Intel Security Libraries for Data Center
Release Notes

***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 XXX 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 Verifications 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(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, ie 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
- 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/folder 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-Requisiste and Build Scripts for Linux and Windows

------------------------------------------------------------------

***Intel(R) 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(R) 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(R) SecL-DC Version 1.0.1***

Updated Javadoc REST API documentation
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.