Securing Your Enterprise with Infineon's TPM Client and Server Solutions

Josef Kohn, Product Manager

Robert Rozario, Application Engineering Manager

Never stop thinking

Turning on the Trust

Why and How

Never stop thinking

Turning on the Trust – Why & How

- TPM-equipped PCs are shipped on the majority of business PCs since several years now
- Why are still less than 1% of them actively used?

Understanding and Removing the Major Barriers

- Which enterprise use-cases and applications can the TPM be used for?
- How can TPM-enabled PCs effectively be deployed and managed in an enterprise environment?

Copyright © Infineon Technologies 2009. All rights reserved.

Agenda and Session Goals

- TPM-enabled PCs
  - The TPM
  - Client and Server Software: Professional Package and TCMS Software
  - 3rd-party Integration SDK
- Demo of typical Use Cases in an Enterprise
  - Platform and User Initialization
  - Dictionary Attack Reset
  - Secure Password Reset

- Understand the Basics
  - The Motivation for a TPM: security features and benefits of a TPM
  - How a TPM is integrated in a PC HW and SW
  - Which and how applications can use the TPM
  - How to deploy and manage TPM-enabled PCs in your company

Copyright © Infineon Technologies 2009. All rights reserved.

What Infineon does for Your Security

For >15 Years the leading Manufacturer for ChipCard and Security Solutions

	Contact-based chip cards	Contactless chip cards, RFID	Other Security ICs
 **Identification** ePassport, National ID Social/Health Card Physical and IT Access			
 **Entertainment** Pay-TV, Gaming Video/Audio			
 **Payment** Credit / Debit, e-purse Transport Ticketing			
 **Communications** Mobile Communication Prepaid Telecom			

Copyright © Infineon Technologies 2009. All rights reserved.

TPM is the PC's Trust Anchor and secure Key Storage

- System Integrity for BIOS and OS:
  - Measure, store, report integrity metrics



- Application Security:
  - Data Protection
  - Strong Authentication
  - Network Access Protection (LAN, WLAN)
  - Policy Enforcement

  - Protect user/platform keys
  - Dictionary attack prevention
  - Seal data to *known-good* configurations
  - Cryptographically bind data to the platform

- TSS/Client Software:
  - Interfaces for OS and 3rd-party applications
  - Application Integration SDK for 3rd-party Software

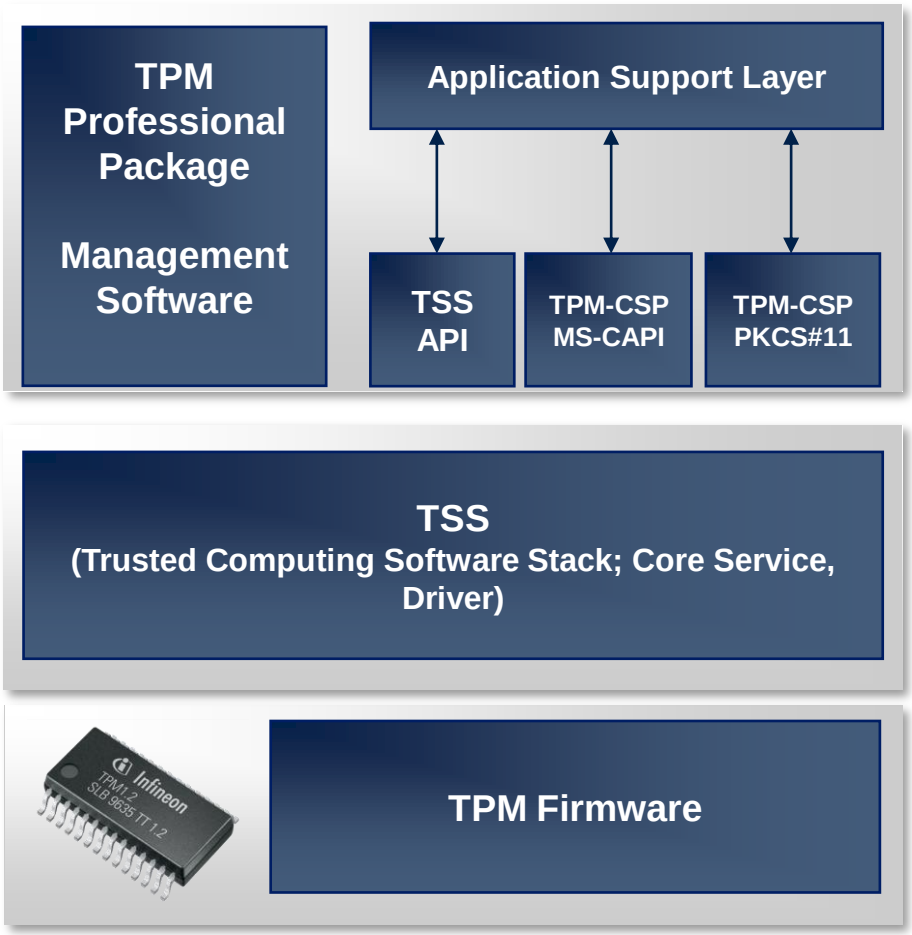
Copyright © Infineon Technologies 2009. All rights reserved.

Infineon TPM Professional Package Software for Windows®

User-friendly Interface



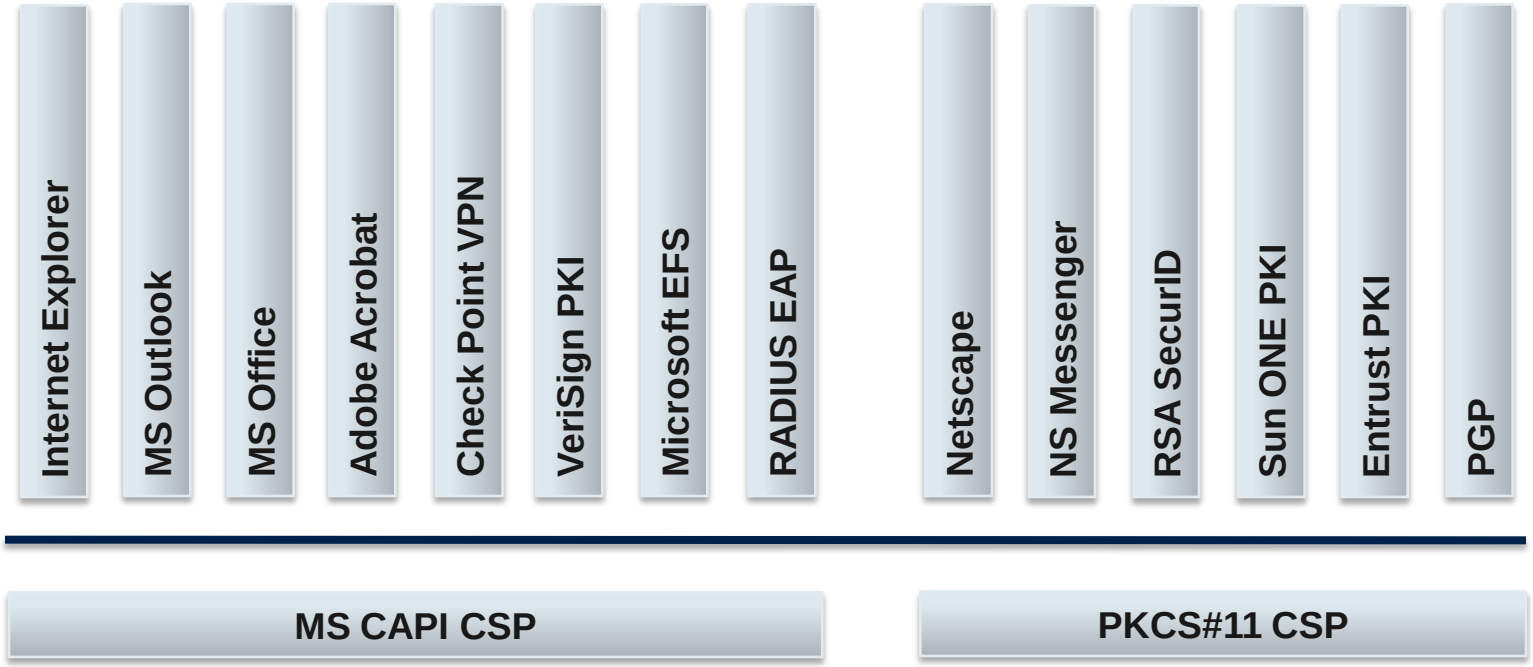
Modular Architecture



Copyright © Infineon Technologies 2009. All rights reserved.

MS-CAPI and PKCS#11 Interfaces allow other applications to easily take advantage of TPM

- Microsoft CAPI Cryptographic Service Provider (CSP)
  - Keys and certificates protection
- PKCS#11 Cryptographic Service Provider (CSP)
  - Keys, certificates and objects protection



This list is subject to change without notification and the information provided does not construe a guaranteed function. For specific questions about supported versions, please contact Infineon or the provider of the 3rd party software

The Challenge: Deployment and Management of TPM-enabled PCs in the Enterprise

- Platform Initialization
  - Take Ownership while setting the Owner Secret
    - Create and install key pair for key backup
    - Save key pair for key backup to removable media
    - Configure key backup archive location
- User related administration tasks
  - Make sure that user credential backups are up-to-date
  - Restore user credentials during platform replacement
  - Support migration of user credentials to other platforms
  - Provide support in case of forgotten password
  - Provide support for Dictionary Attack Detection Reset

Platform and user initialization previously required a certain amount of owner and user interaction

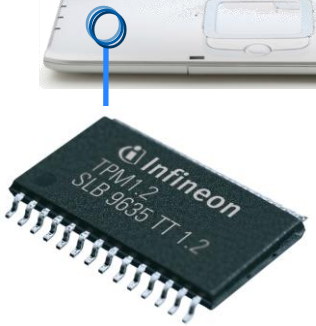
Copyright © Infineon Technologies 2009. All rights reserved.

Trusted Computing components by Infineon

IFX is the only company that provides a complete solution

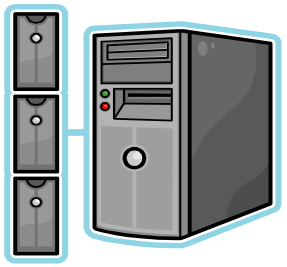
TPM Client SW
(TPM Professional Package)

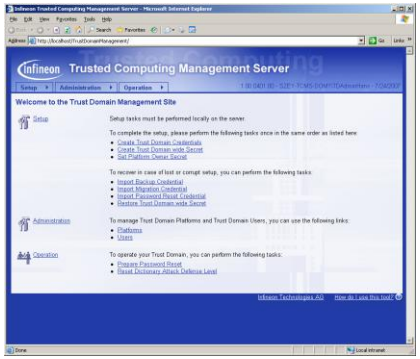




TPM Security Chip

Manages





Server SW
Trusted Computing
Management Server
(TCMS)

- Ensuring platform integrity
- Strong authentication of the Trusted Platform to a network
- Secure Storage of Secrets and Keys

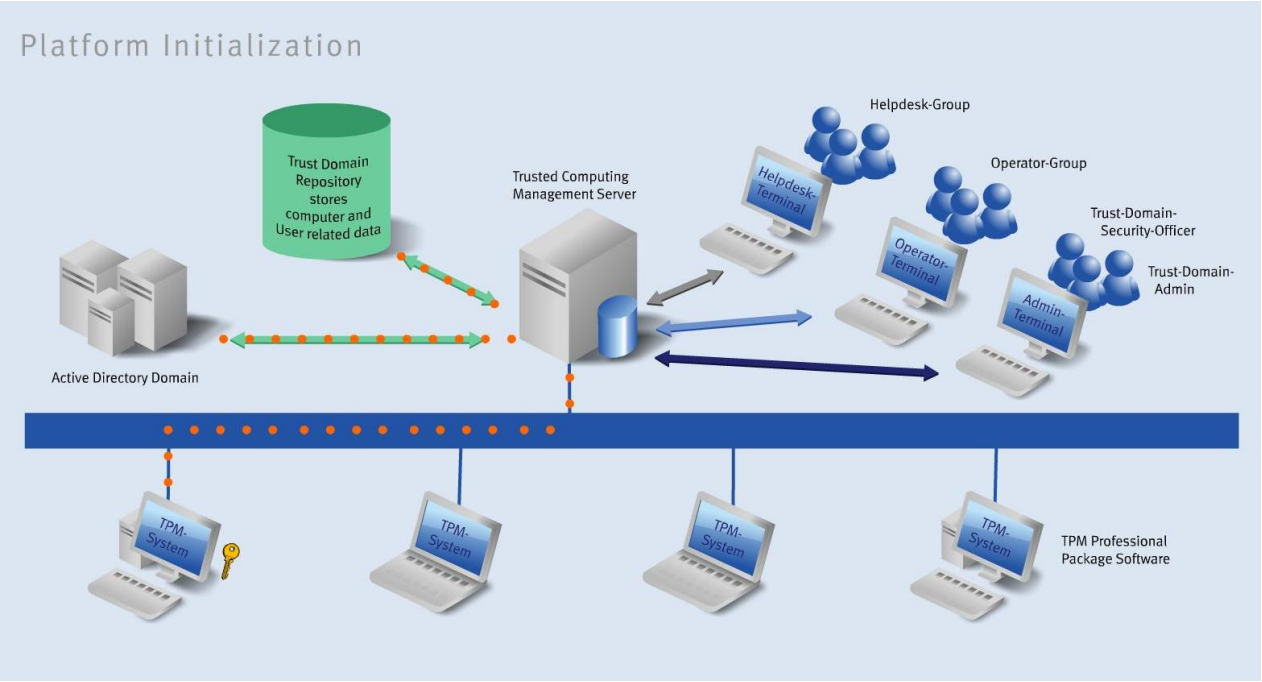
Copyright © Infineon Technologies 2009. All rights reserved.

Trusted Computing Management Server Key Features

- **Platform and User Enrollment/Removal**
  - Automatic enrollment for platforms and users belonging to enrollment group (with Endorsement Key trust verification)
- **TPM User Password Reset**
  - Management GUI allows Trust Domain Administrator to prepare user password reset based on Trust Domain password reset key
- **Dictionary Attack Defense Level Reset**
  - Preparation and automatic reset
- **Platform Restore**
  - Backup/restore feature prevents data loss in event of failure of TPM or storage media
  - Restores key and certificate data, platform security features such as TPM-enhanced Windows Encrypted File System configuration, Personal Secure Drive configuration
- **Full User Roaming**
  - Synchronize credential updates when user logs on to any supported platform
  - Notification of updates, changed credentials

Copyright © Infineon Technologies 2009. All rights reserved.

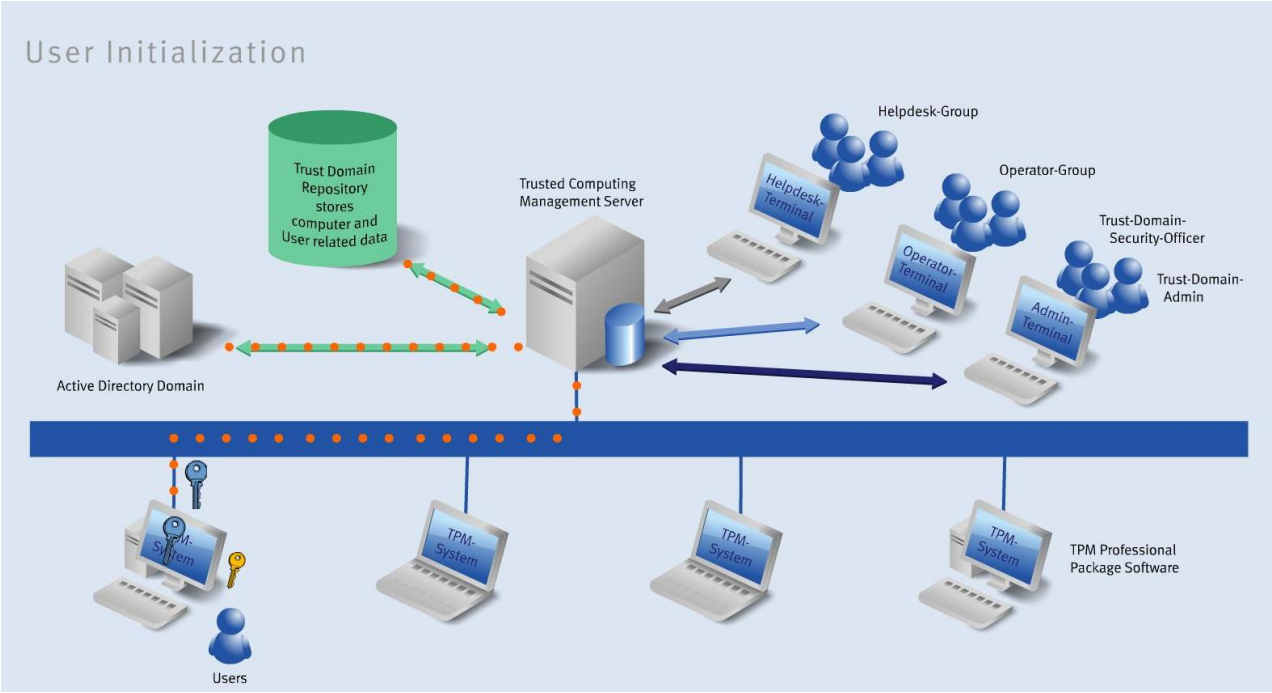
Use Case: Platform Initialization



- Automatic TPM initialization and take-ownership in a *trusted domain*
- Automatic generation or import of platform keys and credential backup

Copyright © Infineon Technologies 2009. All rights reserved.

Use Case: User Initialization

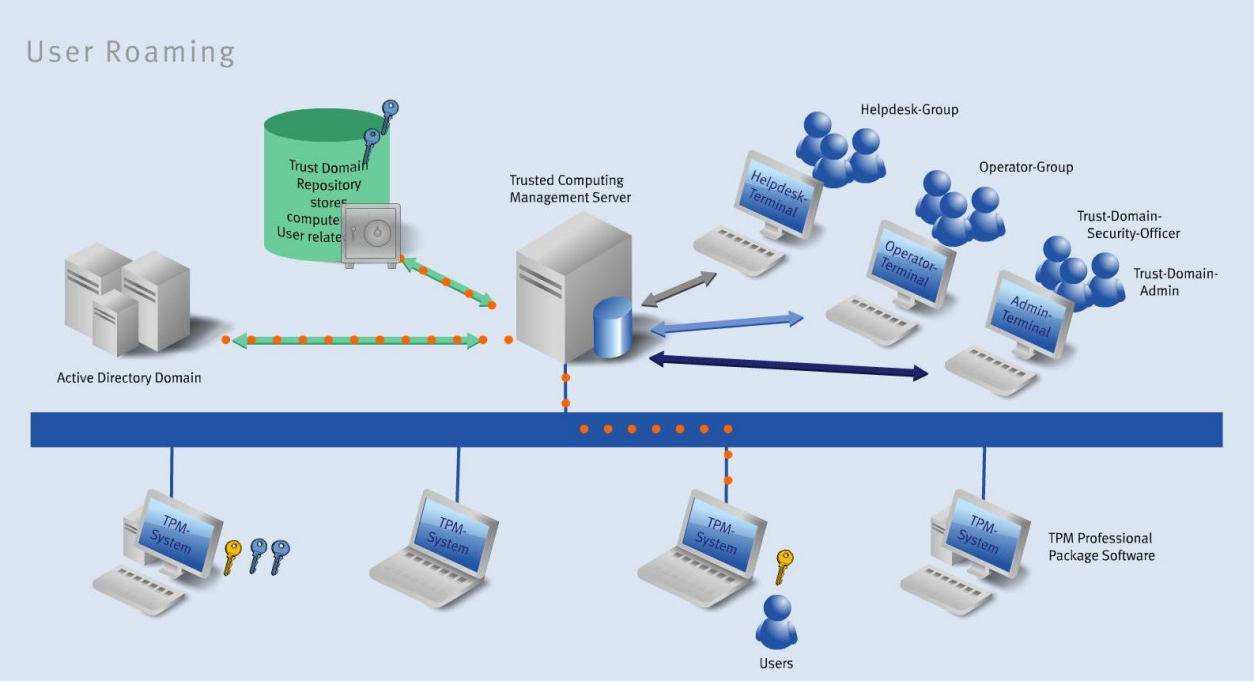


- Automatic user initialization at first logon
- User Key generation or import via MS-CAPI or PKCS#11
- Automatic user credential backup

Copyright © Infineon Technologies 2009. All rights reserved.

Trusted Computing Management Server

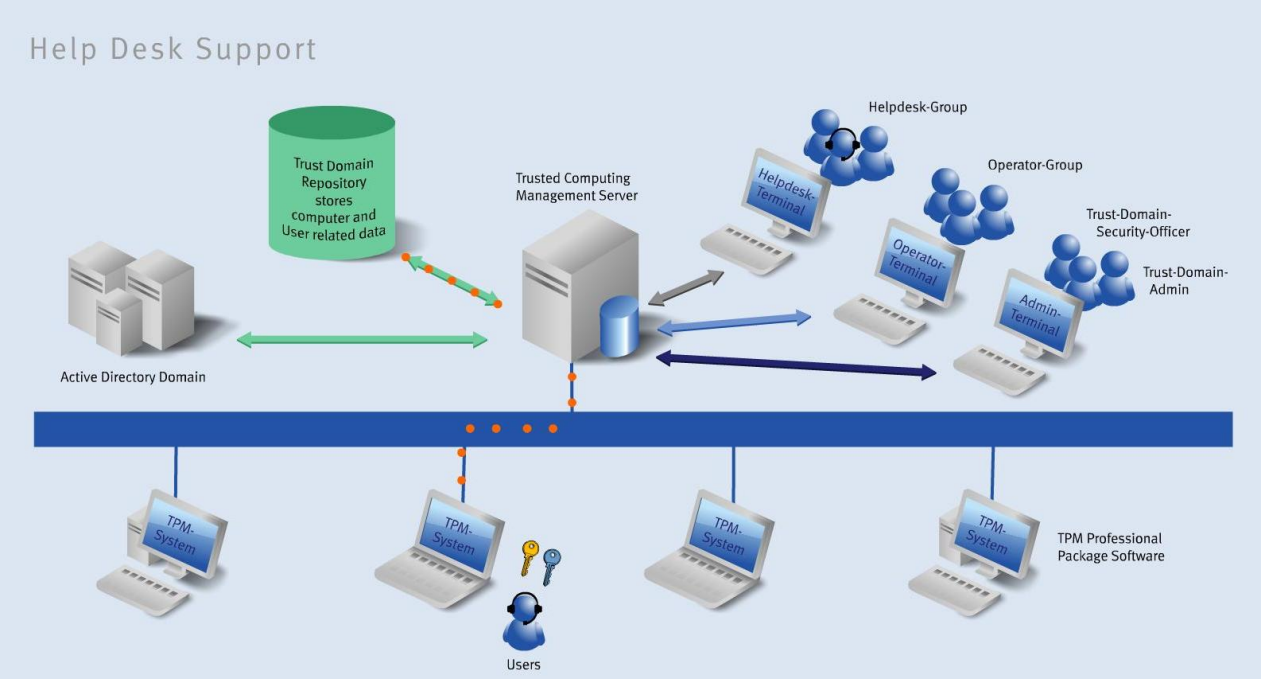
Use Case: *User Roaming*



- Automatic and secure synchronization of TPM-protected User Keys between multiple PCs
- Supports PC-repair/upgrade/ change scenarios

Copyright © Infineon Technologies 2009. All rights reserved.

Use Case: Help Desk Support



- Solves the #1 cause of help desk calls: forgotten passwords
- Helpdesk assisted, secure and auditable password reset

Copyright © Infineon Technologies 2009. All rights reserved.

Demo Setup

- Server- Compaq NC4200 – Windows Server 2003 Enterprise R2
  - TCMS Server
- Client 1: Compaq nx9420 – Windows Server 2008 Enterprise
  - Infineon TPM – Professional Package 3.5
- Client 2: Gateway TA7 – Vista Ultimate
  - ST-Micro TPM – Professional Package 3.5
- Client 3: Dell D630 – Vista Ultimate
  - Broadcom TPM – Professional Package

Copyright © Infineon Technologies 2009. All rights reserved.

Demo Information

- Domain Name: TCMS-Infineon.local.
- User groups: TDUsers, TDAdmins
- Platform group: TDPlatforms (Domain computers is a member of this group)
- All clients are enrolled in the trusted domain and TPM ownership is taken by the TCMS software in server.
- Two users (Alice and Bob) are initialized and enrolled in the trusted user group.
- Both user have their EFS file and encrypted drive (Personal Secure Drive) in the removable media (USB drive)

Copyright © Infineon Technologies 2009. All rights reserved.

Introduction

- Trusted Computing Management Server Interface
  - Setup interface
  - Administration Interface
  - Operation Interface

- Infineon Professional Package
  - Information
  - User Settings
  - Backup
  - Password Reset

Copyright © Infineon Technologies 2009. All rights reserved.

TCMS Features – User Roaming

User is free to roam within the trusted domain clients and keys and certificates are available in machines where ever user is logged on (single or multiple machines). Automatic Backup and restore of TPM keys and credentials by TCMS

- Alice logs into any client
  - Her Keys and credentials are available in that client via TCMS
  - Alice loads her PSD and read files
  - Alice decrypts and reads her EFS file from the drive.
- Alice logs off and logs in another client and performs the same tasks

Copyright © Infineon Technologies 2009. All rights reserved.

TCMS Features – Password Reset

Password reset process is based on 4-eye principle (user and IT Helpdesk) for higher level of security. TCMS keeps all the user credential and settings up to date and synchronized.

- Bob logs on any client and request password reset
- Bob Provides the password reset secret.
- Password reset authorization is generated by TCMS
- Bob gets the authorization directly from the server
- Bob resets his password.
- Bob logs onto another client
- Now Bob needs to updates his credentials and settings in the client.

Copyright © Infineon Technologies 2009. All rights reserved.

TCMS Features – Dictionary Attack Reset

- Alice Logs into one client
- Alice tries to load her PSD with different user password multiple times
- TPM detects the failed attempts and goes to disable mode
- Dictionary attack reset is prepared by TCMS.
- System needs to be rebooted for the reset to take place.

Copyright © Infineon Technologies 2009. All rights reserved.

Summary

- TCMS can manage
  - TPMs from multiple vendors
  - Multiple operating system versions
  - Systems from multiple manufacturers

- Automatic (No Admin or user interaction needed)
  - Platform enrollment
  - Backup and restore of keys and credentials
  - User roaming
  - Synchronization of user keys and credentials across multiple clients

Copyright © Infineon Technologies 2009. All rights reserved.