and exported from the TPM. The encrypted key can only be securely decrypted internally on the TPM. This means unencrypted keys are never stored or visible outside the TPM. The Trusted Computing Group standard version 1.1b [14] specifies that TPM performs the following functions:

- **Key generation:** public key functions for key pair generation using a hardware RNG;
- **Cryptography and secure storage:** public key signature, encryption, and decryption to enable secure storage of data and digital secrets;
- **Integrity measurement:** storage of hashes that enable verifiable attestation of the machine configuration when booted;
- **Unique identity:** an endorsement key that can be used to anonymously establish that an identity key was generated in a TPM; and
- **Ownership:** initialization and management functions that allow the owner to turn TPM functionality on and off, reset the chip, and take ownership of its functions.

The TPM’s RNG generates the seed numbers for the cryptographic processor’s encryption, decryption, and key generation functions. The TPM’s non-volatile memory securely stores encryption keys, including the SRK, endorsement key (EK), and other sensitive data. The TPM employs conventional cryptographic operations in conventional ways. The operations supported by TPM include Asymmetric key generation (RSA), Asymmetric encryption/decryption (RSA) Hashing (SHA-1) and Random number generation (RNG).

The TPM uses these capabilities to perform generation of random data, generation of asymmetric keys, signing and confidentiality of stored data. The TPM may use symmetric encryption for internal TPM use but does not expose any symmetric algorithm functions to general users of the TPM.

The Key Generation component, Figure 2, creates RSA key pairs and symmetric keys. The SHA-1 hash capability is primarily used by the TPM to support measurement taking during platform boot phases and to allow environments that have limited capabilities access to a hash functions. The Opt-In component provides mechanisms and protections to allow the TPM to be turned on/off, enabled/disabled, activated/deactivated. The execution engine runs program code to execute the TPM commands received from the I/O port. Non-volatile memory component is used to store persistent identity and state associated with the TPM. This area has set items like the EK.

A Platform Configuration Register (PCR) is a 160-bit storage location for discrete integrity measurements. There are a minimum of 16 PCR registers. All PCR registers are shielded locations within the TPM chip. The decision of whether a PCR contains a standard measurement or if the PCR is available for general use is deferred to the platform specific specification. An Attestation Identity Key (AIK) is an alias for the Endorsement Key (EK). The EK cannot perform signatures for security reasons and due to privacy concerns. TPMs contain secure non-volatile storage space that is intended to contain measurements of system hardware and software status. Measurement consists primarily of submitting all system software and hardware to a hash algorithm in a predetermined sequence. If this measurement is performed when the system is in a known trusted state, then the resulting hash can be stored in the TPM and compared to the result of a subsequent measurement. Any changes will be detected by the comparison, and appropriate actions can be taken to prevent execution of modified software or hardware. This measurement capability can be used to provide detection of any remote system modifications resulting from malicious viruses or worms.

The purpose of TPM is to provide hardware-based digital certificates for establishing trust since software-based solutions are vulnerable to malicious attacks. TPM is gaining...