congatec Application Note #39

Affected Products	Products featuring firmware supporting the UEFI Secure Boot feature
Subject	Secure Boot BIOS Customizations
Confidential/Public	public
Author	CJR

Revision History

Revision	Date (yyyy-mm-dd)	Author	Changes
1.0	2019-04-23	CJR	Initial release of document

Preface

This Application Note explains the OEM specific customizations required to deploy a Secure Boot enabled BIOS. Although all latest congatec embedded BIOS releases offer Secure Boot support, it is still necessary to customize the BIOS with the OEMs Secure Boot keys, especially the Platform key (PK).

Disclaimer

The information contained within this Application Note, including but not limited to any product specification, is subject to change without notice.

congatec AG provides no warranty with regard to this Application Note or any other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. congatec AG assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the Application Note. In no event shall congatec AG be liable for any incidental, consequential, special, or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this Application Note or any other information contained herein or the use thereof.

Intended Audience

This Application Note is intended for technically qualified personnel. It is not intended for general audiences.

Electrostatic Sensitive Device

All congatec AG products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a congatec AG product except at an electrostatic-free workstation. Additionally, do not ship or store congatec AG products near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original manufacturer's packaging. Be aware that failure to comply with these guidelines will void the congatec AG Limited Warranty.

Technical Support

congatec AG technicians and engineers are committed to providing the best possible technical support for our customers so that our products can be easily used and implemented. We request that you first visit our website at www.congatec.com for the latest documentation, utilities and drivers, which have been made available to assist you. If you still require assistance after visiting our website then contact our technical support department by email at support@congatec.com

Symbols

The following are symbols used in this application note.

Note

Notes call attention to important information that should be observed.

Caution

Cautions warn the user about how to prevent damage to hardware or loss of data.

Warning

Warnings indicate that personal injury can occur if the information is not observed.

Copyright Notice

Trademarks

Product names, logos, brands, and other trademarks featured or referred to within this user’s guide, or the congatec website, are the property of their respective trademark holders. These trademark holders are not affiliated with congatec AG, our products, or our website.

Terminology

Term	Description
BIOS	Basic Input Output System
UEFI	Unified Extensible Firmware Interface
CSM	Compatibility Support Module
RSA	Asymmetric public key cryptosystem named after their inventors **R**ivest, **S**hamir and **A**dleman
SHA	Secure Hash Algorithm

1 Secure Boot Introduction

Secure boot is a security standard to ensure that a PC boots using only software trusted by the Original Equipment Manufacturer (OEM). It was developed to prevent any unauthorized software from loading in the pre-boot space.

When the PC starts, the firmware checks the signature of each piece of boot software, including UEFI firmware drivers (also known as Option ROMs), EFI applications, and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system bootloader.

Secure Boot ensures that only properly signed and verified boot loaders and EFI drivers are executed. Secure Boot was introduced in the UEFI specification version 2.3.1. The current UEFI specification can be downloaded from www.uefi.org.

1.1 Secure Boot Requirements

Two requirements must be met in order to enable Secure Boot:

- CSM must be disabled
- Platform Key (PK) variable must be installed

Caution

The pre-installed default PK (from the BIOS vendor American Megatrends Inc.) MUST NOT be used to deploy Secure Boot.

1.2 Secure Boot Variables

There are two keys and two signature databases that play an important role for the Secure Boot mechanism:

- Platform Key (PK): establishes trust relationship between platform owner (OEM) and platform firmware (BIOS)
- Key Exchange Key (KEK): establishes trust relationship between OS (e.g. MS Windows) and platform firmware (BIOS)
- db (Good Signature Database = White List)
- dbx (Revocation Signature Database = Black List)

In a customized BIOS with Secure Boot support enabled, the PK, KEK and db (optional) variable are typically provided by the customer as OEM certificates.

The dbx variable is kept up to date by congatec by replacing this database with the latest UEFI Revocation list from https://uefi.org/revocationlistfile every time a new BIOS is released.

The Platform Key is a self-signed root key and consists of a public and private key. Only the public part of the key (PK_{pub}) is required for the customized BIOS. The private part of the key (PK_{priv}) must remain with the customer at a secure location.

Caution

Never expose PK_{priv} to the public. PK_{priv} is only used to sign the KEK variable.

A KEK is used to sign the db and dbx signature databases. By default, a KEK variable contains two Microsoft keys. See chapter 2 below for more information.

The UEFI specification defines two additional signature databases not commonly used and also not required and therefore not covered in this document:

- dbt (time stamp signature database)
- dbr (recovery signature database)

1.3 Key Formats

Secure Boot supports the following three key formats:

- RSA-2048 Key with a fixed certificate size of 2048 bits
- SHA256 Hash with a fixed certificate size of 32 bytes
- X509 Certificate with a typical size of >1 kB

A X509 certificate contains information about a key, including:

- name of the issuer
- validity time frame
- relationship to the trusted root certificate key
- digital signature of the key made with the root key

congatec supports the common X509 key certificate in its Embedded BIOS solution. Customers requesting a BIOS with Secure Boot support need to provide their OEM specific keys as x509 ASN.1 DER files (usually ending in .cer).

A key file in PEM format needs to be converted to DER-for example by using the command line OpenSSL:

```
openssl x509 -outform der -in OEM_PK.pem -out OEM_PK.der
```

1.4 Key Provisioning

OEMs have two options to provision their specific keys:

- User initiated from BIOS setup program (time consuming, only suitable for low volume products). See chapter 2 for more information.
- Customized BIOS with built-in (factory) OEM keys (for high volume products). See chapter 3 for more information.

2 Secure Boot Setup Support

The congatec Embedded BIOS allows to configure a system for Secure Boot in BIOS setup. You can find the Secure Boot submenu under the Security tab.

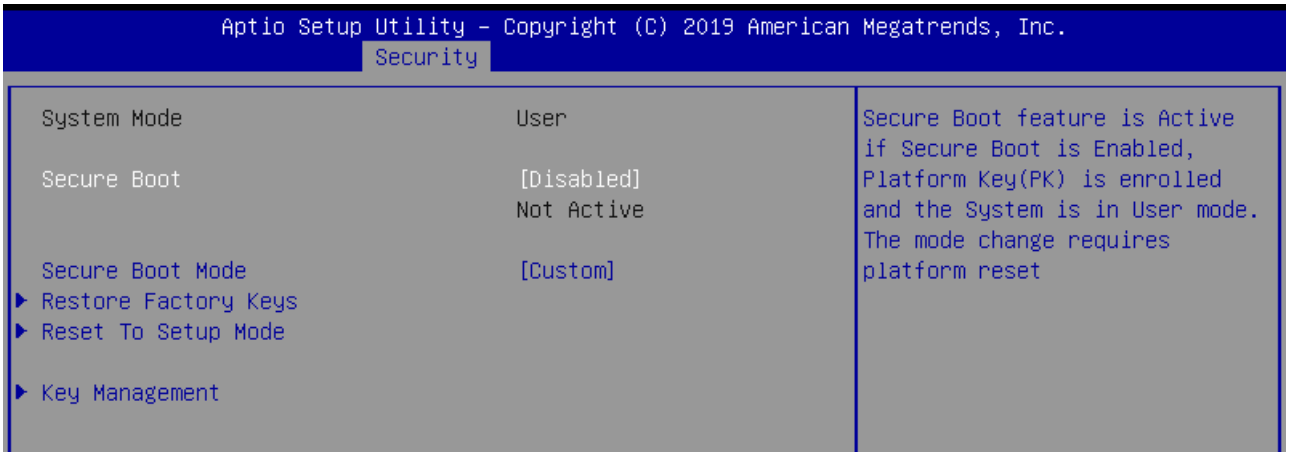

Figure 1: Secure Boot Setup Menu

Before Secure Boot can be enabled, the OEM keys must be added to the BIOS and the **Secure Boot Mode** must be set to **Custom**. Use the **>Key Management** sub menu to add your specific keys, especially the PK and KEK signed with your PK.

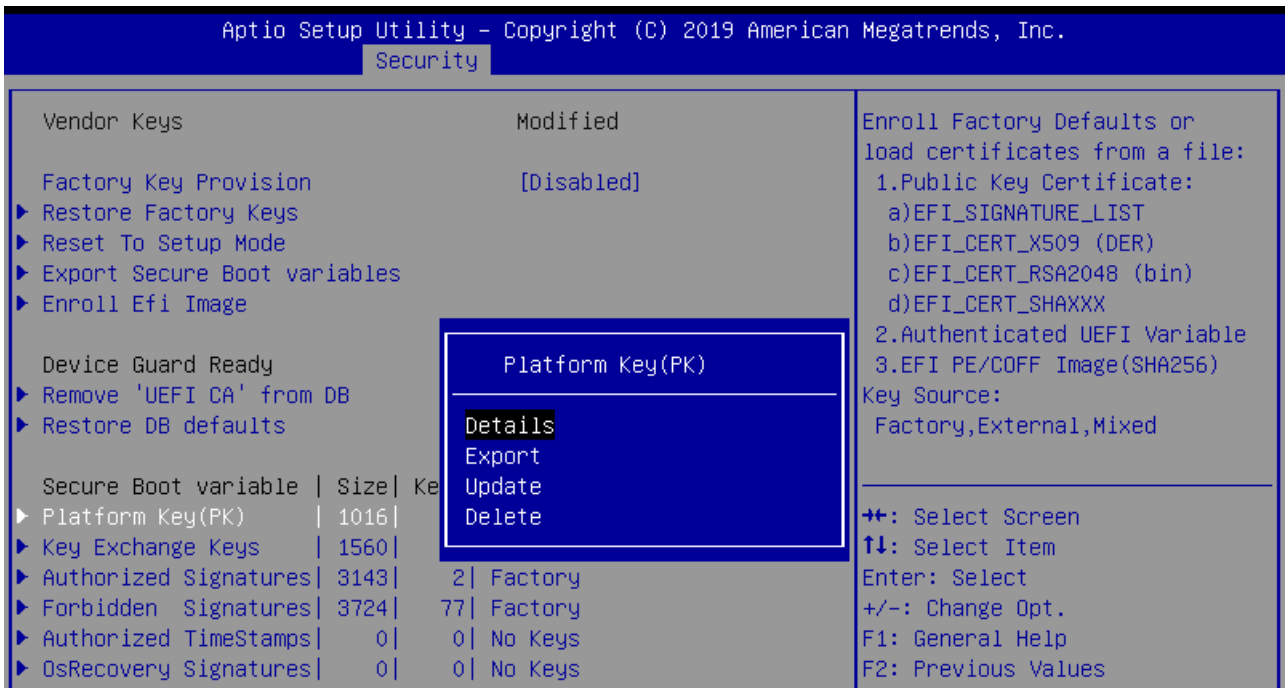

Figure 2: Key Management Support

When the Secure Boot variables are configured for the first time, the Secure Boot is in setup mode. This means that the keys are not installed (as shown in Figure 3 below).

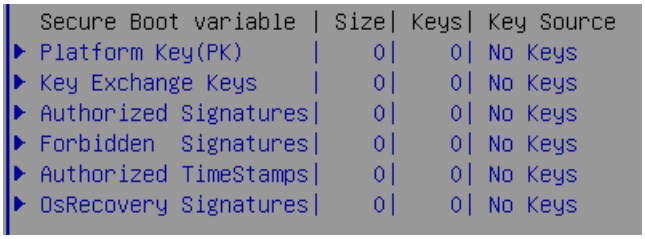

Figure 3: In Setup Mode all keys are removed.

The preferred way to customize the keys in BIOS setup is to first load the built-in default keys. This can be achieved with the setup node **>Restore Factory Keys**. The main purpose is to load valid db and dbx signature databases. The factory PK and KEK must be overwritten with your OEM keys. The Test (AMI) PK is only for Secure Boot testing and **must not** be deployed to the field!

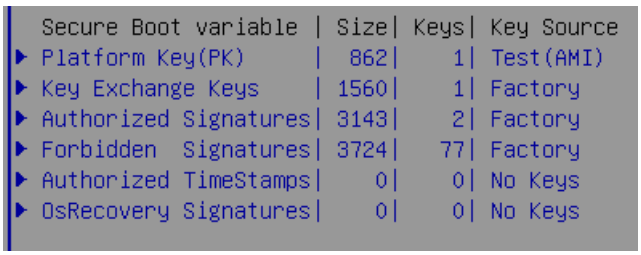

Figure 4: Factory Keys loaded

The key management setup support offers several options to customize the secure boot variables (see Figure 2). Use the **Update** option to replace the factory PK and KEK with your OEM specific keys loaded from a file system (e.g. on a USB stick). Then update the Secure Boot variables. An example is shown in Figure 5 below. PK and KEK were loaded from external storage and the built-in signature databases (db and dbx) are used. You can also replace the factory signature databases with your OEM specific ones.

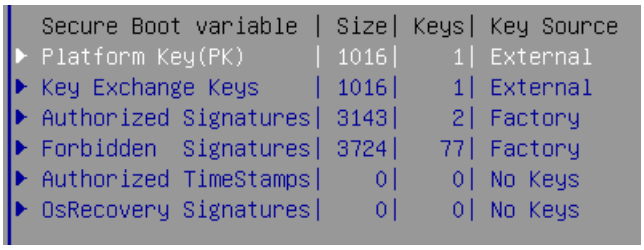

Figure 5: Customized Secure Boot variables

Now that the Secure Boot keys are installed, Secure Boot can be enabled under the Security tab.. After a platform reset, the system is in Secure Boot mode.

Note

Always protect the BIOS setup with a password to prevent non-authorized users from changing the system configuration (disabling Secure Boot).

3 congatec Secure Boot BIOS Customization

congatec developed an OEM Secure Boot support module for quick and easy BIOS customization. OEM keys in X.509 ANS.1 DER Public Key Certificate format can be instantly added to the BIOS build process. Such a full custom (source code) BIOS usually requires the mandatory OEM public PK, KEK and optionally the db keys.

OEMs have three options for the KEK and db signature databases:

1. Use the BIOS default keys:
   - MS Windows PCA (public certificate authority) for Microsoft OS
   - MS UEFI CA for Linux boot loaders and 3rd party EFI drivers
2. Append OEM keys to BIOS default keys:
   - MS Windows PCA
   - MS UEFI CA
   - OEM key
3. Use only OEM keys and remove MS keys: Only starts OEM signed boot loaders and executables. MS Windows and standard Linux boot loaders are not started in this configuration.

Note

1. ***Always protect the BIOS setup with a password to prevent non-authorized users from changing the system configuration (e.g. from disabling Secure Boot).***
2. ***With such a Secure Boot enabled OEM BIOS, the system can only boot certain operating systems/boot loaders. Older operating systems (e.g. MS-DOS, Windows 7) and unsigned Linux bootloaders as well as the UEFI shell cannot be used anymore. This can limit options for system diagnostics and debugging.***
3. ***For more information about congatec's Secure Boot customization, contact congatec technical support at support@congatec.com.***

4 Key Generation and Driver Signing

The most common tools for OEM key generation and driver signing are:

- **signtool.exe** (Windows)
- **MakeCert.exe** (Windows)
- **OpenSSL** (Windows, Linux)

The usage of these tools is beyond the scope of this Application Note. Please refer to available literature for a detailed description how to run these tools to sign drivers and generate key certificates.

Useful links:

Signtool: https://docs.microsoft.com/en-us/dotnet/framework/tools/signtool-exe

OpenSSL: https://www.openssl.org