Seamless Two-Factor Authentication: DS3 Incorporates Support for Intel® Identity Protection Technology

"The reason why I am so bullish about the [Intel] IPT solution is that it offers a new light at the end of the tunnel, where we have the ability to turn on strong authentication for every person out there in the entire online world who has an Ultrabook."

— Teik Guan, CEO, DS3

CHALLENGE

• Providing strong authentication requires supporting a diverse range of tokens and authentication mechanisms, including added support for new technologies that are reaching the market.

• The need for strong, easy-to-use, two-factor authentication has increased as hacker attacks have become more sophisticated and online banking, commerce, and government transactions have become more commonplace.

• Hardware tokens present problems in provisioning, management, and potential loss. Software tokens—while convenient—provide a lower level of security and a prime target for malware.

SOLUTION

• Designing the DS3 Authentication Server to accommodate an extensive range of authentication mechanisms—quickly adapting to powerful, emerging technologies as they are introduced—delivers the flexibility and the rigorous identity protection that enterprise business customers require.

• Incorporating Intel® Identity Protection Technology (Intel® IPT) into a solution, such as the DS3 Authentication Server, strengthens security by using one-time passwords (OTPs) generated within a tamper-resistant module in hardware. These OTPs can be generated and passed through with or without user action.
Reducing Data Theft Risks
The trade-off between rigorous security and ease-of-use has been an ongoing challenge since the earliest days of personal computing. If security practices are too difficult for users to follow on a regular basis, they'll find ways to circumvent the practices or become careless. Lowering the security standards to make the system easier to use exposes sensitive information to loss or theft. Cyber attacks that deliberately target token use have become increasingly successful. With the latest version of the DS3 Authentication Server, which includes support for Intel IPT, the risks of data exposure or theft are substantially diminished.

Based in Singapore, DS3 introduced the DS3 Authentication Server, its flagship enterprise solution, in 2003. In 2012, DS3 added support for Intel IPT to bring the advantages of hardware-based authentication using OTPs to their customers. DS3 continues to follow through on its mission: to give customers the widest possible selection of authentication options. As new, promising two-factor authentication technologies are developed and validated by the industry, DS3 integrates them into its server solutions.

Advanced Protection Technology
Hardware-generated OTPs, coupled with back-end server support, represent one of the most advanced, proven methods for disrupting hacker efforts and reducing the risk of account breaches. Intel IPT is built into all Intel-inspired Ultrabook™ devices, select second-generation Intel® Core™ processors, and Intel® vPro™ technology-based PCs that feature third-generation and second-generation Intel® Core™ vPro™ processors. By supporting this technology in the latest versions of the DS3 Authentication Server, DS3 eliminates the need for customers to acquire and manage separate physical tokens (or rely on software tokens). Multi-factor log-in to the corporate network or VPN is simplified. Those employees with Intel IPT-equipped PCs don’t need to carry and use a separate token. The credentials supplied by the PC itself allow them to access the network.

Capsule Description: DS3 Authentication Server
The DS3 Authentication Server appliance offers multi-factor authentication with end-to-end encryption of keys provided by a FIPS-certified Hardware Security Module. With extensive support for a variety of token types and OTP mechanisms from different vendors (including Intel IPT support), this authentication server accommodates the stringent requirements of financial institutions and is also gaining popularity in other industries where protection against fraud and information theft is vital—including eCommerce sites, telecommunications services, cloud computing portals, logistics operations, educational institutions, and government organizations.

Teik Guan, DS3's CEO, commented, “When we were initially presented with the Intel IPT offering, from a DS3 perspective we saw every IPT-equipped PC as essentially a front-end token. This was naturally a good fit for what DS3 does because we want to be able to offer a platform-free token across the widest range of selections—to both new and existing customers, so that everyone could choose what exactly they needed for their application. It's not so much a decision that is made only at the point of purchase, but a decision based on what tokens a customer's end users will be able to use, throughout the lifecycle of the application.

DS3 encourages customers to select the kinds of tokens and mechanisms that best match their business practices. “By having a back-end system that flexibly combines two or even three of these types of offerings together,” Guan said, “customers will not be restricted by choice of token or by choice of infrastructure. Customers are able to choose what approach makes the best sense for their businesses. That, I would say, is a very good thing. If you

Features and Benefits of Intel® Identity Protection Technology (Intel® IPT)
Most security experts regard hardware-based authentication, as implemented by Intel IPT, as more effective than software-only authentication. Intel IPT offers these features and benefits:

• **One-time password (OTP) generation.** A chipset embedded in an Intel IPT-equipped PC generates a single-use six-digit password in periodic timed intervals (in isolation from the PC operating system). The authentication server synchronizes and confirms this password on the back-end, validating that access is being granted to a user on a trusted platform, not malware.

• **Public key infrastructure (PKI) signing.** Intel IPT also provides access-point protection through a PKI certificate, embedded in the same manner as the OTP credentials. Enterprises can rely on this hardware-based PKI certificate to eliminate a requirement for any additional smart card or token.

• **Protected transaction display.** Encrypted I/O technology that works in combinations with Intel IPT or PKI delivers another layer of protection whenever sensitive online transactions are taking place. This feature confirms the user presence, verifies the transactions, and blocks malware screen scrapers from harvesting data from the PC display.
look at security practices even 10 years ago, most business users were restricted by what they could use and deploy to their customers. They were often told by the security administrator, ‘No, you cannot do this.’ And, now, with a wide choice of front-end devices to offer—with this stronger authentication ecosystem in place—the business users have the ability to decide what best works for them. This, I believe, is a good value proposition and a good fit for the industry.

DS3’s philosophy is to offer customers authentication that matches their security needs and business practices, advancing its solution capabilities as quickly as security technologies evolve. Intel IPT extends powerful new capabilities to DS3 solutions.

“We’re seeing a need for strong authentication that is deployed even for non-financial or government-based applications. Intel IPT provides bank-grade security protocol for the masses. Now when an enterprise wants to secure the remote access for its partners or employees, it can have almost the equivalent level of security as the banks use. It can have this same level of security without needing to set up the same level of infrastructure—where we’re talking about token issuance, token logistics, token management—because all of these can be simply addressed through a combination of the Intel IPT-enabled notebooks, which are the Ultrabook devices, and a flexible back-end authentication system: the DS3 server.”

— Teik Guan, CEO, DS3

Figure 1. Overview of the DS3 Authentication Server and Intel® Identity Protection Technology components.
DS3 Incorporates Support for Intel® Identity Protection Technology

For More Information

For additional details about the DS3 Authentication Server, visit ds3global.com.

For a current list of PCs that feature Intel Identity Protection Technology, visit ipt.intel.com.

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

Solution provided by:

intel®

DS3