TPM as a Virtual Smart Card

John Fitzgerald
Wave Systems
# Challenges

<table>
<thead>
<tr>
<th>Passwords</th>
<th>Multi-factor Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Passwords are easy to break</td>
<td>• Example: Two-factor authentication</td>
</tr>
<tr>
<td>• Password complexity adds to</td>
<td>• Numerous multi-factor authentication products</td>
</tr>
<tr>
<td>user and management complexity</td>
<td>• Need to maintain possession of multiple tokens based on use</td>
</tr>
<tr>
<td>• Password management is</td>
<td>• Existing multi-factor authentication products can be expensive - up to $150/user (Source: Gartner Research 2013)</td>
</tr>
<tr>
<td>expensive</td>
<td>• Not easy to use</td>
</tr>
<tr>
<td>• High-risk for breach</td>
<td></td>
</tr>
<tr>
<td>• $20- $100 /user (Source: SC</td>
<td></td>
</tr>
<tr>
<td>Magazine product review)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A virtual smart card uses software to turn the TPM into a smart card. The smart card is integrated and tied to the platform and can be used much in the same way as a conventional smart card.
Secure multi-factor authentication

Enables only known users and known devices to access corporate resources, devices and applications

Utilizes hardware root of trust to offer easy-to-use, strong authentication

Software solution that uses secure hardware that is always present inside your PC
Wave Virtual Smart Card: Benefits

- Ultra-secure
- Hardware-based security
- Significantly lower Total Cost of Ownership (TCO) than PKI token
- Radically reduce risk of data breach with strong authentication and access control with known devices and known users
- Integrate seamlessly with common enterprise applications
- Available on Windows 7, 8, and 8.1
Virtual Smart Card: Use Case Examples

- User login to Windows tablet/laptop
- User authentication with VPN
- Port-based access control (802.1X)
- Strong encryption – email, BitLocker keys
- Integrity – tamper resistance
• Appears and operates exactly like a physical smart card
• Flexible installation options
• Modern Access Control
• Consistent user experience for Win 7/8/8.1
• Remote or user self-provisioning
• Remote revocation/delete
• Automated PIN recovery/unblock
• Status discovery & reporting
Virtual Smart Card: Summary

- Superior security – Authentication, Encryption
- Available for Windows 7, Windows 8 and 8.1
- Lower Total Cost of Ownership – up to 60% less
- Superior user experience
- Seamless integration with existing applications and services
Backup
The TPM is a standards-based security module that’s built into most laptops, desktops and tablets.

A secure micro-controller with cryptographic features that provides a root of trust enabling the secure generation of keys and the ability to limit their use for encryption/decryption & signatures, and as a secure container for key storage.