

## USAGE MODELS

*Updated 02/07/02*

# Trusted Computing in Action

### Usage model 1: Protection of data

Keys can be bound to a specific platform. Further, the use of the key requires user authentication. Data can then be encrypted using a key that is bound to the platform *and* requires the user's authorization. Since the key is bound to the platform, even if an attacker obtains the key file *and* knows the authorization for the key (e.g., PIN), the data is safe because the key will only work when used on the specific platform. The attacker must obtain both the specific platform *and* possess the authorization for the key to decrypt the data.

### Usage model 2: Attestation of the platform's trust state

A TCPA-enabled platform requests a service from a corporate server (e.g., e-mail). The server's policy is to send e-mail only to platforms that have policies and applications that protect the contents of the e-mail. The e-mail server requests the signed trust state of the client's platform. Based on the signed (therefore trusted) valid value returned, the server sends the requested e-mails to the now trusted client.

What happens in a case where the platform isn't TCPA-enabled? There is no way for the server to trust any "trust statement" from a software-only (i.e., non-TCPA) client — even if it is running software that would otherwise be trusted by the server. Software alone cannot provide the same level of trusted attestation as a TCPA device-based platform. Consequently, the e-mails are denied.

### Usage model 3: Platform and User authentication

A Human Resources department has client platforms for the entire HR staff, including temporary workers, administrative assistants, managers, and the vice president of HR. Even with user authentication, it is desirable to allow specific actions (e.g., salary changes) to originate from only specific and physically secure locations within the department. Using software-only platform authentication, a platform can spoof its location (e.g., spoof its physical network address) making the server believe it is the communicating with the one in the secured location. If the server instead considers only TCPA device-based platforms to be trusted, the rogue platform could not spoof its location. Salary change information would be safe from such a possible breach.