Deeper Levels of Security with Intel® Identity Protection Technology

Now, with its latest release, Intel® Identity Protection Technology (Intel® IPT) introduces capabilities that go beyond one-time password (OTP) solutions embedded in silicon and extend secure computing to a broader range of applications.

These new capabilities include:

- **Public key infrastructure (PKI)** to protect access to business data and bolster communications by means of embedded certificates over a virtual private network (VPN)
- **Protected transaction display (PTD)** to minimize risks when entering PINs and passcodes
- **Near-field communication (NFC)** to facilitate simple and secure sales transactions over the Internet

This paper examines the architecture and technology that is the foundation of Intel IPT and the ways in which solutions built around an embedded token model help to minimize fraud and to substantially reduce the risk of identity theft.

“This technology is something you can take advantage of if your web site has a portal for customers or vendors. Your web site can detect Intel IPT, prompt your customers to opt-in, and significantly lower the likelihood of identity theft for your most trusted relationships.”

– Rick Johnson, Marketing Consultant, writing for Intel® Premier IT Professionals
Expanding the Adoption and Use of Two-Factor Authentication

As more and more individuals and businesses communicate online, carry out sales transactions, and conduct financial business, the risk of online identity theft and hacking of online accounts has become an increasing concern. Conventional online transactions that rely on single-factor authentication—where the user supplies a username and a password to gain access to accounts—are very susceptible to hacking.

Two-factor authentication requires both a valid username and password combination, as well as an additional form of identification, such as OTP generated in hardware or software, offering a stronger method for positively validating a user’s identity. The challenge, however, has been that provisioning and managing hardware tokens or ensuring adequate security with software tokens, creates a substantial burden for IT professionals. In an enterprise with thousands of employees, the loss, theft, tracking, enabling, and disabling of tokens represents a major commitment in time and money.

Intel® IPT strengthens security and simplifies IT management by using tokens that are physically embedded in the computer hardware. Collaborative engineering between Intel and top security software providers that specialize in two-factor authentication has established a reliable foundation for creating OTP solutions that are extensible, flexible, and standards-based. The most recent Intel® Core™ processors and Intel® Core™ vPro™ processors from Intel, shown in Table 1, extend the capabilities of Intel IPT to include support for PKI, PTD, and NFC.

Fundamentals of Intel OTP Solutions

Two-factor authentication validates a user’s identity by taking something the user knows (a username and password) and combining it with something the user has (a hardware or software token, a code sent to a mobile phone, or answers to secret questions). By taking one component of the authentication process—a hardware token—and embedding it in a restricted access region within the chipset, the authentication process is made stronger. In the case of Intel IPT, the second factor in the authentication process, the OTP, is a random, computer-generated six-digit password that remains valid for only a brief time limit. Using this approach, the OTP can be generated from Intel IPT and used transparently as part of a user's login information, improving security and enhancing the user experience.

Table 1. Intel® Identity Protection Technology capabilities by processor.

<table>
<thead>
<tr>
<th>One-time Password</th>
<th>Public Key Infrastructure</th>
<th>Protected Transaction Display</th>
<th>NFC on Select Models</th>
<th>Featured Processor Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>All Ultrabooks™, all 2nd generation Intel® Core™ vPro™ processor-based PCs, and select 2nd gen Intel® Core™ processor-based PCs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>◊</td>
<td>All Ultrabook devices and Ultrabook convertibles; 3rd gen Intel Core vPro processors-based PCs</td>
</tr>
<tr>
<td></td>
<td>◊</td>
<td>◊</td>
<td>◊</td>
<td>Only 3rd gen Intel Core vPro processor-based PCs</td>
</tr>
</tbody>
</table>

Note: NFC (near-field communications) chips are required for communication.
Toward this end, Intel is collaborating with industry leaders and independent software vendors (ISVs) within the security authentication ecosystem to develop authentication solutions that take advantage of the deeper security that can be achieved through the use of embedded hardware tokens. The extensible OTP framework has these characteristics:

- **Simplified provisioning process.** Embedded hardware tokens require less effort to provision on the part of IT groups. The process is easier, faster, and less expensive.

- **Enhanced security.** Using embedded, restricted-access components forged in silicon, PIN verification and sensitive operations are performed in a protected chipset that supports the system processor, minimizing the risks of hacking, key logging, or other types of password theft.

- **Flexible implementation support.** With support for current industry standards, including the OATH algorithms as well as proprietary algorithms, Intel IPT enables a wide range of ISV approaches and provides a framework for innovative solutions.

- **Exceptional ease-of-use.** With a straightforward approach that rivals the simplicity of software tokens, solutions built around Intel IPT—in which the computer itself essentially serves as a hardware token—run algorithms in a secure, isolated chipset. The user’s password can be delivered transparently (without having to be physically typed in), enhancing security while reducing complexity.

- **Strong validation.** The framework for server-based token provisioning ensures that each token corresponds with a valid Intel® processor-based computer with Intel IPT.

Figure 1 illustrates the basic components of Intel Identity Protection Technology and the web server that communicates with the Intel® chipset to access the service.
Deeper Levels of Security with Intel® Identity Protection Technology

- **Flexible access options.** Although the hardware of a PC is linked to an individual account for authentication, most authentication solutions provide additional options that let users access their accounts from other devices, such as tablets or smartphones. One way to do this is to link more than one Intel IPT-equipped PC to an account. Another method is for an account provider to use additional challenge scenarios to confirm identity or to send an SMS message to the user with instructions about how to authenticate the logon to the account.

The supporting architecture for Intel IPT uses specialized components embedded in silicon. These components are included in all Ultrabook devices", Ultrabook convertibles, select 2nd and 3rd generation Intel® Core™ processors-based PCs and 2nd and 3rd generation Intel® Core™ vPro™ processor-based PCs. Intel IPT generates time-based OTPs, running the algorithms in a secure area isolated from the operating system. The OTP remains transparent to the operating system throughout transmission to the authentication server, which is synchronized to verify the incoming code against an equivalent internally generated code within a precise time period. Used in combination with a username and password, the OTP provides exceptionally robust logon authentication to web sites.

With its ease of integration and flexible support for multiple use cases, Intel IPT can be used with OTP solutions that provide web site access, software as a service (SaaS), virtual private networks (VPNs)—anywhere strong, two-factor user authentication is a priority.

**Framework for Intel IPT**

The end-to-end architecture for an authentication solution based on Intel IPT includes components that reside on:

- A PC equipped with Intel IPT running the client application that links the PC to the authentication solution on a target web site or cloud server. The client-based components enable the generation of OTPs. OTPs can be produced using the solution provider’s choice of algorithms.

- The web server that contains the authentication software solution. This server is either within an on-premise environment or based on a cloud service. The server extension components provide the necessary support for token provisioning.

The client-side components of an OTP solution based on Intel IPT include:

- **Embedded Intel IPT App.** The OTP algorithm(s) are implemented as an Embedded OTP (eOTP) App.

- **Intel IPT Middleware.** These components facilitate communication between the Embedded IPT App and both the Browser Application (with the IPT Plug-In) and the Windows application for the client.

- **Windows® Application.** This application uses the Intel IPT Middleware to communicate with the Embedded Intel IPT App.

- **Browser Application with IPT Plug-in.** This component enables web sites to access Intel IPT client components without requiring a standalone client application.

The components on the web server side of an OTP solution using Intel IPT include:

- **Intel Service Verification Server.** Provided as reference code, this component adds confidentiality and integrity to the authentication solution provider’s provisioning protocol. It is required to use Intel IPT functionality.

- **Intel OATH Server Library.** This set of components is provided as reference code, providing OATH provisioning and Intel OTP verification functionality.

**Token Provisioning Using Intel® Identity Protection Technology**

Intel IPT has been developed to work in concert with a wide range of protocols and authentication methods. Solution providers developing an OTP solution that incorporates Intel IPT can select whatever communication protocol best suits their software for communicating with the Intel IPT provisioning components. The technology does not impose the use of a specific communication protocol.

Typically, the solution provider’s OTP Web Server includes these components:

- **OTP Provisioning Service Application.** Handles provisioning of OTP tokens on the client end, implementing the solution provider’s provisioning protocol.

- **Intel Service Verification Server.** Interfaces with the OTP Provisioning Service Application, running the Intel Service Verification Protocol.

- **OTP Verification Server.** Validates the OTPs generated by the Intel IPT-enabled PC clients.

- **Token Storage.** Stores the OTP tokens that are provisioned on the Intel IPT-based client system.

The token provisioning process is secured by always ensuring that communication is taking place with Intel IPT-based hardware. The Intel Service Verification Server, a software component installed on the solution provider’s Token Provisioning Service Application, runs the Service Verification Protocol (SVP) in parallel with the solution provider’s protocol to perform the communication verification. The SVP also ensures the integrity and
confidentiality of solution provider-specific data transferred to the Intel IPT-based chipset. Based on the Intel SIGMA protocol, the SVP helps create a mutually authenticated connection between the chipset and solution-provider server.

The token encryption on the client PC relies on a machine-specific key that the Intel chipset generates (see Figure 2). The solution provider software must handle token storage and retrieval on both the OTP Web Server and the client. After an OTP is generated and sent to the solution provider’s OTP Web Server, the solution provider’s software assumes the responsibility of completing the authentication or validation of that OTP.

The use of the four components described in this section is typical, but there is no requirement that ISVs configure their server-side components in the same manner. Developers have the flexibility to make use of the Intel IPT capabilities in a way that extends and strengthens the authentication features of their existing software. Intel IPT is engineered to minimize any re-coding of the software with which it interoperates.

**OTP Generation Using Intel Identity Protection Technology**

The approach used for OTP generation with Intel IPT is to install the eOTP algorithms once and then load them on demand into the restricted access chipset as needed. If an ISV is not using the OATH algorithm, the preferred algorithm that they use can be delivered as part of a software installer or made available for download from a web page.

For example, if someone is browsing on a computer and accesses a page that uses an OTP solution based on the OATH algorithm, the OATH algorithm gets loaded and run in the embedded environment to generate an OTP. If the next site accessed is using a proprietary algorithm, the Intel IPT components manage the use of that algorithm, loading it into the embedded environment to generate the token. Intel IPT does not dictate the deployment method used for the algorithms. Solution providers can accomplish this task using Microsoft Windows applications or browser plug-ins to manage the tokens and generate OTPs.

Because the OTP can be submitted directly to the server back-end components for validation, authentication solutions can be designed so that the password (OTP) is not exposed for possible theft by a screen scraper. The user does not have to physically enter the password on a web page, where a key logger could extract it during entry. The OTP can be programatically entered into a hidden field on a web page or programatically entered so that the user never actually sees the password. Using a method where the OTP is directly submitted to the back end is more secure than alternate methods where a user types an OTP from a hardware token or receives an SMS with the OTP and then must enter it. Intel IPT helps provide

![Ultrabook™ Device or Desktop Computer Featuring Intel® Identity Protection Technology (Intel® IPT)](image)

**Figure 2.** A machine-specific key is used in the one-time password provisioning process.
Deeper Levels of Security with Intel® Identity Protection Technology

Ultrabook™ or PC Featuring Intel® Identity Protection Technology (Intel® IPT)

Web Browser-based Application
- HTML/JavaScript®
- intelwebapis.js
- Intel IPT Plug-in

Windows* Application
- Windows Application

Intel IPT Middleware
- Services COM/JNI

IPT Middleware
- Intel-provided Component
- ISV/Relying Party Component

Figure 3. Secure submission of one-time password takes place through middleware.

Deeper Levels of Security with Intel® Identity Protection Technology

Deeper protection through use of the restricted access chipset.

Time-based OTP implementations are supported by a built-in clock within the Intel® chipset that cannot be accessed or modified by the OS, placing it beyond the reach of hacking tools that might compromise the approach. Software tokens, of course, are less secure than a hardware-based solution because they are exposed and accessible through the OS, making them subject to various forms of attack.

Extending the Intel IPT Framework

The extensible framework that Intel IPT supports gives developers broad flexibility in crafting OTP solutions. Because Intel IPT does not impose a communications protocol between the server and the back end, developers are free to use the communication protocol that best complements their OTP solution.

Provisioning can be accomplished in an on-premise environment or using a cloud-based model.

Intel IPT also does not dictate the use of specific algorithms in an OTP solution. Developers can use algorithms that they have used previously in solutions or incorporate the industry-standard OATH algorithm. Intel IPT is not involved with the validation of OTPs. Similarly, the Intel® software does not handle or gain access to the areas where tokens are stored. Intel IPT provides mechanisms to complement and bolster existing OTP solutions—bringing the benefit of embedded hardware to protect and conceal operations—without becoming intrusive or placing demands on developers to adapt their code to fit the model. This approach has the flexibility and ease of use of a software token, while providing the extra security of a dedicated, protected-hardware solution.

The standards-based model that Intel IPT uses also simplifies interoperability with other third-party components.

The open framework of Intel IPT provides a versatile, extensible platform for innovation and a solid platform for implementing strong, two-factor authentication solutions.

To work with the embedded token to develop an OTP solution, Intel offers complete documentation of the functions exposed by the Intel IPT programming interfaces. As the OTP ecosystem expands and the importance of strong authentication increases, Intel will continue to work with the development community to help engineer secure solutions that match the latest processor architectures to the leading software advances.

Fundamentals of Intel® Identity Protection Technology with PKI

The addition of Intel IPT with PKI capabilities to 3rd gen Intel Core vPro processors provides hardware-based RSA private key protection. Business-class Ultrabook devices and other systems equipped with this technology can securely engage in transactions, including VPN authentication, Secure Sockets Layer web site authentication, and email and document signing.

Through a system of digital certificates, certificate authorities, and other registration authorities, PKI positively verifies and authenticates Internet transactions conducted between two parties, ensuring the credentials of the user and server are valid. Intel IPT stores PKI certificates in a tamper-resistant region in firmware where they can be accessed for authentication, as well as to encrypt and digitally sign documents.
with Intel IPT with PKI can be integrated into an IT infrastructure that is already enabled for PKI operations without requiring any additional tokens or smart cards. The PC itself serves as the hardware device representing the second factor.

The Microsoft CryptoAPI software layer can access Intel IPT with PKI software as a cryptographic service provider (CSP) component in a manner similar to software-based CSPs, but with the additional security afforded by having the algorithms embedded in hardware.

Using the software functions that are exposed through Intel IPT with PKI, the CryptoAPI can:

- Generate persistent, tamper-resistant RSA key pairs securely within the Intel Management Engine
- Generate PKI certificates from RSA key pairs that are protected in hardware
- Perform RSA private key operations within a protected area in the hardware

This functionality also enables protected PIN transactions when using the PTD capabilities that are also part of Intel IPT with PKI.

The solution stack for Intel IPT with PKI consists of the following components:

- **Third Party Applications.** Includes all applications developed for this platform that access Intel IPT with PKI to access routines within the Intel IPT CSP, using Microsoft CryptoAPI.
- **Microsoft CryptoAPI.** Software that uses the CryptoAPI can select the Intel IPT CSP to perform cryptographic operations. The CryptoAPI itself is a Dynamic Link Loader (DLL) developed by Microsoft to serve as a framework of creating CSPs. Intel components do not replace the CryptoAPI or modify it.
- **Intel IPT CSP.** When the Intel IPT CSP is installed in a system, it becomes visible and available. Applications can then designate the CSP for cryptographic operations.
- **Intel IPT Library.** This DLL provides the core Intel IPT capabilities and Secure PIN Pad capabilities.
- **Intel Dynamic Application Loader (DAL) Host Interface Service.** This Intel IPT component is installed as a part of the Intel Manageability Engine firmware tool-kit installation. Functionality that was developed for the Intel IPT with OTP features is being reused for Intel IPT with PKI. The component serves as a communication pipeline for sending commands and receiving responses through an applet running in the DAL environment. The applet operates at a higher level—through the Intel DAL Host Interface Service—so that developers need not be concerned with the details of low-level communication operations.
- **Intel IPT Applet.** This Java* applet runs in the Intel Manageability Engine and performs many of the operations involved with Intel IPT with PKI. For example, to send a key as part of an operation, you send a command through the Intel IPT DAL Host Interface Service to the applet with the key wrapped in a protective layer. The applet decrypts the key, completes the operation, and returns a response.

![Figure 4. PKI solution stack components available through Intel® Identity Protection Technology (Intel® IPT).](image)
Fundamentals of Intel Identity Protection Technology with PTD

The PTD capabilities of Intel ITP are available on 3rd gen Intel Core processors and Intel Core vPro processors in systems featuring the built-in graphics chipset from Intel. In a system equipped in this manner, such as a business-class Ultrabook, display information involving PINs can be protected from tampering, and the presence of a human operating the PC can be confirmed, minimizing the risks associated with a number of sophisticated hacker attack methods. This PTD technology can be incorporated into solutions using either Intel ITP with PKI or Intel ITP with OTP.

When this technology is in use, the Intel Manageability Engine draws the PIN input window on the display and accepts mouse clicks as input, as shown in Figure 5. This shields the PIN entry from the operating system and application that is running, but allows the user to see the input and complete the entry process. A potential hacker sees the blacked out screen shown on the right side of Figure 5. Numbers appearing on the PIN pad appear in different positions each time the PIN pad is launched to further conceal the specifics of the entry, preventing malware from identifying a PIN based on a pattern of mouse clicks at points on the display.

Key protections provided by Intel ITP with PTD include:

- **Randomized keypad display.** The keypad is generated by the graphics chipset, so the keypad is not visible to malware or hackers. The numbers in the PIN window appear in different positions each time the keypad is launched, preventing pattern recognition.

- **PTD technology.** Intel ITP with PTD foils attempts by screen scrapers or malware to perform a screen capture of the PIN window or numbers.

- **Secure number entry.** PIN entries on the keypad are handled by a protected area in hardware that is never exposed to the running applications or operating system.

- **Prevention of brute force attacks.** After a set number of incorrect PIN entries, additional entries are shut down for a fixed period, minimizing the risk of a brute force attack detecting the valid PIN.

Fundamentals of NFC

NFC—a short-range wireless communication technology—describes a protocol for handling peer-to-peer data exchanges between a pair of end points. Intel ITP has a built-in function to provide positive identity confirmation by means of cryptographic binding between Intel ITP and the data that is communicated through the NFC sensor from an NFC-enabled credit card, identity cards, or device.

To facilitate easy and secure sales transactions over the Internet using an Intel ITP-equipped computer, the NFC feature lets users connect to a merchant pay site, pay for a product by tapping an NFC-enabled credit card against an NFC sensor in the computer, and complete the transaction with positive identity authentication.

**Trusted Partners**

Intel works with a number of solution providers and online web properties to integrate Intel ITP into end-to-end authentication solutions. These partners include:

- BR Token
- ChangingTec
- Feitian
- Data Security System Solutions
- DynamiCode
- IBM Security Services
- InfoSERVER
- Nordic Edge (now part of McAfee)
- Symantec
- VASCO
For More Information

To obtain a copy of the "Intel® Identity Protection External Product Specification for One-Time Password," contact your Intel customer representative.

For a current list of PCs that feature Intel Identity Protection Technology, visit http://ipt.intel.com/Protected-PCs.aspx

To watch a video that explains how Intel Identity Protection Technology works, go to http://ipt.intel.com/how-it-works.aspx

For additional details about Intel IPT with Public Key Infrastructure, visit http://ipt.intel.com/Home/How-it-works/protect-your-business/ipt-with-pki.aspx

To download a technology overview of Intel IPT with Public Key Infrastructure, go to http://ipt.intel.com/Libraries/Documents/Intel_R_IPT_with_PKI_Technology_Overview_2012.sflb.ashx

1 No system can provide absolute security under all conditions. Requires an Intel® IPT-enabled system, including a 2nd generation or 3rd generation Intel® Core™ processor, enabled chipset, firmware, and software. Available only on participating web sites. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages.

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. Unless otherwise agreed in writing by Intel, the Intel products are not designed nor intended for any application in which the failure of the Intel product could create a situation where personal injury or death may occur.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel’s Web site at www.intel.com.

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core, Intel vPro, and Ultrabook are trademarks of Intel Corporation in the U.S. and other countries.

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