REFERENCE

TCG Glossary

Version 1.1
Revision 1.00
May 11, 2017

Contact: admin@trustedcomputinggroup.org

TCG

Published

Disclaimers, Notices, and License Terms

Revision History

Revision	Date	Description
None	Dec 13, 2012	Original release (In previous format without version / revision numbers)
1.00	May 10, 2017	Initial release in new format. Refined and update terminology

Table of Contents

1. Scope

This glossary contains commonly used terms in TCG documents. This glossary may not contain all terms use by TCG document. For example, terms which are specific to a technology or document and not used by other documents may not have an entry in the glossary.

The description contained in this glossary are not intended to fully describe the term, rather, it is intended to provide the reader with a hint or reminder of the term's meeting.

2. Glossary

Acronym	Term	Description
	AIK Credential	A credential issued by a Privacy CA that contains the public portion of an AIK key signed by a Privacy CA. The meaning and significance of the fields and the Privacy CA signature is a matter of policy. Typically it states that the public key is associated with a valid TPM.
	Attestation	The process of vouching for the accuracy of information. External entities can attest to shielded locations, protected capabilities, and Roots of Trust. A platform can attest to its description of platform characteristics that affect the integrity (trustworthiness) of a platform. Both forms of attestation require reliable evidence of the attesting entity.
	Attestation by the TPM	An operation that provides proof of data known to the TPM. This is done by digitally signing specific internal TPM data using an AIK. The acceptance and validity of both the integrity measurements and the AIK itself are determined by the Verifier. The AIK credential is obtained using either the Privacy CA or DAA protocol.
AIK	Attestation Identity Key	In TPMv1.2, an AIK is a special purpose signature key created by the TPM; an asymmetric key, the private portion of which is non-migratable and protected by the TPM. The public portion of an AIK is part of the AIK Credential, issued using either the Privacy CA or DAA protocol. An AIK can only be created by the TPM Owner or a delegate authorized by the TPM Owner. The AIK can be used for platform authentication, platform attestation and certification of keys. An AIK helps provide privacy when used to identify the platform in transactions. The AIK's Credential vouches that the AIK is tied to an authentic TPM, but there is no way to know which TPM the AIK is tied to. Only the user and the CA know that.
	Attestation of the Platform	An operation that provides proof of a set of the platform's integrity measurements. This is done by digitally signing a set of PCRs using an AIK in the TPM.
	Attestation to the Platform	An operation that provides proof that a platform can be trusted to report integrity measurements; performed using the set or subset of the credentials associated with the platform; used to create an AIK credential.
	Authenticated Boot	A boot after which the platform's Root-of-Trust-for-Reporting (RTR) can report an accurate record of the way that the platform booted.
AC	Authenticated Code	Authenticated code is comprised of an executable module plus a value that attests to the authenticity of the module. The value is signed with a private key corresponding to a public key known to a computing device that is to execute the module. If the module is able to verify the signature, the computing device may execute the module.
	Authentication	The process of verifying the claimed attributes, such as an identity, of an entity or user
	Authentication of the Platform	Provides proof of a claimed platform identity. The claimed identity may or may not be related to the user or any actions performed by the user. Platform Authentication is performed using any non-migratable signing key (e.g., an AIK). Since there are an unlimited number of non-migratable keys associated with the TPM there are an unlimited number of identities that can be authenticated.
	Authorization	Granting access to a resource based on an authenticated identity
BLOB	Binary Large OBject	Encrypted or opaque data of fixed or variable size. The meaning and interpretation of the data is outside the scope and context of any entity other than the Subsystem (the TPM in this case) that created the BLOB.

Acronym	Term	Description
BORE	Break Once Run Everywhere	A security design that includes a critical security value that is the same on all instances of the design. If an attacker can access that critical security value on any instance of the design, that information can be used to compromise every instance of the design. For example, a product is designed to use encryption to protect user information and the same encryption key is hard-coded in all instances of the product. If the attacker can acquire the key from one copy of the product, he can use that key to access personal information in all copies of the product.
CMK	Certified Migration Key	A key whose migration from a TPM requires an authorization token created with private keys. The corresponding public keys are incorporated in the CMK and referenced when a TPM produces a credential describing the CMK. If a CMK credential is signed by an AIK, an external entity has evidence that a particular key (1) is protected by a valid TPM and (2) requires permission from a specific authority before it can be copied.
	Challenger (Identity Challenger)	An entity that requests and has the ability to interpret integrity metrics. See also “Integrity Challenge”
CRTM	Code Root of Trust for Measurement	The instructions executed by the platform when it acts as the RTM. [Formerly described as “Core Root of Trust for Measurement”. Code Root of Trust for Measurement is the preferred expansion.] This acronym expansion is preferred.
	DAA Issuer	A known and recognized entity that interacts with the TPM to install a set of DAA-credentials in the TPM. The DAA issuer provides certification that the holder of such DAA-credentials meets some criteria defined by the Issuer. In many cases the Issuer will be the platform manufacturer, but other entities can become issuers.
	Delegation	A process that allows the Owner to delegate a subset of the Owner's privileges (to perform specific TPM operations).
DAA	Direct Anonymous Attestation	A protocol for vouching for an AIK using zero-knowledge-proof technology.
	DMA Mapping	Controls how hardware devices access Host Platform memory; DMA requests to access memory may be mapped to an alternate memory address. Similar to user mode processes use of virtual memory where page tables control the mapping to physical memory pages. Examples are IOMMU or VT-d.
	DMA Protections	Provide a mechanism to allow a Host Platform to prevent hardware devices from accessing certain Host Platform memory. Examples are a DMA exclusion scheme or DMA mapping.
	Duplicable Object	In TPM 2.0, a key or data object that is not bound to a specific TPM and with suitable authorization can be used outside a TPM or moved (copied) to another TPM. (See Migratable)
D-HRTM	Dynamic Hardware Root of Trust for Measurement	A D-RTM implemented using an HRTM.
DL	Dynamic Launch	This describes the process of starting a software environment at an arbitrary time in the runtime of a system.
D-RTM	Dynamic Root of Trust for Measurement	A platform-dependent function that initializes the state of the platform and provides a new instance of a root of trust for measurement without rebooting the platform. The initial state establishes a minimal Trusted Computing Base.

Acronym	Term	Description
		This is a function that is built into the Host Platform and is started by the Dynamic Launch Event (DL Event). This function is a Trusted Process. Even though the D-RTM executes after the S-RTM, the D-RTM's transitive trust chain will not necessarily have a trust dependency on the S-RTM's transitive trust chain.
DCE	Dynamic Root of Trust for Measurement Configuration Environment	The software/firmware that executes between the instantiation of the D-RTM CPU instruction and the transfer of control to the Dynamically Launched Measured Environment (DLME). The DCE is responsible for ensuring the platform is in a trustworthy state. Normally this is defined by the CPU manufacturer, chipset manufacturer, and the platform manufacturer.
DLME	Dynamically Launched Measured Environment	The software executed after the DCE- instantiated TCB is established. The DLME would nominally be supplied by an OS vendor.
EK	Endorsement Key	An asymmetric Key pair composed of a public key (PubEK) and private (PrivEK).The EK is used to prove the TPM is genuine.
	Endorsement Key Credential	A credential associated with an PubEK. The credential asserts that the associated PrivEK is unique to a security device conforming to TCG specifications.
H-CRTM		A synonym for the S-HRTM. The preferred term is S-HRTM.
HRTM	Hardware Root of Trust for Measurement	An RTM where hardware performs the initial measurement.
	Immutable	Unchangeable
ILP	Initiating Logical Processor	The processor that initiates the D-RTM
	Integrity Challenge	A process used to send accurate integrity measurements and PCR values to a challenger.
	Integrity Logging	The storage of integrity metrics in a log for later use.
	Integrity Measurement (Metrics)	A value representing a platform characteristic that affects the integrity of a platform
	Integrity Reporting	The process of attesting to the contents of integrity storage.
	Locality	A mechanism for supporting a privilege hierarchy in the platform
	Migratable (key)	A key which is not bound to a specific TPM and with suitable authorization can be used outside a TPM or moved to another TPM.
	Non-duplicable Object	In TPM 2.0, a statistically unique object (usually a key) that may only be used on the TPM that created the object.
	Non-migratable (key)	A key which is bound to a single TPM; a key that is (statistically) unique to a single TPM. In TPM 1.2, the key may be moved between TPMs using the maintenance process
NV (storage)	Non-volatile (shielded location)	A shielded storage location whose contents are guaranteed to persist between uses by Protected Capabilities.
	Operator	Anyone who has physical access to a platform
	Owner	The entity that has administrative rights over the TPM.
	Platform	A platform is a collection of resources that provides a service.
PCR	Platform Configuration Register	A shielded location containing a digest of integrity measurements.
	Platform Credential	A credential, typically a digital certificate, attesting that a specific platform contains a unique TPM and TBB.

Acronym	Term	Description
		A credential that states that a specific platform contains a genuine TCG Subsystem.
PCA	Privacy CA	An entity that issues an Identity Credential for a TPM based on trust in the entities that vouch for the TPM via the Endorsement Credential, the Conformance Credential, and the Platform Credential.
PrivEK	Private Endorsement Key	The private portion of the EK.
	Protected Capabilities	The set of commands with exclusive permission to access shielded locations
PubEK	Public Endorsement Key	The public portion of the EK.
RoT	Root of Trust	A component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or update. It is trusted always to behave in the expected manner, because its misbehavior cannot be detected (such as by measurement) under normal operation.
RTC	Root of Trust for Confidentiality	An RoT providing confidentiality for data stored in TPM Shielded Locations.
RTI	Root of Trust for Integrity	An RoT providing integrity for data stored in TPM Shielded Locations.
RTM	Root of Trust for Measurement	An RoT that makes the ***initial*** integrity measurement, and adds it to a tamper-resistant log. Note: A PCR in a TPM is normally used to provide tamper evidence because the log is not in a shielded location.
RTR	Root of Trust for Reporting	An RoT that reliably provides authenticity and non-repudiation services for the purposes of attesting to the origin and integrity of platform characteristics.
RTS	Root of Trust for Storage	The combination of an RTC and an RTI
RTU	Root of Trust for Update	An RTV that verifies the integrity and authenticity of an update payload before initiating the update process.
RTV	Root of Trust for Verification	An RoT that verifies an integrity measurement against a policy.
	Shielded Location	A place (memory, register, etc.) where it is safe to operate on sensitive data; data locations that can be accessed only by Protected Capabilities.
S-CRTM	Static Code Root of Trust for Measurement	An S-RTM implemented using a CRTM.
S-HRTM	Static Hardware Root of Trust for Measurement	An S-RTM implemented using an HRTM. [NOTE: The TPM 2 Library Specification uses the term H-CRTM introduced in Revision 116.]
S-RTM	Static Root of Trust for Measurement	An RTM where the initial integrity measurement occurs at platform reset. The S-RTM is static because the PCRs associated with it cannot be re-initialized without a platform reset.
SRK	Storage Root Key	A key with no parent that is the root key of a hierarchy of keys associated with a TPM's Protected Storage function.
TSS	TCG Software Stack	Untrusted software services that facilitate the use of the TPM and do not require the protections afforded to the TPM.
	TPM Shielded Location	A location within a TPM that contains data that is shielded from access by any entity other than the TPM and which may only be operated on by a Protected Capability

Acronym	Term	Description
TSS	TPM Software Stack	An unofficial alias of the term TCG Software Stack. TCG specifications should not use the term TPM Software Stack when referring to the TSS
	TPM-Protected Capability	An operation performed by a TPM on data in a Shielded Location, usually in response to a command sent to the TPM
	Transitive Trust	Also known as "Inductive Trust", in this process a Root of Trust gives a trustworthy description of a second group of functions. Based on this description, an interested entity can determine the trust it is to place in this second group of functions. If the interested entity determines that the trust level of the second group of functions is acceptable, the trust boundary is extended from the Root of Trust to include the second group of functions. In this case, the process can be iterated. The second group of functions can give a trustworthy description of the third group of functions, etc. Transitive trust is used to provide a trustworthy description of platform characteristics, and also to prove that non-migratable keys are non-migratable
	Trust	Trust is the expectation that a device will behave in a particular manner for a specific purpose.
TBB	Trusted Building Block	The parts of the Root of Trust that do not have shielded locations or protected capabilities. Typically platform-specific. An example of a TBB is the combination of the CRTM, connection of the CRTM storage to a motherboard, the connection of the TPM to a motherboard, and a mechanisms for determining Physical Presence.
	Trusted Component	A Trusted Device within a Trusted Platform or another Trusted Device.
	Trusted Computing Platform	A Trusted Computing Platform is a computing platform that can be trusted to report its properties
	Trusted Device	A Trusted Platform that is not intended to reprogrammed except through a maintenance process.
	Trusted Platform	A platform that uses Roots of Trust to provide reliable reporting of the characteristics that determine its trustworthiness.
TPM	Trusted Platform Module	A composite of the RTR and the RTS
TPM	Trusted Platform Module	An implementation of the functions defined in the TCG Trusted Platform Module Specification; the set of Roots of Trust with Shielded Locations and Protected Capabilities. Normally includes just the RTS and the RTR. The set of functions and data that are common to all types of platform, which must be trustworthy if the Subsystem is to be trustworthy; a logical definition in terms of protected capabilities and shielded locations.
TPS	Trusted-Platform Support Services	The set of functions and data that are common to all types of platform, which are not required to be trustworthy (and therefore do not need to be part of the TPM).
	User	An entity that is making use of the TPM capabilities. An entity that uses the platform in which a TPM is installed. The only rights that a User has over a TPM are the rights given to the User by the Owner. These rights are expressed in the form of authentication data, given by the Owner to the User, which permits access to entities protected by the TPM. The User of the platform is not necessarily the “owner” of the platform (e.g., in a corporation, the owner of the platform might be the IT department while the User is an employee). There can be multiple Users.
	Validation Credential	A credential that states values of measurements that should be obtained when measuring a particular part of the platform when the part is functioning as expected.

Acronym	Term	Description
	Validation Data	Data inside a Validation Credential; the values that the integrity measurements should produce when the part of a platform described by the Validation Credential is working correctly.
	Validation Entity	An entity that issues a Validation Certificate for a component; the manufacturer of that component; an agent of the manufacturer of that component.
	Verifier	An entity that evaluates credentials to produce a credential. Example 1: the entity that interacts with the TPM using the DAA protocol to verify that the TPM has a valid set of DAA-credentials. The verifier may then produce an AIK credential, without reference to the platform EK. Example 2: the entity that requests, receives, and evaluates attestation information based on the EK. A trusted third party (such as a Privacy CA) may then produce an AIK credential, after verifying the platform EK.