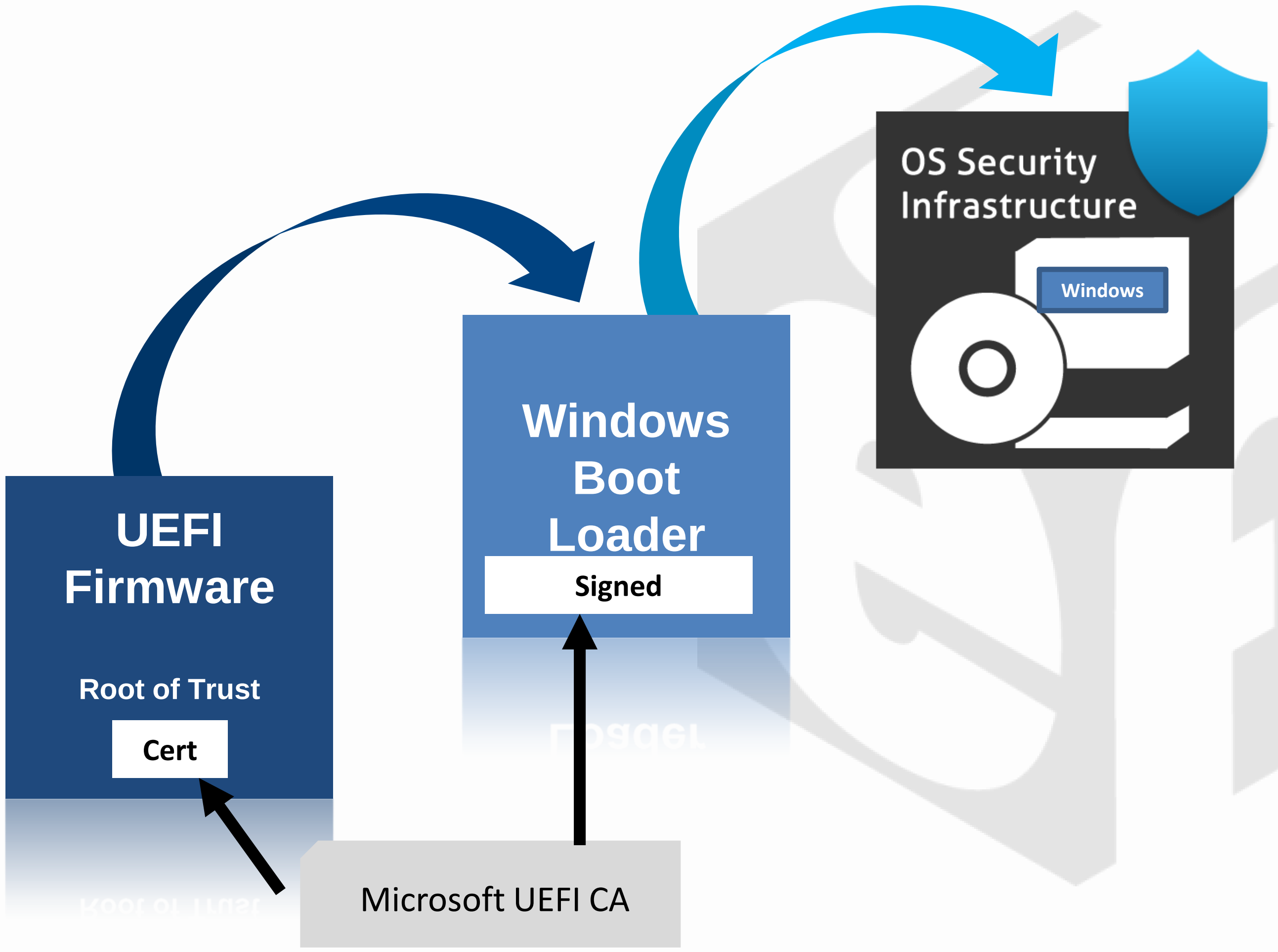
  - Possible, plenty of room in the database

  - Need to convince OEMs to include

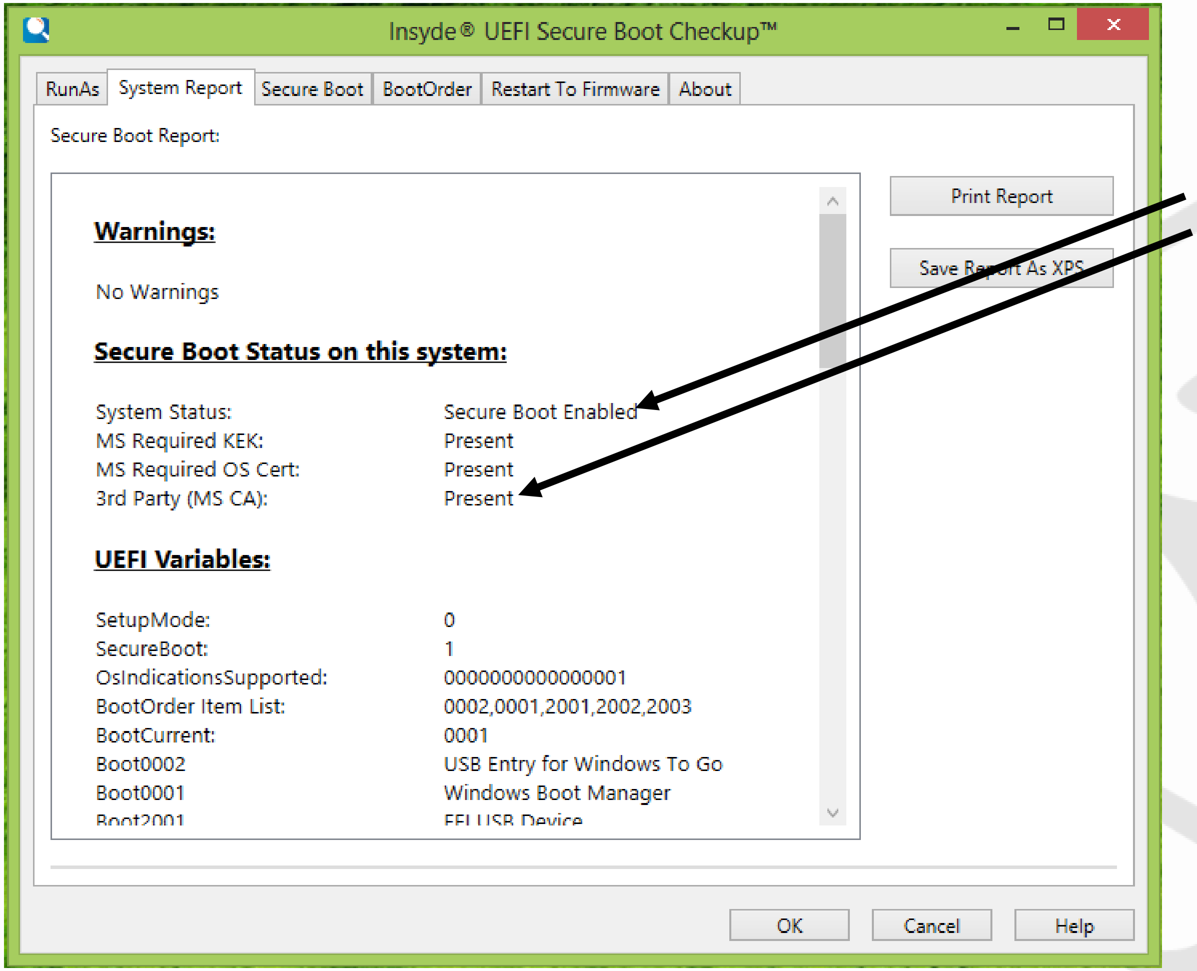
Secure Boot, Linux, & Chain of Trust



Secure Boot, Windows, & Chain of Trust



DEMO #1 – Is my System Ready?



Secure Boot Report:

Warnings:

No Warnings

Secure Boot Status on this system:

```
System Status:            Secure Boot Enabled
MS Required KEK:          Present
MS Required OS Cert:      Present
3rd Party (MS CA):        Present
```

UEFI Variables:

```
SetupMode:                0
SecureBoot:               1
OsIndicationsSupported:   0000000000000001
BootOrder Item List:      0002,0001,2001,2002,2003
BootCurrent:              0001
Boot0002                  USB Entry for Windows To Go
Boot0001                  Windows Boot Manager
Boot2001                  EFI USB Device
```

1. Secure Boot Enabled
2. MS CA Cert Present

Sign up for beta copy at: **appsupport@insyde.com**

Goals for UEFI Forum in 2013 and Beyond

- Progress toward wide adoption is an important goal!
- Also launching UEFI-style Secure Firmware Update for smoother user experience

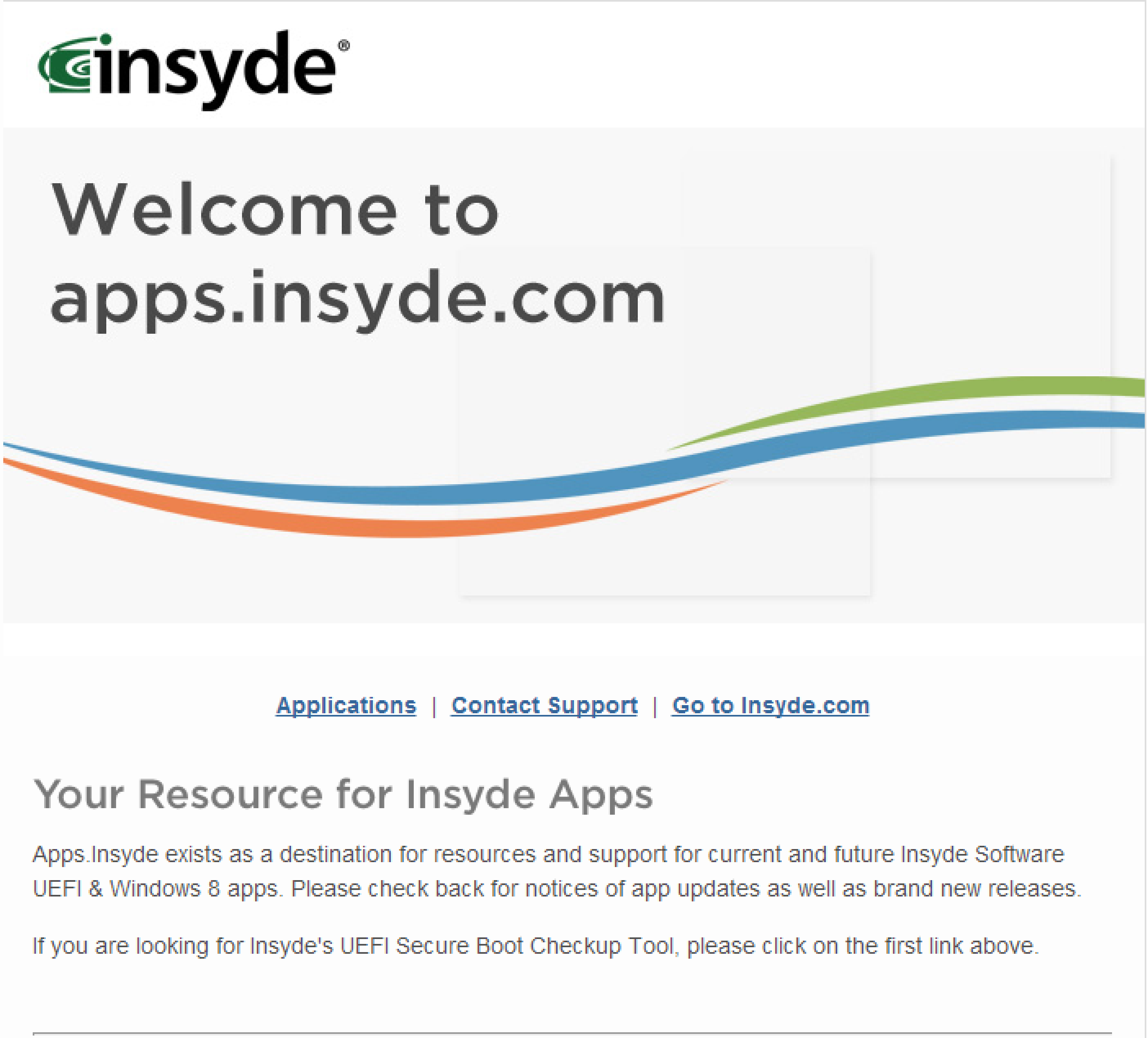
- To achieve this UEFI community promises:
  - Attention to all elements of the ecosystem
    - Systems, expansion cards, firmware and OS
  - Education on the benefits
  - Responsive to the needs of each segment

Thanks for attending the UEFI Spring PlugFest 2013

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

insyde®



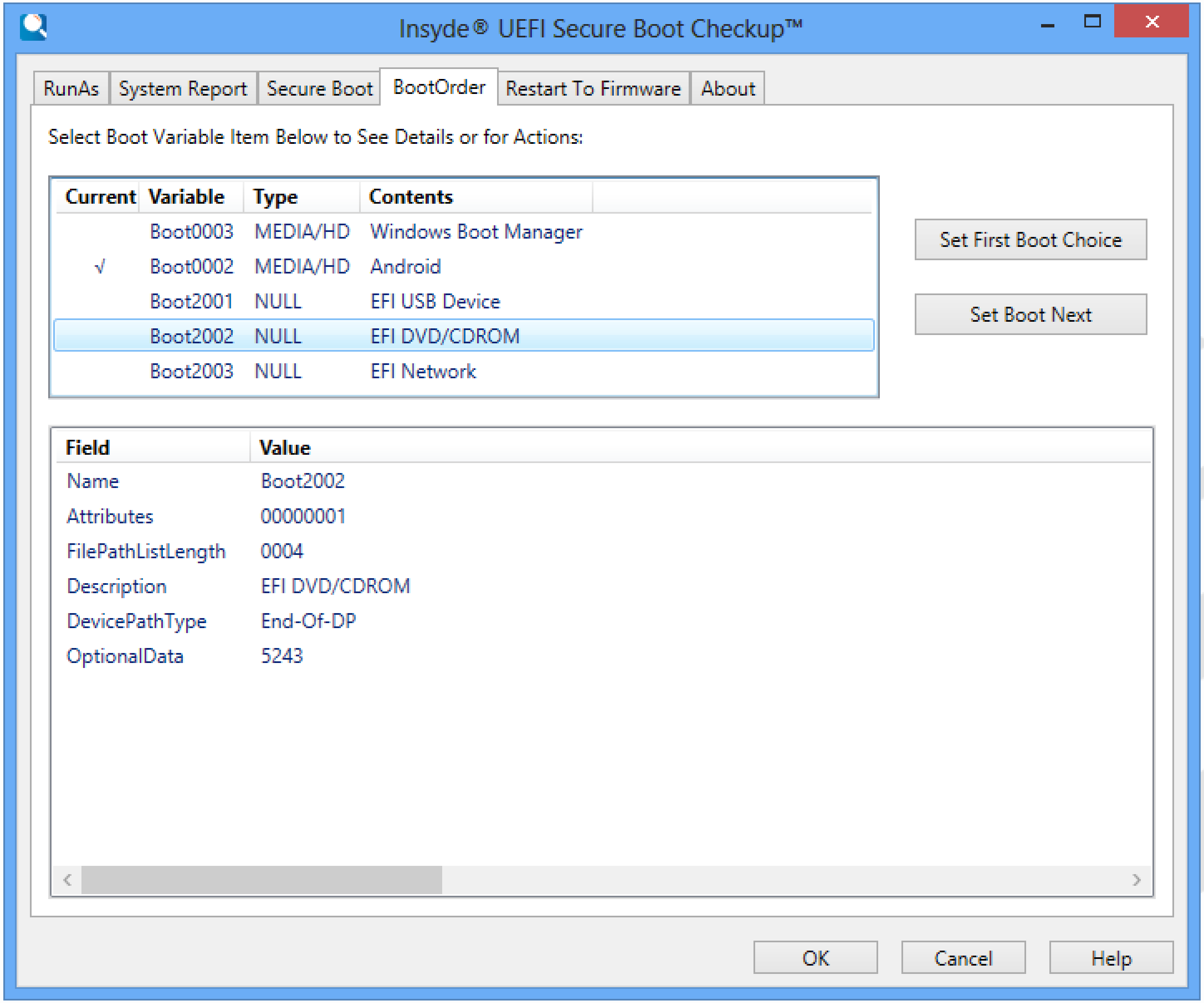
Welcome to apps.insyde.com

Applications | Contact Support | Go to Insyde.com

Your Resource for Insyde Apps

Apps.Insyde exists as a destination for resources and support for current and future Insyde Software UEFI & Windows 8 apps. Please check back for notices of app updates as well as brand new releases.

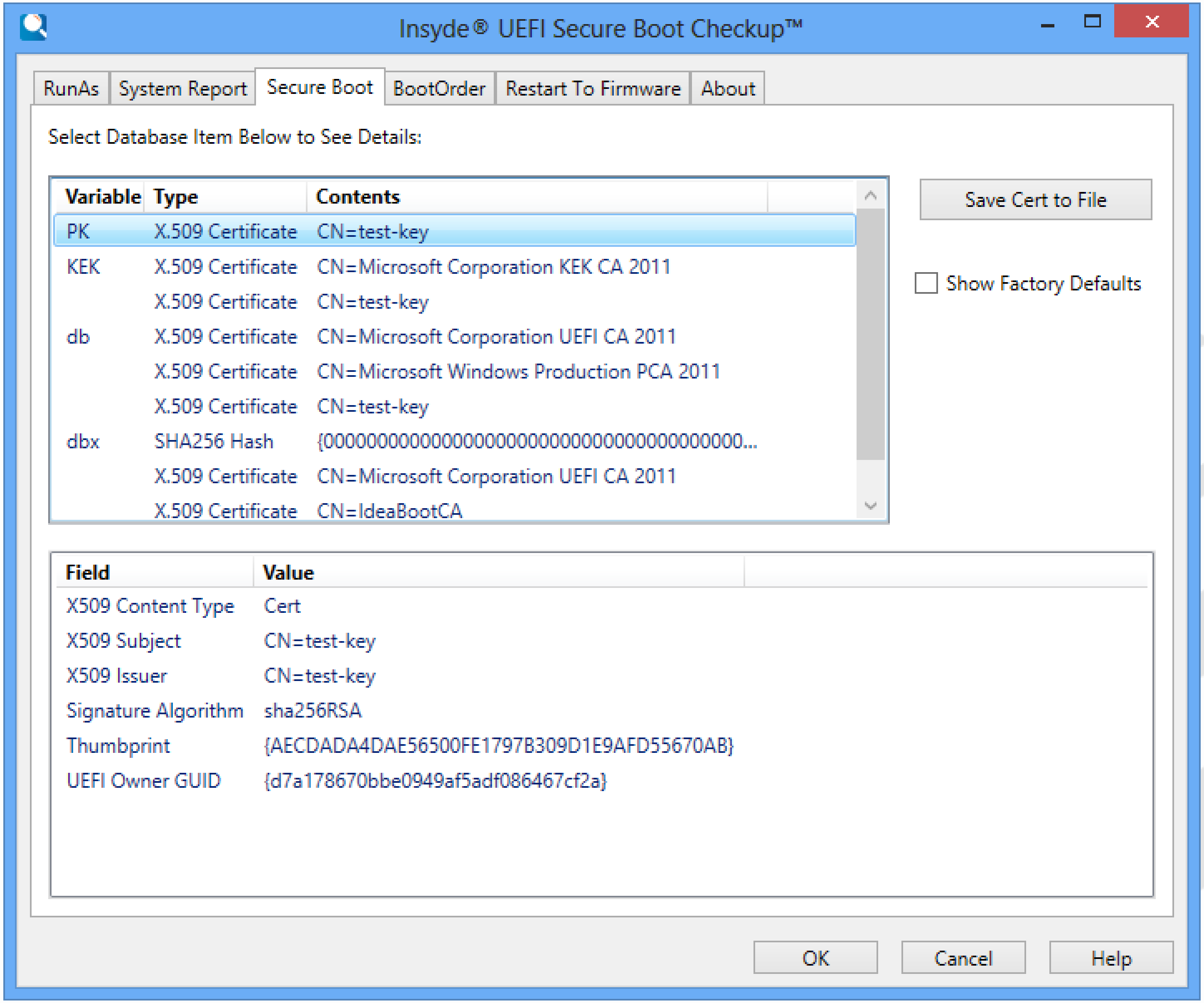
If you are looking for Insyde's UEFI Secure Boot Checkup Tool, please click on the first link above.



Select Boot Variable Item Below to See Details or for Actions:

Current	Variable	Type	Contents
	Boot0003	MEDIA/HD	Windows Boot Manager
√	Boot0002	MEDIA/HD	Android
	Boot2001	NULL	EFI USB Device
	Boot2002	NULL	EFI DVD/CDROM
	Boot2003	NULL	EFI Network

Field	Value
Name	Boot2002
Attributes	00000001
FilePathListLength	0004
Description	EFI DVD/CDROM
DevicePathType	End-Of-DP
OptionalData	5243

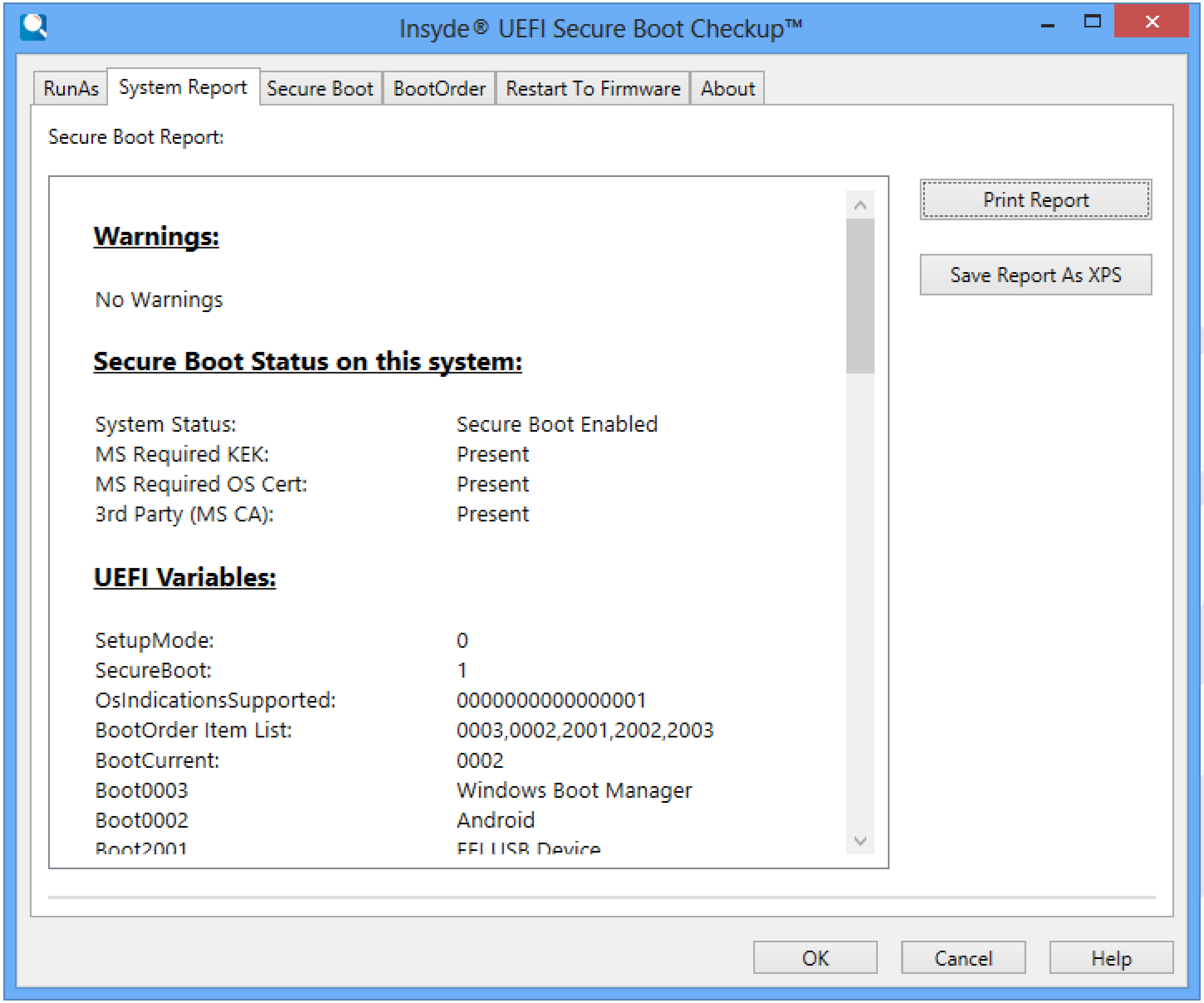


Select Database Item Below to See Details:

Variable	Type	Contents
PK	X.509 Certificate	CN=test-key
KEK	X.509 Certificate	CN=Microsoft Corporation KEK CA 2011
	X.509 Certificate	CN=test-key
db	X.509 Certificate	CN=Microsoft Corporation UEFI CA 2011
	X.509 Certificate	CN=Microsoft Windows Production PCA 2011
	X.509 Certificate	CN=test-key
dbx	SHA256 Hash	{00000000000000000000000000000000000000...
	X.509 Certificate	CN=Microsoft Corporation UEFI CA 2011
	X.509 Certificate	CN=IdeaBootCA

□ Show Factory Defaults

Field	Value
X509 Content Type	Cert
X509 Subject	CN=test-key
X509 Issuer	CN=test-key
Signature Algorithm	sha256RSA
Thumbprint	{AECDADA4DAE56500FE1797B309D1E9AFD55670AB}
UEFI Owner GUID	{d7a178670bbe0949af5adf086467cf2a}



Secure Boot Report:

Warnings:

No Warnings

Secure Boot Status on this system:

```
System Status:              Secure Boot Enabled
MS Required KEK:            Present
MS Required OS Cert:        Present
3rd Party (MS CA):          Present
```

UEFI Variables:

```
SetupMode:                  0
SecureBoot:                 1
OsIndicationsSupported:     0000000000000001
BootOrder Item List:        0003,0002,2001,2002,2003
BootCurrent:                0002
Boot0003                    Windows Boot Manager
Boot0002                    Android
Boot2001                    EFI USB Device
```