presented by

Secure Boot Factory Tools

UEFI Spring Plugfest – May 8-10, 2012
Presented by Kevin Davis
VP of Engineering, Core Development
Insyde Software

Agenda

- Secure Boot Factory Tools
- Secure Firmware Updates
- Summary

Secure Boot Factory Tools

UEFI 2.3.1 Secure Boot Begins at the Factory

1 Pre-Production

Certificate Generating Station @ OEM

2 Production

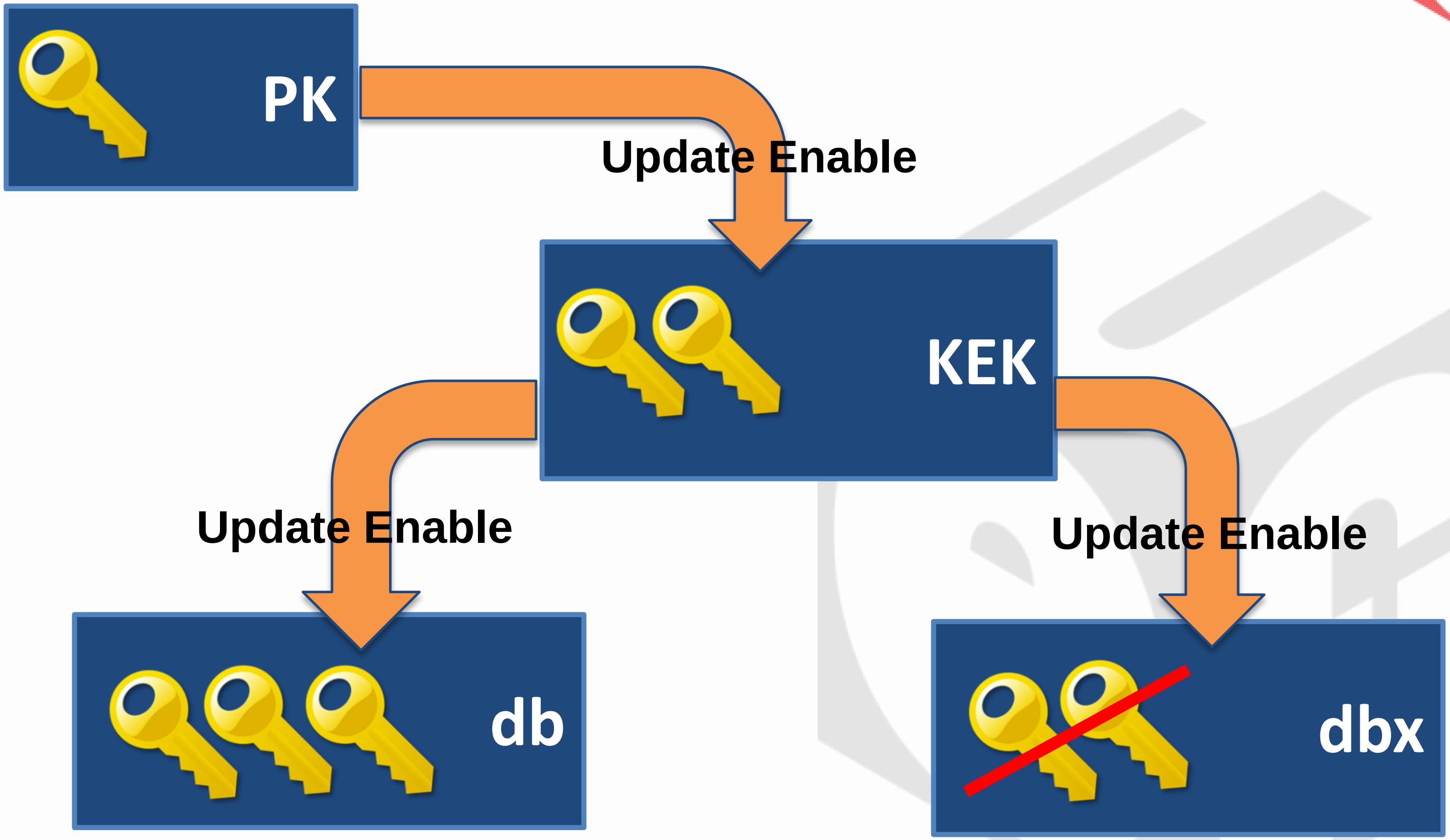
Initial Security Load

3 Protected User

Every New System receives Initial Security Database

OEM is Responsible for Initializing Secure Boot

UEFI Secure Boot Database Review



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

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

Public vs. Private Keys

- A pair of keys, one public, one private, are created
- Private keys stay secure at Partner or in the OEM's Security Office
- Private keys are used to 'sign' objects
- Only Public keys loaded into the Platform
- Public keys are used to check signatures

Public
Private

Private Keys Must be Stored Securely!

Who "Owns" The System Security Keys?

- PK – Key pair is created by Platform Manufacturer
  Typically one PK pair used for a model or model Line
- KEK – Key supplied by OS Partner,
  Optional: Include 2nd key created by OEM
- db – OS Partner supplies Key,
  CA Partner supplies Key,
  Optional: OEM App Signing Key

Signature Tests using db Keys Block Rogue S/W!

OEM Administration

- Keys are installed for testing with target OS
- Keys are installed in the factory before shipping

- **Preparation Tasks**

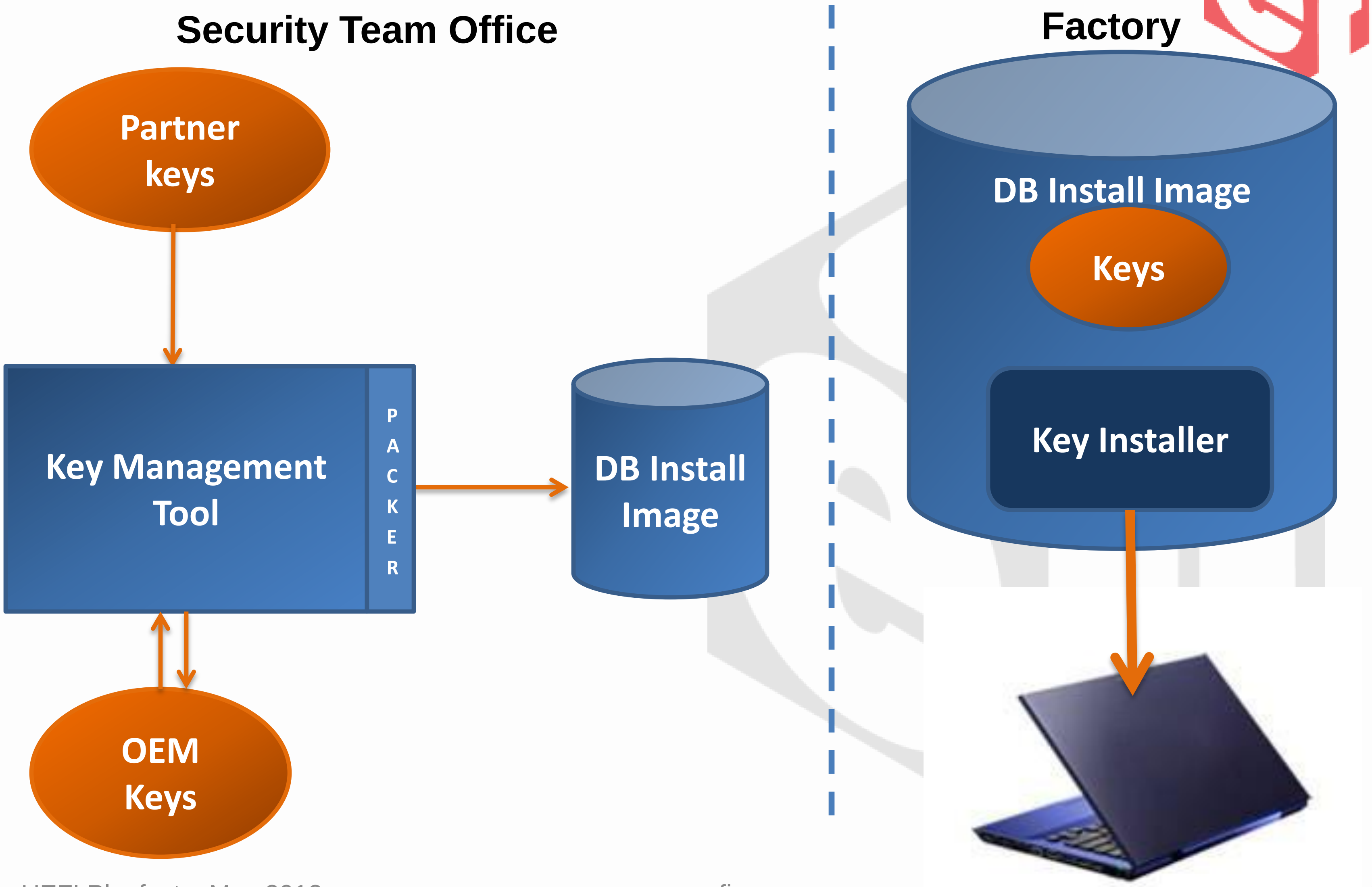
1. Gather public keys from partners
2. Generate PK for model
3. Make a package of initial key load
4. Occasional maintenance of forbidden list

- **Repetitive Tasks**

1. Factory will boot and install the initial key load

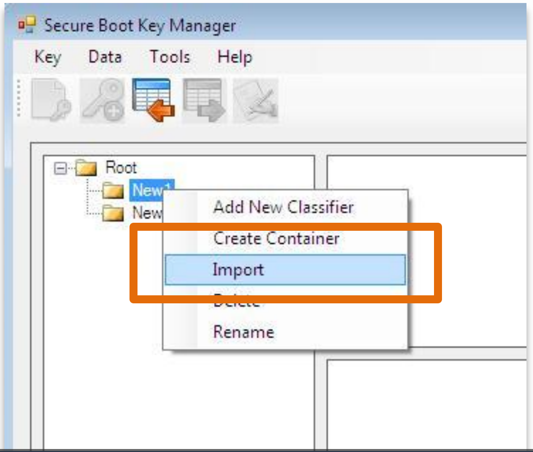
Careful Preparation Delivers Successful Launch

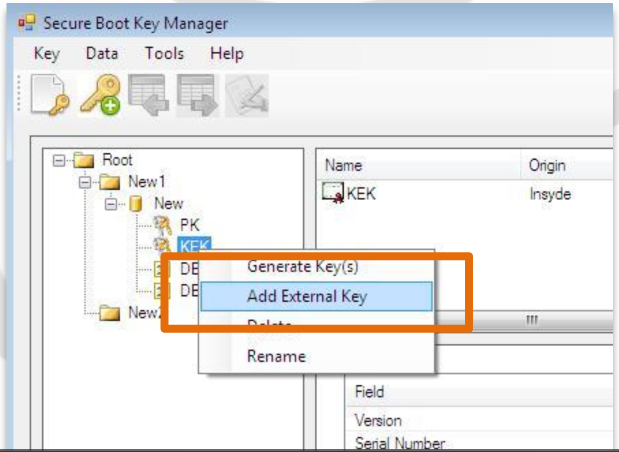
Major Components of the Tool Set



Key Generator and Management Tool

- InsydeH2O® Key Manager Imports
  - Partner’s KEKpub
  - Public signing keys for db (example Microsoft Signing Authority, Windows Signing key, OEM signing authority)
  - Current Revoked keys or hash list for dbx

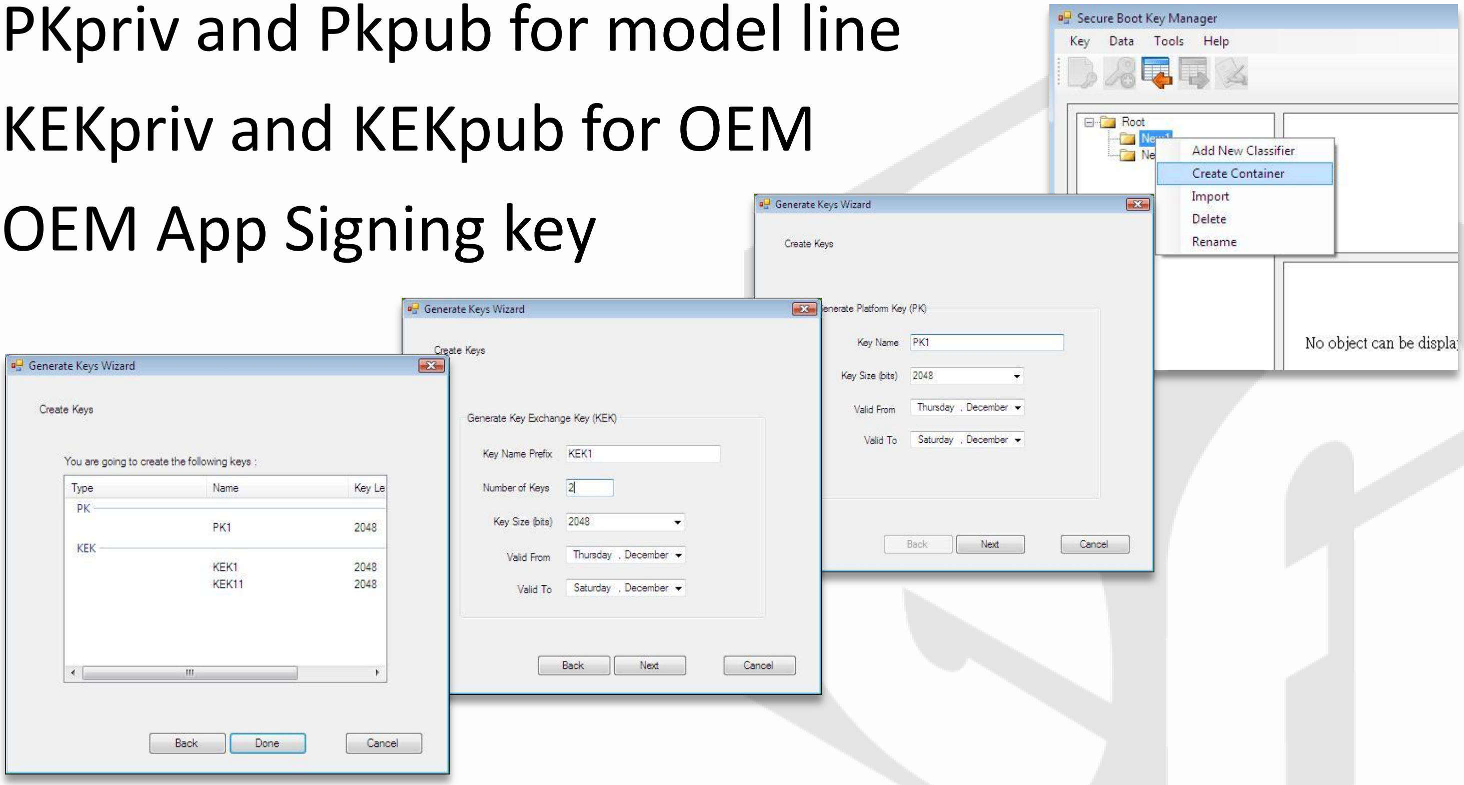




Key Manager Organizes Database Prep

Key Generator and Management Tool

- Use Key Manager to Create:
  - PKpriv and Pkpub for model line
  - KEKpriv and KEKpub for OEM
  - OEM App Signing key



No object can be displa

Create Keys

enerate Platform Key (PK)

Key Name: PK1

Key Size (bits): 2048

Valid From: Thursday , December

Valid To: Saturday , December

Create Keys

Generate Key Exchange Key (KEK)

Key Name Prefix: KEK1

Number of Keys: 2

Key Size (bits): 2048

Valid From: Thursday , December

Valid To: Saturday , December

Create Keys

You are going to create the following keys :

Type	Name	Key Le
PK		
	PK1	2048
KEK		
	KEK1	2048
	KEK11	2048

Key Manager Creates OEM Required Keys

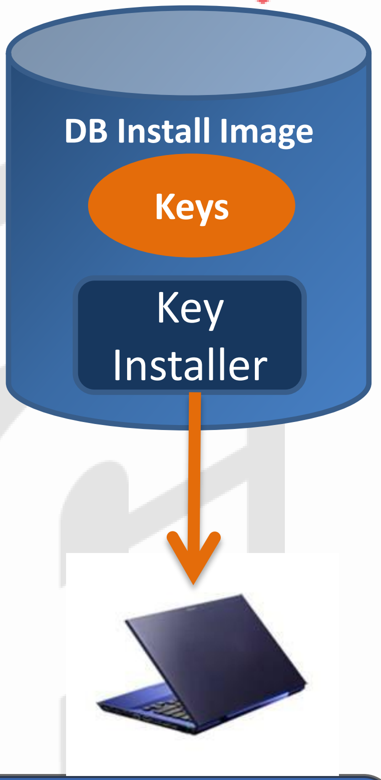
Insyde Factory Install Image File

(1) Key Installer

- Runs in WIN8 or WINPE
- Checks it's own integrity
- Installs the Secure Keys

(2) Initial Database Image

- PK – System Master Key
- KEK – OEM and Partner Management Keys
- db – Industry Recognized Driver/app signing Keys
- dbx – Revoked signing keys



Single Signed Installer File Means No Opportunity for Factory Tampering

Secure Boot Factory Tools

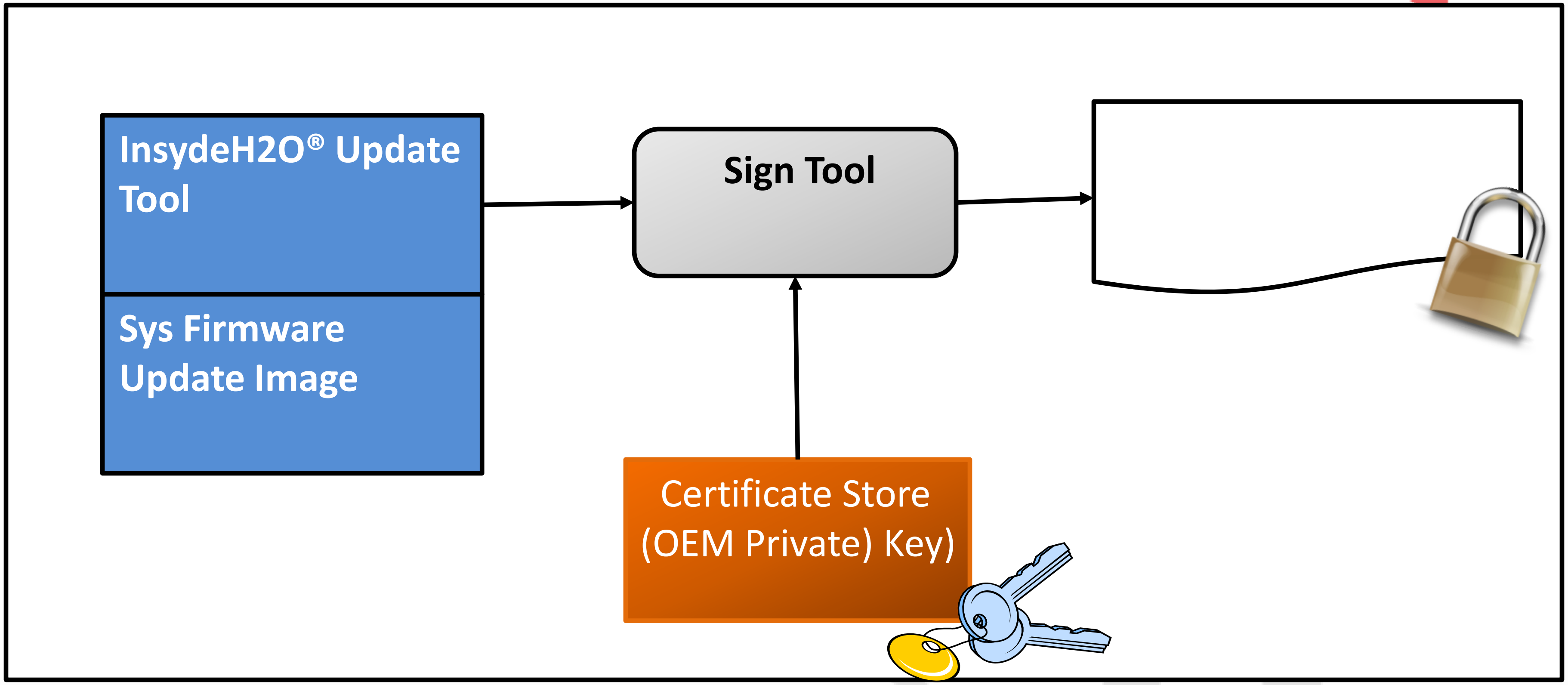
Secure Firmware Updates

Secure Field Update to Firmware Store

- Field Firmware Update must support all elements of NIST 800-147 Recommendations
  - Any update to the firmware flash store but be signed by creator
  - Firmware must check signature of the update
  - Firmware updates are signed by another key – not PK
  - Policy must remain in effect even if Secure Boot Database is cleared by user

All Firmware Updates Must be Signed at Factory

Signing Firmware Update Files:


InsydeH2O® Update Tool
Sys Firmware Update Image
Sign Tool
Certificate Store (OEM Private) Key)

InsydeH2O® Secure Update Meets NIST Requirements

Secure Boot Factory Tools

Summary

Summary

- UEFI 2.3.1. adoption will start in 2012
- Secure Boot with UEFI 2.3.1 can be fast and secure
- Factory tools for key insertion can be fast and efficient to keep the factory line running
- With the Benefits of Secure Boot come new responsibilities for OEMs in management of security database.

Call to Action

System OEMs and their partners need to carefully plan the switch to UEFI 2.3.1 Secure Boot:

1. Contact Insyde for assistance with Firmware Implementation and new Factory Tools
2. Develop Procedures and Assign Clear Responsibilities for Security Tasks

Q&A

Thanks for attending the
UEFI Spring Plugfest 2012

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

presented by

insyde®