Dell Client BIOS: Signed Firmware Update

An Implementation and Deployment Guide to NIST SP800-147 BIOS Protections for Dell Client BIOS

Rick Martinez

Dell Client BIOS

Executive summary

In April 2011, the National Institute of Standards and Technology (NIST) released Special Publication 800-147 *BIOS Protection Guidelines* to offer BIOS vendors, OEMs, and end customers the information needed to help protect the system BIOS from malicious attacks.

The NIST document defines guidelines on how to protect the BIOS code on a system from unauthorized modification and also provides deployment strategies to allow customers to take full advantage of these protections.

This white paper outlines the BIOS implementation building blocks and remote management details necessary to understand and deploy these protections on Dell Client systems and is intended for technical audiences who have an interest in the endpoint security in their organizations.

Contents

NIST released SP800-147 *BIOS Protection Guidelines* in April 2011

Introduction

Computer and network security represents a major piece of today's connected landscape and culture. Computer security is not only critically important with respect to protecting customer data and privacy in an isolated infrastructure but it also plays an expanding role in society's security in general; every day we get closer to the vision that "computer security *is* security."[i]

Securing the endpoints, the devices that we use every day, is a fundamental goal in any enterprise level security strategy. The most prevalent endpoints in many corporate infrastructures are the "client" systems, also known as the personal computers: desktops, notebooks, workstations, and tablets. These endpoints are typically the last link in the chain of sensitive data extending from the enterprise "cloud" all the way down to the end user. It is important that these endpoints remain protected at all levels of the software stack.

Nearly all client systems rely on the system BIOS (Basic Input/Output System)[ii] to initialize hardware and prepare the platform for the operating system. The BIOS is typically stored on flash memory on the motherboard and occupies a very privileged role in the system based on several factors: it has full control of the hardware during system boot, includes persistent storage for code and data, and it even maintains some capabilities after the operating system has loaded.

The unfortunate consequence of these privileges is that the BIOS has become an attractive target for attack. There have been several viruses and research papers targeted at or describing how to replace or modify BIOS code for malicious purposes and this trend is expected to continue. Most of these attacks have centered on legacy BIOS bugs or other vulnerabilities to gain entrance to the BIOS realm.

In April 2011 the National Institute of Standards and Technology (NIST) released Special Publication 800-147 *BIOS Protection Guidelines*[iii] to give BIOS vendors, OEMs, and end customers the data needed to combat the growing threat of attacks against BIOS. This comprehensive document provides guidelines on how to protect the BIOS code on a system from unauthorized modification and also provides deployment strategies to allow customers to take full advantage of these protections.

Dell engineers put significant effort into hardening the BIOS protection and authentication capabilities on client systems in accordance with NIST SP800-147 to support Dell's customers. This white paper delves into the implementation and deployment details that are specific to Dell Business Client systems to increase customer awareness of the security technologies employed to assist in managing these technologies across the enterprise.

This paper assumes that the reader is familiar with the terminology in the NIST document and has an understanding of security concepts such as digital signing.

What is "Dell Client BIOS"?

The support and behavior described in this document are applicable to Dell Business Client systems. These platforms are commonly referred to as Dell Client systems and this terminology will be used in the rest of this document. The brands that are included in this group are:

- OptiPlex
- Latitude
- Dell Precision

Several other Dell platforms and brands include support for NIST SP800-147 in the system BIOS but the details of implementation are beyond the scope of this document.

Analysis of NIST Recommendations

The following capabilities are summarized in *Appendix A – Summary of Guidelines for System BIOS Implementations* of the NIST Special Publication 800-147 BIOS Protection Guidelines document:

- Approved BIOS Update Mechanisms
- BIOS Update Authentication
- Integrity Protection
- Non-Bypassability

Dell Client BIOS platforms implement these NIST requirements as part of the Signed Firmware Update functionality included in Dell's customer BIOS update support. Other computer OEMs and BIOS vendors may implement these requirements differently. The following sections include a brief analysis of each of these requirements from a Dell Client BIOS implementation perspective.

Approved BIOS Update Mechanisms

Dell Client BIOS releases that support the Signed Firmware Update functionality are available on the Dell Support website (http://support.dell.com) for many of Dell's enterprise-level client systems. These BIOS update releases represent one half of the authenticated BIOS update mechanism as specified in the NIST documentation, the "approved BIOS update".

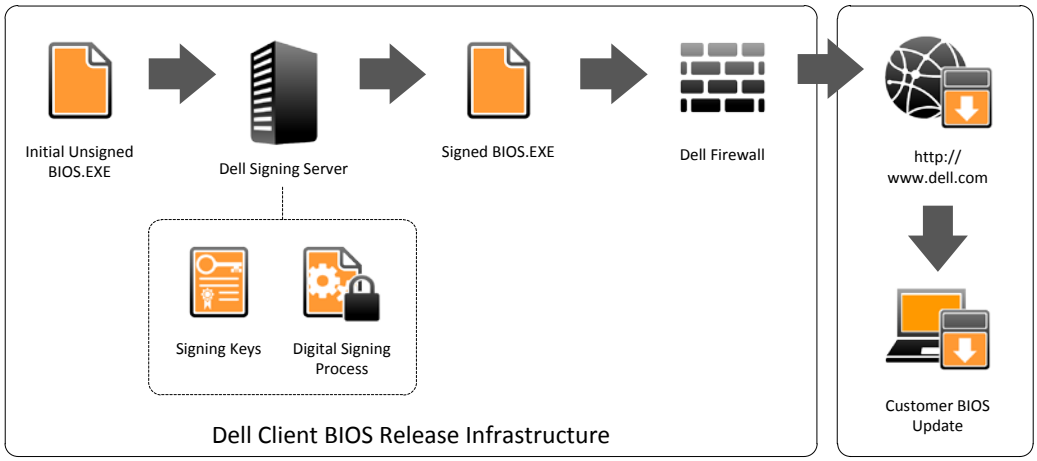
These approved BIOS releases are DOS/Windows executable files developed by Dell that include BIOS and onboard firmware update payloads that have been signed by a Dell process using protected private signing keys. End users can download these releases and use them to update the BIOS on endpoint systems.

The other half of the authenticated BIOS update mechanism exists in the BIOS Root of Trust for Update (RTU) of the system BIOS running on Dell systems that support Signed Firmware Update. This RTU module already in the system BIOS will use the appropriate stored public key(s) to verify the authenticity of the BIOS and firmware payloads before allowing any update to the system BIOS flash memory.

In summary, the BIOS running on a system that supports Signed Firmware Update contains information in its RTU that supports a cryptographically hardened verification mechanism which allows only approved BIOS updates to modify the system BIOS code. More details about how this works is provided in the following sections.

Figure 1 below illustrates the high level process that is used to create an approved BIOS update for a Dell Client platform.

Figure 1. BIOS Signing Flow



BIOS Update Authentication

Dell Client BIOS uses a "capsule" type update that is invoked by the end user or enterprise manager by running an update executable under the user operating system. This update executable copies the BIOS and firmware payloads and corresponding digital signatures to system memory where they will persist until the system reboots. After reboot, the currently running BIOS (the Root of Trust for Update, i.e. the RTU) detects these payloads in the system memory, verifies the digital signatures, and updates the BIOS and firmware upon successful verification.

As described in the previous section, the RTU is located in the system BIOS running on Dell Client BIOS systems and includes both the list of approved public keys (the "key store") and the signature verification algorithm to allow authentication of all

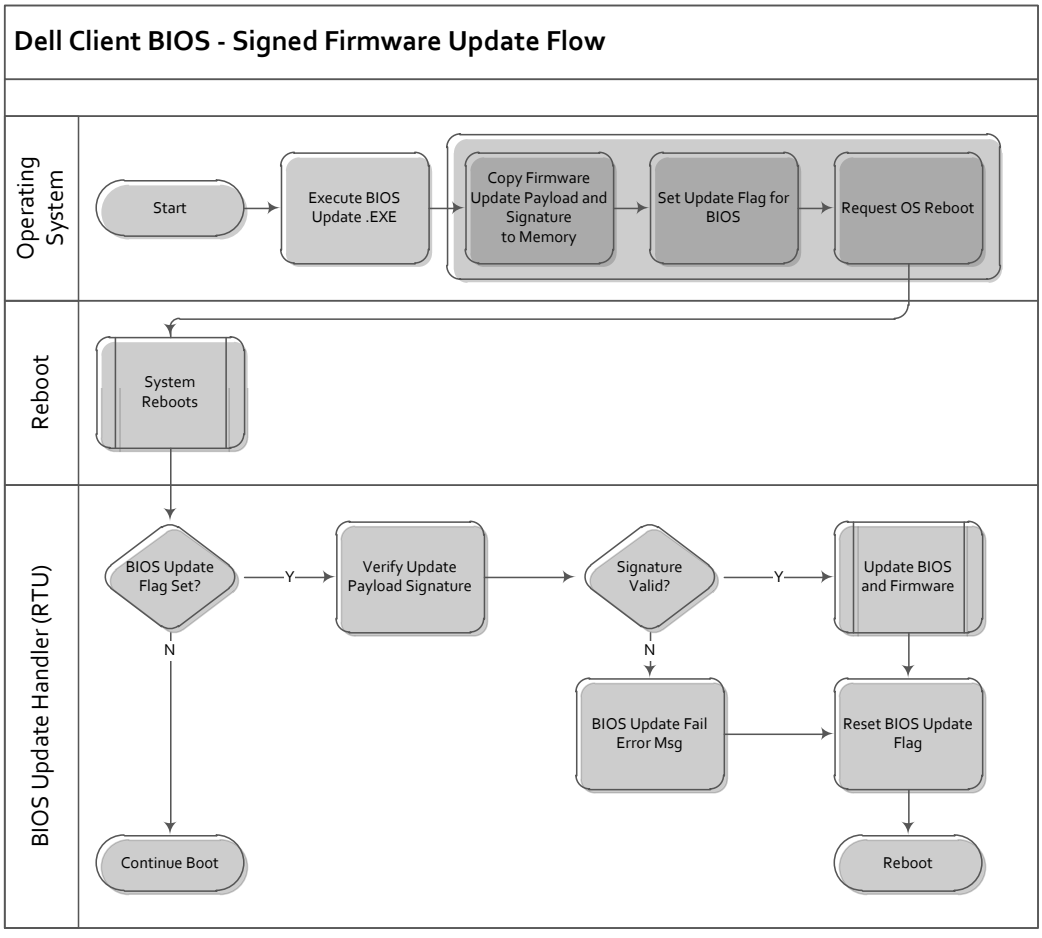
BIOS updates. The RTU is protected by Dell proprietary flash locking mechanisms at the hardware level and all updates to the RTU must be signed.

In this implementation, the BIOS key store includes the full public key used to verify the signature of all BIOS and firmware updates. This public key can be injected into the BIOS update executable during the BIOS signing process but is only programmed into the RTU during an authenticated RTU update. This can coincide with a normal BIOS update when needed.

All BIOS update images are signed using the RSA PKCS #1 v2.1 algorithm with RSA 2048-bit keys as per FIPS Publication 186-3 *Digital Signature Standard (DSS).* The SHA-256 algorithm was selected to hash the payload in the signing and verification process based on this algorithm's acceptance in NIST Special Publication 800-131A. Update images are verified by the BIOS using the public key contained in the RTU before the BIOS or other firmware currently running on the system is modified.

The full Signed Firmware Update cycle is illustrated in Figure 2 below.

Figure 2. Signed Firmware Update Flow



Integrity Protection

The RTU and BIOS are protected from unauthorized modification using Dell proprietary cycle trapping and locking mechanisms supported by the system hardware. All unauthorized attempts to enable writes to the flash storage are trapped and blocked by these mechanisms. These protections are instantiated by the BIOS during system boot.

All programmatic code update attempts that are not approved by the RTU verification mechanisms and any attempts to update BIOS data not approved by the BIOS storage handler are blocked from the system flash memory using flash disable mechanisms. These mechanisms are not designed to protect against physical access to the motherboard with a hardware programmer.

Non-Bypassability

The Signed Firmware Update mechanism in the RTU that enforces authenticated updates is the exclusive mechanism for modifying the system BIOS. This enforcement cannot be bypassed by any firmware or software running on the platform that is not controlled by the RTU.

Client BIOS Deployment

The Dell Client BIOS and Dell Enterprise manageability offerings allow customers to detect the Signed Firmware Update capability on Dell Client systems in their enterprise for inventory purposes as well as provide mechanisms for Dell to help protect the customers from possible BIOS threats in the future.

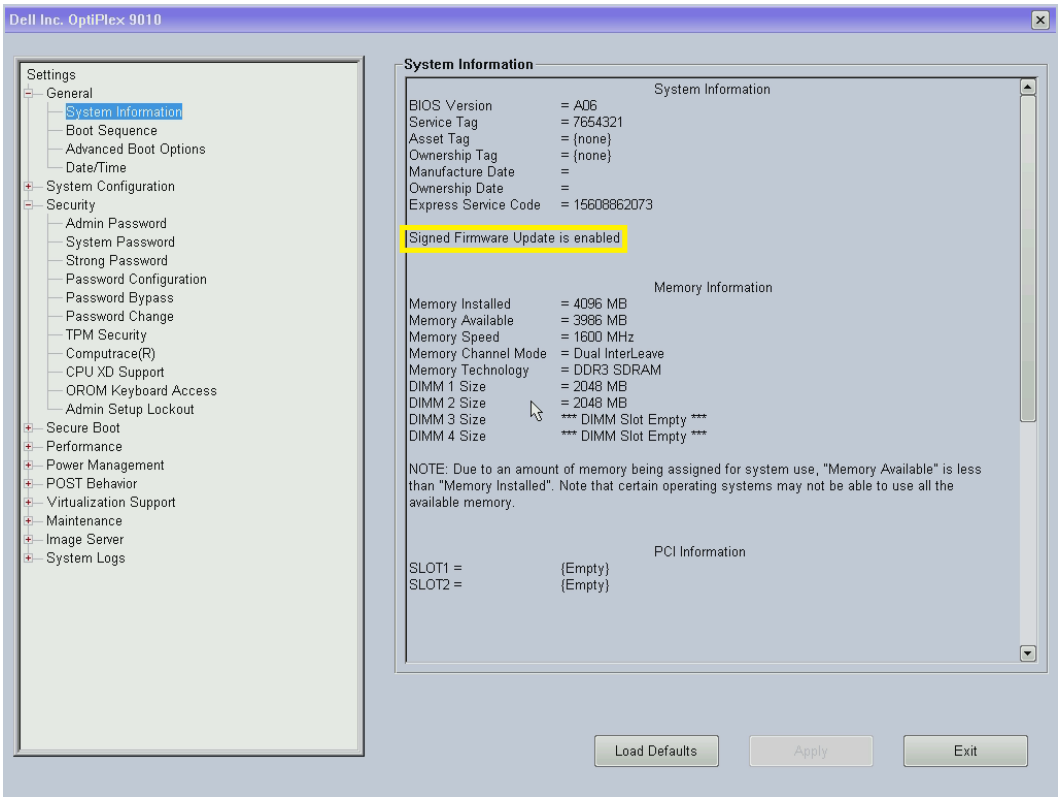
Signed Firmware Update Detection

There are two different ways to verify whether a particular system is protected by the Signed Firmware Update feature: locally through the BIOS Setup interface or remotely through the Dell Client Configuration Toolkit (CCTK).

Detection via BIOS Setup

The Signed Firmware Update feature is enabled by default on all new Dell Client systems and can be verified in BIOS Setup. The BIOS Setup interface is invoked using F2 at boot or through the F12 boot menu. After entering Setup the user can check the feature in the General → System Information → BIOS pane by looking for the text string “Signed Firmware Update is enabled”. This string indicates that the BIOS is enforcing digital signature checking on all firmware updates. This text is highlighted in yellow in Figure 3.

Figure 3. Enable Signed Firmware Update



Detection via CCTK

Customers can use the Dell Client Configuration Toolkit (CCTK) version 2.1 and later to detect Signed Firmware update on Dell Client systems. More details about the toolkit are available at http://www.dell.com[iv].

The status of the Signed Firmware Update feature can be verified using the following command:

```
cctk.exe --sfuenabled
```

This command returns the following output based on the status of the Signed Firmware Update feature:

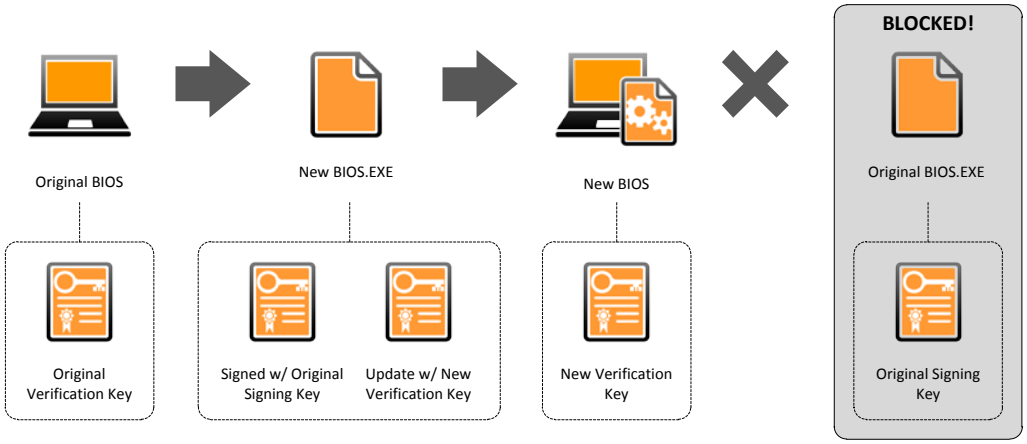
CCTK Returns	Signed Firmware Update is…
`sfuenabled=no`	Not enabled.
`sfuenabled=yes`	Enabled.

Anti-Rollback Support

The Signed Firmware Update feature provides an opportunity for Dell to protect customers from potential BIOS vulnerabilities that may be discovered in the future. The feature allows Dell to prohibit customers from rolling back to a potentially undesirable BIOS by providing a mechanism to enforce anti-rollback support through signing key revocation. This protection can be invoked by the Dell BIOS team by releasing a new BIOS with an updated verification key in the RTU that unconditionally blocks flash updates to all earlier BIOS revisions that were previously signed with the old (revoked) key.

The anti-rollback through key revocation concept is illustrated in Figure 4.

Figure 4. Anti-Rollback by Key Revocation



Signed Firmware Update Systems

The systems listed in the following table were the first Dell Client platforms to support the Signed Firmware Update feature at launch. All BIOS revisions for these systems provide Signed Firmware Update protections by default with no option to disable and all BIOS updates for these systems are digitally signed per NIST recommendations.

All Dell Client systems released after the systems in the list will follow this same model.

Dell Latitude	
Latitude E6230	Latitude E6330
Latitude E6430	Latitude E6530
Latitude E5430	Latitude E5530
Latitude E6430s	

Dell OptiPlex	
OptiPlex 3010	OptiPlex 9010
OptiPlex 7010	OptiPlex 9010 All In One

Dell Precision Mobile	
Precision M4700	Precision M6700

Dell Precision Workstation	
Precision T7600	Precision T5600
Precision T3600	Precision T1650

Systems released prior to those in the above list may support Signed Firmware Update through a BIOS update. For more details about these legacy systems, please see Appendix A.

Summary

This whitepaper walked through an analysis of the recommendations in the NIST Special Publication 800-147 *BIOS Protection Guidelines* and provided educational insights into the Dell Client BIOS implementation pertaining to the processes and functionality developed in accordance with these recommendations. The Dell-specific details in this document provide the reader with the security fundamentals and understanding needed to confidently deploy Dell Client systems protected by Signed Firmware Update.

The Signed Firmware Update feature, including digitally signed and authenticated BIOS updates, BIOS-hardened flash locking, and the inability for attackers to programmatically bypass these protections continues to provide an important piece in the endpoint security solution for all customers who use Dell Client systems in their enterprise, small business, or at home.

Appendix A. Legacy BIOS Support

Several BIOS feature and behavioral changes were necessary to securely implement the Signed Firmware Update feature on legacy platforms that were already in the field during NIST SP800-147 publication. These changes are discussed in the following sections.

Legacy BIOS Updates

Many systems that did not originally include support for the Signed Firmware Update feature at launch can be updated to a BIOS that offers NIST 800-147 protection. Updated BIOS releases supporting the feature are available for the legacy systems listed in the "Legacy Systems Supported" section.

BIOS Setup Changes

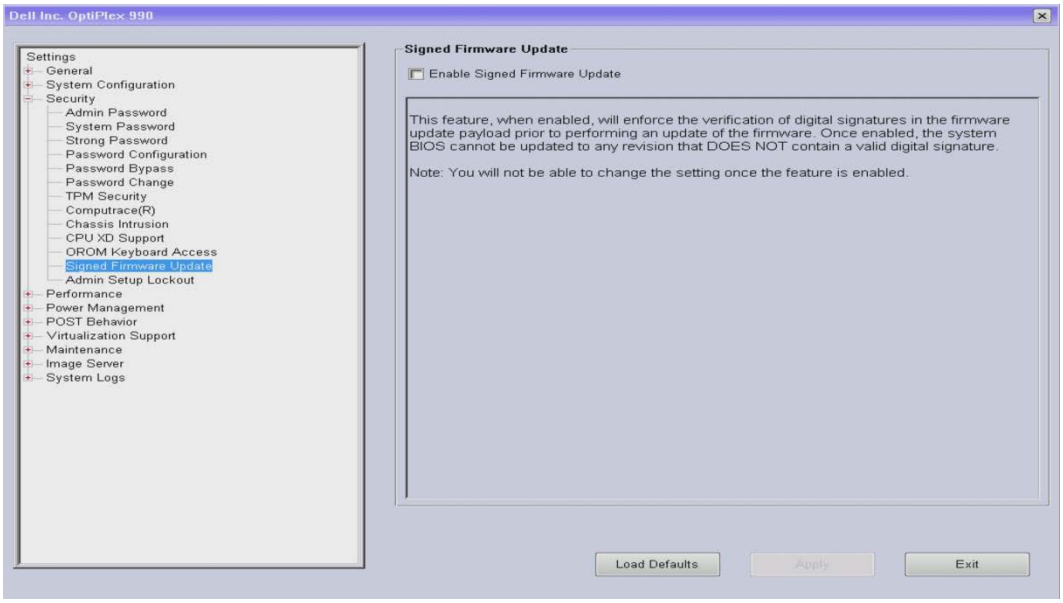
The Signed Firmware Update feature was launched on shipping platforms in the form of block release BIOS updates available at http://support.dell.com. At the time of customer BIOS update it is not possible to determine whether each end customer wishes to accept the behavioral changes required to securely support a digitally signed firmware update.

To meet the needs of all Dell customers and provide the desired protections to meet the NIST requirements, a write-once BIOS setup option was added to the BIOS to allow the customer to "opt-in" to the Signed Firmware Update feature if the enhanced security is desired. This option is set to "disabled" by default and is locked down by the BIOS protections once "enable" has been selected and confirmed by the customer.

BIOS Setup Option

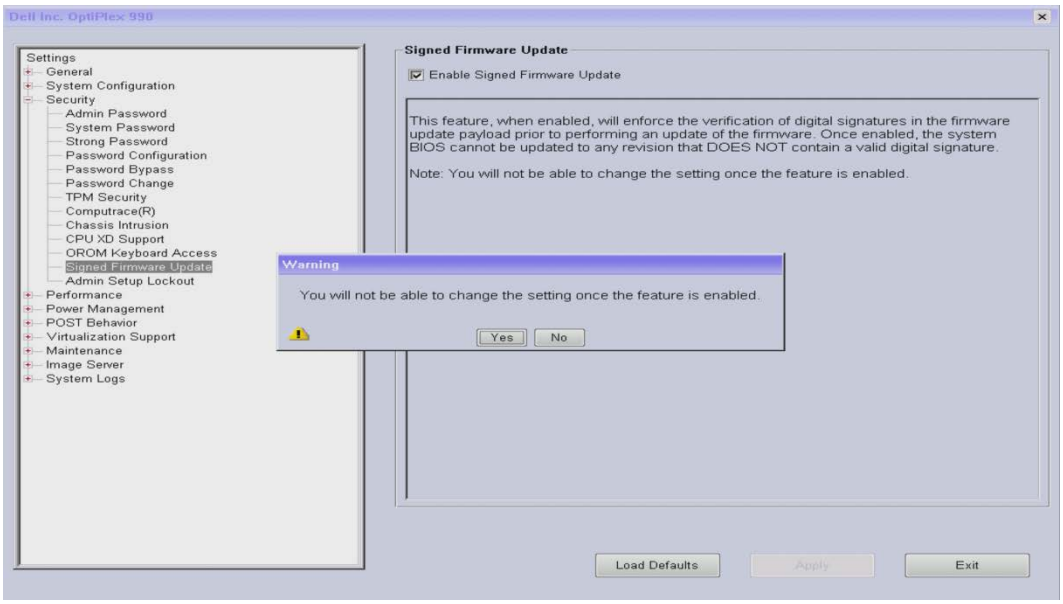
The BIOS Setup option is accessible through the BIOS Setup interface invoked by F2 during system boot or from the F12 boot menu. The new option is labeled "Signed Firmware Update" and is located in the "Security" section of the left pane Setup screen. The "Enable Signed Firmware Update" checkbox is the user's only choice in the right pane as shown in Figure 5 on the next page.

Figure 5. Signed Firmware Update Setup Screen



After selecting "Enable Signed Firmware Update", the BIOS Setup engine will prompt the user, as shown in Figure 6, to verify before saving the selection since it cannot be undone. The "Signed Firmware Update" option will no longer show up in the BIOS Setup left pane after the user has opted in.

Figure 6. Signed Firmware Update Prompt



Setup Help Text

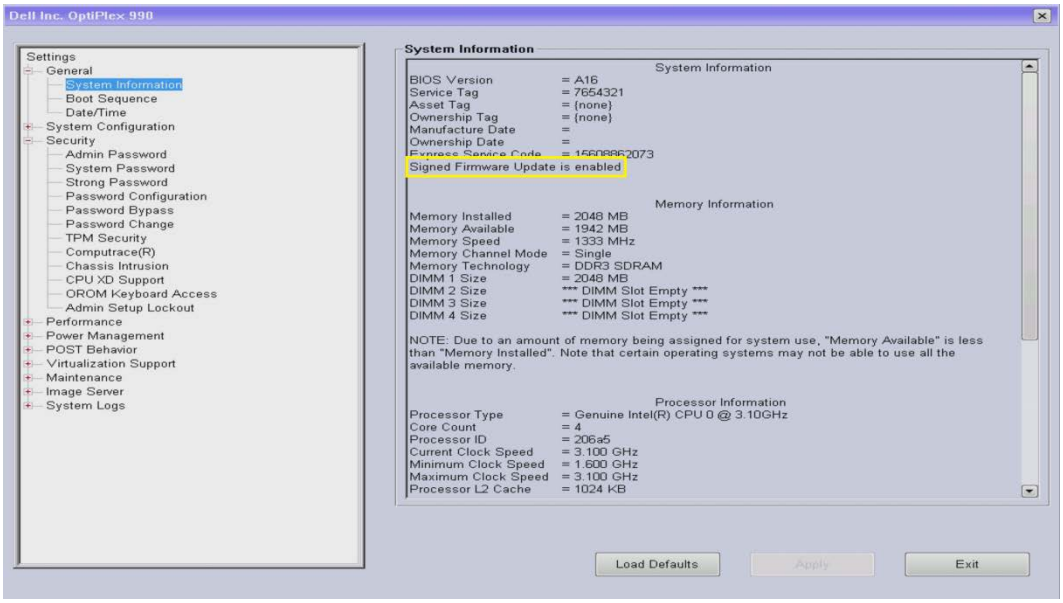
Setup option help text is included below:

```
[ ] Enable Signed Firmware Update

This feature, when enabled, will enforce the verification of
digital signatures in the firmware update payload prior to
performing an update of the firmware. Once enabled, the system
BIOS cannot be updated to any revision that DOES NOT contain a
valid digital signature.

Note: You will not be able to change the setting once the
feature is enabled.
```

Opt-In Status

After the customer has opted in to "Signed Firmware Update" the setup option will disappear but the opt-in status is displayed to the customer in the General → System Information → BIOS pane with the text "Signed Firmware Update is enabled". The user can use this text to verify that the BIOS is enforcing digital signature checking on all firmware updates and the indicator is present on all new Dell Client systems as well. This text is highlighted in yellow in Figure 7.

Figure 7. Signed Firmware Update Enabled



Remote Management

Customers can use the Dell Client Configuration Toolkit (CCTK) version 2.1 and later to enable Signed Firmware update on all systems listed in this appendix. More

details about the toolkit are available at http://www.dell.com; a brief summary of its capabilities with respect to Signed Firmware Update is as follows.

The following command line can be invoked to enable Signed Firmware Update using CCTK:

```
cctk.exe --sfuenabled=yes
```

If a BIOS admin password has been set to protect the BIOS Setup option from non-administrator access, the valsetuppwd modifier must be used on the command line:

```
cctk.exe --sfuenabled=yes –-valsetuppwd=<admin password>
```

The status of the Signed Firmware Update feature enable can be verified using:

```
cctk.exe --sfuenabled
```

The command returns the following output based on the status of the Signed Firmware Update feature:

CCTK Returns	Signed Firmware Update is…
`sfuenabled=no`	Not enabled.
`sfuenabled=yes`	Enabled.

Note: Some of the first BIOS releases that implemented Signed Firmware Update did not properly support the tokens above. These have been fixed in subsequent BIOS releases.

Transition BIOS Concept

Some Dell Client platforms supported an older type of authentication of BIOS updates well before the Signed Firmware Update feature was introduced. The challenge faced during the initial deployment of signed BIOS on these systems was that the new BIOS updates needed to support the old authentication mechanism and also needed to deploy the new RTUs to support digital signature verification as required for Signed Firmware Update.

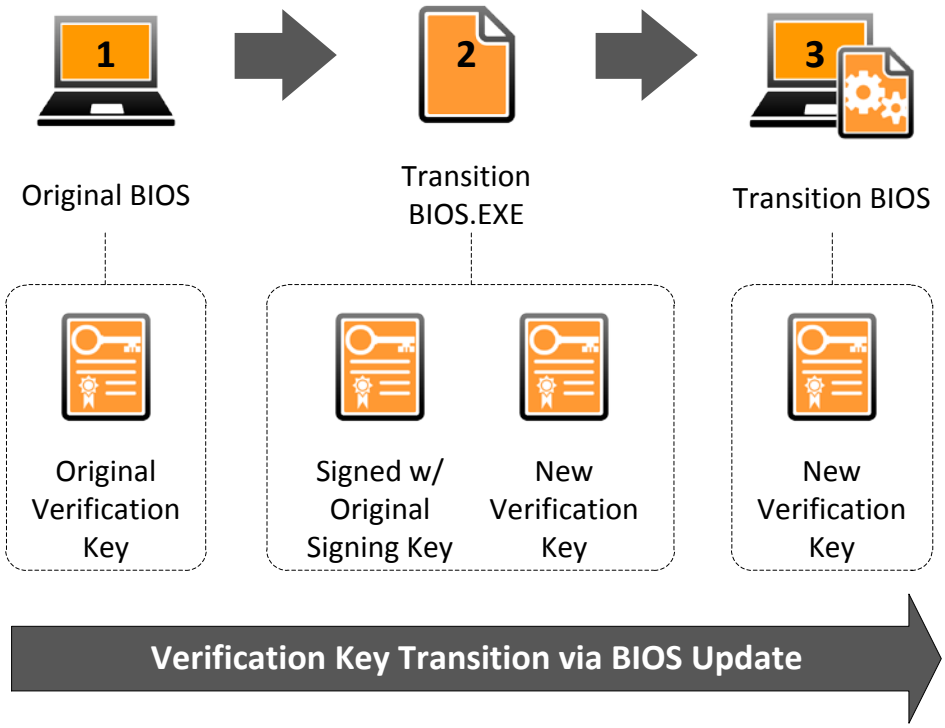
This scenario required a “transition” or “pre-requisite” BIOS to transition or “bridge the gap” between the old authentication mechanism and the new signature verification support. There are three important aspects of the transition BIOS that should help to highlight this type of scenario:

- Transition BIOS must be the first Signed Firmware Update capable BIOS flashed onto a system that is running a BIOS that does not support Signed Firmware Update
- Transition BIOS includes all Signed Firmware Update protections for the BIOS including verification of future BIOS updates (if enabled) and other hardened BIOS protections in accordance with the NIST specification
- Transition BIOS does not imply that a second BIOS update is required immediately after updating to the transition BIOS. It can be deployed and is supported just like any other Dell BIOS

Details about how the keys are transitioned in this scenario can be seen in the following procedure and illustrations.

1. System is running the original BIOS without Signed Firmware Update support. This BIOS includes an older RTU that expects all BIOS updates to be signed with the old signing mechanism.
2. Customer runs the transition BIOS executable on the system to update the BIOS and firmware. This BIOS is signed with the original signing key but includes an updated RTU that includes the new verification key as per the NIST recommendations.
3. System is running the transition BIOS with Signed Firmware Update support and is protected from unauthorized updates as per the NIST recommendations.

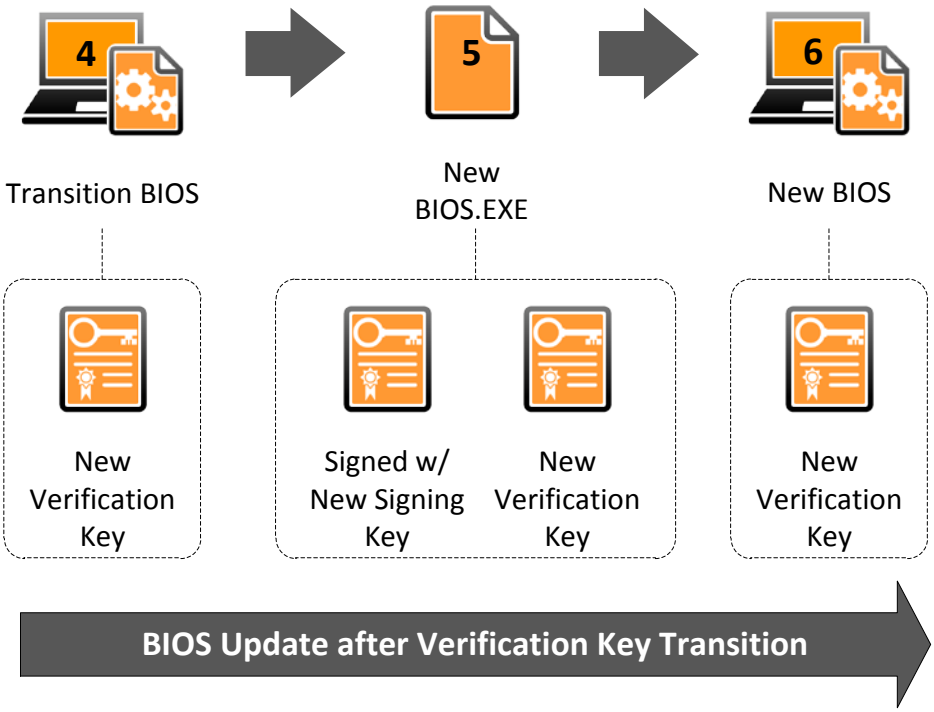
Figure 8. Update to Transition BIOS



Now that the transition BIOS is running on the system and assuming Signed Firmware Update has been enabled, all future BIOS updates must be signed with the new signing key. This update may happen days, months, or years after the original transition BIOS was flashed onto the system, or may never happen at all depending on customer requirements. This next phase is detailed in the following procedure and illustrations.

4. System is running the transition BIOS with Signed Firmware Update support and is protected from unauthorized updates per the NIST recommendations.
5. Customer runs a new BIOS update executable signed with the signing key that matches the verification key in the transition BIOS. BIOS RTU in the transition BIOS verifies this update per NIST recommendations and flashes the new BIOS on the system.
6. System is running the new BIOS with Signed Firmware Update support and continues to be protected from unauthorized updates per the NIST recommendations.

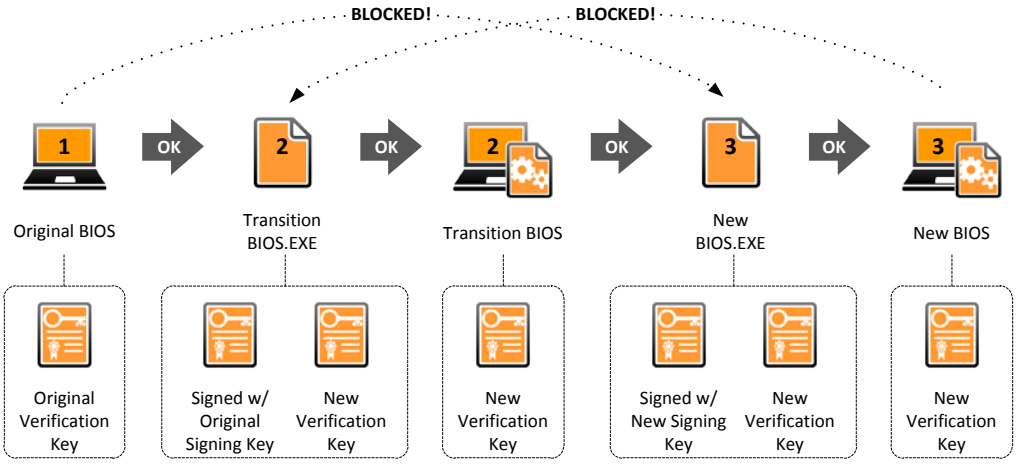
Figure 9. Update to Post-Transition BIOS



Transition BIOS Limitations

Unfortunately, the transition BIOS concept does create some specific limitations with respect to update, backdate, and skipping BIOS revisions. These limitations are highlighted in Figure 10 below:

Figure 10. Transition BIOS Blocked Scenarios



In the illustration above:

1. BIOS 1 – original BIOS without Signed Firmware Update support
2. BIOS 2 – transition BIOS signed with old key but protected by hardened mechanisms and new keys per the NIST recommendations once flashed on the system
3. BIOS 3 – any new BIOS released after the transition BIOS, signed with the new keys per the NIST recommendations

The following table further highlights the allowed/disallowed BIOS transitions:

	Allow update to this BIOS?			
Starting BIOS	BIOS 1	BIOS 2	BIOS 3	Future BIOS
BIOS 1	Yes	Yes	No	No
BIOS 2	No	No	Yes	Yes
BIOS 3	No	No	Yes	Yes
Future BIOS	No	No	Yes	Yes

Legacy Systems Supported

The following systems support the Signed Firmware Update feature and protections through BIOS update from http://www.dell.com.

Dell Latitude	
Latitude 5420	Latitude E4310
Latitude 5520	Latitude E5400
Latitude 6320	Latitude E5500
Latitude 6420 / ATG	Latitude E5410
Latitude 6420 XFR	Latitude E5510
Latitude 6520	Latitude E6220
Latitude D430	Latitude E6400 / ATG / XFR
Latitude D531	Latitude E6410 / ATG
Latitude D630	Latitude E6500
Latitude D631	Latitude E6510
Latitude D830	Latitude XT2
Latitude E4200	Latitude XT3
Latitude E4300	Latitude Z600

Dell OptiPlex	
OptiPlex 330	OptiPlex 760
OptiPlex 360	OptiPlex 780
OptiPlex 380	OptiPlex 790
OptiPlex 390	OptiPlex 960
OptiPlex 745	OptiPlex 980
OptiPlex 755	OptiPlex 990

Dell Precision Mobile	
Precision M2300	Precision M4600
Precision M2400	Precision M6300
Precision M4300	Precision M6400
Precision M4400	Precision M6500
Precision M4500	Precision M6600

Dell Precision Workstation	
Precision R5400	Precision T5400
Precision R5500	Precision T5500
Precision T1600	Precision T7400
Precision T3400	Precision T7500
Precision T3500	

Learn more

Visit Dell.com for more information on Dell Client platforms.

About the author

Rick Martinez is a BIOS Security Architect at Dell working with internal and external customers on the Strategy, Development, and Deployment of BIOS Security infrastructure and solutions for Dell Client BIOS. Rick has over 15 years of experience providing innovative technology solutions, development support, and consulting for clients ranging from Small and Medium Businesses to Fortune 100 companies.

January 2013 | Rev 1.0

---

[i] *The Importance of Security Engineering*. http://www.schneier.com/crypto-gram-1209.html
[ii] *BIOS*. http://en.wikipedia.org/wiki/BIOS
[iii] *NIST SP800-147: BIOS Protection Guidelines*. http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf
[iv] *Dell TechCenter*. http://en.community.dell.com/techcenter/systems-management/w/wiki/1952.dell-client-configuration-toolkit-cctk.aspx