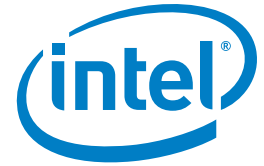


## TECHNOLOGY BRIEF

### Intel® Identity Protection Technology

Available on select 2nd generation Intel® Core™ processor-powered PCs



# Access Accounts More Securely with Intel® Identity Protection Technology

## A solution for sending cybercriminals elsewhere

The escalating problem of online identity theft results in millions of dollars in losses every year and produces incalculable disruptions in the lives of victims whose accounts are illegally accessed. Rather than letting computer users become victims, new technology from Intel takes a proactive approach, stopping cybercriminals before they can get started. Whether the risk is the assets in your bank account or the accumulated treasures in your online gaming account, it's far easier to protect against identity theft than to try to clean up the damage after your account has been breached.

Phishing attacks—an online version of identity theft where a bogus Web site attempts to capture your login data—represent a growing threat. Highly adaptable cybercriminals follow trends, shift tactics, and often move to points of greatest activity to exploit vulnerabilities. For example, phishing sites focusing on social media showed sharp increases, jumping 80 percent in October 2010 from the previous month, according to Symantec's "State of Spam & Phishing: A Monthly Report."<sup>1</sup>

McAfee has also detected a sharp increase in threats over recent months. "Our Q3 Threat report shows that cybercriminals are not only becoming more savvy, but attacks are becoming increasingly more severe," said Mike Gallagher,<sup>2</sup> senior vice president and chief technology officer of Global Threat Intelligence for McAfee. "Cybercriminals are doing their homework and are aware of what's popular, and what's insecure. They are attacking mobile devices and social networking sites, so education about user activity online, as well as incorporating the proper security technologies are of utmost importance." These dangers are not going unnoticed. A recent Gartner survey<sup>3</sup> of the world's leading CIOs established identity management as the single most important security objective for 2010.

### Strengthening Security with Hardware-Based, Two-Factor Authentication

Protecting your identity and personal data stored in the cloud requires strong authentication that is, ideally, rooted in hardware. Security experts widely regard hardware-based authentication as a more effective approach than software-only authentication. Two-factor authentication using a one-time password (OTP) combines something the user knows (a username and password) and something the user has (typically, a token or key fob that produces a six-digit number—valid for only a short period of time—on demand). In the case of Intel® Identity Protection technology (Intel® IPT), that six-digit number is generated from

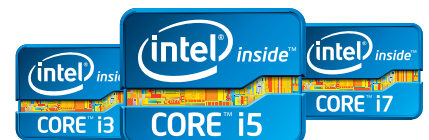
an embedded processor, the Manageability Engine (ME), on the computer motherboard. The ME is tamper-resistant and operates in isolation from the operating system for added security. Algorithms developed by Intel's third-party partners (see Trusted Partners on page 2) run in the ME, performing the operations that link select PCs to a validated site and ensure strong authentication.<sup>4</sup>

With this approach, everyday computer users are the primary beneficiaries, gaining access to technology that substantially lowers the likelihood of identity theft. However, Web site operators, service providers, and anyone offering a customer portal experience benefit as well with a security solution that is simple to administer and avoids the expense and management issues of physical OTP tokens that are easily lost or stolen. Generating the OTP inside the computer hardware—using Intel IPT—provides a powerful authentication method that ties an individual user's PC to the site being accessed.

### Embedded Tokens: Creating a Secure Place within the PC

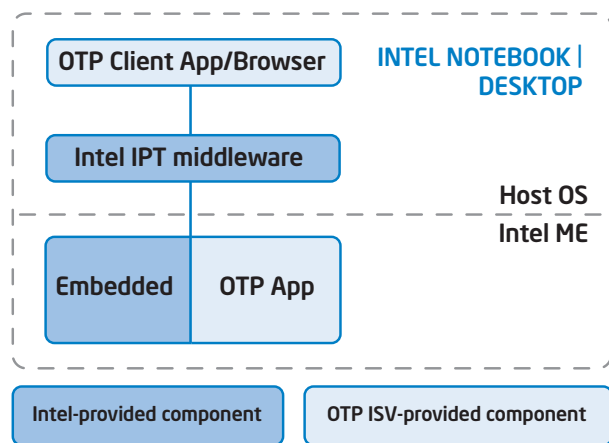
Intel IPT, featured in PCs based on select 2nd generation Intel® Core™ processor, works in combination with established authentication mechanisms created by leading security companies. The major difference with this technology is that it replaces the customary physical token with an embedded token that uses ISV algorithms to generate the six-digit codes or OTPs. Calculations to create the OTPs are performed in a protected place within the computer hardware. When it is entered into a participating, validated Web site, portal, or virtual private network (VPN) authentication screen, a comparison is made with a number created by the server with the same seed and algorithm. A match signifies positive authentication and ensures that the user's identity has been confirmed using a much stricter standard than simply a username and password.

Anyone with a properly equipped PC visiting a participating Web site, using an enabled software as a service (SaaS) application, or accessing a VPN protected by one of Intel's partner technologies can immediately opt-in and add this robust security to their account. After successful authentication, the user's PC becomes linked to this account. Depending on the implementation, individual sites may vary in when and how they ask the user for this six-digit number. It might be provided during login, as a step during certain transactions, or handled behind the scenes by the server application.



Users can associate a select 2nd generation Intel Core processor PC featuring Intel® IPT with multiple Web sites and accounts. The algorithms and seeds used to generate the six-digit codes always execute in the Intel Manageability Engine, which is reserved for code supplied by only Intel and its trusted partners.

Figure 1 shows the layers of client components in this solution, from the ME to the client application that the individual ISV provides.



**Figure 1.** Security components associated with Intel® Identity Protection Technology.

Hackers never stop devising new ways to steal usernames and passwords. One of the strongest techniques for avoiding the threat of identity theft is to link your physical PC to each online account that you use. This significantly reduces a hacker's opportunities to illicitly access your account from any other computer. The computer itself and the codes generated in isolation by the ME provide the second authentication factor that inextricably couples the computer to an account, making it extremely difficult to defeat this layer of protection.

If you are away from your PC that is equipped with Intel IPT, you can still gain access to your online accounts. However, extra security measures will be used to confirm your identity. For example, you might have to answer security questions or receive a text message from the Web site to check your credentials. More than one PC can be linked to your account. You can, for instance, use this technology for online banking from both your home PC and your laptop at work.

The vast majority of security professionals agree: A simple username and password does not provide enough protection against identity theft. Enhance your security and guard against illicit access to your data and personal information with Intel IPT and a computer powered by a 2nd generation Intel Core processor.

## For More Information

For a current list of PCs that feature Intel Identity Protection Technology, visit [ipt.intel.com](http://ipt.intel.com). This site also lists the Web sites that have been validated for this technology and details the security companies with which Intel is currently partnering.

<sup>1</sup> No system can provide absolute security under all conditions. Requires an Intel IPT enabled system, including a 2nd generation Intel Core processor, enabled chipset, firmware, and software. Available only on participating websites. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit [ipt.intel.com](http://ipt.intel.com).

<sup>1</sup> [http://eval.symantec.com/mktginfo/enterprise/other\\_resources/b-state\\_of\\_spam\\_and\\_phishing\\_report\\_03-2010.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_and_phishing_report_03-2010.en-us.pdf)

<sup>2</sup> [http://newsroom.mcafee.com/article\\_display.cfm?article\\_id=3708](http://newsroom.mcafee.com/article_display.cfm?article_id=3708)

<sup>3</sup> <http://www.gartner.com/technology/summits/na/identity-access/agenda.jsp>

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

Copyright © 2011 Intel Corporation. All rights reserved. Intel, the Intel logo, and Intel Core are trademarks of Intel Corporation in the U.S. and other countries.

0211/SK/MESH/PDF

324770-001US

## Requirements for Using Intel® IPT

For customers, clients, or employees to use this security technology, three conditions must be met:

- Users must be on a PC powered by a select 2nd generation Intel Core processor, produced by an OEM that has enabled Intel IPT (consult the Intel Identity Protection Web site, [ipt.intel.com](http://ipt.intel.com), for a complete list of models).
- The Web site, VPN, or SaaS application being accessed must be one that offers this protection, as supported by Symantec or Vasco.
- This form of security is provided as an opt-in service, so the user must actively choose to link the PC to authenticate the account.

## Trusted Partners

### SYMANTEC

Symantec, a global leader in providing security, storage, and systems management solutions, helps customers—from consumers and small businesses to the largest global organizations—secure and manage their information against risks, completely and efficiently. The company focuses on eliminating risks to information, technology, and processes independent of the device, platform, interaction, or location. Companies using Symantec's VIP solution for two-factor authentication will automatically accept the embedded tokens on select 2nd generation Intel Core processor computers—delivering a trusted and safe online experience to consumers, employees, and partners.

### VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services, specializing in Internet security applications and transactions. VASCO has positioned itself as a global software company for Internet security serving a customer base of over 10,000 companies in more than 100 countries, including more than 1,500 international financial institutions. VASCO's prime markets are the financial sector, enterprise security, e-commerce, and e-government. Companies that use VASCO to protect their account holders should update to the latest level of VACMAN Controller or IDENTIKEY Server, and follow the instructions for accepting embedded DIGIPASS on select 2nd generation Intel® Core processor computers.

