SECURITY FEATURES

Alexande Melnikov
Field Application Engineer
September 2018

Legal Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. Check with your system manufacturer or retailer or learn more at intel.com.

No computer system can be absolutely secure.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/benchmarks .

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit http://www.intel.com/benchmarks .

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

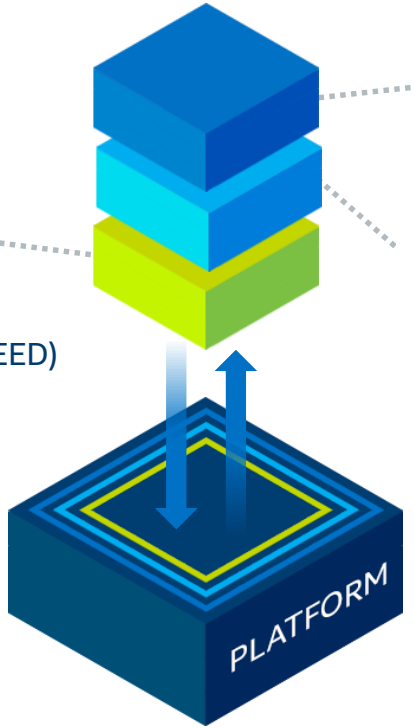
Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

© 2018 Intel Corporation.
Intel, the Intel logo, and Intel Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.
*Other names and brands may be claimed as property of others.

Intel's Trusted Infrastructure: Essential from the Bottom Up

1. BUILD ESSENTIAL TECHNOLOGIES INTO THE PLATFORM

- Root of trust module (Intel® PTT, TPM)
- Built-in instruction set for verification (Intel® TXT)
- Fast, high quality random number generator (RDSEED)
- Firmware assurance (Boot Guard, BIOS Guard)



3. PARTNER FOR OPTIMIZED ISV SECURITY SOLUTIONS

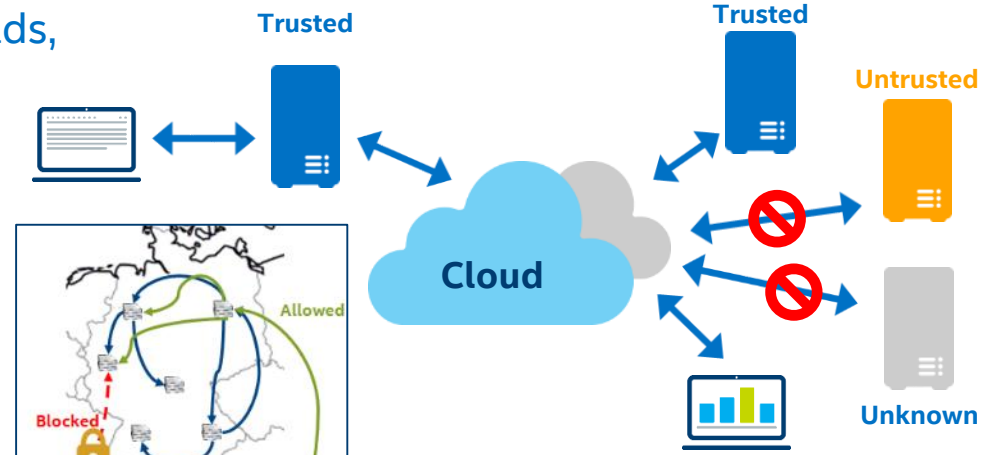
2. ENABLE WITH SOFTWARE

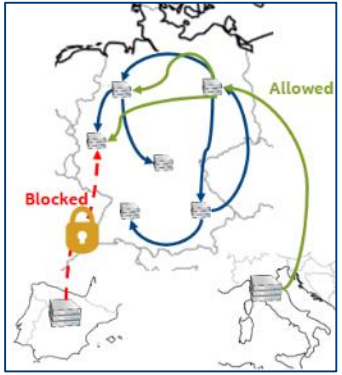
- Efficient provisioning and initialization with One-Touch Activation
- Scalable management with policy enforcement (Intel® CIT)

Intel® Cloud Integrity Technology (Intel® CIT)

Tamper-proof integrity assurance of system platforms / applications / workloads, with a chain of trust rooted in hardware

- Core Attestation Authority
- Applicable to Compute, Network, Storage, and Devices
- Integrity Assurance: Launch-time and runtime assurance
- Leverage hardware mechanisms like Intel® TXT, Boot Guard, etc for measured boot
- Integrate into various Orchestration, Scheduling, and Policy Management environments for 'Trust-based' application placement and execution
- Enable security controls, and meet Continuous Monitoring & Compliance requirements





Use Model 1: Trusted Platform and Workloads Launch

Attestation provides information about platform and workloads (VMs, containers, VNFs…) trust to improve response to malware threats

Use Model 2: Trusted Compute Pools

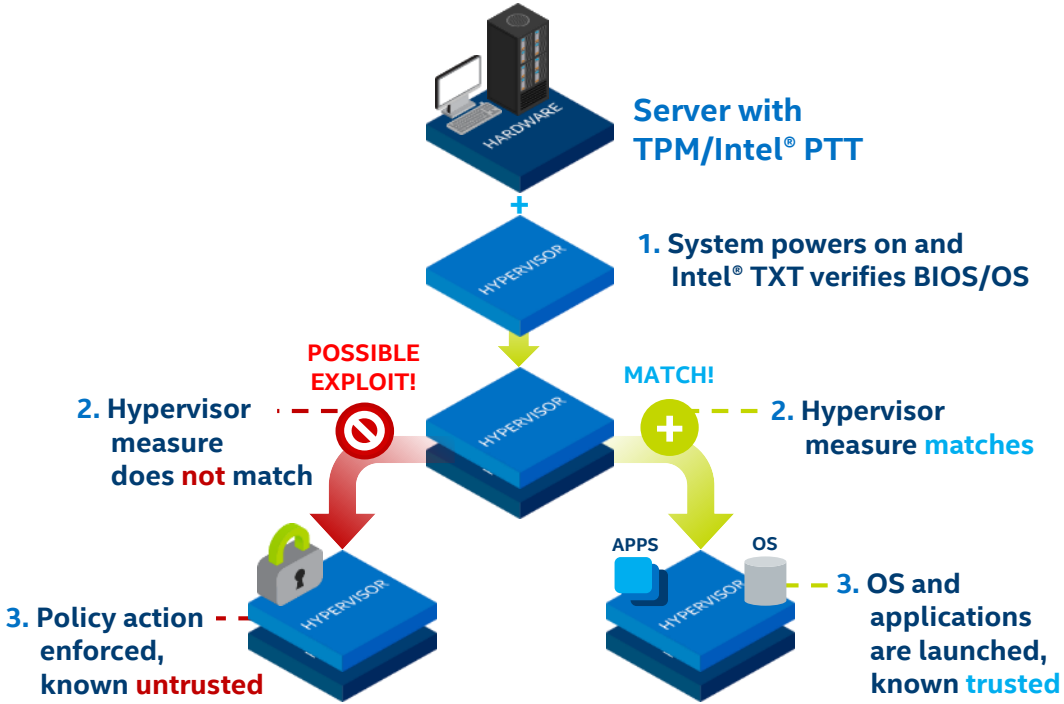
Attestation provides information to inform which systems are trustworthy for hosting workloads

Use Model 3: Compliance

Attestations allow verification of platform and workloads trust for comparison against policy and use in audit—this includes *Geo-boundaries*

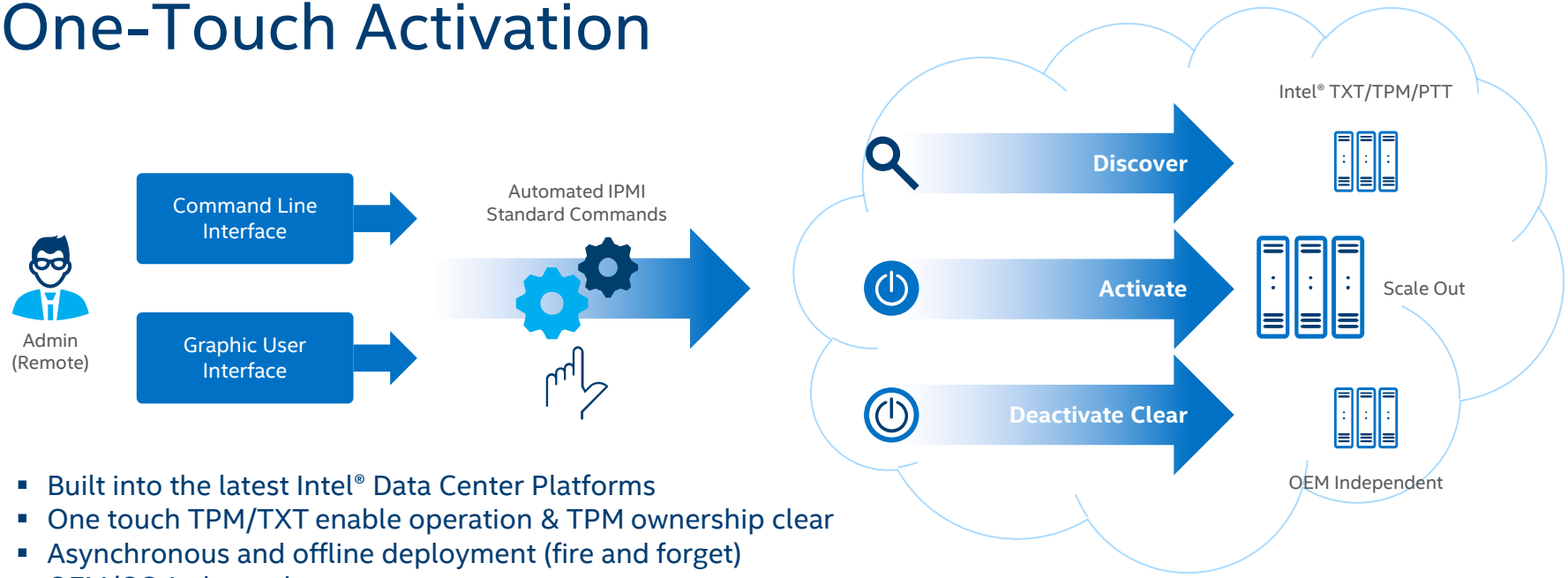
Intel® Trusted Execution Technology (Intel® TXT) with One Touch Activation (OTA)

Now enhanced with Remote & Out-of-Band (OOB) provisioning



- System boot stack gets crypto-hashed before execution
- Hash values get safely stored in a Trusted Platform Module (TPM) or **Intel® Platform Trust Technology (Intel® PTT)** ...new on Purley
- Match to known-good values determines system trust status
- **One-Touch Activation**: OOB TXT/TPM remote discovery, enablement, activation independent of OEM/OS ...new on Purley

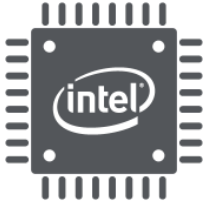
Hardware Root-of-Trust Now Made Easier with One-Touch Activation



- Built into the latest Intel® Data Center Platforms
- One touch TPM/TXT enable operation & TPM ownership clear
- Asynchronous and offline deployment (fire and forget)
- OEM/OS-independent
- No more than one reboot required (saves time)
- Easily scalable to cloud levels
- Replaces Intel® Platform Trust Enabler (Intel® PTE) functionality

All Platforms Need a **Root of Trust**

Choose a Discrete TPM or TPM Functionality Built-into Protected Firmware



Intel® Platform Trust Technology (Intel® PTT)

- Full TPM-2.0 functionality integrated as firmware in the Intel® Management Engine (in silicon)
- Simple Updates
- Compatible with Intel® Node Manager

Uses

- Easily enables Intel® TXT, TXT-based trusted compute pools, and other TXT features
- Intel TXT requires either discrete or firmware TPM

Intel® Platform Trust Technology (Intel® PTT) provides real customer value

Easier Trust enablement allows for more security control

Intel® PTT provides an integrated TPM (iTPM) for customers

Customer Benefits

Auto Trust Enablement

- Low attached rate due to complexity
- PTT makes Trust enabling painless

Flexibility

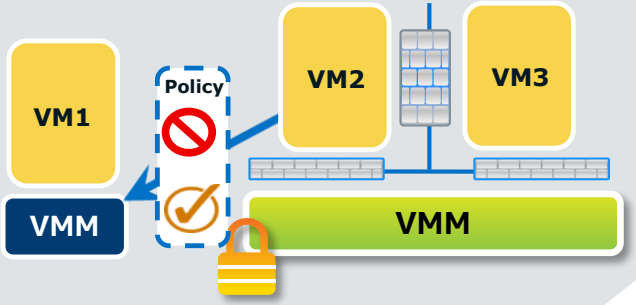
- Allows OEM's TPM ubiquity
- May choose to turn TPM on/off easily
- Makes TPM updates easier for customer

Technical Benefits

Establishes "trusted" status

Provides better visibility into system integrity to enforce control over virtualized environments

Intel® TXT



Intel® Platform Trust Technology

Easier trust activation & maintenance for simpler enablement of trust solutions

Benefits

Simpler Trust Activation

- PTT integrated into platform vs. a discrete solution
- Automatically integrated into platform

Simple Updates

- PTT updates provided via Intel, single supplier
- Compatibility validated

Advantages over discrete TPM

- Supports optional dTPM commands (e.g. encrypt, decrypt, send keys, etc.)
- No need to integrate a hardware dTPM for trust solutions
- Enhanced physical bus-level security
- Required for Intel® Key Protection Technology (Intel® KPT)

Limitations of PTT compared to dTPM

Compliance

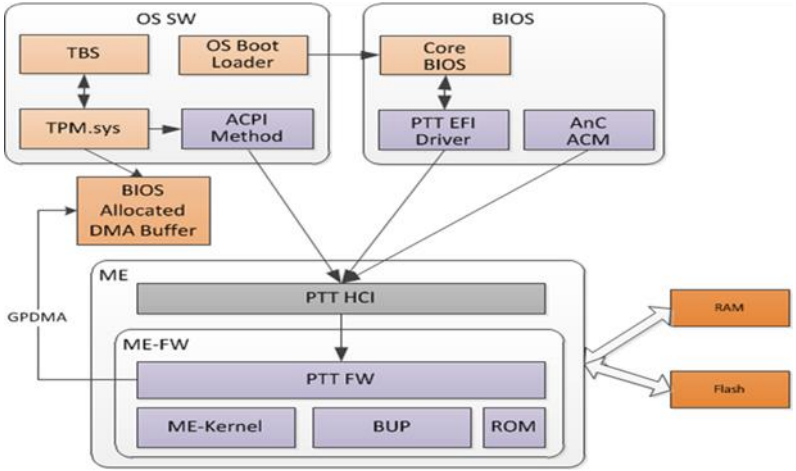
- PTT is not certified by Trusted Compute Group and cannot be used by customers requiring dTPM level compliance
- PTT is TCG compliant
- No support for SMx algorithms on Purley-Skylake

Intel® Platform Trust Technology (PTT)

- Full TPM-2.0 functionality integrated as firmware in Intel® ME, available as an option versus discrete chip
- Implements the TPM 2.0 command response buffer (CRB) interface. Compatible with Intel® Node Manager.
- All volatile and non-volatile data is encrypted and integrity protected
- During manufacturing, PTT can be enabled/disabled as default using an FPF or a Soft-strap
- During run time, BIOS can enable/disable PTT via private command before EOP (if not disabled by default)
- Positioned specifically for Server Platforms not covered by the Intel® vPro™ standard which specifies a dTPM

Option to integrate TPM-2.0 as “firmware”

PTT Architectural Overview



http://www.trustedcomputinggroup.org/resources/tpm_library_specification

Intel® Boot Guard and BIOS Guard™ 2.0

Intel® Boot Guard Reduces a chance of malware exploiting the hardware and/or software components with 3 secured boot options for Purley

Benefits:

Measured Boot

- Intel® Boot Guard puts cryptographic measurement of the Early Firmware* into the platform protected storage device such as a TPM or Intel® Platform Trust Technology (Intel® PTT)

Verified Boot

- Intel® Boot Guard cryptographically verifies the Early Firmware* using the OEM provided policies

Measured + Verified Boot

- Performs both the above

Intel® BIOS Guard™ is an augmentation of existing chipset-based BIOS flash protection capabilities, now with fault-tolerant boot block update capability on Purley

Benefits:

- Protect the BIOS flash from modification without platform manufacturer's authorization
- Protect the BIOS during BIOS updates

http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/security-technologies-4th-gen-core-retail-paper.pdf

Intel® Quick Assist Technology (Intel® QAT)

Now integrated directly into the Lewisburg Chipset

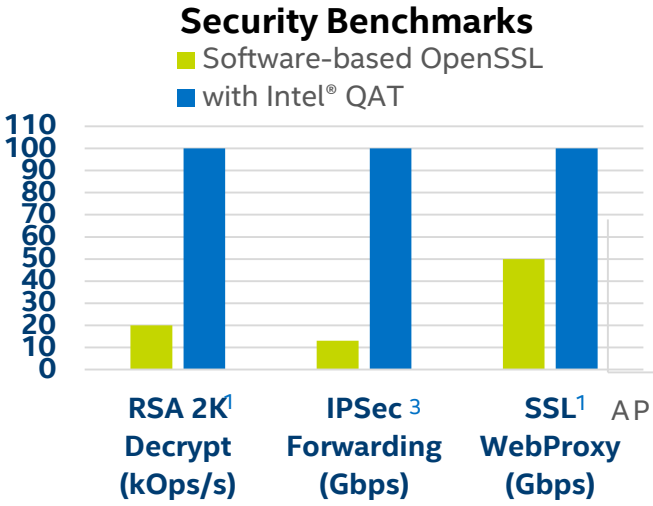
- Set of scalable hardware accelerators exposed to IA. More efficient packet processing, and Functions acceleration. Crypto (public and Pvt keys), and Compression (codecs)
  - Server: secure browsing, email, search, big-data analytics (Hadoop), secure multi-tenancy, IPsec, SSL/TLS, OpenSSL
  - Networking: firewall, IDS/IPS, VPN, secure routing, Web proxy, WAN optimization (IP Comp), 3G/4G authentication
  - Storage: real-time data compression, secure storage.
- Intel® QAT on Purley offers outstanding capabilities: 100Gbs Crypto, 75-80Gbs Compression, 100kops RSA , 2k Decrypt
- Technology genesis in the IXP28xx Network Processors; continuously enhanced since then, in every generation

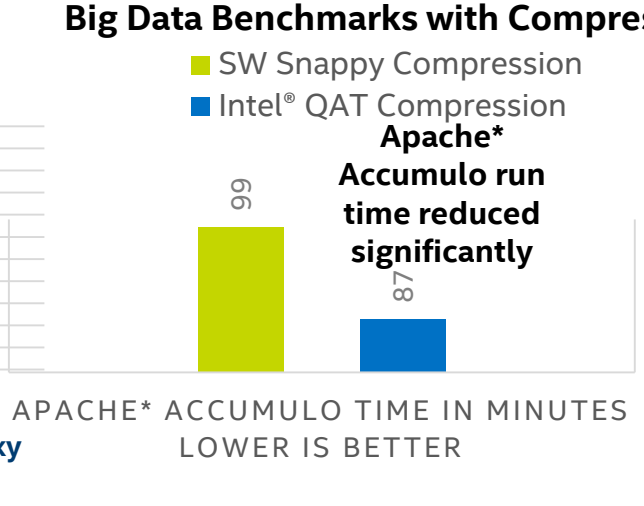
Packet processing & functions acceleration

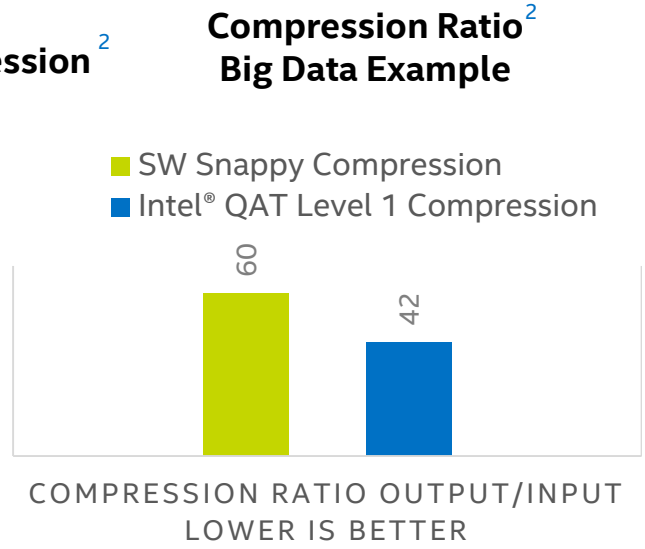
Symmetric cryptography functions including cipher operations and authentication operations
Public key functions including RSA, Diffie-Hellman, and elliptic curve cryptography
Compression and decompression functions including DEFLATE

https://www.intel.com/content/www/us/en/architecture-and-technology/intel-quick-assist-technology-overview.html

Intel® QuickAssist Technology







1. NGINX* and OpenSSL* connections/second. Conducted by Intel Applications Integration Team. Claim is actual performance measurement.
Intel® microprocessor. Processor: Intel® Xeon® processor Scalable family with C6xxB0 ES2
Performance tests use cores from a single CPU, Memory configuration:, DDR4–2400. Populated with 1 (16 GB) DIMM per channel, total of 6 DIMMs
Intel® QuickAssist Technology driver: QAT1.7.Upstream.L.0.8.0-37 Fedora* 22 (Kernel 4.2.7) BIOS: PLYDCRB1.86B.0088.D09.1606011736

2. Cloudera* 5.4.2 with Snappy* Software vs. Intel® QuickAssist Technology hardware solution. Conducted by Intel Applications Integration Team.
Claim is actual performance measurement. Intel® Xeon® processor E5-2699 v4 (56 cores enabled) 256 GB DDR4 1.6 TB NVMe SSD 1 Intel® C6xxx-based card (24x) 10 Gbps CentOS* 6.7 w/ 2.6.32 kernel Cloudera* 5.4.2
QAT driver 0.9.1 Snappy* 1.1.2 (popular, fast compression codec)
One NameNode Eight DataNodes 10 Gbps network

3- 24 Core Intel(r) Xeon Scalable Platform -SP @1.8GHz, Single (UP) Processor configuration. Intel(r) C627 PCH with crypto acceleration capability (in x16 mode) Neon City platform. DDR4 2400MHz RDIMMs 6x16GB(total 96 GB), 6 Channels, 1 x Intel® Corporation Red Rock Canyon 100GbE Ethernet Switch in the x16 PCIe slot on Socket 0. 8 cache ways allocated for DDIO.

Intel® QuickAssist Technology integrates hardware acceleration for compute intensive workloads Such as Bulk Cryptography, Public Key Exchange & Compression on Intel® Architecture Platforms

* Other names and brands may be claimed as the property of others.

Intel® Key Protection Technology (Intel® KPT)

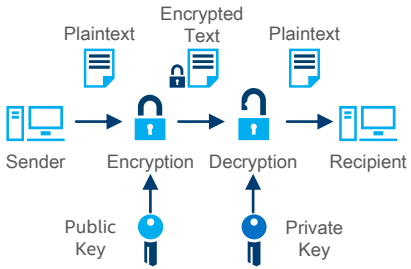
Private keys never exposed in the open in system memory

Everything needs to be authenticated

Everything needs to be encrypted

Encryption & authentication need keys

Keys need to be stored securely



Key Protection Needs:

1. Secure Keys At Rest
2. Secure Keys In Flight
3. Secure Keys In Use

Integrated solution within the Lewisburg chipset

Other use cases include: HTTPS-based applications, VPN tunneling, Certificate Authority, SecureDNS…

Enabled by Intel® QAT + Intel® PTT
…new on Purley

Intel® Key Protection Technology in Purley

1. Key Generation

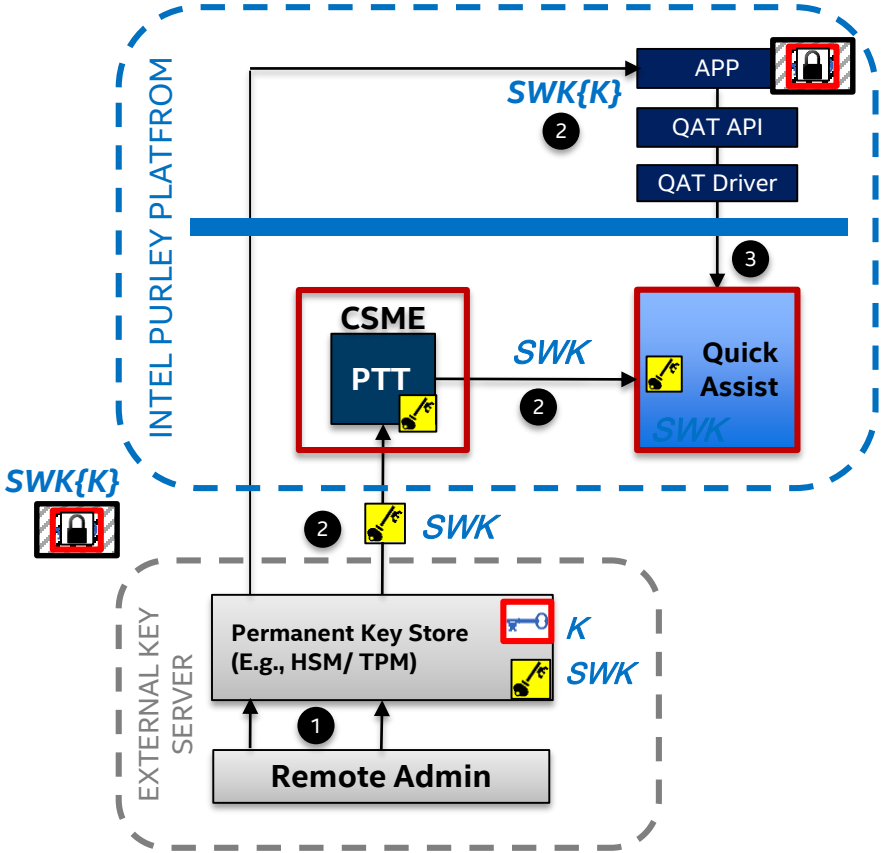
- Remote (eg: Private keys), Enclave (eg: Symmetric IPsec keys/IKE)
- Generate Symmetric Wrapping Key (SWK). Application/Remote Admin uses SWK to Wrap application keys

2. Secure Key Transfer

- Remote Admin provisions ***SWK*** securely in Intel PTT
- ***SWK{K}*** is co-located with application

3. Run Time usage

- Application passes ***SWK{K}*** to QAT
- QAT device unwraps ***SWK{K}*** before executing the crypto operation



Purley SKX KPT Features

FEATURE	DESCRIPTION
Root of Trust and Persistent Key Storage	Intel Platform Trust Technology (PTT) running on CSME. PTT will conform to TPM 2.0 specification (updated with AC_Send family of commands under review by TCG)
Key Types Protected	All asymmetric signing keys, asymmetric decryption keys as applicable to RSA, DSA, EC Point Multiplication, ECDSA. Applicable to all key sizes supported in QAT. This includes RSA key sizes upto 4096 bits and ECC key sizes up to 521 bits.
Crypto Algorithm Services	All QAT asymmetric services but ephemeral Diffie Hellman variants.
Enabling Protocols, CSPs and Applications	OpenSSL, PKCS#11
Enabling Use Cases and Applications	Reference applications exemplifying the usage of wrapped keys must be demonstrated TLS as the underlying network security protocols. (I.e., Nginx and OpenSSL should be modified to work with wrapped keys) <u>Reference Applications Included in Intel SDK</u>: 1. Basic STV Test Application 2. OpenSSL + Nginx with PEM extensions to support wrapped private keys 3. Virtualization Use Case in Cloud/ Data Center
Key Wrapping Algorithms	AES128-GCM, AES256-GCM, AES128-CBC, AES256-CBC with multiple iterations
Virtualization	KVM Virtualization

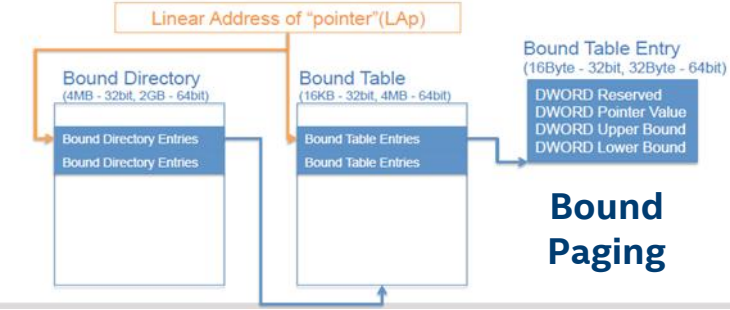
Intel® Memory Protection Extensions (Intel® MPX)

- Attacks are able to exploit software bugs – e.g. invalid memory access which is possible due to buffer overflow/underflow has been exploited. The existing techniques to avoid such memory bugs are software only solutions, that have been resulting in poor protection & performance.
- Intel® MPX introduces new hardware registers and new instructions that operate on these registers. Intel® MPX allows prevention of attacks by testing memory (both stack and heap) buffer boundaries prior to memory accesses. Linux kernel 3.19 onwards support Intel® MPX.
- With Intel® MPX, new "bounds" registers on Intel silicon can now store a pointer's lower bound and upper bound limits. Whenever the pointer is used, the requested reference is checked against the pointer's associated bounds, thereby preventing out-of-bound memory access (such as buffer overflows and overruns). Out-of-bounds memory references initiate a #BR exception which can be handled subsequently.

Foil attacks like "Heartbleed"

https://software.intel.com/sites/default/files/managed/9d/f6/Intel_MPX_EnablingGuide.pdf

- Bounds mapping management mechanism like memory paging
- Bounds paging requires to allocate linear address space



New Instruction	Function
BNDMK b, m	Creates LowerBound (LB) and UpperBound (UB) in bounds register b.
BNDCL b, r/m	Checks the address of a memory reference or address in r against the lower bound.
BNDCU b, r/m	Checks the address of a memory reference or address in r against the upper bound.
BNDCN b, r/m	Checks the address of a memory reference or address in r against the upper bound in one's compliment.

Mode Based Execution Control (XU/XS bits)

- Existing Extended Page Table (EPT) specify the executability of each guest page (via XD bits), regardless of CPU privilege level. Mode-Based Execute Control (XU/XS bits) allow finer granularity - executability of user (XU) and supervisor (XS) pages can be specified.
- Finer granularity of control over code execution can inhibit execution of malicious code, and thereby increase security.
- Deliver platforms on which hypervisors can more reliably verify and enforce the integrity of kernel level code.
- The value of XU/XS bits is delivered through hypervisors, so hypervisor support is necessary. Microsoft is planning to support this feature in Hyper-V next

Executability of user (XU) and supervisor (XS) pages can be specified