TPM Enterprise Key Management requires centralized Hardware-based Security

Bernhard Weiss

Utimaco Safeware AG
BU Transaction Security
bernhard.weiss@aachen.utimaco.de

Abstract
Finding a way in which to administrate the sensitive Trusted Platform Module (TPM) key information and benefit from the potential of TPM’s is currently a major issue in most large companies. Enterprise customers are requesting centralized security management to guarantee reliable security. Thus security mechanisms whose use is controlled by the user do not provide companies with reliable security.

When compared to standard data backup utilities today’s operating systems do not provide any backup and recovery procedures for TPM specific keys. Furthermore existing key recovery solutions tend to place the burden for backup and restore onto the individual user. By combing readily available technology a centralized backup, recovery and migration solution, based upon a hardware-security-module, is proposed which fulfills the requirements of enterprise customers.

1 Introduction

Seen as a strange 'Fritz chip' attracting negative attention in the past, the Trusted Platform Module (TPM) has now moved to an accepted standard (see Chapter 1.1). TPM’s can now be found in an increasing number of devices, as shown in http://www.tonymcfadden.net/tpmvendors.html. Furthermore it is expected that the market for TPM modules in Desktops and Notebooks will growth by the next years. It is assumed that nearly 100% of all Notebooks and around 90% of all Desktops shipped in 2010 will have a TPM embedded (see Chapter 1.2 for more details).

But what is provided by a TPM? The TPM is a microcontroller that stores keys, passwords and digital certificates securely. Furthermore it adds core security technologies that can generate keys for use in digital certificates, create digital signatures and provide encryption. Security operations are accessed and controlled through the secure subsystem using the defined interfaces. Applications like harddisk encryption, secure e-mail and identity/access management will benefit from the security functions provided by the TPM.

The question now is how to allow an IT organization to manage and control the sensitive TPM key information, rather than leaving it up to individual users.

Finding a way in which to administrate the sensitive TPM key information and benefit from the potential of Trusted-Platform-Modules is currently a major issue in most large companies. The areas of particular interest are the reduction of administration costs, the increase of interoperability between the different TPM implementations and the simplification of backup and restore of the sensitive key information needed to secure the associated information stored on the notebook or desktop.
The topic of key generation plays a significant role in the introduction of TPM's. When introducing TPM's, great care must be taken to set up appropriate procedures for powerful cryptography and effective key management.

The first part of this paper illustrates the challenges faced by the deployment of TPM's. The second part then details a concept, based on a centralized hardware security module (HSM), as a solution for TPM enterprise key management.

1.1 TPM background

The Trusted Platform Module (TPM) is a comprehensive approach to enterprise security. It is based upon an open specification for the modules building the TPM and its environment [Arch]. The specifications are led by the Trusted Computing Group (TCG) and include input from many sectors of the IT industry. Members and nonmembers of the TCG can use these specifications royalty free. A broad variety of products has already been released.

The range of specifications developed by the TCG include not only the TPM as microcontroller but also accompanying software, client PCs, storage devices, mobile phones, servers, secure network access and defines policies like backup and migration.

Today TPM's are mainly integrated into notebook and desktop computers sold to enterprises. Further implementations into servers, network devices, and secure mobile systems are in the works.

1.2 TPM market

It is assumed [Kay] that the TPM market will growth substantially as shown in Figure 1 over the next years.

![TPM Modules Forecast](image)

For the year 2006 50 million TPM units are expected. This will quadruple by 2010 exceeding 250 million units per year.