Identity Protection Technology

Ned Smith
PC Client Group
October 2011
Legal Notices and Disclaimers

• INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY
ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN
INTEL’S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS
ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES
RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER
INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING
APPLICATIONS.

• Intel may make changes to specifications and product descriptions at any time, without notice.

• All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

• Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to
deviate from published specifications. Current characterized errata are available on request.

• Any code names featured are used internally within Intel to identify products that are in development and not yet publicly announced
for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or
marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

• No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system,
including a 2nd gen Intel® Core™ processor enabled chipset, firmware and software, and participating website. Consult your system
manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit

• Intel product plans in this presentation do not constitute Intel plan of record product roadmaps. Please contact your Intel
representative to obtain Intel’s current plan of record product roadmaps.

• Intel, Intel Inside, the Intel logo, Centrino, Intel Core, Intel Atom, Pentium and UltraBook are trademarks of Intel Corporation in the
United States and other countries.

• *Other names and brands may be claimed as the property of others.

• This document contains information on products in the design phase of development.

• Copyright © 2011 Intel Corporation, All Rights Reserved
Intel® Identity Protection Technology Uses

Online Gaming
Online Banking
Email and document signing
VPN Access
SaaS Apps
Custom Apps

Consumer
SMB
Enterprise
How does Intel® IPT fit with Intel?

Intel is positioning ourselves to lead in three areas: energy-efficient performance silicon, connectivity and security. There’s an urgent need for security innovation as people are spending more time online and the amount of data is growing.

Security
Comunication
Energy Efficient

Identity Protection & Fraud Deterrence
Detection & Prevention of Malware
Securing Media, Data and Assets
Recovery and Enhanced Patching

Intel IPT introduced on select 2nd generation Intel® Core™ processor-based PCs in 2011
IPT: One Time Password (OTP)

The first generation of Intel® IPT is a dynamic code generated on 2nd generation Intel® Core™ processor-based PCs that allows a corporation, financial firm, or social media site to authenticate that you are logging in from a trusted PC

• Single use, (i.e. 30 second, time-limited code → OTP )
• A hardware level 2nd factor of authentication
• Works with leading OTP Solutions from Symantec & Vasco

Traditional OTP token

Now embedded into your PC
IPT: Embedded Smartcard

Embeds an additional factor of user authentication into the platform that allows a corporation or web service to remotely verify keys are protected by a trusted PC

Platform Embedded Asymmetrical Token (PEAT)

- Private keys stored in hardware
- Useful for authentication, signing and encryption
- Compliant with industry standard CSP, KSP and PKCS interfaces

Traditional Smartcard token

Now embedded into your PC
True Cove is Input Protection

An encrypted I/O technology built using Intel’s protected display capability

**Tx Authorization**

**View seen by a user**

**View seen by malware**

**Encrypted bitmap with randomized keypad**

**User Presence**

**Randomized OK button**

**CAPTCHA: Today...**

**... with TrueCove**
Web login with Intel® IPT One-time Password

1. User visits Bank’s login page

2. User enters UN & PWD

3. True Cove is invoked

4. User enters OTP PIN using mouse clicks

5. PIN is validated

6. OTP is generated and filled in

7. UN + PWD + OTP sent to Bank for login
Transaction Protection with True Cove

1. User authenticates and initiates a transaction
2. Website sends encrypted confirmation screen
3. True Cove is invoked to display confirmation screen
4. User enters PIN
5. Transaction confirmation returned
6. PIN is extracted and verified. Transaction is authorized.

Transfer: $50
From: Me (AC 10051)
To: You (AC 34287)

Please enter your PIN: ****

Cancel  CLR  OK

Intel® IPT protected the online transaction from browser tampering
Enterprise VPN Usage

Step 1:
IT instructs user to run a setup app that generates a PEAT key pair that will require a user PIN

Step 2:
User connects to a PKI server to enroll a certificate. CA issues a certificate for use with VPN client

Step 3:
Setup app installs a single-click VPN connection option

Step 4:
User launches VPN app. VPN client automatically selects the PEAT cert. The user is prompted to enter a PIN via TrueCove
Cloud Services Login Use Case

The user logs into a cloud service that requires user authentication using a certificate.

The user authenticates to Intel® IPT using TrueCove PIN pad.

A TLS VPN is established followed by cloud app interactions.

Browser cookie identifies client certificate capability and selects PEAT key certificate.

The user authenticates to Intel® IPT using TrueCove PIN pad.

No Need for Cloud Service to Maintain Passwords.
PEAT Capabilities

Embedded Cryptographic Token
- HW based Public/Private Key crypto
- Industry standard interfaces (CSP, KSP, PKCS11, ...)

Protected PINPAD (via True Cove)
- Key use authorization
- Trusted path to the user

Attestation
- Keys are protected by trustworthy hardware
- Zero-touch provisioning
Intel® IPT Security Model

- **Intel® IPT** protects authentication and smartcard identities in a hardened environment enabled by **Intel® Core™ vPro™ Processor and Chipset**

- **Identity management providers** can verify the trust boundary using **EPID-based attestation**
Intel® IPT Attestation

Motivation: Provide evidence to Service Provider that PEAT key and OTP seed is protected by Intel security engine.

How:

• Enhanced Privacy IDentifier (EPID)
  – Asymmetric key embedded into Intel HW at manufacturing time

• Sigma provisioning protocol
  – Diffie-Hellman key exchange protocol signed by EPID

• EPID Key Attestation Evidence (EKAЕ):
  – Digitally signed certificate enrollment extension to PKCS#10
Market Drivers for Cloud Identity Management
What are the User to Cloud Access Challenges?

**Multiple Logins / Weak Security**
- Single Sign On (SSO)
- & Strong Authentication

**Lack of Visibility**
- Centralized Management Console

**Manual Provisioning**
- Auto Account Provisioning & Profile Sync

**ID Infrastructure Integration**
- AuthN & Provisioning Connectors
- AD & IAM

**Audit Silos**
- Centralized Audit Logging

**Scalable, Federated Trust**
- Standards Based
Intel® ECA 360 – With Focus on Strong Auth Advantage

**Enterprise to Cloud SSO**

- **To the Cloud**
  - Provision Access
    - Provision/de-provision user accounts
    - AD integration
    - Sync Id Profiles
  - Adaptive Strong Auth
    - Selectively apply 2nd factor OTP AuthN
    - Variety of software AuthN methods & devices- mobile devices, SMS, email
  - Secure SSO
    - Federate windows/AD log in
    - To popular SaaS like Salesforce & Google Apps
  - Regulatory Compliance
    - Rich audit trail of user login showing AuthN level
    - De-provision & orphan account reports

**Securing Custom or SaaS Apps**

- **In the Cloud**

Tagline: Go Beyond SSO with Strong Auth and Provisioning

Intel® ECA 360 – With Focus on Strong Auth Advantage
Added Strong Authentication

- 2\textsuperscript{nd} factor authentication using One Time Password (OTP) soft-tokens
- Supports a wide range of authentication methods:
  - Mobile Token – Pledge*
  - USB Key – YubiKey*
  - SMS, Email
  - Runs on all platforms: iPhone*, BlackBerry*, WinMobile*, etc.
- Adaptive based on type of application accessed
- Delivers a more secure Internet SSO

Provides extra security at federated log-in since access is granted to many cloud apps
• Intel® IPT seamlessly integrated with CloudAccess360
  • Client based OTP authentication
  • Federated SSO infrastructure to the cloud
Ecosystem for Intel® IPT

Intel® IPT PCs

HP Compaq* 6200 Pro, 8200 Elite
ALL new HP Laptops!

Latitude* E6520, E6420, E6320,
E6220, E5520, E5420
Optiplex* 790, 990

Thinkpad* T420, T520,
x220, ThinkCenter* M91

Shipping

Enhance your experience by installing a Free Symantec* VIP client
(found at symantec.com, intel.com, or retailer)

Vasco* customers will need to update their server and implement the latest version of Vasco* Digi-Pass for Web to implement their clientless Intel® IPT solution

Building your own PC? Check our website for Intel® IPT requirements & driver downloads
Origins of Cloud Access 360

- Federated Single sign-on (SSO)
- OTP & Provisioning Server
- Cloud Identity Manager

Sold thru McAfee
CloudAccess360 is Part of a Comprehensive Cloud Security Solution

Cloud Ecosystem

Partners
Cloud Vendors
Applications
Customers

Unified Management, Policy and Reporting, ePO Integration

Services Gateway
Cloud Identity Manager

Email Security
Data Loss Prevention
Web Security

Global Threat Intelligence
Cloud Security Platform
Enterprise

Mobile Users
Enterprise Users
Private Cloud Applications
Conclusion

• Intel® IPT adds important client-base authentication capabilities

• Support for OTP, certificates and trusted path to the user

• Hardened and attestable isolated environment

• Integration with cloud-based identity management infrastructure