SOLUTION BRIEF

6th and 7th Gen Intel® Core™ vPro™ Processors
Public Sector

Strengthening Client Security with FIPS-certified, Hardware-based Cryptography

Intel® Identity Protection Technology (Intel® IPT)

- Enhanced Trust with 6th and 7th Gen Intel Core vPro Processors
- A FIPS-certified, Hardware-based Cryptography Engine
- Hardware-enhanced Authentication using Intel IPT with PKI
- Strong, Multifactor Authentication using Intel IPT with PTD

Today's malware and hacker attacks are increasingly sophisticated, stealthy, patient, and purposeful—and new attacks are emerging faster than ever before. This escalating threat matrix places heavy pressures on client security teams in government agencies as they work to protect sensitive information across a growing range of mobile usage models. Government contractors and many commercial organizations face similar challenges, especially those working in healthcare, financial services, and other tightly regulated industries.

Security Must Be Strong and Flexible—and Fully Compliant

Strong security solutions are needed, yet they must integrate easily into existing security environments, which are based on Personnel Identity Verification (PIV) cards and Public Key Infrastructure (PKI). These technologies form the backbone of government identity-verification solutions. PIV cards provide physical and digital identity verification for millions of workers. PKI provides the foundation for digital authentication and encryption processes, which are used to protect the privacy and integrity of network communications.

New security solutions must align with guidelines and regulations, such as those established by the National Institute of Standards and Technology (NIST), including:

- **Federal Information Processing Standards (FIPS) 140-2**[1] which defines requirements for digital authentication.
- **NIST Special Publication 800-63-2**[2] which provides comprehensive guidelines for constructing electronic authentication systems.

To build security solutions based on these guidelines and regulations, government agencies typically use products and technologies that are certified as compliant, to ensure they are building on a sound foundation. PCs and laptops based on 6th and 7th Gen Intel® Core™ vPro™ processors offer a valuable resource for agencies that are looking to strengthen security without sacrificing compliance.

These systems provide built-in security technologies that help to effectively protect data, applications, and identities. They also provide built-in support for strong, multifactor authentication using a FIPS-certified, hardware-based cryptography engine that helps to eliminate security gaps that are inherent in software-only solutions.

Enhanced Trust with 6th and 7th Gen Intel Core vPro Processors

Intel has been integrating hardware-based security technologies into its platforms for years to help strengthen and extend software-based security solutions. Today, 6th and 7th Gen Intel Core vPro processors power Intel's most trusted platforms. These systems include built-in support for:

- **Trusted boot** (including early launch anti-malware drivers) to help enforce that systems can only boot into known good states. By measuring and verifying the launch state, these technologies help to protect against sophisticated threats, such as root kits, that can compromise a system before the operating system (OS) and security applications have loaded.

- **Secure enclaves** to help protect systems, data, and running applications by preventing unauthorized software from accessing sensitive resources.
- **Agent monitoring** to quickly identify and respond if an anti-malware agent has been turned off or removed.
- **Out-of-band management** so that client systems can be securely managed and repaired remotely, even if the OS or hard drive has crashed, been powered down, or been otherwise compromised.[3,4]

Systems based on 6th and 7th Gen Intel Core vPro processors also provide Intel® Identity Protection Technology (Intel® IPT) with Public Key Infrastructure (PKI) and Protected Transaction Display (PTD). These technologies provide a built-in, hardware-enhanced solution for multifactor authentication that is well-suited to the needs of enterprises and government agencies. Intel IPT with PKI and PTD supports strong security without the cost and complexity of separate physical devices, such as PIV smart card readers or USB security tokens. It offers a relatively simple and flexible way to increase client security, and is ideal for mobile usage models.

For organizations that do not use PKI, systems based on 6th and 7th Gen Intel Core vPro processors also support Intel IPT with One Time Password (OTP). This technology offers another method for multifactor authentication. In addition to a user's normal sign on procedures, the platform authenticates itself to the network using a unique, six-digit number that is used just once and automatically refreshed every 30 seconds.

A FIPS-certified, Hardware-based Cryptography Engine

Most mainstream computing systems perform cryptography by using software applications that run on the main processor. These systems store keys, certificates, and PINs in software where they are potentially vulnerable. If the OS is compromised, for example, the security solution may be exposed to malware or hackers. Furthermore, maintaining a FIPS-certified system is challenging when software-based solutions are frequently updated.

Trusted Platform Modules (TPMs) were developed to close this gap by providing dedicated, security-hardened storage and execution resources that are isolated from the rest of the platform. TPMs have not been widely adopted, however, because they increase platform costs and integrating them into existing environments can be a challenge.

Systems based on 6th and 7th Gen Intel Core vPro processors provide a built-in alternative to TPM. These platforms include a hardware-based cryptography engine running within the Intel® Management Engine (Intel® ME). The Intel ME is an isolated hardware environment running in the chipset and beneath the OS. It includes its own CPU, memory, I/O channels, and firmware, and supports tightly controlled, security-hardened interactions with the rest of the platform.

This isolated environment can be used to generate and store encryption keys and certificates, and to perform other core cryptographic operations. When the isolated environment is used in this way, keys and certificates never leave the Intel ME in unencrypted form. Even if the OS were compromised, it would be difficult, if not impossible, for malware or hackers to expose these critical security secrets.

Intel worked closely with NIST and followed its FIPS certification process to ensure FIPS 140-2 compliance and validation for this built-in cryptography engine. The Cryptographic Module Validation Program that NIST established issued certificate number 2720 for the Cryptographic Module for Intel® vPro™ Platforms' Security Engine Chipset. As a result, it can now be used in combination with other FIPS-compliant systems and software to fundamentally improve platform trust without sacrificing compliance.[5]

Hardware-enhanced Authentication

The FIPS-certified cryptography engine provides the foundation for hardware-enhanced authentication using Intel IPT with PKI. With this usage model, a worker's PIV card is used to generate a Derived PIV Credential (based on NIST SP 800-157 guidelines). The Derived Credential can be stored directly within a desktop or mobile device and used in place of the physical PIV card to authenticate the system during online interactions. This eliminates the need for a separate card reader, making it simple and cost-effective to implement and support.

Although Intel IPT with PKI provides the enhanced security of a hardware-based solution, it can be deployed and managed with the ease of a software solution. Applications that work with the Microsoft* Crypto API will work with Intel IPT. The only application change required is the creation of an additional digital certificate template on the Certificate Authority, which is used by the application so the certificate is properly formatted during processing.

Strong, Multifactor Authentication

Intel IPT with Protected Transaction Display (PTD) provides a built-in, tamper-resistant keypad solution. The keypad can be used to input a user PIN that unlocks the RSA keys and certificates.

Like the cryptography engine, PTD runs in the isolated execution environment of the Intel ME. The keypad is independent of the OS. It cannot be accessed or monitored by the OS or by applications, such as keyloggers or malware, that run on the OS. Users view the keypad through a hardware-protected video channel, and the numbers are randomized to protect against attack strategies that attempt to decipher mouse-click or touch patterns. With these protections, the keypad is visible and useable only by a user that is physically present in front of the device. It is also strongly protected against potential hacker and malware attacks.

When signing onto a protected network using Intel IPT with PKI and PTD security features, the system must contain the appropriate Derived Credential and the user must be able to input the correct PIN, which provides two factors for authentication. Both the credential and the PIN are hardware-protected throughout the transaction. Either solution alone provides important security benefits versus a software-only solution. Together, they provide built-in support for hardware-enhanced, multifactor authentication that is cost-effective, easy to implement, and simple to use.

Finding the Right Client Platforms for Intel IPT

Intel IPT has been built into select Intel platforms for many years. IPT PKI was introduced later and only on Intel Core vPro platforms that are specifically oriented toward enterprise customers. FIPS-compliance for the cryptography engine is even more recent, and is currently available only in platforms based on 6th and 7th Gen Intel Core vPro processors. For use cases that do not require FIPS compliance, a number of additional platform options are available (see Table 1 for details).

PLATFORM	INTEL® PROCESSORS *(Find Intel processors by Generation)*		INTEL IPT TECHNOLOGIES			FIPS-CERTIFIED CRYPTOGRAPHY ENGINE
			OTP	PTD	PKI	
	6th generation and higher	Intel® Core™ vPro™ processors	◆	◆	◆	◆
	3rd generation and higher	Intel Core vPro processors	◆	◆	◆	
	2nd generation and higher	Intel® Core™, Intel® Xeon®, Pentium®, and Intel® Celeron® processors	◆	◆		
	Intel® Atom™ processor Z3795 (Android*, Windows*)		◆	◆	◆	
	Intel Atom processors Z3XXX (Android, Windows)		◆	◆		
	Intel Atom processors Z25XXX (Android)		◆	◆		

Source: Intel research. For more complete information about performance and benchmark results, visit www.intel.com/benchmarks

Table 1. Intel® Identity Protection Technology (Intel® IPT): Supported Platforms

Summary—A Simple Path to Strong, Compliant Security

Systems based on 6th and 7th Gen Intel Core vPro processors provide a strong foundation for protecting hardware, software, and data from today's increasingly sophisticated malware and hacker attacks. A range of security technologies are built into the hardware to help protect the system during boot and runtime. Built-in technologies also support out-of-band management, which can help IT organizations maintain security-hardened configurations and respond to security issues effectively and with less effort than software-based in-band management solutions.

These platforms also include Intel IPT with PKI, PTD, and OTP, which provide built-in support for strong, multifactor authentication. To simplify integration, Intel IPT is built on top of a standards-based, 140-2 FIPS-certified cryptography engine. For federal agencies, federal contractors, and other organizations with strict security and regulatory requirements, this built-in solution provides a relatively simple and cost-effective way to extend and strengthen security for today's increasingly mobile usage models.

Where to Get More Information

- **7th Gen Intel® Core™ vPro™ Processors**
  http://www.intel.com/content/www/us/en/products/processors/core/core-vpro.html
- **Intel® vPro™ Technology**
  http://www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-technology-general.html

References:

[1] Written by Donald L. Evans, Secretary, U.S. Department of Commerce, Phillip J. Bond, Under Secretary for Technology, Technology Administration, and Arden L. Bement, Jr., Director, National Institute of Standards and Technology, published May 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[2] Written by William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, and W. Timothy Polk of the Computer Security Division Information Technology Laboratory, and Sarbari Gupta and Emad A. Nabbus of Electrosoft Services, Inc., published August 2013. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. For more information and a list of Annexes, visit http://csrc.nist.gov/groups/STM/cmvp/standards.html

[3] Intel® vPro™ technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environments. To learn more, visit: www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-technology-general.html.

[4] Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware, and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit www.intel.com/technology/vpro/index.htm

[5] Note: FIPS-compliance for the cryptography engine in 6th Generation Intel® Core™ vPro™ processors requires an update to the default firmware that is typically performed by the system manufacturer. Check with your preferred vendor for details.