Endorsement Key (EK) and Platform Certificate Enrollment Specification
Frequently Asked Questions
April 2013

Q. What is this specification about?
A. This specification describes design and implementation requirements for an EK (Endorsement Key) and Platform certificate enrollment protocol based on the Certificate Management messages over the CMS (CMC) protocol. This new enrollment protocol is used to request TCG EK and platform certificates, thereby making deployment of Trusted Platform Modules (TPMs) easier than has been possible previously.

Q. What benefit is there to this new specification? How will it help users set up and manage TPMs, which historically have been difficult to provision?
A. This new specification, based on IETF standard certificate enrollment protocols, allows certificate authorities (CAs) already supporting CMC to add support for issuance of TCG EK and platform certificates.

Enabling support for existing CAs should significantly simplify the task of provisioning certificates for TPMs, and this in turn will facilitate integration of TCG attestation and authentication protocols into existing access control infrastructure.

For enterprises, this will result in true machine-level identity – and make deployment of TPMs using certificates easier.

Q. Why is this specification important?
A. TCG previously released a specification for enrollment of AIK (Attestation Identity Key) certificates in 2011, and is currently working on a specification for TPM-based platform identity keys. AIKs allow the TPM to produce cryptographically signed attestation evidence (statements) about the operational state of the platform. When these signed statement are conveyed using the PTS Protocol Binding to IF-M, they can augment the current Trusted Network Connect (TNC) protocols, making them more resilient to local attacks by malware, and to attempts by endpoints to misrepresent their operational state.

In a related fashion, TPM platform identity keys allow devices to authenticate using robustly protected credentials that are protected by TPM hardware. Based on the chain of trust created by the EK, platform, and AIK certificates, a relying party can verify that a given key is TPM-resident, bound to a particular platform.

While various TCG protocols can be implemented without the presence of a TPM, the value of these protocols is dramatically increased when the root of trust is based in hardware. EK and platform certificates are a fundamental enabling technology for such applications.

Q. What's an EK?
A. An Endorsement Key is a special purpose TPM-resident RSA key that is never visible outside of the TPM. Because the EK can only be used for encryption, possession of the private EK can only be proved indirectly, by using it to decrypt a value that has been encrypted with the public EK. Therefore, while the EK cannot be used to produce a digital signature, it is able to provide for TPM authentication based on decryption operations.

Q. How is an EK different from other RSA keys?
A. A private EK is much more constrained than a general RSA private key, in that it can only be used by the TPM to decrypt specific, well-defined structures.

Q. What is an EK certificate used for?
A. An EK certificate is used to bind an identity, in terms of specific security attributes, to a TPM. The primary use of an EK certificate is to authenticate device identity during AIK certificate issuance.

Q. What is a Platform certificate, and what is it used for?
A. A Platform certificate attests that a specific platform contains a unique TPM and certain platform configuration elements. Nominally, the issuer of a Platform certificate is the platform manufacturer (for example, an OEM), but in practice, this is not always the case. Platform certificates are used together with EK certificates to facilitate issuance of AIK certificates.

Q. How does this specification tie into existing industry standards and efforts?
A. The protocol defined by the specification is based upon CMC, an IETF standard protocol that is implemented by a number of commercial and open source products. The certificates created by this protocol may be used to facilitate the TCG AIK certificate enrollment protocol, and/or to facilitate creation of TPM platform identity keys.

Q. What are CMC and CMS?
A. CMC, or “Certificate Management messages over CMS”, is an IETF-standard certificate management protocol. CMS, or “Cryptographic Message Syntax”, is an IETF standard for cryptographic protection of messages. CMC defines a certificate management protocol that is based on CMS.

Q. Why can’t we use existing enrollment protocols for EKs and Platform certificates?
A. CMC *is* an existing enrollment protocol. However, there are limitations in the way certain proofs and assurances critical to the enrollment process can be provided with respect to EKs, so this specification articulates precisely how these things may be accomplished in a way that allows interoperation between independent implementations.

Q. Do existing commercial and/or open source Certification Authority (CA) products support this protocol?
A. A number of existing products support the CMC protocol. However, those products will generally require a supporting module that implements this protocol in order to add EK and platform certificate enrollment support. It is not uncommon to add such modules to support specific enrollment requirements.

Q. Who implements/supports this specification?
A. This is a new specification, and there are no public implementations as of yet. However, AIKs and TPM platform identity keys can be used to significantly enhance existing Trusted Network Connect (TNC) implementations, as well as other security protocols, provided that supporting infrastructure exists. This enrollment protocol is a fundamental element in such a supporting infrastructure, so it is anticipated that implementations will be forthcoming.