Intel® SecL-DC

Intel(R) SecL-DC Version 4.0 GA

Foundational/WL Use Cases:

• Support for Client Intel® PTT (fTPM) has been added. ISecL has always supported the server implementation of PTT. However, the client implementation has a difference in the endorsement certificate hierarchies that would cause the TPM authenticity verification to fail during Trust Agent provisioning. This alternative implementation is now supported.

• Support for TPM SHA384 PCR banks has been added. Newer TPMs support SHA384, and ISecL has added support for this algorithm. The addition of another PCR bank algorithm has also forced changes in the way the HVS will behave when it encounters multiple available PCR banks. By default, the most secure PCR bank will be preferred when importing flavors or performing attestations. If a host only has one bank enabled, that bank will be used. If a host has multiple banks enabled, the HVS will choose the “best” available algorithm and disregard the others. In most cases this will not be noticeable. In the specific case where the same flavor will be used on hosts with different PCR banks enabled, however, this may result in “untrusted” results:

  o Importing a flavor from a host with SHA256 and SHA384 enabled will generate a flavor using SHA384.

  o If host is attested that only has a SHA256 bank enabled and does not have SHA384, the host will appear untrusted because no flavors can match the SHA256 hashes available, even if the servers are otherwise identical.

    o This specific scenario requires separate flavors for the SHA256 systems. A datacenter may require a RHEL 8.4 SHA384 flavor, and also a RHEL 8.4 SHA256 flavor. The OS can be identical, but the measurements used at attestation time need to match the measurements in the flavors.

• Platform-info gathering from the Trust Agent has been changed to now pull platform details directly from UEFI and ACPI tables, instead of working through intermediary applications like dmidecode.

  o Previous Trust Agent dependencies like dmidecode have been removed

  o Additional PCR event logs are now available that were previously invisible. This allows far more visibility and granularity in remote attestations and flavor definitions.

• Intel SecL now exposes Flavor templates. Previously the definitions for which PCRs and events would belong in each flavor part were hard-coded. Given specific host conditions (which security technologies are enabled, etc) and the specific flavor part (PLATFORM, OS, etc), the HVS would use specific PCRs and events. These definitions were previously not changeable by the end user. This new feature adds the capability to create new templates that cumulatively apply definitions to flavor parts based on what’s detected on the host. This allows an administrator to define which PCRs and events should be used for each flavor part, and to control those definitions based on conditions present on the host.

• The Key Broker now requires that the KMIP client certificate include Subject Alternative Names with the KMIP server’s hostname.
NOTE: this requirement may mean that older KMIP client certificates will no longer be valid after an upgrade to version 4.0, if the previously generated certificates did not contain the needed SAN.

• Support for the filesystem key manager in the Key Broker Service has been removed. This feature was provided as a POC-level function to help customers get started using the Key Broker and was not intended for production use. This functionality has been removed. The Key Broker now requires a 3rd-party KMIP key manager.

• The Trust Agent and HVS now support communication in NATS mode. This does not replace the default HTTP communication but is provided as an alternative. By default, the Trust Agent exposes REST API endpoints Intel® SecL-DC 3 Release Notes through an open port, and communication is initiated by the HVS to make API requests to the Trust Agent. NATS mode provides an option for an alternative messaging system. In NATS mode the Trust Agent does not expose any API endpoints. Instead, the Agent will establish a connection to a NATS server that acts as a messaging system. The HVS will also route Trust Agent communication via the NATS server, allowing the same functionality provided in HTTP mode. NATS is a third-party application; additional documentation can be found at https://nats.io. Sample configuration information for a NATS Server are provided in the Intel® Security Libraries Product Guide.

• The Trust Agent has changed how it utilizes TPM ownership. Previously the Agent would assert TPM ownership at service startup. This is no longer required. Instead, TPM ownership is not only required at the time of TPM provisioning, when the AIK is generated and endorsed by the HVS. This makes the Trust Agent much easier to use for administrators who also need to use their TPMs for purposes outside of Intel® Security Libraries. The ownership secret is also no longer stored in the config.yml file. As part of this change, the Trust Agent now supports and defaults to a NULL TPM ownership secret. If the TPM_OWNERSHIP_SECRET variable is provided in trustagent.env, the installer will use the specified secret. If no secret is specified, or if the value of the variable is empty, the Agent will use a NULL TPM ownership secret by default. This change is intended to allow administrators to control and manage the platform TPM and how ownership is used. Defaulting to a NULL secret also means that the Trust Agent will no longer require clearing the TPM ownership in any but the rarest of cases. The Trust Agent will also now support TPM ownership secrets other than the previous 20 byte hex secret. Any ASCII string can now be utilized. To force a string to be treated as hex, prefix the secret with "hex:". Again this allows significantly greater control over the secret for the platform administrator.

NOTE: This change will require upgrades to version 4.0 to re-provision the Trust Agent. This means that for upgrades to version 4.0, the installation bearer token must be provided. In addition, if the TPM owner secret is already set, the secret must be provided at provisioning time as well (which will typically be when the upgrade is executed). This can also be an opportunity to clear the TPM ownership and use the NULL secret or one of the other new options.

• Support for the Docker container runtime interface has been deprecated for the container confidentiality feature. Intel® SecL now supports only the CRI-O container runtime interface for container confidentiality.

Known Issues:

**Important Note:** SGX Attestation fails when SGX is enabled on a host booted using tboot
**Root Cause:** tboot requires the "noefi" kernel parameter to be passed during boot, in order to not use an unmeasured EFI runtime services. As a result, the kernel does not expose EFI variables to user-space. SGX Attestation requires these EFI variables to fetch Platform Manifest data.

**Workaround:**

The EFI variables required by SGX are only needed during the SGX provisioning/registration phase. Once this step is completed successfully, access to the EFI variables is no longer required. This means this issue can be worked around by installing the SGX agent without booting to tboot, then rebooting the system to tboot. SGX attestation will then work as expected while booted to tboot.

1. Enable SGX and TXT in the platform BIOS
2. Perform SGX Factory Reset and boot into the “plain” distribution kernel (without tboot or TCB)
3. Install tboot and ISecL components (SGX Agent, Trust Agent and Workload Agent)
4. The SGX Agent installation fetches the SGX Platform Manifest data and caches it
5. Reboot the system into the tboot kernel mode.
6. Verify that TXT measured launch was successful:
   ```
   txt-stat | grep "TXT measured launch"
   ```
7. The SGX and Platform Integrity Attestation use cases should now work as normal.

**Intel(R) SecL-DC Version 3.6 GA**

Foundational/WL Use Cases:

- Containerization Deployment of Foundational and Workload Security Use Cases supported and validated with RHEL and Ubuntu OS
- Added support for pyKMIP integration with Workload Security Use Cases
- Additional performance and scalability improvements
- Common Integration Hub to support both Foundational/WL Use Cases and SKC/SGX Attestation Use Cases

SKC/ SGX Attestation Use Cases:

- Additional performance and scalability improvements
- SGX Sample Application with quote verification signature added

**Known Issues:**
• While upgrading components normally requires no installation answer files, the Integration Hub when upgrading from version 3.5 to 3.6 will require an answer file containing “HVS_BASE_URL=https://hvs.server.com:8443/hvs/v1” variable. This is required because the variable and its corresponding configuration setting for the Hub changed between these release versions. No other variables or env files are otherwise required for upgrades.

Intel® SecL-DC

**Intel(R) SecL-DC Version 3.5 GA**

Foundational/WL Use Cases:

• Additional performance and scalability improvements
• Added new filter criteria to the /v2/hosts API. Hosts can now be searched by trust status, and the response data when retrieving host details can now optionally also include the host-status and Trusted state. See the HVS Swaggerdoc for details.
• Host searches will now return data in a consistent order (based on the timestamp when the host was registered), and can be sorted by ascending or descending order. See the HVS Swaggerdoc for details.
• The CLI command "setup server" has been replaced by "setup update-service-config" across all Foundational Security services. See the Product Guide for details.

SKC/ SGX Attestation Use Cases:

• Containerization Deployment of SKC and SGX Attestation Use Cases supported
• Added support for pyKMIP integration with SKC Use Case; See Quick Start Guide for deployment details
• Additional performance and scalability improvements
• Added new filter criteria to the /v2/hosts API. See the HVS Swagger docs for details.
• SGX Sample Application and Verifier Enhancements

**Known Issues:**

• Sometimes the SGX Compute node may becomes inaccessible after the secure key transfer. See guidance in Product Guide.
• Running SHVS Setup Task after changing a config value fails. See guidance in Product Guide.

**Intel(R) SecL-DC Version 3.4**

Foundational/WL Use Cases:

• Some environment variables have changed for clarity/consistency. These changes are in:
  - populate-users.env
  - trustagent.env
  - wpm.env

Release Notes
See the Product Guide for details.

- Backend changes have been made to improve the performance of the HVS, particularly for large scale deployments.

SKC/ SGX Attestation Use Cases:

- Streamline discovery and registration flows
- Upgrades & Bug Fixes: Upgraded to DCAP PV version & few Security and Performance bug fixes
- Support added for SGX Sample Verifier App & Integration

Intel(R) SecL-DC Version 3.3

Foundational/WL Use Cases:

- The Integration Hub installation variables have been adjusted. See the Product Guide for details on the updated .env file options.
- Compatibility updates for integration with OpenStack Ussuri
- Validated with RHEL8.3

Known Issues

- Due to a change in Libvirt behavior, there is a new prerequisite Libvirt configuration change for Workload Confidentiality with Virtual Machines. Before installing the Workload Agent, in /etc/libvirt/qemu.conf, ensure that the setting "remember_owner" is set to 0, and then restart the libvirtd service. If this step is not performed before launching encrypted VMs, on VM restart you will see errors similar to the following:
  "Error starting domain: internal error: child reported (status=125): Requested operation is not valid: Setting different SELinux label on /var/lib/nova/instances/15d7ec2f-27ad-41ed-9632-32a83c3d10ef/disk which is already in use"

SKC Use Cases:

- Added Openstack* Ussuri* support for Security Aware Orchestration
- Compatibility upgrades to align with the Intel DCAP APIs for easier integration of SKC/SGX Attestation Use Cases

Intel(R) SecL-DC Version 3.2

Foundational/WL Use Cases:

- The Key Broker now supports both Secure Key Caching and Foundational Security workflows with a single codebase. Previously separate KBS builds were required for each of these use cases, and they have now been merged into a single service.
- Vmware Cluster Registration has been re-enabled in the Host Verification Service. This function allows registration of an entire vCenter cluster object, which will cause ESXi hosts to automatically be registered or un-registered for attestation in the HVS as they are added to or removed from the vCenter cluster.
- Performance Improvements

SKC Use Cases:
- SKC workload and SGX Agent support Ubuntu 18.04 for the Secure Key Caching usecase
- Added support for SGX Attestation

**Intel(R) SecL-DC Version 3.1**

Foundational/WL Use Cases:
- Added support for CRI-O and Skopeo to the Container Confidentiality use case. Previously only the Docker container runtime was supported for this use case.
- The Integration Hub now also pushes information about enabled hardware security features to Kubernetes in addition to the existing Trust and Asset Tag information.
- Added deployment support through Ansible Galaxy; please see quick start guide for details.
- Postman collections created for SKC Use case; please see quick start guide for details

SKC Use Cases:
- Added containerized workload support for Secure Key Caching based on Intel(R) SGX technology
- Added support for choosing Sandbox or Production PCS through caching service answer file
- Added support for Secure Key Caching in the Integration Hub;
- Added deployment support through Ansible Galaxy; please see quick start guide for details.
- Postman collections created for SKC Use case; please see quick start guide for details

**Intel(R) SecL-DC Version 3.0**

Updated name - Intel(R) Security Libraries encompasses use cases and enablement solutions for multiple Intel(R) security features. As new features are covered by Intel(R) SecL, the need has arisen to distinguish use cases based on different classes of security features. Documents and applications that build on platform integrity attestation solutions related to hardware Root of Trust technologies will be referred to as "Foundational Security" elements. Other Intel(R) SecL solutions will have their own documentation and applications, including those for SGX.
- Added support for Secure Key Caching based on Intel(R) SGX technology
- The Verification Service has been renamed the Host Verification Service and rewritten in GO
• The baseurl for all HVS APIs has been updated to replace "mtwilson" with "hvs". The previous baseurl will remain functional for a time for backward compatibility, but users are advised to update any integrations to use the new "hvs" baseurl.

• All HVS CLI commands have been changed from "mtwilson" to "hvs"

• The installation answer file has been renamed from "mtwilson.env" to "hvs.env"

• Installation variables and configuration elements have changed; please see the Product Guide for details.

• The Integration Hub has been rewritten in GO

• The installation answer file has been renamed "ihub.env"

• Installation variables and configuration elements have changed; please see the Product Guide for details.

• The Hub no longer uses an API webserver, and no longer requires configuration of "tenants" or assigning hosts to tenants. Instead, a separate Hub must be deployed for each integration endpoint (OpenStack, Kubernetes, etc). See the Product Guide for details.

• Some CLI commands have changed. See the Product Guide for details.

• The Intel(R) SecL Custom Resource Definitions for Kubernetes integration have been updated to be entirely container-based. The installer binary will now configure containers on the Kube Master node to handle the CRD functions.

Intel(R) SecL-DC Version 2.2.1

• Removed IP address salt for TA and VS

Bug Fixes

• Resolved an issue where the TA provisioning would fail with certain TPM modules

Intel(R) SecL-DC Version 2.2

Bug Fixes

• Resolved an issue where the Key Broker uninstall would fail to remove some files
• Resolved an issue that would cause the Integration hub to fail to retrieve attestation report updates
• Resolved an issue that would occasionally cause containers protected by the Container Confidentiality feature to have multiple failed start attempts before starting successfully
• Updated sample Postgres installation scripts to use an appropriate number of max_connections
• Resolved an issue where Trust Agent hosts could appear untrusted after restarting the Agent

Intel(R) SecL-DC Version 2.1

Added support for 3rd-party KMIP key managers to the Intel(R) SecL-DC Key Broker

• The Key Broker still supports a built-in basic key management system for POCs, not intended for use in production
- The Key Broker will support KMIP version 2.0 compatible 3rd-part key managers.

**Added support for Trusted Virtual Kubernetes Worker Nodes**

- Addresses the Chain of Trust for Kubernetes Worker Nodes running as Virtual Machines
- VM Attestation Reports are now created in the Workload Service for all VM starts through libvirt, including VMs not encrypted by the Workload Confidentiality feature. Currently the trust status of the VM is effectively the trust status of the underlying host.
- Database clients for the Workload Service and the Authentication and Authorization Service will now validate the database server certificate Subject Alternative Names and Common Name. Corresponding changes to the Verification Service are planned for a future release.
- The provided install_pgdb.sh and create_db.sh scripts have been modified to use new env file options (ISECL_PGDB_CERT_DNS, ISECL_PGDB_CERT_IP) to configure the database certificate. If these env file variables are not set, the database scripts will generate a self-signed certificate using localhost and 127.0.0.1 as the SAN list, meaning the database will be accessible only on the local server. These variables must be configured with the appropriate IP address/hostname if a remote database will be used.

**Known Issues**

When using Workload Confidentiality to launch multiple Docker container replicas, containers may go to the CrashLoopBackOff state. The replicas will still start as expected after a small number of failed attempts, impacting container startup performance.

**Intel(R) SecL-DC Version 2.0**

The Trust Agent is now written in GO

- The Trust Agent installer no longer automatically installs tboot. Instructions for tboot installation are now included in the Product Guide.
- The Trust Agent installer no longer automatically installs the Workload Agent.
- Trust Agent configuration file and CLI commands have changed with the migration to GO. See the relevant sections in the Product Guide for details.

- All services now support a granular permissions-based model for roles (instead of only predefined roles with hard-coded permissions)
- Added support for RHEL 8.1
- Removed support for RHEL 7
- Resolved an issue where, if a software manifest was deleted from a Trust Agent host, the host could still appear trusted even though the measurements required in the flavor would now be missing.

**Intel(R) SecL-DC Version 1.6.1**

Updated the Workload Agent for Workload Confidentiality using Docker Container Encryption. An update to the Docker runtime required adjustment to the Secure Docker Daemon used to manage encrypted containers.
Intel® SecL-DC

**Intel(R) SecL-DC Version 1.6**

**Added the Signed Flavor feature**

- Allows the Verification Service to sign Flavors and verify the signature at attestation time to maintain the integrity of the Flavors.

**Added the Workload Confidentiality feature**

- Allows image owners for virtual machines or Docker containers to encrypt the source images of their workloads. Encryption keys remain under the image owner's control, and are released to specific servers, sealed to that server's TPM, upon a successful integrity attestation with attributes that meet policy requirements determined by the workload image owner. Because the image decryption key is sealed to the TPM of the host that was attested, this means that only a server that meets the requirements of the image owner as proven by an attestation report can successfully access the image.
- Adds the new Workload Service (WLS)
  - The Workload Service manages mapping image IDs (as they exist in image storage, i.e., OpenStack Glance) to key IDs
- Adds the new Workload Agent (WLA)
  - Manages the compute node/worker node operation, intercepting attempted launch of encrypted workloads, makes requests for keys, and manages crypto volumes for accessed images.
- Adds the new Key Broker Service (KBS)
  - Acts as the policy manager for handling key requests. Verifies that received attestation reports are signed by a known Verification Service and that the attestation attributes match policy requirements.
- Adds the new Workload Policy Manager (WPM)
  - Application that encrypts a new workload image

Authentication for new components (WLS, WLA) now uses token-based authentication provided by the new Authentication and Authorization service (AAS). This is planned to replace the existing authentication mechanisms for all Intel SecL services in the 1.6 release version.

Added the new Certificate Management Service (CMS). This service will replace and centralize all existing certificate management functions in all Intel SecL services for the 1.6 release version. In the BETA release, this is currently integrated for the AAS and WLS.

**Intel(R) SecL-DC Version 1.5**

- Updated algorithms to use SHA384 instead of SHA256
- Updated key generation to use RSA-3K

Release Notes
• Added support for additional Root of Trust options – Intel BootGuard and UEFI SecureBoot – including removing the tboot requirement if UEFI SecureBoot is enabled (due to incompatibility)
• Added integration support for Kubernetes pod scheduling based on Intel® SecL security attributes
• Added the Application Integrity feature
  • Allows the Chain of Trust to extend above the OS kernel using a new measurement agent (tbootXM) built into initrd
  • Supports boot-time measurement and attestation of any static files/folders on the bare-metal Linux file system, allowing administrators to identify application-specific collections of files and folders to attest as part of a new SOFTWARE Flavor part.
  • Includes a default manifest of Intel® SecL Trust Agent components so that the Agent itself will be included in Platform Integrity attestation
  • Example use cases include creating a SOFTWARE Flavor for QEMU/KVM and Libvirt for virtualization platforms, or for docker.d or other container runtimes for container-based platforms

Intel(R) SecL-DC Version 1.4

Resolved Bugs:

Additional security enhancements following penetration testing

New Features:

• Changed "BIOS" Flavor part to "PLATFORM" Flavor Part for more accurate naming and applicability for future features
• Removed "COMBINED" Flavor. This feature is better served using Flavorgroups without making special Flavors that do not match the normal Flavor standards.
• Updated to support RedHat Enterprise Linux 7.6
• Changed TPM interface to use TSS APIs instead of tpm2-tools and tpm-tools

Intel(R) SecL-DC Version 1.3

Resolved Bugs:

• Updated the versions of some of the 3rd party open source dependent components to the latest version to address the CVEs found in them.
• Updated to use the latest .NET framework and VC runtime version for the Windows Trust Agent.

New Features:

• Script for Installing the Pre-Requisite Packages for the Linux Build System
• Script for automating the complete build process from source and generate docker containers binaries for Linux Trust Agent, Verification Service and Integration Hub
• Documentation on steps to run the Pre-Requisite and Build Scripts for Linux and Windows

Intel® SecL-DC Version 1.2

New Features:

• Added support for running the ISecL services in Docker Containers (Verification Service, Trust Agent, and Integration Hub)
• Added support for Platform Attestation of TPM 2.0 ESXi hosts with vSphere 6.7u1. Asset Tag is currently not supported for TPM 2.0 with VMWare hosts at this time; TPM 1.2 ESXi hosts remain supported

Intel® SecL-DC Version 1.1

New Features:

• Added support for RHEL 7.5 (Verification Service, Trust Agent, and Integration Hub)
• Added support for OpenStack Rocky integration

System Improvements:

• Improved database structure for improved performance and scalability
• Added database rotation to natively prevent unbounded disk utilization and improve query performance
• Updated default database and other configuration settings for stability at large scale
• Improved error handling and performance of queue operations (flavor matching, etc)

Intel® SecL-DC Version 1.0.1

Updated Javadoc REST API documentation
Intel® SecL-DC

Intel(R) SecL-DC Version 1.0.

New Features:

Hardware-rooted Platform Trust Attestation

Intel Security Libraries leverage Intel Trusted Execution Technology and the Trusted Compute Group standards to establish a measured boot environment for servers that use Intel Xeon processors and a Trusted Platform Module. This measured boot environment allows a server's actual boot state to be compared to known-good values, which enables the detection of malicious code injection, rootkits, unacceptable firmware or software version, etc. Remote attestation of this comparison through ISecL allows a clear audit report of the boot state of servers in the datacenter to ensure compliance and improve security.

Asset Tag Attestation

Intel Security Libraries allow the generation and provisioning of user-defined key/value pairs that can be securely provisioned into the physical TPM of a host and included in the remote attestation process. This allows datacenter administrators or cloud consumers to gain visibility into tagged attributes, such as the location of the server hardware.

Support for Red Hat Enterprise Linux, Microsoft Windows Server, and VMWare vSphere

Support for TPM 1.2 and TPM 2.0

Unified "Flavor" whitelisting architecture

"Flavors" describe acceptable configuration elements in server firmware and software in a standardized, extensible format.

Automatic Flavor Matching for easy datacenter lifecycle management

The ISecL Host Verification Service features automatic matching of Flavors to Hosts in the datacenter, allowing for easy yet extremely customizable management of acceptable datacenter configurations.

Parallel delivery of functionality through integration libraries and combined Services

Intel Security Libraries is distributed in two forms:

- As a set of integration libraries targeted at system integrators, ISVs, and customers who want to develop their own solutions based on ISecL functions
- As a set of full Service components that offer already-integrated functionality and a ready-to-use REST interface

Integration Hub provides an easy integration point for scheduler services

Scheduler services (such as in OpenStack) can consume the Trust and Asset Tag attestation information to make scheduling decisions, controlling where workloads are allowed to launch or move based on the attestation status or asset tags of the hosts in the datacenter.