Supporting Third Party Attestation for Intel® SGX with Intel® Data Center Attestation Primitives

Vinnie Scarlata, Simon Johnson, James Beaney, Piotr Zmijewski
Intel Corporation
{vincent.r.scarlata, simon.p.johnson, james.d.beaney, piotr.zmijewski}@intel.com

ABSTRACT

Intel® Software Guard Extensions (SGX) has an attestation and sealing capability that can be used to remotely provision secrets and secure secrets to an enclave [1]. In [2], Intel describes how Intel® Enhanced Privacy Identifier (EPID) based attestation keys are provisioned and describes the Intel provided online services to support this architecture.

This paper describes additional services and primitives available to allow 3rd parties to build their own attestation infrastructure, using classical public key algorithms such as ECDSA or RSA. This paper also describes an example deployment pipeline with important trade-offs to be considered when deploying Intel® SGX at scale using these new elements.

1 Introduction

Intel® SGX is a set of processor extensions for establishing a trusted execution environment inside an application [3]. This execution environment is called an enclave. SGX enclaves are created without secrets. Secrets can be delivered after the enclave has been instantiated on the platform. The process of demonstrating that the enclave has been established in a secure hardware environment is referred to as remote attestation. In [1] and [2], Intel describes an attestation architecture based on Intel provided attestation enclaves and the Intel managed Attestation Service for Intel® SGX (IAS) [4]. Intel created a online managed service to ensure that attestation capabilities existed at SGX launch time, to minimize the complexity of handing multiple security versions for a platform's SGX Trusted Computing Base (TCB) and to introduce the use of Intel® Enhanced Privacy ID (EPID) to provide privacy properties.

IAS simplifies verification of EPID attestations. Intel SGX now provides flexibility to allow non-Intel parties to author their own Intel® SGX attestation infrastructure, which can benefit certain use cases, such as:

1) Entities that run large parts of their networks in environments where Internet based services cannot be reached.
2) Entities that are risk averse in outsourcing trust decisions to 3rd parties.
3) Certain application models working in a very distributed fashion (e.g. Peer-to-Peer networks) and using a single point of verification is suboptimal for this model.
4) Environments that have requirements that conflict with the privacy properties that EPID provides.

To address these and other use cases, Intel has been working with our partners in the Intel® SGX ecosystem to provide environments and businesses an architecture that allows them to also benefit from remote attestation whilst not having to use an Intel service to validate their attestations.

To this end this paper outlines extensions to our existing attestation architecture to enable non-Intel parties to build and manage their own Intel® SGX attestation infrastructure. Section 2 provides background on the existing EPID based Intel® SGX attestation architecture. Section 3 describes the additional extensions on the platform that allow 3rd parties to write a Quoting Enclave and generate attestations. Section 4 describes the new online-services Intel will provide to enable 3rd parties to evaluate attestations without run-time reliance on Intel. Section 5 provides an illustrative example of how one could manage the initialization steps needed to enable remote attestation capabilities for these platforms as well as ongoing maintenance from a TCB Recovery operation.

2 Intel® SGX Attestation

Attestation is the process of demonstrating that a software executable has been properly instantiated on a platform. An Intel® SGX based attestation allows a remote party to gain confidence that the intended software is running within an enclave on an Intel® SGX enabled platform. The attestation also conveys the following information in an assertion:

- Identities of software being attested.
- Details of unmeasured state (e.g. the mode software is running in).
- Data which software associates with itself.

Intel® SGX uses an asymmetric attestation key, representing the Intel® SGX TCB, to sign an assertion with the information listed above.

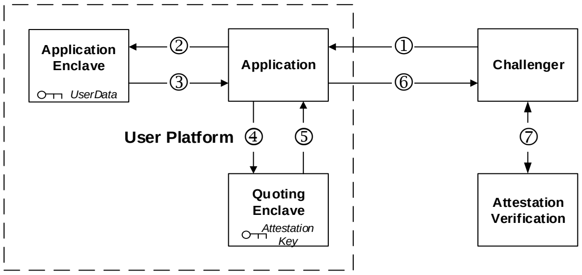


Figure 1: Attestation Flow

In Figure 1 when an application receives an attestation request from an off-platform challenger (1), the application requests that its enclave produce an attestation (2). A two-part process follows involving the application sending a local attestation (3 & 4) [1] from its enclave to a Quoting Enclave (QE). The Quoting Enclave verifies the local-attestation and converts it into a remote attestation (a Quote) by signing the local attestation using its asymmetric attestation key. The Quote (a remote attestation) is returned to the application (5) and then to the challenger (6). Finally, the Challenger can use an Attestation Verification Service (7) to perform Quote verification.

2.1 Intel® EPID Based Attestation

In [2] Intel outlined its offering for a privacy enhanced attestation service using the Intel ® Enhanced Privacy Identifier (EPID) algorithm. EPID is an extension to the Direct Anonymous Attestation (DAA) algorithm that was implemented in the TPM 1.2 [4]. It shares the privacy enhancing properties of DAA, and has an additional signature-based revocation mode. Figure 2 shows how all the different elements in the EPID system relate to one another.

Intel Signing Key (ISK) – is the main signing key used by Intel to authenticate objects it produces. This serves a similar function to the root key of a Certification Authority.

Intel Signing Key Certificate – contains the public signature verification key that is paired with the Intel Signing Key. This is similar to the root certificate of a Certification Authority.

EPID Group Master Key – each group has a master issuing key. This secret key is used in the creation of the group public key and the member join process.

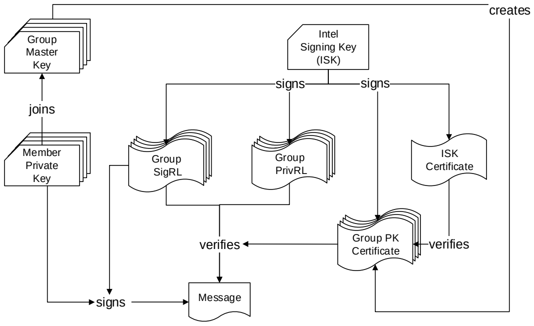


Figure 2: EPID Infrastructure Elements

EPID Member Private Key – each member of an EPID group has their own private key. Intel never knows a members' private key. The key is randomly generated through a blinded join protocol between the provisioning enclave on the platform and Intel

EPID Private Key Revocation List (PrivRL) – is a list of EPID private keys that Intel knows have been compromised, because Intel has been given the EPID private keys.

EPID Signature Revocation List (SigRL) – is a list of EPID signatures which were signed by EPID keys that are suspected to have been compromised.

EPID Group Public Key Certificate – is the certified form of the EPID Group Public Key. EPID Group Certificates are signed by the Intel Signing Key.

2.2 Managing TCBs

SGX was designed so that if a vulnerability is fixed by an update to the platform, relying parties can verify that the update is in place. The process of updating the platform attestation to reflect the update is called TCB Recovery. A new attestation key is created to reflect the update in the platform's attestations. The new TCB will be reflected in attestations that occur following the replacement of the attestation key. Should an individual platform become permanently revoked due to an irrecoverable attack, the platform should not receive a new attestation key.

Each element of the SGX TCB is assigned a Security Version Number (SVN). For the hardware, these SVNs are referred to collectively as the CPUSVN, and for software referred to as ISVSVN[3]. A TCB is considered up to date if all components of the TCB have SVNs greater than or equal to a threshold published by the author of the component. Section 4.2.3 goes into more detail about how Intel publishes SVNs of SGX TCB components.

In addition to conveying that an attestation is properly signed, it is also the responsibility of an Attestation Service to evaluate the status of the TCB that created the Attestation. The service should identify/manage which TCB's are up to date and those which are not.

3 Intel® SGX Third Party Attestation

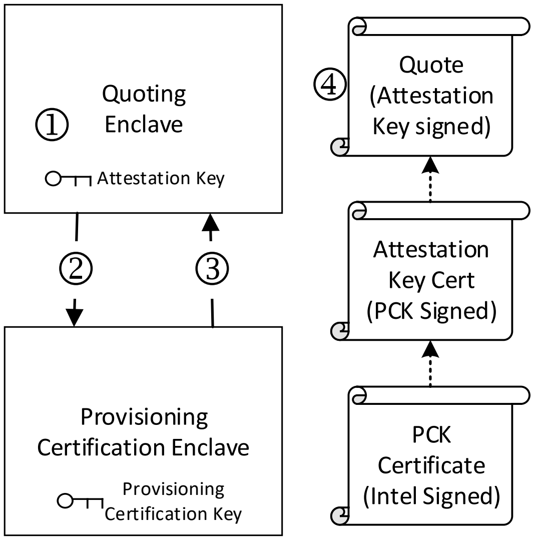
3.1 Overview

To support non-Intel attestation infrastructures for Intel® SGX, Intel provides a general certification infrastructure to certify Quoting Enclaves with a certificate chain rooted to an Intel issued certificate.

The foundation of this infrastructure, shown in Figure 3, is an Intel-provided enclave called the Provisioning Certification Enclave (PCE), which acts as a local Certificate Authority for local Quoting Enclaves (i.e. running on the same platform as each other). The Quoting Enclave(s) generate their own Attestation Keys using their preferred method and algorithm (1). The QE provides the PCE with the attestation public key (2). The PCE authenticates the request and issues a certificate-like structure identifying the QE and the Attestation Key (3). This structure is signed by a device and Trusted Computing Base–specific signing key called the Provisioning Certification Key (PCK). Intel publishes certificates and certificate revocation lists (CRLs) for the PCKs in all genuine Intel platforms. This results in a complete signature chain from the Quotes to an Intel CA (4). The resulting Quote can be verified by anyone with the complete certificate chain and CRLs.

3.1.1 Provisioning Certification Enclave (PCE)

The PCE uses two values to facilitate serving as a local CA. Both values are derived from hardware keys available from the EGETKEY instruction.



Quoting Enclave
①
Attestation Key
②
③
Provisioning Certification Enclave
Provisioning Certification Key
④
Quote (Attestation Key signed)
Attestation Key Cert (PCK Signed)
PCK Certificate (Intel Signed)

Figure 3: Quote Certificate Chain

The first value, the Provisioning Certification Key, is an IETF RFC 6090 [5] compliant 256 bit Elliptic Curve signing key, using the NIST p-256 curve. It is unique to the device, the current Intel® SGX TCB SVNs, and the PCE's ISVSVN. The *CertifyKey()* API allows an enclave to request that provided data be certified using that key.

The other value is the Platform Provisioning ID (PPID), which is unique to the platform and PCE identity, but not to the specific TCB. This values and corresponding TCB SVNs are used to identify the platform when requesting the corresponding PCK certificate from Intel.

3.1.1.1 Certify Key API

To be meaningful, the certificate-like structure created by the PCE must contain the measurement identity of the enclave requesting the signature. The PCE uses the SGX local attestation architecture to identify the requester. The caller provides a REPORT created by EREPORT including caller-specified ReportData. The caller also specifies which PCK should be used, identifying it by the CPUSVNs and PCE ISVSVN for the key. The reason for specifying the CPUSVN is that it allows the flexibility to request a key be signed by a lower CPUSVN if certificates do not exist or are not available for the current TCB.

The PCK is a unique hardware identifier, which some users will prefer not be generally accessible, particularly consumer platforms leveraging Intel's EPID attestation. In order to prevent the PCK from being exposed to software not authorized to access the unique IDs, the PCE will only honor requests from enclaves with ATTRIBUTES.PROVISIONKEY set to 1. Authority to set the PROVISIONKEY attribute is controlled by the Launch Enclave, which is selected by the Operating System. [3]

3.1.1.2 GetPCInfo() API

The PCE's *GetPCInfo()* API allows other enclaves to request a copy of the platform's PPID and PCE's SVN. Similar to *CertifyEnclave()*, the *GetPCInfo()* API will only honor requests from enclaves with the ATTRIBUTES.PROVISIONKEY set to 1.

Additionally, the PPID is encrypted in transit from the PCE to the calling enclave. The caller specifies a public key in the request, and the PCE encrypts it using that key. The caller can also specify the crypto algorithm, however the initial version of the PCE only support is RSA 3072 with OAEP padding.

The method of selecting the encryption key is based on the privacy requirements for the environment it's used in. For privacy sensitive attestation environments, the PCK Certificate Service's key (Section 4.2.1) might be used, to ensure the unique IDs have end to end confidentiality between the PCE and back end. When non-privacy sensitive environments, the key can be an ephemeral key generated by the Quoting Enclave prior to calling the API.

3.1.2 Quoting Enclave

In addition to the Intel's EPID-based Quoting Enclave, Intel will release an open source Quoting Enclave that creates ECDSA-based Quotes that can be verified without the need for an Intel managed attestation service. Intel will also release a signed binary version of the QE to be used by providers looking to remain outside their customers TCBs.

The Intel provided ECDSA Quoting Enclave supports IETF RFC 6090 compliant 256 bit Elliptic Curve signing keys, using the NIST p-256 curve.

3.1.2.1 Attestation Signing Key Generation

Unlike group signing algorithms such as EPID, traditional asymmetric signing algorithms do not require a "join" step with a back-end server. Attestation Keys can be generated locally and then certified as being created and owned by a specific platform protected with a specific TCB.

The Intel Quoting Enclave generates the attestation key using a derivative of its Seal Key (from EGETKEY) as a seed to a key derivation algorithm in order to generate a repeatable signing key. This key is not known to Intel and changes to OwnerEpoch will cause a new Attestation Key to be developed, but this key will be the same when generated anywhere on the platform at the same TCB and across resets and does not require persistent storage.

If it's desired that the same Quoting Enclave generate a different key, for example when invoked in different VMs, a QE developer can alternatively generate the attestation key using the hardware DRNG. Note that this will give different VMs unique Quoting Keys, but they will be certified by the same platform Provisioning Certification Enclave (PCE).

If a new attestation key is required, such as after a TCB Recovery, the Quoting Enclave generates a new ECDSA key using the same procedure.

3.1.2.2 Certification

The Intel provided QE implements separate APIs for key generation and key certification functions. In the event that the PCE or Provisioning Certification Key are compromised but not the Quoting Enclave, the existing Attestation Key can be re-certified rather than requiring a new QE key be generated.

4 Attestation Verification

4.1 Overview

To verify an Intel® SGX attestation, the verifier should take the following steps.

1) Verify the integrity of the signature chain from the Quote to the Intel-issued PCK certificate.
2) Verify no keys in the chain have been revoked.
3) Verify the Quoting Enclave is from a suitable source and is up to date.
4) Verify the status of the Intel® SGX TCB described in the chain.
5) Verify the enclave measurements in the Quote reflect an enclave identity expected.

These steps can either be taken by the relying party or one or more steps can be offloaded to a dedicated Attestation Verification Service. Typically even when using an Attestation Verification Service, step 5 will be done by the relying party since a general purpose verification service in less likely to know the expected enclaves of the relying party.

4.2 Provisioning Certification Service for Intel® SGX

In order to complete the steps listed in Section 4.1, the verifier needs access to several pieces of information, in addition to the Quote itself.

1) Intel-issued Certificate for the PCK that certified the attestation key,
2) Revocation list that applies to the PCK certificate and any intermediate CA used to certify it,
3) Up-to-date SVNs for the CPU & PCE.
4) Identity of Quoting Enclave trusted to generate attestation key and issue Quotes.

The Provisioning Certification Service for Intel® SGX that is provided as part of the Intel® Software

Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) will provide access to items #1-3 for users of both Intel and non-Intel Quoting Enclaves. For customers using Intel's open source ECDSA Quoting Enclave, Intel® SGX DCAP will also provide access to #4.

The following sections highlight the functions of this service.

4.2.1 Provisioning Certification Key Certificate API

The Provisioning Certification Key Certificate API distributes X.509 certificates for PCKs in Intel® SGX platforms. This service offers two options: single certificate and bulk certificates.

In the first variant, the requester specifies the PPID encrypted by a key owned by the certificate service (from the PCE.GetPCInfo API), the CPUSVN (appears in EREPORT), the PCE's ISVSVN (from PCE.GetPCInfo API, a special collection tool, or Intel® SGX Platform Software documentation), and PCEID. This is useful when verifying a single Quote.

In the second variant, the requester only specifies the encrypted PPID and PCEID, and the service will respond with certificates for the current SVNs and all historic configurations. This is useful when hosting an Attestation Service that must be prepared to verify attestations from arbitrary software configurations, such as a Cloud Provider whose customers configure their own VMs.

In addition to the public PCK key and standard x509 fields, PCK certificates also include custom fields with the following information: PPID, CPUSVN, PCE's ISVSVN, Family-Model-Stepping-Platform Type-SKU of the CPU, and additional product type specific fields.

Sometimes the SVN of an SGX TCB component is incremented for non-security reasons. In this a case, a certificate may not be issued for the incremented SVN. Rather the platform should continue using the certificate with the SVN of the last security related increment. The PCK Certificate API will automatically return the certificate that best describes the security posture of the platform, though it may be for a set of SVN values lower than those currently executing.

4.2.2 Provisioning Certification Key Certificate Revocation List API

The PCK Certificate Revocation List (PCK CRL) API distributes x509 certificate revocation lists for PCKs certificates and CA certificates (intermediate and root) used when certifying PCK certificate chain.

4.2.3 TCB Info API

The TCB Info API distributes a list of supported CPUSVN and PCE ISVSVN for a given platform type (together with their statuses). The requester specifies the Family-Model-Stepping-Platform Type-CustomSKU (FMSPC). These values are available from the PCK certificate for that platform. While certificates may not be available for all possible SVN combinations, a certificate is available from the PCK certificate API for every combination found in the TCB Info structures list.

TCB information is signed and dated by the service. This allows it to be stored and verified in the future. For example, a logging system may store an enclave's transaction, a Quote of its signing key, and the current TCB Information. Later an auditor can verify that the transaction was computed by the correct enclave and at the time of the transaction, the platform TCB was up to date.

The up-to-date SVNs are the SVNs of latest software/firmware release for which Intel has issued a PCK certificate. It is possible the up-to-date SVNs returned by the service to be lower than the SVNs returned by EREPORT on the platform as described in Section 4.2.1.

The service may also provide a list of "out of date" SVN sequences. These reflect configurations that were released as product release but have been superseded by newer versions due to security issues.

In the event that an SVN is not up to date, the verifier is responsible for deciding whether to interact with this platform. Note that if the attestation includes SVNs that are lower than the lowest value in the list, a pre-production/development is present within the TCB and the appropriate policy must be used (e.g. use only pre-production secrets).

4.2.4 Quoting Enclave Identity API

The Quoting Enclave Identity API distributes the measurements and SVN of the most up-to-date ECDSA Quoting Enclave released by Intel. The API is similar in nature to the TCB Info API, but focuses on the QE, while TCB Info focuses on the hardware, CPU firmware and the PCE. Similar to the TCB Info Structure, the QE Identity is signed and dated. Environments not using an Intel Quoting Enclave can disregard this service.

4.3 Verifying the Intel® SGX TCB status

Once an attestation verifier has verified the Quote signature chain using used the PCK certificate, it should evaluate the current status of the Intel® SGX TCB of the target platform. It does this with the TCB

Info structure for this platform type, identified by comparing the FMSPC from the PCK Certificate and FMSPC in the TCB Info structure.

The TCB Info structure contains a list of recognized hardware SVN configurations, PCE SVNs, and status codes for the specific hardware. The verifier should compare the 16 SVN components and PCESVN from platform's PCK certificate to those in the TCB Info structure until a record is found such that all values in the PCK certificate are greater than or equal to the corresponding value in the TCB info structure. If no entry in the structure meets this condition, then the TCB is unsupported and may likely contain a pre-production or debug module.

The status code associated with the matching SVNs indicates the current status of the TCB. Current status codes will reflect that the TCB is up-to-date, out-of-date, additional configuration is required, or revoked.

5 Example Attestation Infrastructure for Data Center or Cloud Deployments

This chapter describes an example deployment flow for a Cloud Service Provider (CSP) to host an Attestation Service capable of verifying Quotes created by their platforms without any "runtime" connectivity to Intel® SGX DCAP or other services. This flow, shown in Figure 4, combines collection of PPIDs, creation of Attestation Keys, retrieving certificates/TCB information, and attestation verification.

5.1 Identifying Platforms

During the deployment phase when the new platform is prepped, tested, and initial software loaded, the platform registers itself with the CSP's infrastructure.

The Quoting Enclave retrieves the encrypted PPID from the PCE. A software agent delivers the PPID, CPUSVNs, and PCEID to a CSP-owned Inventory Management Service (IMS). The IMS can be a self-sufficient service or just a logical set of functions and databases that are part of a larger, possibly pre-existing infrastructure. The IMS's role is to track Intel® SGX attestation identities and retrieve PCK certificates for the Attestation Service.

The Encrypted PPID is provided to the IMS to enable the service to identify the platform when requesting PCK certificates from Intel. This only has to be collected once during deployment since the PPID remains constant for the lifetime of the platform.

Once registered, the platform then continues through deployment process.

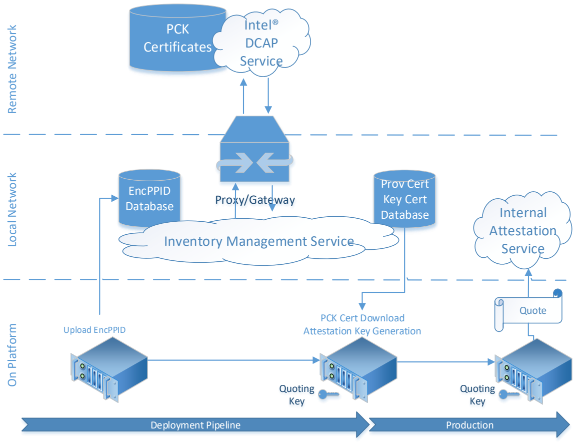


Figure 4: Example Deployment Pipeline

5.2 Acquiring PCK Certificates

While the platform continues through deployment process, the Inventory Management Service uses an Internet gateway to the Intel® DCAP services and requests the PCK certificates for each CSP-owned platform using the interface that retrieves both current and historic certificates for each platform. This provides the Attestation Service with multiple certificates for different TCBs, providing the greatest chance that the service will have an appropriate PCK certificate for whatever attestation software their customer installs in their environment.

5.3 Certifying Attestation Keys

To ensure that PCE certifies the new Attestation Key with a PCK for which a certificate exists, it's recommended that before generating the attestation key, a software agent download the PCK certificate from the Inventory Management Service. The PCK certificate contains the CPUSVN value that corresponds to that PCK. After generating the Attestation Key, the Quoting Enclave can specify this value when requesting the PCE to certify the Attestation public key.

5.4 TCB Recovery

After an Intel® SGX TCB element is updated, the process for establishing a new attestation key depends on what type of element was updated.

If a Quoting Enclave was updated, the QE can simply be upgraded and a new attestation key can be generated and certified as described in Section 3.1.2.2. This may not require interaction with the attestation infrastructure.

If a CPU-related component, such as microcode updates or the PCE was updated, a new PCK is required for the PCE. When this occurs, in addition to the QE generating a new attestation key, the infrastructure must also acquire new PCK certificates, CRLs, and TCB Info structures.

The CSP Inventory Service requests updated certificates for all CSP-owned platforms affected. If the inventory service maintains a database of encrypted PPIDs and model information for the CSP's platforms, it will have all the information necessary to request new certificates without any interaction with the platforms.

CSPs may choose to continue to use the previous Attestation Keys until all platforms are upgraded and all certificates are downloaded and provided to the CSP Attestation Service. This ensures that the Attestation Service will always have the material needed to verify a Quote and will never need to contact external services in real-time.

6 Summary

The Intel® SGX Attestation Service simplifies the management of attestation keys, platform security versions and attestation verifications. For those service providers that wish to offer their own classical PKI-based services, the Intel® SGX third party attestation support architecture enables non-Intel parties to author their own Intel® SGX attestation infrastructure. The Intel® SGX Data Center Attestation Primitives provides platform software, infrastructure tools, reference code, and online services to facilitate 3rd parties deploying and managing their own infrastructures. Further information about SGX can be found at http://software.intel.com/sgx .

7 References

[1] I. Anati, S. Gueron, S. P. Johnson and V. R. Scarlata, "Innovative Instructions for Attestation and Sealing," 2013. [Online]. Available: https://software.intel.com/en-us/articles/innovative-technology-for-cpu-based-attestation-and-sealing.

[2] S. Johnson, V. Scarlata, C. Rozas, E. Brickell and F. Mckeen, "Intel(r) Software Guard Extensions: EPID Provisioning and Attestation Services," March 2016. [Online]. Available: https://software.intel.com/sites/default/files/managed/57/0e/ww10-2016-sgx-provisioning-and-attestation-final.pdf.

[3] Intel, "Intel(r) 64 and IA-32 Architectures Software Developers Reference Manual," November 2015. [Online]. Available: http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html.

[4] Trusted Computing Group, "Trusted Platform Module Main Specification (TPM1.2)," March 2011. [Online]. Available: http://www.trustedcomputinggroup.org/resources/tpm_main_specification.

[5] D. McGrew, K. Igoe and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms," *RFC 6090,* February 2011.

[6] E. Brickell and J. Li, "Enhanced privacy ID from bilinear pairing for Hardware Authentication and Attestation," *International Journal for Information Privacy, Security and Integrity,* vol. 1, no. 1, pp. 3-33, 2011.

[7] F. Mckeen, I. Alexandrovich, A. Berenzon, C. Rozas, H. Shafi, V. Shanbhogue and U. Savagaonkar, "Innovative Instructions and Software Model for Isolated Execution," in *Hardware and Architectural Support for Security and Privacy*, 2013.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® processors may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details.