CESG IA Top Tips 2011/01

Trusted Platform Modules

Trusted Platform Modules (TPMs) are security chips present in many enterprise computing platforms in HMG and throughout the world, particularly in laptops, but also in desktop PCs and servers. TPMs can offer a number of security features, but these are rarely enabled.

The TPM specification is an internationally recognised standard, coordinated by the Trusted Computing Group; see http://www.trustedcomputinggroup.org.

As remote access to secure networks becomes ubiquitous across government, it is essential that data on mobile platforms is protected and that all devices connecting to a network can be identified and managed. TPMs can provide additional security and assist with device management at low cost. **Government departments should consider whether cost savings can be made by introducing TPMs**. The first two use cases below can be deployed today using commercial tools; the remainder could be deployed on existing hardware once suitable products become available.

i) Key storage for disk encryption or data protection

Storing all or part of the key in the TPM adds tamper protection, helping to defend the key if the device is stolen or subjected to a brute force attack.

ii) Secure Device Identity

A private signing key can be stored in the TPM and used to sign data without the key leaving the TPM. This key can then be used to provide strong identification of the device, and cannot be changed or stolen by malware. This is cheaper than using a separate physical token for authentication, and the same mechanism can be used to store VPN authentication credentials securely.

iii) Signing of Configuration and Health Status Reports

The TPM can sign device configuration and health reports created on the platform, providing strong authentication and integrity protection for asset management, health checks and access decisions.

iv) Verified Boot

The TPM can store keys and measurements that can verify the integrity of firmware and software when a platform is switched on. The data can then be used to make access decisions or analysed in bulk to search for anomalous platform behaviour.