This glossary contains definitions of terms created by TCG, or terms that have a particular meaning in trusted computing, or terms that cause particular confusion in trusted computing.

Acronym	Term	Description
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.
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.
	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.
	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.
	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.
	Authentication	The process of verifying the claimed attributes, such as an identity, of an entity or user
	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.
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, suppose a product is designed to use encryption to protect a user's personal information and the same encryption key is hardcoded into all instances of the product. By reverse engineering one copy of the product, an attacker may be able to determine the key, and thus use that information to access personal information from any copy 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.
CRTM	Core Root of Trust for Measurement	The instructions executed by the platform when it acts as the RTM (Root of Trust for Measurement)
	Challenger (Identity Challenger)	An entity that requests and has the ability to interpret integrity metrics. See also “Integrity Challenge”
DAA	Direct Anonymous Attestation	A protocol for vouching for an AIK using zero-knowledge-proof technology.
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.
D-CRTM	Dynamic Core Root of Trust for Measurement	The Core Root of Trust for the D-RTM. 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-CRTM executes after the S-CRTM, the D-RTM's transitive trust chain will not necessarily have a trust dependency on the S-CRTM's transitive trust chain.
	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).
DL	Dynamic Launch	This describes the process of starting a software environment at an arbitrary time in the runtime of a system.
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.
	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.
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.
EK	Endorsement Key	EK; an RSA Key pair composed of a public key (EKpu) and private (EKpr). The EK is used to recognize a genuine TPM. The EK is used to decrypt information sent to a TPM in the Privacy CA and DAA protocols, and during the installation of an Owner in the TPM.
	Endorsement Key Credential	A credential containing the EKpu that asserts that the holder of the EKpr is a TPM conforming to TCG specifications. Most TPMs are implemented in hardware, but this is not mandatory. A credential containing a public key (the endorsement public key) that is used to recognise a genuine TPM.
ILP	Initiating Logical Processor	The processor that initiates the D-CRTM
	Integrity Challenge	A process used to send accurate integrity measurements and PCR

		values to a challenger.
	Integrity Measurement (Metrics)	Values that are the results of measurements on the integrity of the platform. The process of obtaining metrics of platform characteristics that affect the integrity (trustworthiness) of a platform, and putting digests of those metrics in shielded locations (called Platform Configuration Registers: PCRs).
	Integrity Logging	The storage of integrity metrics in a log for later use.
	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-migratable (key)	A key which is bound to a single TPM; a key that is (statistically) unique to a single TPM but 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 owns the platform in which a TPM is installed. Since there is, by definition, a one-to-one relationship between the TPM and the platform, the Owner is also the Owner of the TPM. The Owner of the platform is not necessarily the “user” of the platform (e.g., in a corporation, the Owner of the platform might be the IT department while the user is an employee.) The Owner has administration rights over the TPM. The entity responsible for the platform's security and privacy policies that is distinguished by knowledge of the Owner authorization data.
PCR	Platform Configuration Register	A shielded location containing a digest of integrity digests.
	Platform	A platform is a collection of resources that provides a service.
	Platform Credential	A credential, typically a digital certificate, attesting that a specific platform contains a unique TPM and TBB. A credential that states that a specific platform contains a genuine TCG Subsystem.
PrivEK	Private Endorsement Key	The private key of the key pair that proves that a TPM is a genuine TPM. The PRIVEK is (statistically) unique to only one TPM.
	Protected Capabilities	The set of commands with exclusive permission to access shielded locations
PubEK	Public Endorsement Key	A public key that proves that a TPM is a genuine TPM. The PUBEK is (statistically) unique to only one TPM.
PCA	Privacy CA	An entity, typically a Trusted Third Party (TTP), that blinds a verifier to a platform's EK. An entity (typically well known and recognized) trusted by both the Owner and the Verifier, that will issue AIK Credentials. A Verifier may also adopt the role of a Privacy CA. In that case the roles are co-located but are logically distinct.

		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.
RoT	Root of Trust (component)	A component that must always behave in the expected manner, because its misbehavior cannot be detected. The complete set of Roots of Trust has at least the minimum set of functions to enable a description of the platform characteristics that affect the trustworthiness of the platform.
RTM	Root of Trust for Measurement	A computing engine capable of making inherently reliable integrity measurements. Typically the normal platform computing engine, controlled by the CRTM. This is the root of the chain of transitive trust.
RTR	Root of Trust for Reporting	A computing engine capable of reliably reporting information held by the RTS.
RTS	Root of Trust for Storage	A computing engine capable of maintaining an accurate summary of values of integrity digests and the sequence of digests.
	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".
SRK	Storage Root Key	The root key of a hierarchy of keys associated with a TPM's Protected Storage function; a non-migratable key generated within a TPM.
TBB	Trusted Building Block	The parts of the Root of Trust that do not have shielded locations or protected capabilities. Normally includes just the instructions for the RTM and the TPM initialization functions (reset, etc.). Typically platform-specific. One 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 mechanisms for determining Physical Presence.
	TPM-protected capability	A function which is protected within the TPM (that is, only occurs within the TPM and does so within a hardware security envelope, if the TPM is equipped with such a feature), and has access to TPM secrets. See “Protected Capabilities”
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
TSS	TCG Software Stack	Untrusted software services that facilitate the use of the TPM and do not require the protections afforded to the TPM.
	Transitive Trust	Also known as "Inductive Trust", in this process the 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.
	Trusted Computing Platform	A Trusted Computing Platform is a computing platform that can be trusted to report its properties
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, that 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.
	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	In the DAA model: 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. In the "Trusted Third Party" model: the entity that requests, receives, and evaluates attestation information based on the EK. The TTP (Privacy CA) may then produce an AIK credential, after verifying the platform EK.