Attestation Identity Key (AIK) Certificate Enrollment Specification
Frequently Asked Questions
September 2011

Q. What is this specification about?
A. This specification describes design and implementation requirements for an AIK (Attestation Identity Key) certificate enrollment protocol based on the Certificate Management messages over the CMS (CMC) protocol. This new enrollment protocol is used to request a TCG AIK certificate, thereby making deployment of Trusted Platform Modules (TPMs) easier than has been possible previously. The spec and additional information are available at http://www.trustedcomputinggroup.org/resources/tcg_infrastructure_working_group_a_cmc_profile_for_aik_certificate_enrollment.

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 AIK certificates.

Enabling support for existing CAs should significantly simplify the task of provisioning certificates for AIKs, and this in turn will facilitate integration of TCG attestation 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. 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. Therefore, having an interoperable, easy to use method for AIK enrollment is fundamental to enabling robust platform attestation

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. AIK certificates are a fundamental enabling technology for such applications.

Q. What's an AIK?
A. An Attestation Identity Key is a special purpose TPM-resident RSA key that is used to provide platform authentication based on the attestation capability of the TPM.

Q. It was reported widely this year that an RSA key was hacked. Does this specification do anything to protect the RSA key?
A. By enabling true machine-level identity utilizing TPM-resident keys, the system is more secure than if the key were stored elsewhere, whether hardware or software.

Q. How is an AIK different from other RSA keys?
A. An AIK is much more constrained than a general RSA key, in that it can only be used by the TPM to sign specific TPM-originated structures.

Q. What is an AIK certificate used for?
A. An AIK certificate is used to attest to the presence of an AIK within a TPM. It is also used to attest that other keys certified by the AIK originated from that particular TPM.

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.

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 AIKs?
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 AIKs, 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 AIK 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 can be used to significantly enhance existing Trusted Network Connect (TNC) implementations, 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.