IT@Intel White Paper

Intel IT

IT Best Practices

IT Consumerization and Information Security

March 2013

Securely Connecting Smartphones and Tablets to the Enterprise

Yaniv Berkovich
Connectivity and Security Engineer, Intel IT

Sharon Biton
Authentication Engineer, Intel IT

Yair Gordon
Connectivity and Security Product Manager, Intel IT

Derek Harkin
Mobility Engineer, Intel IT

Shachaf Levi
Connectivity and Security Engineer, Intel IT

Noam Maman
Connectivity and Security Engineer, Intel IT

Aideen Moohan
Project Analyst, Intel IT

Ayelet Naor
Connectivity and Security Engineer, Intel IT

We have published 15 new web applications and enabled five native applications with connectivity using VPN. Employee response has been positive, with the web applications averaging 3,175 unique users per month over the last seven months.

Executive Overview

To make it easier for employees to use small form factor devices to accomplish job duties, Intel IT is developing an enhanced connectivity solution. This solution will help us broaden the range of applications available to managed devices and eventually unmanaged devices using our mobile device management application.

We also want application developers to be able to choose the delivery mechanism—native, web, or hybrid—that best fits their application, and we want to provide users with the best user experience possible.

Some of the unique aspects of our enhanced security connectivity solution include the following:

- A virtual private network (VPN) on-demand authentication, so employees do not have to separately launch the VPN client
- A restricted VPN profile to limit network access to only what is required for specific applications
- A new web application gateway dedicated to mobile devices
- Customized two-factor authentication mechanism
- A single sign-on process that uses Kerberos protocol transition
- A software-based one-time password (OTP) solution that requires no additional hardware

These components provide benefits to the users by requiring less typing during authentication, allowing an application's appearance to change depending on device screen size, and freeing users from having to carry extra hardware for OTP generation. We also expect benefits to IT, such as fewer support calls relating to hardware token failures, fewer maintenance issues, and a reduction in OS password resets.

We have published 15 new corporate applications using the new web application gateway and have enabled five native applications with connectivity using a secured VPN connection and a mobile VPN client on the device side, with seamless authentication for the user. Employee response has been positive, with the web applications averaging 3,175 unique users per month over the last seven months.

Contents

Executive Overview 1

Background 2
- Managed Devices 2
- Unmanaged Devices 2

Solution 3
- Mobile VPN 3
- Web Application Publishing 3
- Improved Authentication for One-time Password 4

Results 7

Next Steps 7

Conclusion 8

For More Information 8

Acronyms 8

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

Intel employees want to use a broader range of companion devices, including smartphones and tablets, with their Intel-supplied mobile business PCs. In particular, employees want to use small form factor (SFF) devices whenever they need quick access to an application or faster completion of a specific task, instead of having to turn on a laptop and complete the full log-on process.

Initially Intel IT provided SFF devices with access to email, contacts, and calendar services. However, Intel employees want access to more than just these basic services. A demand exists for both general availability applications, such as an online company phonebook, and business-specific applications, such as an expense reporting application. Our goal is to meet both these types of needs while providing an optimal user experience (UX).

Giving employees a choice of SFF devices enables them to choose the platforms and devices that best fit their needs, providing them with greater flexibility and ultimately making them more productive. We plan to enable more enterprise and dedicated business-unit applications to be consumed safely from SFF devices, from any location and at any time, and with an acceptable level of security.

We have developed a solution that can provide secured connectivity to native, web, and hybrid applications, using various connectivity methods and authentication mechanisms. We provide differentiated services and levels of access to managed and unmanaged devices, based on the different levels of security between managed and unmanaged devices.

Managed Devices

We are in the process of expanding our set of applications that are available to managed SFF devices. A managed device can be personally owned or corporate owned, has certain minimum security features, and is managed by our mobile device management (MDM) system. Approximately 17,000 managed SFF smartphones and tablets, both personally owned and corporate owned, can currently access these applications. We expect to expand access to the same set of applications to an additional 10,000 managed SFF devices by the end of 2012.

Unmanaged Devices

Currently, unmanaged devices—those devices without an active MDM—can access only filtered email and basic contacts and calendar services, although we plan to offer web-based applications in the future. Unmanaged devices are usually personally owned devices that have technical limitations or devices for which the user choses to not accept the IT policies, such as screen lock and encryption, that the MDM system requires.

SOLUTION

To meet our goals of providing additional corporate applications to SFF devices and to quickly and efficiently publish web-based applications, we needed to develop secure connectivity, while still providing an optimal UX.

We use two connectivity methods, building on the foundation provided by our MDM system.

- A mobile virtual private network (VPN) for native applications
- Web application publishing using the Kerberos protocol transition (KPT)

We have also implemented an improved one-time password (OTP) solution used for authentication that requires no additional hardware.

Implementing these types of components can help foster additional productivity from employees with managed SFF devices, while maintaining enterprise information security. Also, having two connectivity methods enables application development teams to use the delivery mechanism—mobile VPN or web application publishing—that makes the most sense for a particular application, based on technical considerations that relate to local storage and resources, the type of application, when the application is needed, and UX and security considerations.

Mobile VPN

Mobile VPN provides secured connectivity and ease-of-use for native applications. Currently, we have enabled five native applications using mobile VPN. Because the VPN client is at a lower network layer than the applications are, the applications can assume that if the VPN client is active, authentication has already occurred. As a result, users don't need to authenticate more than once, and application developers are insulated from authentication and connectivity issues. Also, because the VPN already authenticates using a certificate and a password, two-factor authentication occurs by default. To further enhance security, we configure our VPN connections with a short idle time, after which the VPN connection is closed.

Because unmanaged devices are a higher risk than managed devices, we provide VPN access to only managed devices that include security features such as remote wipe; strong, hardware-based encryption; and the ability to require a PIN to unlock the device. Even for managed devices we do not provide full network access through a regular VPN connection. Instead, we provide limited access to specific servers. As part of the development process, an application developer can request that a server, assuming it matches the security policy, be added to the approved list of servers.

VPN ON-DEMAND

Recently we introduced VPN on-demand for managed, personally owned devices, a streamlined method of authentication that requires minimal user intervention. Previously, employees had to complete multiple steps in order to launch the VPN client: choose the desired application, type a username and password to authenticate, and then launch the application. Although this approach worked, the nature of typing on an SFF device made the process cumbersome and prone to error.

With the new VPN on-demand approach, employees no longer need to separately launch the VPN client or enter additional authentication criteria. The solution protects the user's credentials and in the background a VPN connection profile automatically defines on which fully qualified domain names (FQDNs) the VPN connection can open. When a user launches an application that requires VPN, the FQDN check is performed in the background, transparently to the user. If the application is launching on an approved FQDN, the VPN client automatically launches and connects in the background with no further user interaction needed.

The VPN on-demand capability has had a positive effect on user satisfaction for employees using native applications. In a study that focused on the employee travel app, user satisfaction increased from 85 percent to 95 percent when using the VPN on-demand feature, with the increase in satisfaction stemming from the reduction in the number of the steps required to start the application. VPN on-demand also reduced the obstacles to native application usage, with employees being more likely to use the solutions regularly.

Web Application Publishing

While mobile VPN provides connectivity for native applications, web application publishing is a more appropriate connectivity method for other types of applications. Although publishing applications to the Web is not new at Intel, we have renewed our focus on providing an optimal UX and customized two-factor authentication. In addition, the advent of HTML5 is enhancing the portability of code, enabling application developers to target multiple OSs while writing an application only once.

AN OPTIMAL USER EXPERIENCE

The existing web application gateways at Intel did not support a satisfactory mobile UX, such as the ability to adjust the display of the application based on screen size. To address the problem, first we certified a gateway dedicated to mobile devices and installed it in the demilitarized zone. So far, we have published more than 15 corporate web applications using the gateway.

Figure 1. Our web application gateway enables us to adjust the display based on screen size.

Kerberos Protocol Transition

Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications. Kerberos uses cryptography to protect security keys, which enables a client to prove its identity to a server across an insecure network connection. Cryptography is also used to protect further communications across the network connection, helping to ensure data confidentiality and integrity.

If an application cannot use Kerberos authentication to authenticate its users, it is possible to use Kerberos protocol transition to switch from an alternate authentication mode, such as use of a one-time password or certificate authentication, to Kerberos authentication.

The gateway product we chose is customizable using scripts and HTML5 and also supports most SFF devices. We developed a customized Mobile Portal that dynamically adjusts the login page so that it suits any screen size and adheres to the guidelines and standards for human factors engineering. Figure 1 shows an example of how the list of available applications appears on two SFF devices: a smartphone on the left with a narrow screen and a tablet on the right with a wide screen.

During development of the Mobile Portal, we conducted several surveys to elicit employees' opinion on what could be improved. For example, upon learning that employees disliked having to enter two text-based authentication factors, we changed the authentication mechanism so that users no longer have to type both authentication factors.

WEB APPLICATION SECURITY CONSIDERATIONS

Our largest challenge associated with making web applications available to a wide variety of both managed and unmanaged devices was to secure the connection while providing a reasonable UX. Currently, web applications are available to only managed devices. In developing a solution that balances security with usability, we considered a variety of factors, such as what data remains resident on the device, how to control that data, authentication requirements, the strength of the device's security, and what happens if the device gets stolen or compromised.

Employees with SFF devices also wanted to have single sign-on (SSO) capabilities for web applications. With SSO, employees need to log in only once and are then able to access multiple web applications. However, because of the risk of credentials being captured from a stolen or compromised device, we did not want to use the user's domain credentials for SSO. Instead, users log in with different credentials, such as an OTP, then access to web applications is granted using the Kerberos protocol transition (KPT) (see the sidebar). KPT allows us to translate the OTP authentication into Kerberos for SSO. This approach to SSO for SFF devices enables an optimal UX without compromising security.

We plan to continue adding improvements to the authentication process to make connecting to applications even more secure, seamless, and easy to use.

Improved Authentication for One-time Password

Our goal to eventually provide unmanaged devices with access to web applications makes it necessary to have a strong but user-friendly authentication mechanism. While digital certificates work well on managed devices, they are not appropriate for unmanaged devices or devices with weaker security capabilities. In these cases, we cannot provision the certificate or ensure the device is not compromised. Our solution provides an OTP, which allows users to authenticate on unmanaged devices.

We chose to implement a numeric OTP to improve the user's ease of entry. An OTP is valid for only one login, and is usually valid for a limited duration, such as two minutes. The other factor in the two-factor authentication is traditionally a static password, such as a PIN.

Our original OTP solution used hardware tokens generated by a physical device similar to a USB stick. This approach was relatively secure, but not user-friendly. The employee had to carry the token generator all the time, and if the token generator became lost, the employee could not access the network. For IT, the token solution presented manageability and maintenance challenges, such as having to register tokens and mail the token generator to the employee. There were also hardware expenses and the complexity associated with maintaining and upgrading back-end servers.

We anticipate that the new OTP solution will help reduce the frequency and number of support ticket escalations relating to hardware token failures and maintenance issues, and to Microsoft Windows* password resets if employees forget their password or if there are changes in authentication policies.

As shown in Figure 2, with our new OTP solution we can send the password by SMS if the employee provides a personal cell phone number. Alternatively we provide employees with a software-based OTP password generator that can be installed on almost any device and can generate the OTP locally. This approach enables us to provide OTPs to external suppliers and employees who do not want to provide their personal cell phone number or who do not have a cell phone.

We also ask users to provide us with their company email address, which we use to send administrative notifications as well as instructions for the initial OTP application installation.

We have simplified the enrollment process to make it as seamless as possible for the user. Users of the solution include both employees and contingent workers. After the user downloads the OTP generator from the application store, they are automatically enrolled and can use the OTP application for authentication.

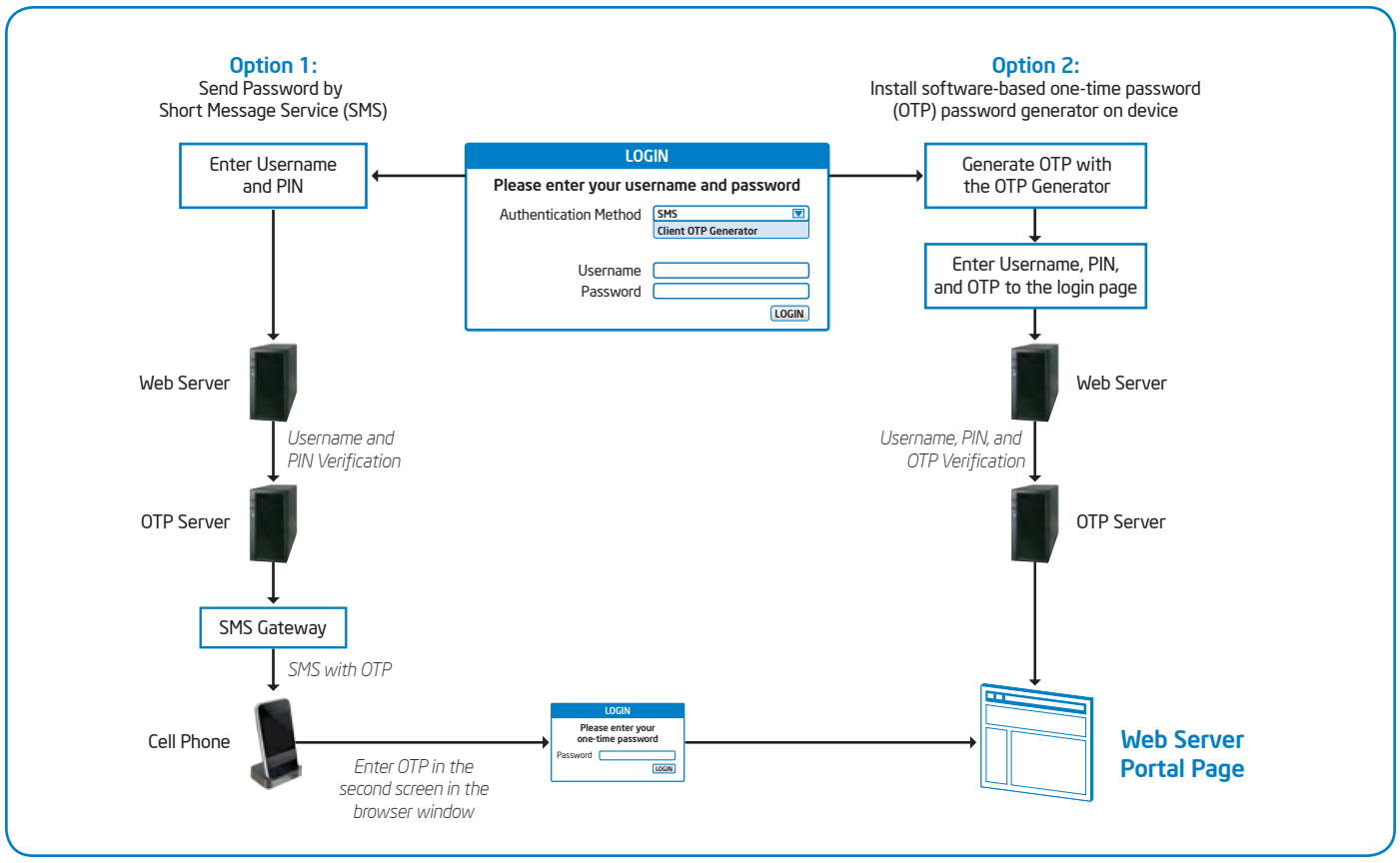

Figure 2. Our one-time password (OTP) solution supports sending the OTP to a personal cell phone number or generating an OTP locally.

Addressing Privacy Concerns

When we began to investigate a one-time password (OTP) solution based on SMS, we realized privacy considerations would be a critical factor in deployment.

With the new solution, employees no longer need to carry a hardware token generator. We can provide the OTP directly to the employee's smartphone if we know the employee's personal mobile phone number and a corporate email address, both of which are stored in a database. However, obtaining this personal information raises privacy concerns for our employees, who are located at company sites worldwide. This situation can be particularly problematic if non-work-related personal information is obtained or accessed.

An end-to-end review of the work flow and transfer of personal information resulted in significant changes to the original design concept through applying concepts from Privacy by Design.[§]

During the assessment, we tracked the personal information through the various components of the authentication process flow, shown below.

Flow of the Authentication Process

We assessed each component through which the personal information passed, verifying that the component had the appropriate security controls in place. The primary components that use, store, or share the personal information are the OTP servers that host the OTP database, the company gateway that provides login time stamps and source and destination IP addresses, and the client/server protocol servers that provide authentication time stamps.

We also developed retention policies for personal information and defined appropriate use, limiting access to only those people with a business need to know. In addition, we developed secured hosting and retention policies for the personal information (mobile phone number and email address) in compliance with company privacy policy.

We developed a privacy notice that is made available to employees on the OTP Administration and Provisioning web page and supplements the Global Employee and Global Contingent Worker Privacy policies.

Conducting the privacy assessment and developing the privacy notice and retention policies involved significant effort from the product, networking/gateway, and privacy teams, as well as from Intel Legal, and took more than a year to complete. Our master plan design for both the SMS-based and locally generated OTP delivery methods means that we do not have to insist on obtaining the private mobile phone numbers or email addresses of employees or contingent workers.

[§] For more information on the concepts of Privacy by Design, see www.privacybydesign.ca.

RESULTS

As shown in Figure 3, we are experiencing a fairly steady increase in demand for the applications we are making available to managed devices through the Mobile Portal. By expanding web application access first to additional managed devices and then later to unmanaged devices, we estimate that the number of Mobile Portal users will grow from about 16,000 devices to an estimated 38,000 devices. We are currently conducting proofs of concept for this expansion.

Although we have published fewer native applications than web applications, employees are using these native applications. For example, 500 unique users per month access the employee travel application.

As shown in Figure 4, some web applications, such as employee phonebook and paystub applications, are more popular than others.

NEXT STEPS

We are committed to expanding and improving our enhanced security connectivity solution.

Our future plans include the following:

- Offer additional web-based applications to unmanaged devices and additional operating systems in use at Intel—an estimated 15,000 devices—when our new, granular trust-based model is deployed in late 2012. In addition, we want to extend the number of web applications we offer, support more applications, and allow SSO using KPT to all devices, which will help to improve the UX.
- Create a direct link capability for certain web applications. A user will install a lightweight client application that, when launched, will directly open a specific application, with minimal authentication. This approach will provide a UX that more closely resembles accessing a native application.
- Further improve the UX for the OTP solution by generating the OTP on behalf of the user, directly from the login page. Currently, users first need to generate the OTP and then launch the application and enter the OTP on the login screen.

  The user launches the application and enters the appropriate username and password. Once submitted, the user receives a message to approve the OTP generation. The OTP is then generated in the background using the OTP generator and sent to the OTP server to complete the authentication process, with minimal user intervention.
- Continue exploring different options to provide VPN on-demand capabilities to additional SFF device operating systems, by developing in-house solutions.

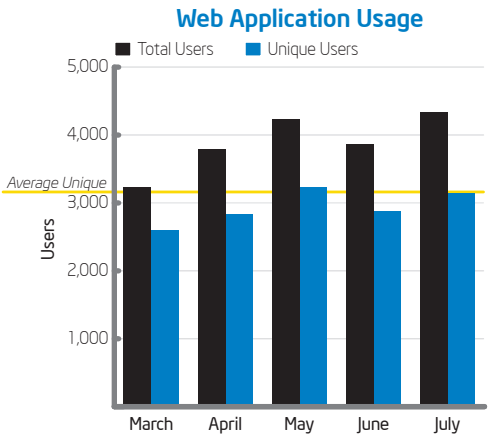

Figure 3. Employees are taking advantage of available web applications from their managed devices, with an average of about 3,175 unique users per month over the last seven months.

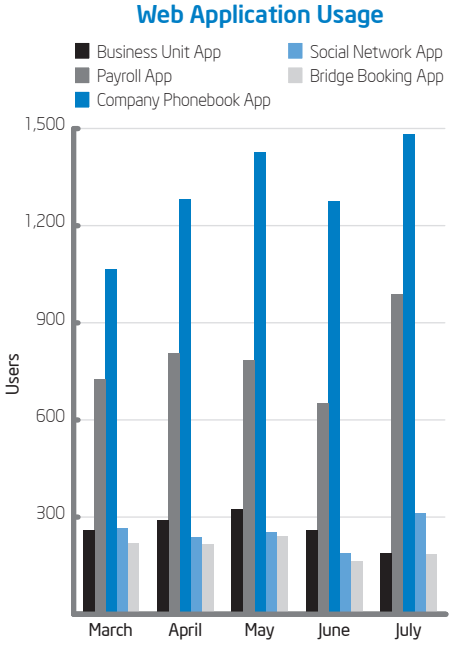

Figure 4. Some applications are more popular with employees than others.

CONCLUSION

With the proliferation of SFF devices—both corporate owned and personally owned—in use at Intel, we want to provide a more secure way for these devices to access native and web applications using an optimal UX. We also want to enable developers to publish their applications using their choice of enhanced security delivery mechanism.

We have implemented web application publishing and a mobile VPN for managed devices; we are in the process of providing access to web applications for unmanaged devices as well. Innovative components of our solution include the following:

- A streamlined approach to VPN authentication, where the VPN client launches in the background when an employee opens an application
- An improved web application gateway that is dedicated and tailored to mobile devices
- Restricted VPN profiles that limit network access to only what is required for specific applications
- A customized two-factor authentication mechanism for web application access
- A unique approach to SSO that uses KPT
- An improved OTP solution that requires no additional hardware

Employees have responded positively to our efforts to enable connectivity and security for personally owned devices—we have experienced an average of 3,175 unique users per month over the last seven months. Our enhanced security connectivity solution will help improve the agility and flexibility of our services, and increase employee productivity and job satisfaction.

FOR MORE INFORMATION

Visit www.intel.com/it to find white papers on related topics:

- Granular Trust Model Improves Enterprise Security

CONTRIBUTORS

Doron Hartuv
Amir Itzhaki
Ayelet Naor

ACRONYMS

FQDN	fully qualified domain names
KPT	Kerberos protocol transition
MDM	mobile device management
OTP	one-time password
SFF	small form factor
SSO	single sign-on
UX	user experience
VPN	virtual private network

For more information on Intel IT best practices, visit www.intel.com/it.

Printed in USA ♻ Please Recycle 0313/JGLU/KC/PDF 327762-002US