Intel® Identity Protection Technology (IPT)

Hormuzd Khosravi, Principal Engineer, Intel Corporation

Legal Information

Intel technologies, features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice. Notice Revision #20110804

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, Intel vPro, Look Inside., the Look Inside. logo, Intel Xeon Phi, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Agenda

Problem Statement and Introduction

Identity Protection Technology Overview

Intel® IPT with PKI

Intel® IPT with MFA

Summary

Q&A

Agenda

Problem Statement and Introduction

Identity Protection Technology Overview

Intel® IPT with PKI

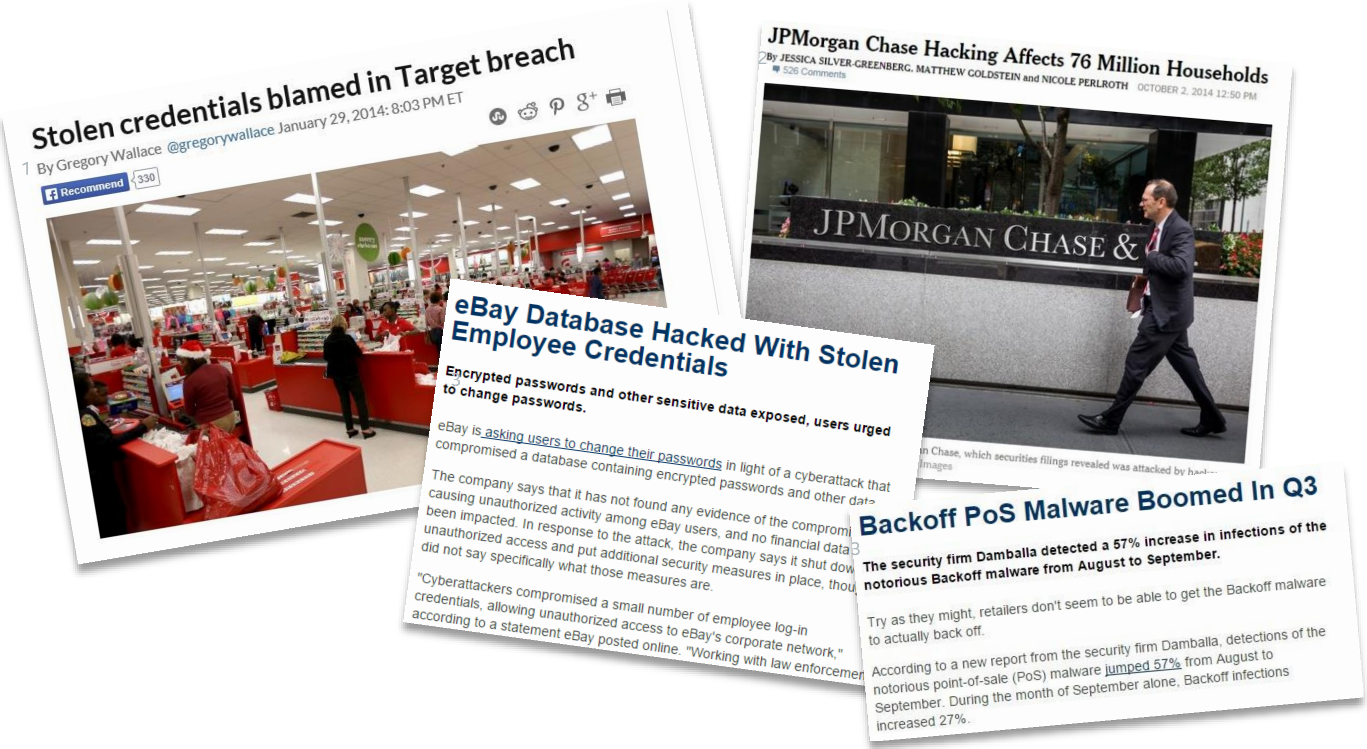
Intel® IPT with MFA

Summary

Q&A

Compromised Credentials Lead to Breach and Data Loss

Top Organizations Attacked



Stolen credentials blamed in Target breach

[1] By Gregory Wallace @gregorywallace January 29, 2014: 8:03 PM ET

Recommend 330

JPMorgan Chase Hacking Affects 76 Million Households

[2] By JESSICA SILVER-GREENBERG, MATTHEW GOLDSTEIN and NICOLE PERLROTH OCTOBER 2, 2014 12:50 PM

526 Comments

n Chase, which securities filings revealed was attacked by hack

Images

eBay Database Hacked With Stolen Employee Credentials

[3] **Encrypted passwords and other sensitive data exposed, users urged to change passwords.**

eBay is asking users to change their passwords in light of a cyberattack that compromised a database containing encrypted passwords and other data

The company says that it has not found any evidence of the comprom causing unauthorized activity among eBay users, and no financial data been impacted. In response to the attack, the company says it shut dow unauthorized access and put additional security measures in place, thou did not say specifically what those measures are.

"Cyberattackers compromised a small number of employee log-in credentials, allowing unauthorized access to eBay's corporate network," according to a statement eBay posted online. "Working with law enforcemen

Backoff PoS Malware Boomed In Q3

[3] **The security firm Damballa detected a 57% increase in infections of the notorious Backoff malware from August to September.**

Try as they might, retailers don't seem to be able to get the Backoff malware to actually back off.

According to a new report from the security firm Damballa, detections of the notorious point-of-sale (PoS) malware jumped 57% from August to September. During the month of September alone, Backoff infections increased 27%.

Ground Zero for many attacks is compromised *Identity*

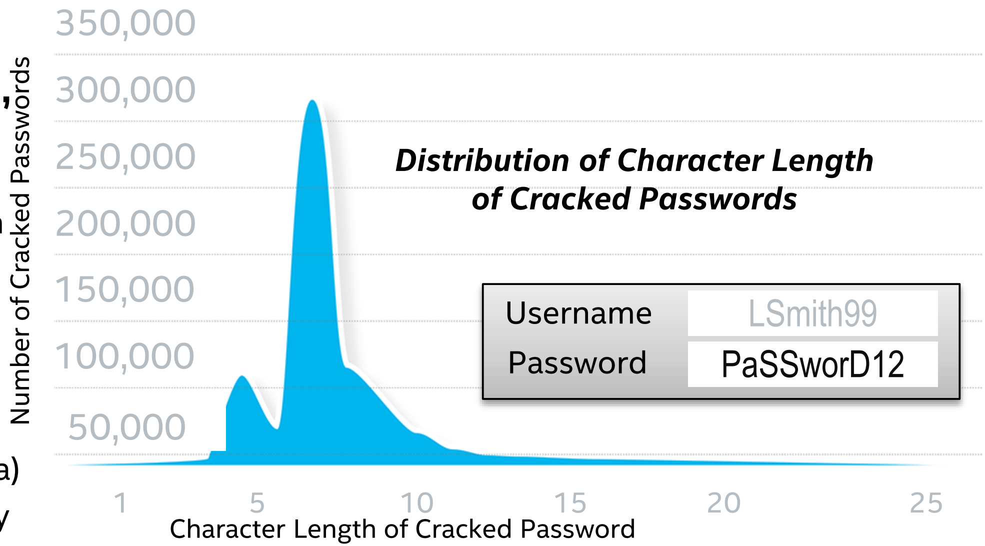
[1]CNN Money 2014 [2]NY Times 2014 [3]DarkReading.com 2014

Problem Statement

Passwords are Problematic for end users and IT

Complex Passwords are not the answer:

- **Users can't remember complex passwords, costly to IT:**
  - 35-40% of helpdesk calls are password resets, 20-30% of helpdesk calls result from lost, stolen or broken credentials (Gartner*)
  - 20-30% of Helpdesk calls are related to lost, stolen, broken credentials for enterprises using discreet tokens (Gartner)
  - Cost of Helpdesk call to reset token or issue temporary credential averages $25 per call (Meta)
  - Complex password policies generate more costly helpdesk calls without added security (Wired* Article)


Distribution of Character Length of Cracked Passwords

Passwords are easily cracked, key-logged, phished & Intercepted, making them a security *risk*

[1]Trustwave *2014 Business Password Analysis

Identity and Access Management (IAM)

Securing the Front Door a Key Challenge

- Many authentication factors including Passwords, Tokens, Key Infrastructure. **But** no unifying framework to simplify implementation, management, enforcement.

- Known challenges with *current* authentication methods:
  - *Passwords*: **Complex** Users and IT = vulnerable
  - *Tokens and Smart Cards*: **Costly** to maintain
  - *Software-based Keys:* are at **greater risk**
  - *User Presence and context*: Location confirmation is **difficult**

Many weaknesses in *traditional* security make it difficult and expensive to optimize identity and access management

How Big is the Emerging Attack Surface?

An Average Day In An Average Enterprise[1]

Every **1 min** a host accesses a malicious website

Every **3 mins** a bot is communicating with its command and control center

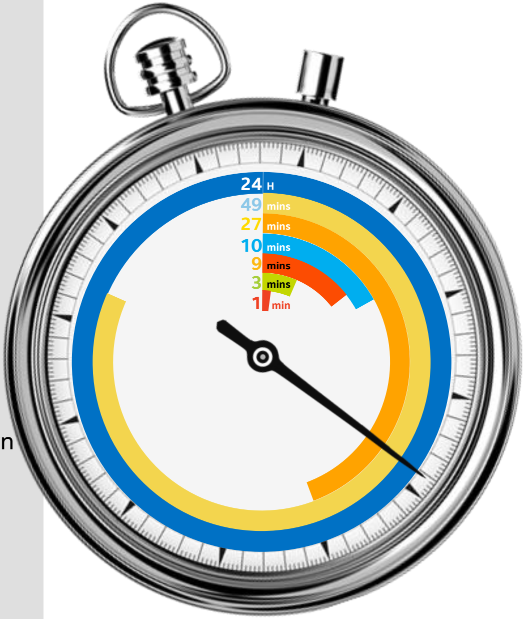
Every **9 mins** a High Risk application is being used

Every **10 mins** a known malware is being downloaded

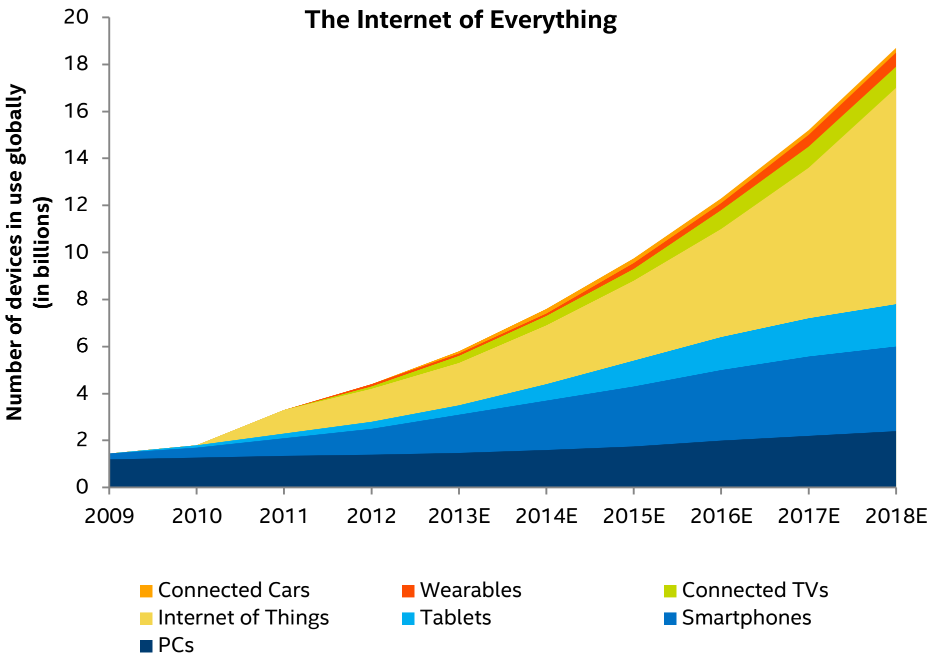
Every **27 mins** an unknown malware is being downloaded

Every **49 mins** sensitive data is sent outside the organization

Every **24h** a given host is infected with a bot



Forecast: Global Internet Device Installed Base[2]



[1] source: Check Point Security Report 2014
[2] source: BI Intelligence Investments 2014

The Four Pillars of Intel’s Security Focus

Protect		Detect	Correct
Identity	Data Protection	Anti-Malware	Resiliency
Protect user & device identities	Protect data at rest and in transit	Detect malware based on signature & behavior	Correct security weaknesses & breaches

Intel® platforms ship with Security built-in!

Note: Not all features available across all products

Agenda

Problem Statement and Introduction

Identity Protection Technology Overview

Intel® IPT with PKI

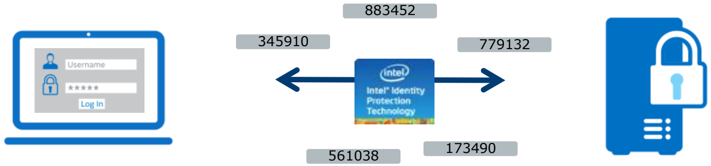
Intel® IPT with MFA

Summary

Q&A

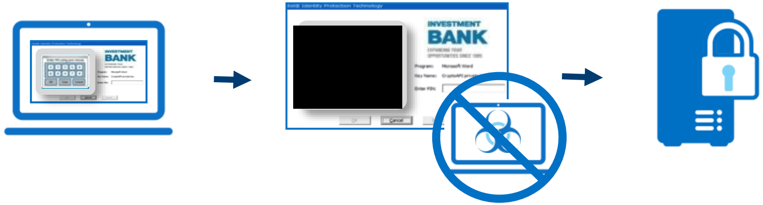
Intel® Identity Protection Technology

ONE-TIME PASSWORD (OTP)



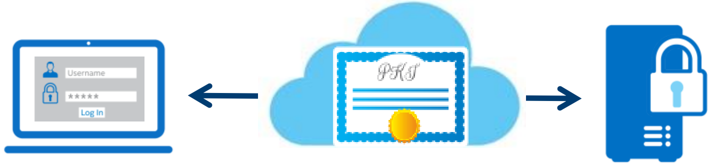
One-Time Password token built into the chipset, enabling frictionless factor user authentication for more secure website and corporate access

PROTECTED TRANSACTION DISPLAY+



Helps protect PC display from malware scraping and proves human presence at PC. Great for transaction verification and ACH fraud prevention+

PUBLIC KEY INFRASTRUCTURE



Uses hardware protected PKI certificates to authenticate user and server to each other and to encrypt and sign documents

Intel® Identity Protection Technology: Embedded security ingredients to help protect confidential business data, and employee and customer identities++

intel
Intel® Identity Protection Technology

+Protected Transaction Display requires a device with Intel® Integrated Graphics

++No computer system can provide absolute security. Requires an Intel® Identity Protection Technology-enabled system, including an enabled Intel® processor, enabled chipset, firmware, software and Intel integrated graphics (in some cases) and participating website/service.

Intel® Identity Protection Technology with Multi Factor Authentication

Key Use Cases:

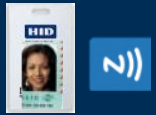
- Domain/OS Login
- Remote Cloud Services Single Sign On
- Web log-in
- VPN Login & Key Storage
- Walk-Away Lock of Platform & Services
- Drive Encryption Login

Potential Hardened Authentication Factors:

PIN
Protected Transactions

Proximity
Bluetooth, BLE

Logical Location
Intel® AMT Location



Tap to Login
NFC

Biometrics
Face, Voice, Fingerprint

Easy to use while strengthening authentication, factors and policies through hardware enhanced Multi -Factor Authentication for Corporate applications and services

Agenda

Problem Statement and Introduction

Identity Protection Technology Overview

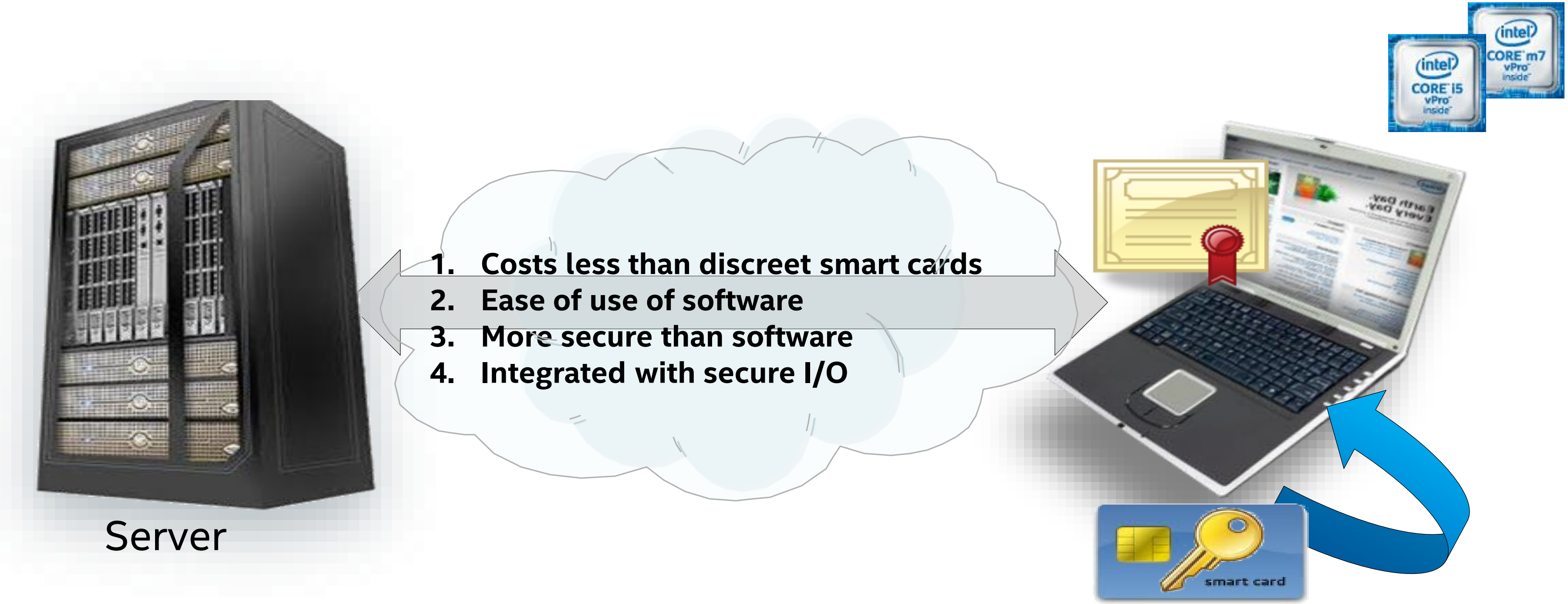
Intel® IPT with PKI

Intel® IPT with MFA

Summary

Q&A

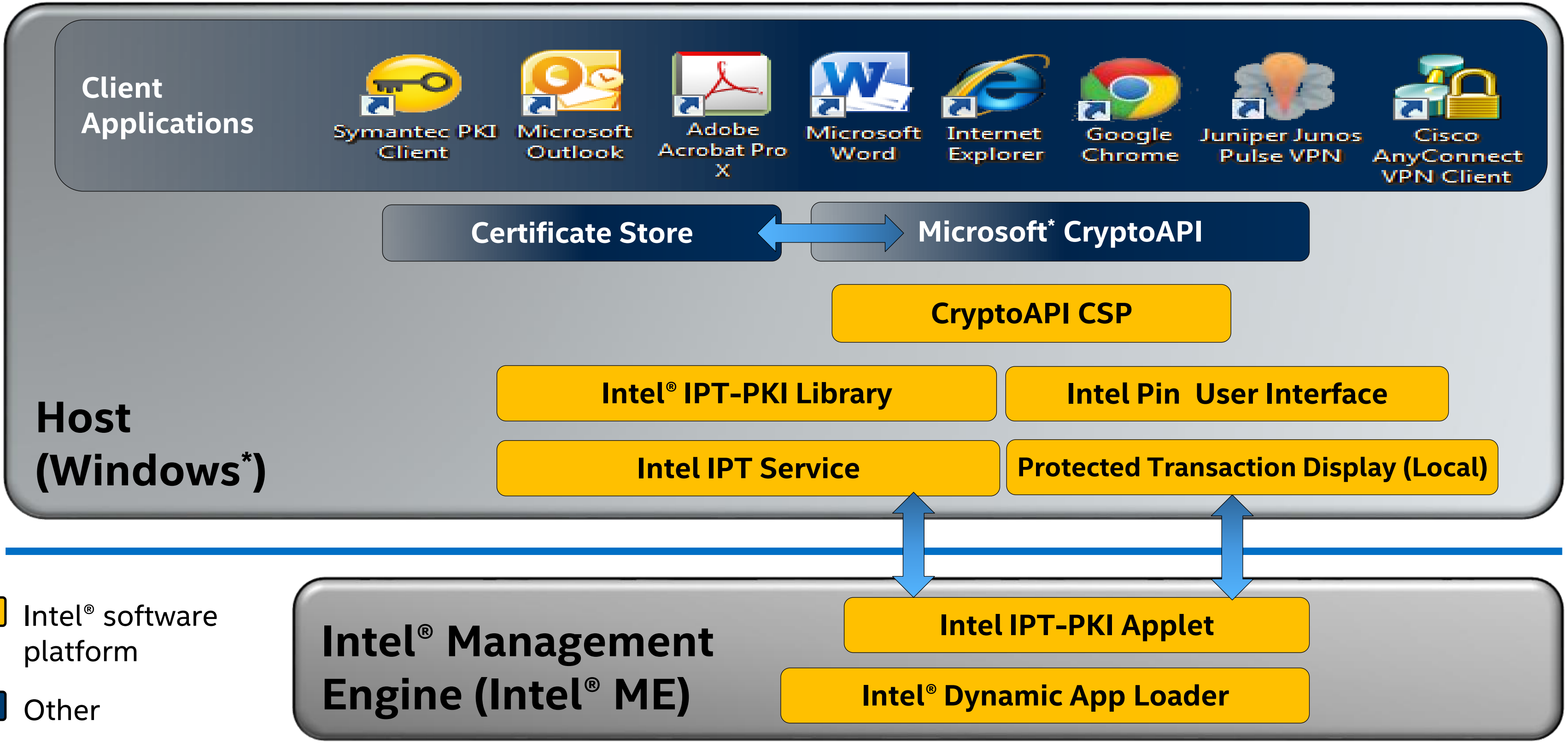
Intel® Identity Protection Technology with PKI



1. Costs less than discreet smart cards
2. Ease of use of software
3. More secure than software
4. Integrated with secure I/O

Intel® Identity Protection Technology with PKI provides a second factor of authentication embedded into the PC that allows businesses to validate that a legitimate user is logging in from a trusted PC

Intel® Identity Protection Technology with PKI v1.0 Architecture



Client Applications

Symantec PKI Client

Microsoft Outlook

Adobe Acrobat Pro X

Microsoft Word

Internet Explorer

Google Chrome

Juniper Junos Pulse VPN

Cisco AnyConnect VPN Client

Certificate Store

Microsoft* CryptoAPI

CryptoAPI CSP

Intel® IPT-PKI Library

Intel Pin User Interface

Intel IPT Service

Protected Transaction Display (Local)

Host (Windows*)

Intel® Management Engine (Intel® ME)

Intel IPT-PKI Applet

Intel® Dynamic App Loader

🟨 Intel® software platform

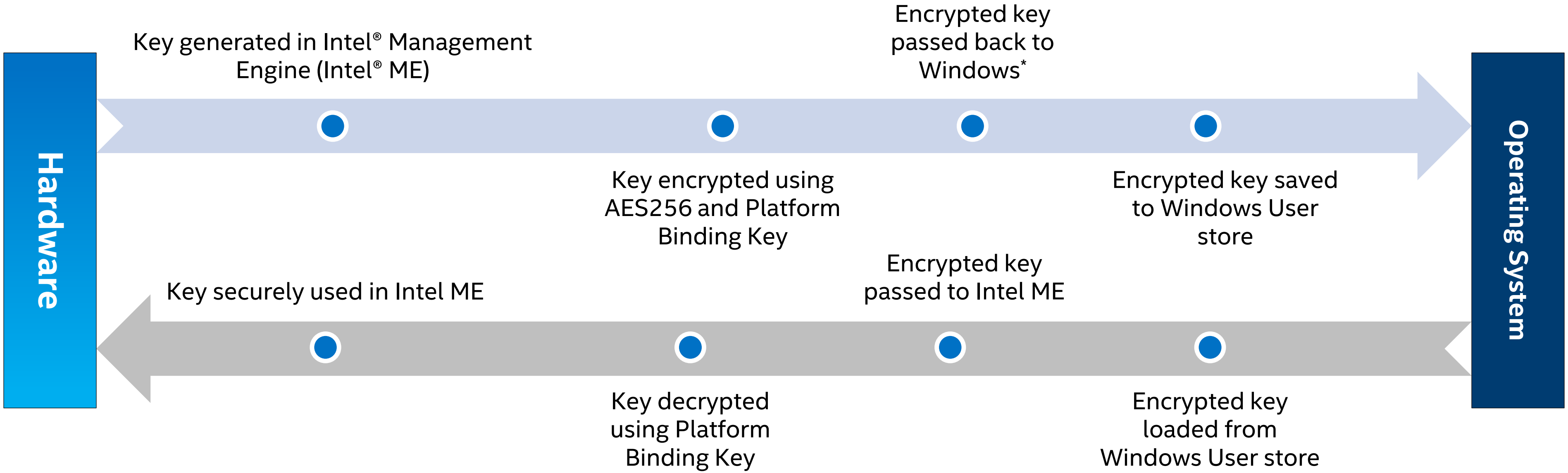
🟦 Other

Supported Cryptographic Algorithms

Algorithms	Type	Intel® IPT-PKI Support	Proxy support
RSA 1024/2048 private key usage	Asymmetric	✗	
RSA 1024/2048 public key usage	Asymmetric		✗
DES, Triple DES, 2 key triple DES, RC2, RC4, AES128, AES192, AES256	Symmetric		✗
SHA1, SHA256, SHA384, SHA512, SHAMD5	Hashing		✗
MAC, HMAC	MAC		✗

Intel® Identity Protection Technology with PKI (Intel® IPT-PKI) supports full cryptographic suite to maximize app compatibility

Key Usage and Storage



Hardware

Key generated in Intel® Management Engine (Intel® ME)

Key encrypted using AES256 and Platform Binding Key

Encrypted key passed back to Windows*

Encrypted key saved to Windows User store

Operating System

Encrypted key loaded from Windows User store

Encrypted key passed to Intel ME

Key decrypted using Platform Binding Key

Key securely used in Intel ME

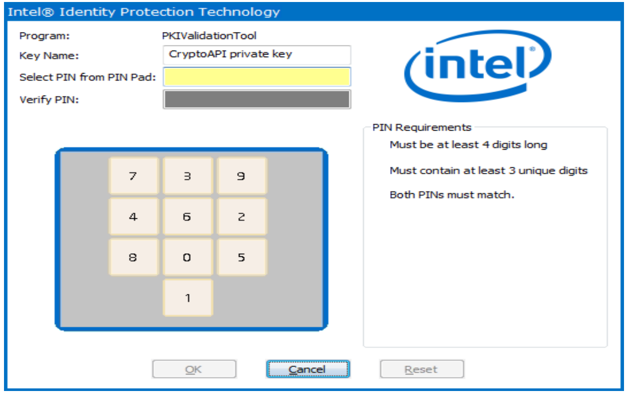
Intel® Identity Protection Technology with PKI key storage is not limited by flash memory or Intel® ME memory

Intel® Identity Protection Technology (Intel® IPT) with Protected Transaction Display

Protects private key usage with PIN

- Created on key generation
- Requested on key usage
- PIN pad randomized
- Button values protected by PAVP
- Provides PIN policy enforcement
- Graphics generated on the client

What an End-User Sees



Intel® Identity Protection Technology

Program: PKIValidationTool

Key Name: CryptoAPI private key

Select PIN from PIN Pad:

Verify PIN:

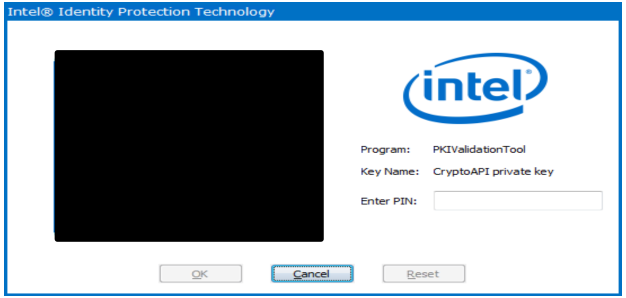
PIN Requirements

Must be at least 4 digits long

Must contain at least 3 unique digits

Both PINs must match.

What a Hacker Sees



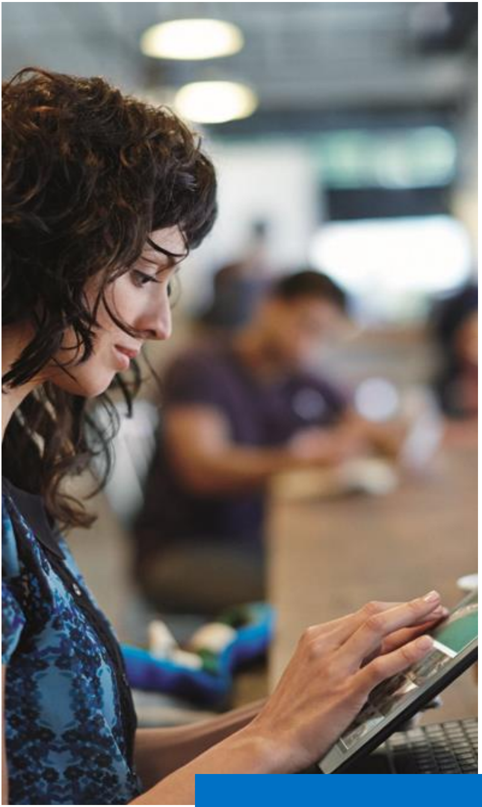
Intel® Identity Protection Technology

Program: PKIValidationTool

Key Name: CryptoAPI private key

Enter PIN:

Intel® Identity Protection Technology with PKI Version 3.0



Secure Import for PKI key-pair/certificate

- Based on Intel® IPT with PKI Import certificate
- Scales Intel IPT with PKI to protect non-self-generated certificates in the Enterprise

Hardware based Key Attestation based on Enhanced Privacy ID (EPID)

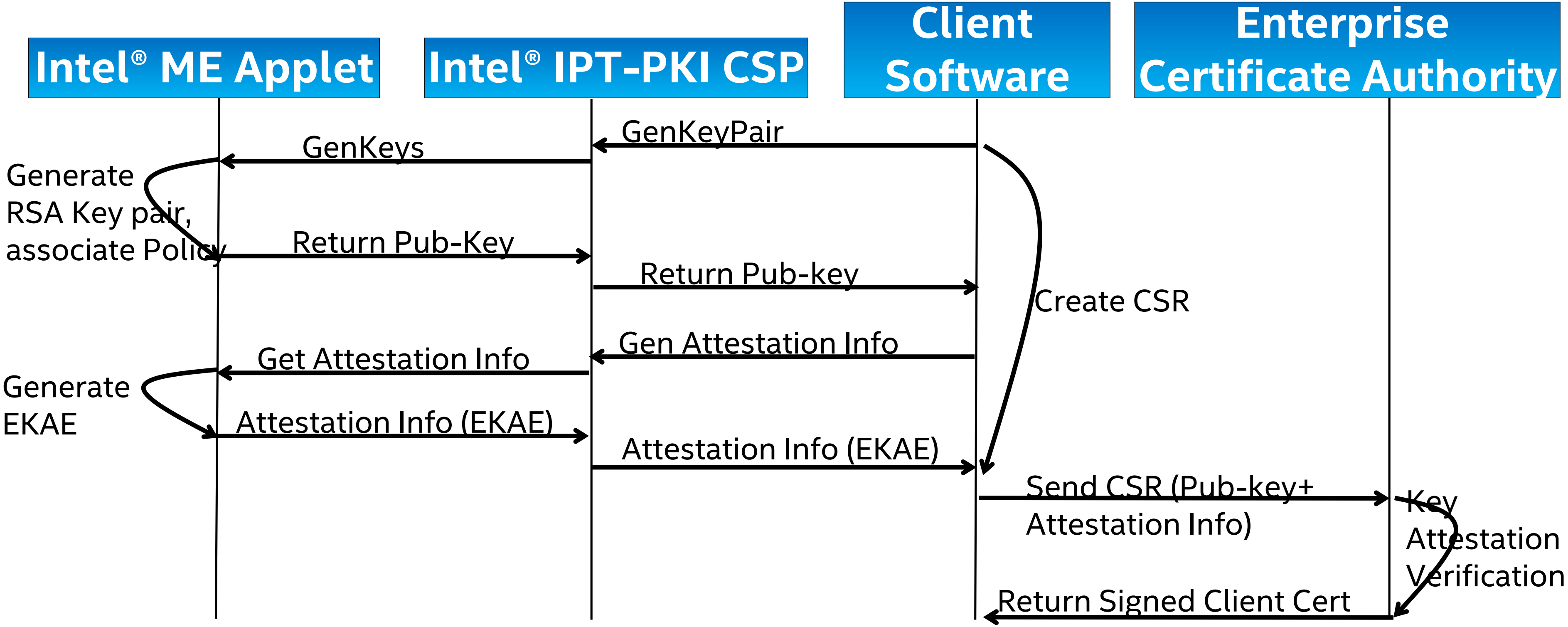
- Based on EPID Signature
- Provides additional protection against man-in-the-middle attacks

Enables new Enterprise usages

- Secure cloud storage and file services
- Usages across multiple devices

IPT with PKI v3.0 Enables New Enterprise Usages and Features

Enterprise Certificate Enrollment Process with Intel® IPT-PKI v3.0 Key Attestation



Intel® Management Engine (Intel® ME)
Intel® Identity Protection Technology with PKI (Intel® IPT-PKI)

Intel® IPT with PKI v3.0 - Secure Import

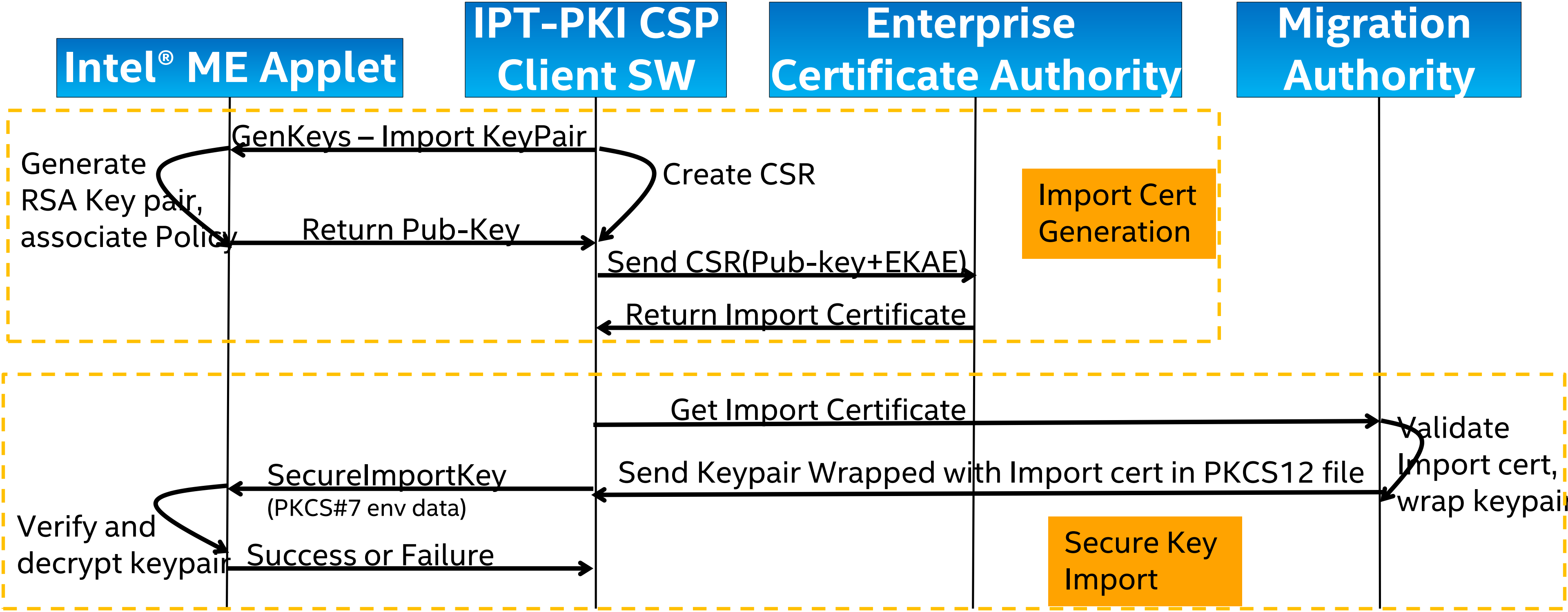
Import Certificate/Key-pair properties:

- MUST be generated by Intel IPT-PKI
- MUST not be exportable
- CANNOT be used for general encrypt/decrypt operations, only import operations
- MUST contain the special “Import” OID specified in the Extended Key usage

Enterprise PKI Infrastructure responsibility:

- Enterprise IT MUST create an import certificate template which specifies the key is non-exportable, used for signing operations only, and includes a special “Import” OID specified in the Extended Key usage
- Enterprise IT MUST ensure that a client has non-revoked import certificate
- Enterprise IT MUST ensure they are encrypting the keys to be imported with the correct import certificate

Secure Import (PKCS12 Public-key Privacy Mode)



Independent Software Vendor (ISV) Integration

Certificate Issuer

Symantec* Managed PKI Service

- 4-6 week effort
- Primarily enabling certificate templates

Microsoft* Certification Authority (CA)

- No change to Microsoft Certificate Authority
- Create/enable certificate templates

Certificate Consumer

Cisco*, MS Office*, Adobe*, Juniper*, Internet Explorer*, etc.

- All enabled with no software change

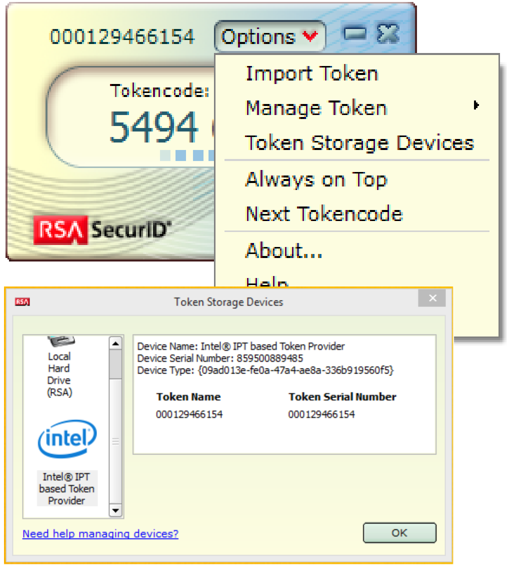
Solution builds on top of standard Microsoft* CryptoAPI

Intel® Identity Protection Technology with PKI (Intel® IPT-PKI) solution requires minimal ISV integration effort!

Market Leading Identity Provider RSA* Now Integrated with 5th Generation Intel® vPro™ Platforms

The Security Division of EMC

- RSA® SecurID® Software Token is protected in hardware by Intel Identity Protection (IPT) based Token Provider
  - SecurID seed record protected and signed by encryption key that is stored on Intel chipset
  - SecurID seed record cannot be removed (by malware) and run on a different machine
- Offers hardware level token security with the convenience of a software token
- Easy to install
  - Driver install package then same process as provisioning SecurID software token



Device Name: Intel® IPT based Token Provider
Device Serial Number: 859500889485
Device Type: {09ad013e-fe0a-47a4-ae8a-336b919560f5}

Token Name	Token Serial Number
000129466154	000129466154

Agenda

Problem Statement and Introduction

Identity Protection Technology Overview

Intel® IPT with PKI

Intel® IPT with MFA

Summary

Q&A

Intel® IPT with MFA

For Corporate and *Managed* Small Businesses

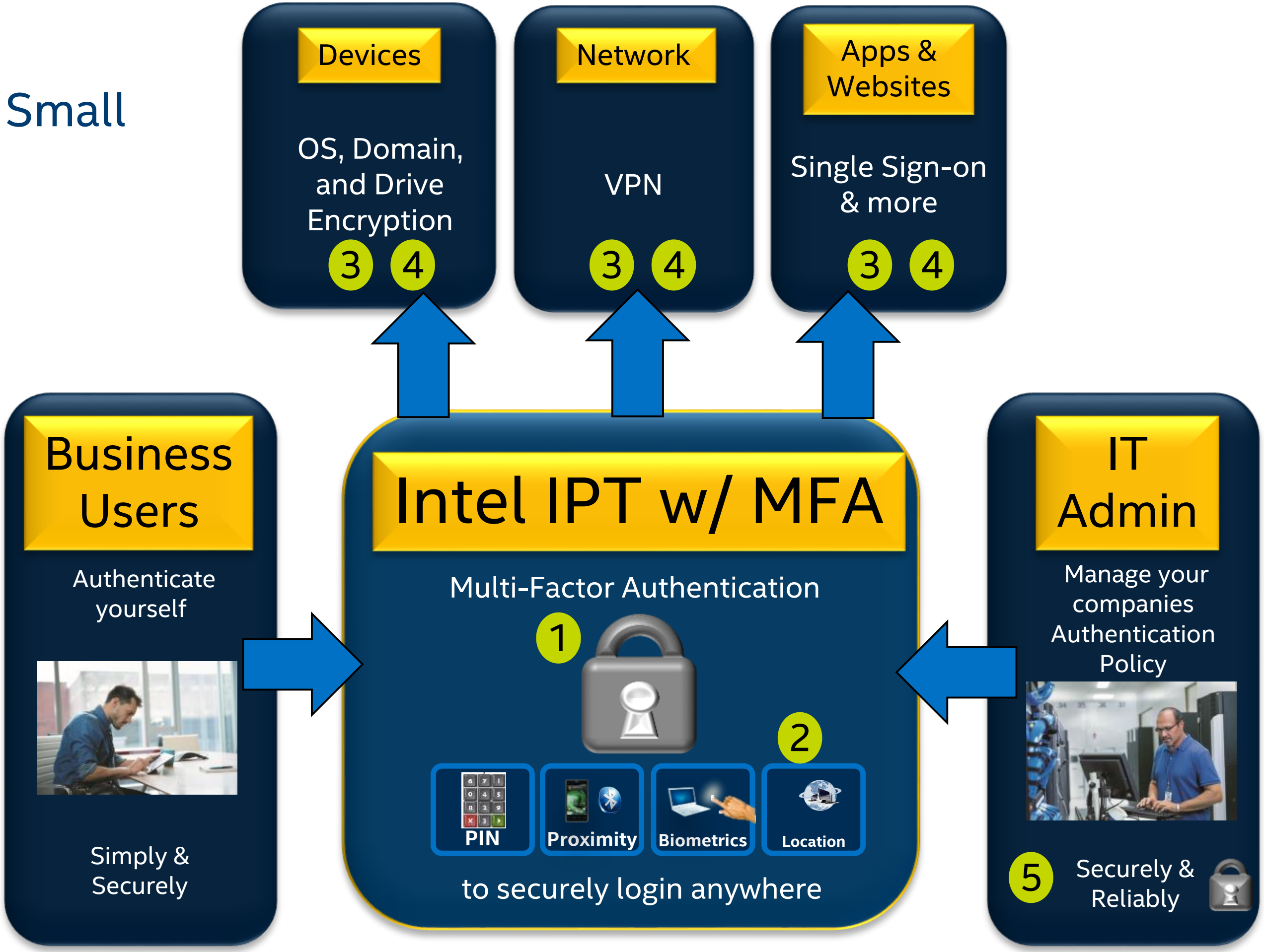
1 Hardened with Intel's Security Technologies rooted in firmware and hardware

2 Supports a variety of hardened authentication factors

3 Designed as a horizontal capability and available to ISVs & OEMs

4 Easily integrates with existing corporate infrastructure

5 Provides hardened MFA policy management using your choice of console (e.g. McAfee ePO, Microsoft* SCCM)



Devices

OS, Domain, and Drive Encryption

3 4

Network

VPN

3 4

Apps & Websites

Single Sign-on & more

3 4

Business Users

Authenticate yourself

Simply & Securely

Intel IPT w/ MFA

Multi-Factor Authentication

1

2

PIN

Proximity

Biometrics

Location

to securely login anywhere

IT Admin

Manage your companies Authentication Policy

5 Securely & Reliably

MFA: *IT Flexibility with HW-assisted Enterprise Security*

1

User to Device Authentication

Domain login using

- Bluetooth®
- PKI
- Password hash

2

Device to Network Authentication

VPN login using

- PKI
- Bluetooth Technology/ Bluetooth Low Energy

3

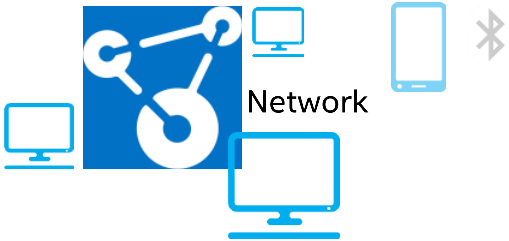
User Presence Protection

Walkaway lock/unlock

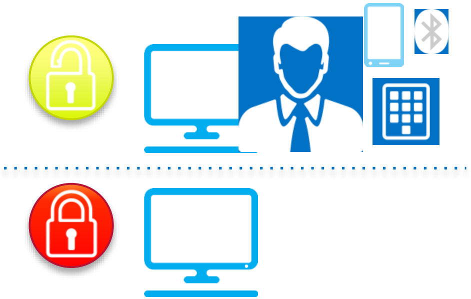
- Bluetooth Technology/Bluetooth Low Energy with PIN

New Ways to Authenticate

Single Sign on



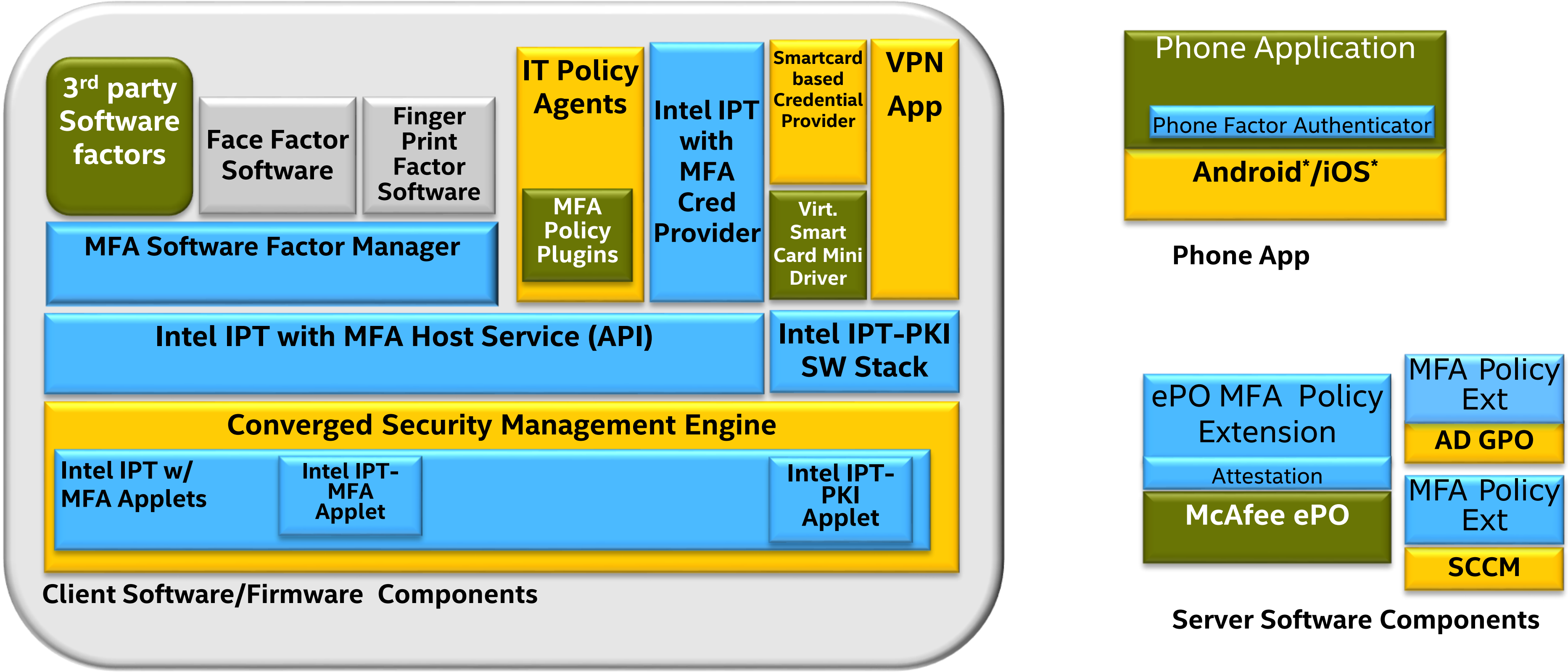
User Presence Protection



4

IT Admin MFA Policy Management

Intel® IPT with MFA End-to-End Solution Stack (Gen 2)



3rd party Software factors

Face Factor Software

Finger Print Factor Software

MFA Software Factor Manager

IT Policy Agents

MFA Policy Plugins

Intel IPT with MFA Cred Provider

Smartcard based Credential Provider

Virt. Smart Card Mini Driver

VPN App

Intel IPT with MFA Host Service (API)

Intel IPT-PKI SW Stack

Converged Security Management Engine

Intel IPT w/ MFA Applets

Intel IPT-MFA Applet

Intel IPT-PKI Applet

Client Software/Firmware Components

Phone Application

Phone Factor Authenticator

Android*/iOS*

Phone App

ePO MFA Policy Extension

Attestation

McAfee ePO

MFA Policy Ext

AD GPO

MFA Policy Ext

SCCM

Server Software Components

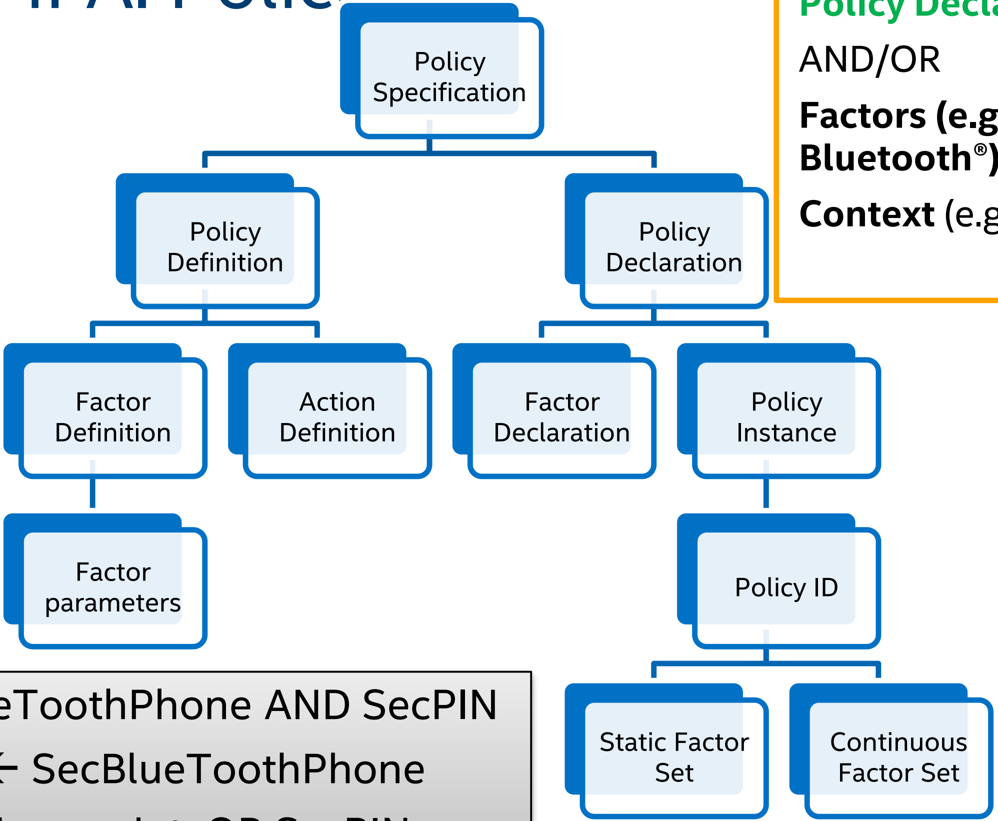
🟩 Intel and/or 3rd party Software

🟦 Intel Software

🟨 Existing product

⬜ OEM / IHV

Intel® IPT with MFA: Policies



Policy Declaration Options:

AND/OR

Factors (e.g., SecPIN, Bluetooth®)

Context (e.g. Time, Location)

Policies are designed to be expressive to support multiple factors and applications

Example

(OS Logon, Alice) ← SecBlueToothPhone AND SecPIN

(WalkAwayLock, Alice) ← SecBlueToothPhone

(VPN Logon, Alice) ← Fingerprint OR SecPIN

SecPIN = Secure PIN (Intel® Identity Protection Technology with Protected Transaction Display)
Intel® Identity Protection Technology with Multi Factor Authentication (Intel® IPT with MFA)

Agenda

Problem Statement and Introduction

Identity Protection Technology Overview

Intel® IPT with PKI

Intel® IPT with MFA

Summary

Q&A

Summary

- Ground Zero for many cybersecurity attacks is compromised *Identity*
- Intel® platforms ship with Security built-in at hardware level
- Intel® IPT with PKI provides a second factor of authentication embedded into the PC
- Intel® IPT with MFA provides ease of use while strengthening authentication, factors and policies through hardware for corporate applications and services

Questions?

Please visit Exhibit Booth #100 to see our Demos!

intel®