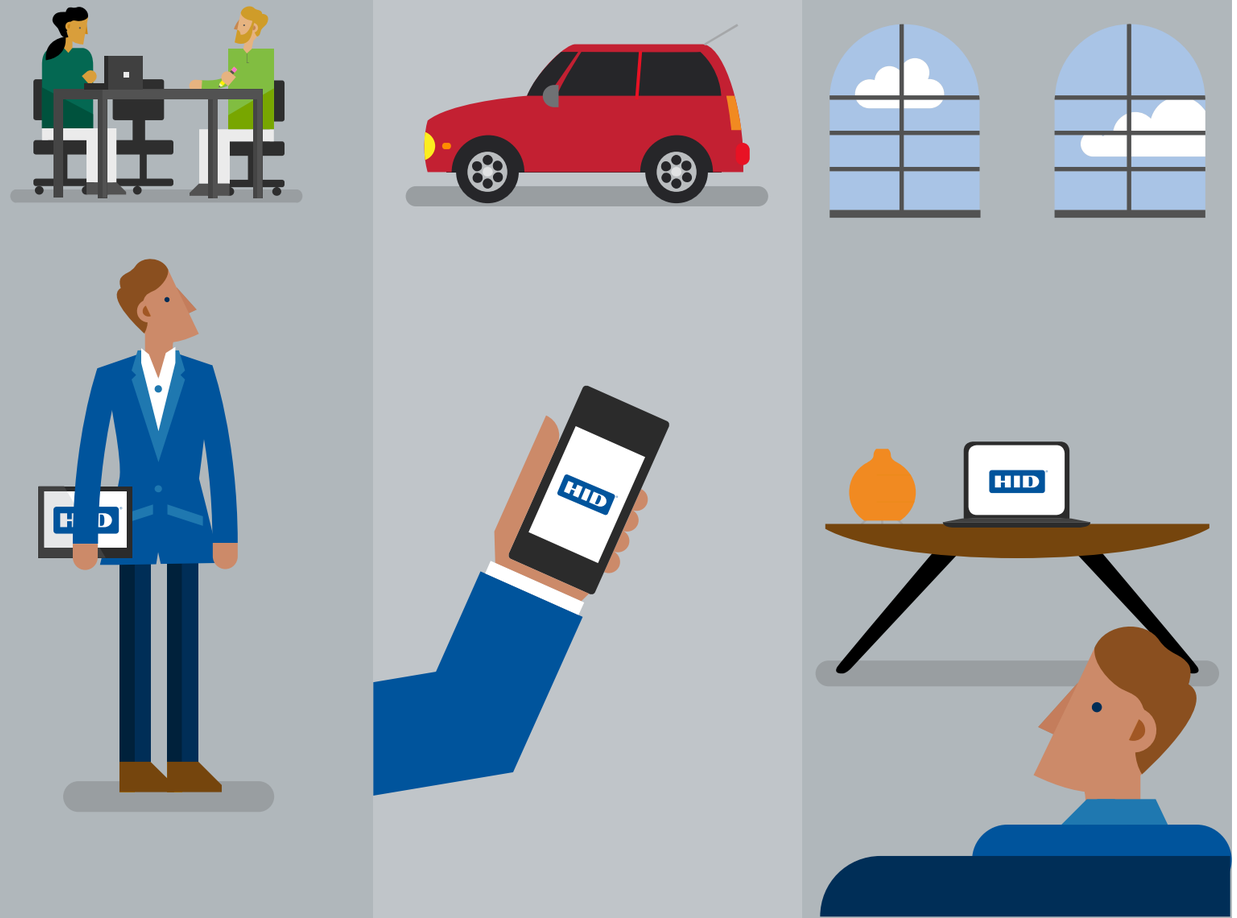
Security Solutions for Mobile Users in the Workplace

In partnership with

Microsoft Azure

Multitasking means **multiple devices** for busy end users



Introduction

Cloud computing helps organizations operate with less infrastructure, reducing capital costs while making company resources available to a global workforce. Gartner estimates that more than 50 percent of organizations will have moved to cloud-based services by 2017.

At the same time, the popularity of mobile devices has blurred the line between office and home. According to recent research from Forrester[1], global tablet and smartphone use in the enterprise is rising: nearly 20% of worldwide tablet purchases will be made directly by enterprises by 2017, allowing employees to more easily access company documents as they move from the office to home and all points in between.

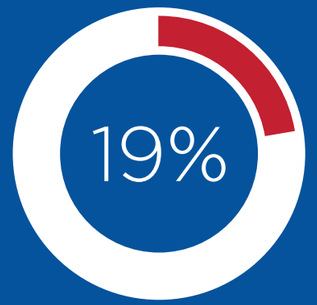
[1] "Global Business And Consumer Tablet Forecast Update, 2013 To 2017." Forrester Research.

Mobile devices change the security landscape

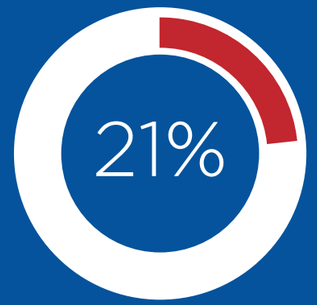
In a cloud-based mobile world, users need solutions that enable quick access to information and services. Current authentication methods, designed for use with keyboards, are awkward or sometimes just not possible with mobile devices. Furthermore, the growth of bring-your-own-device (BYOD) in the workplace increases security risks for an organization. According to a 2015 study by HID Global® and Tech Target of global IT professionals, nearly half of the respondents responded that increased mobility has significantly increased their risk for security breaches and/or data loss.

Both IT managers and the end users they support need authentication solutions that enable them to be productive quickly without typing in additional codes or keywords. Employers need to balance providing a simple and friendly user experience with protecting company assets from malware, loss and theft.

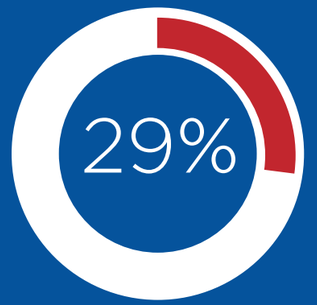
This e-book describes the security landscape for mobile devices and how near field communications can improve the user experience on mobile devices while allowing companies to protect their assets and manage costs efficiently.



in lost revenue



in lost productivity



reduction in reputation management[2]

[2]2014 IBM Security Services Cyber Security Intelligence Index Report

Current Security Solutions for Mobile Devices

All organizations want to validate the identity of people accessing company data and make sure they have the rights to do so. But existing authentication methods don't mesh well with mobile devices.

Two-factor authentication

Two-factor authentication combines single sign-on authentication (a combination of user name and password) with a one-time password (OTP) generated by a hardware device, email or text. The unique password provides an additional level of security to the single sign-on process.

But typing passwords using a phone or tablet isn't easy. Companies typically require complex passwords — and on a mobile device that means switching between character, numeric and special character keyboards to enter a password. If a user has to connect a hardware device to generate an OTP password or wait for an email or text, the process can take even longer. Single and two-factor authentication protocols are also prone to phishing attacks.

Smart card and certificates

Based on asymmetric cryptography, smart cards and certificates provide a high level of security. These solutions require a reader for authentication, which is often not physically possible with a mobile device. Reader sleeves for mobile devices are available, but are bulky to use. Costing between $100 and $200 per sleeve, the sleeves are expensive solutions for an organization to buy and manage.

How Near Field Communications Works on Mobile devices

Near field communications (NFC) is a wireless communications protocol based on ISO Radio Frequency Identification (RFID) standards. NFC doesn't require a discovery and pairing stage, so the connection time is as quick as 0.1 milliseconds. In comparison, the connection time for a Bluetooth connection is approximately six seconds (www.nfc-forum.org).

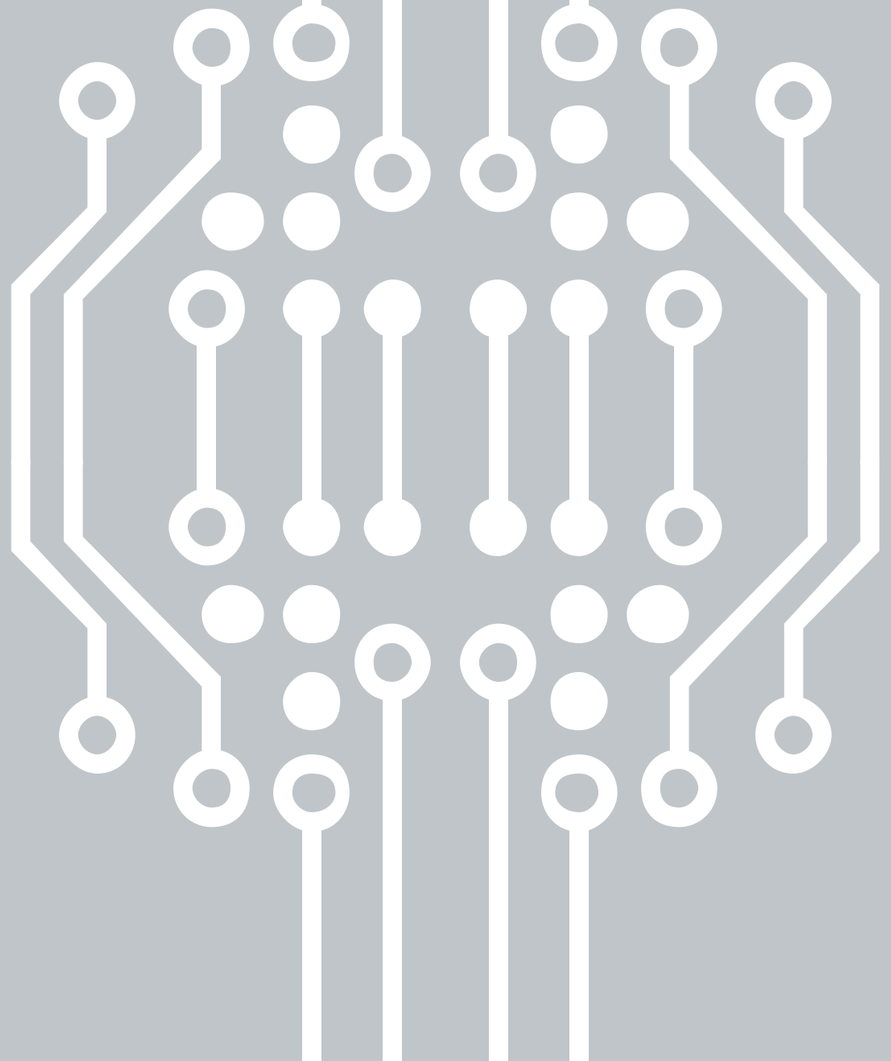
Using NFC technology, two smart phones can exchange contacts, photos and other information with each other. Users with NFC-enabled phones can pay for purchases and store electronic airline boarding passes, event tickets, and product identification among other uses. NFC-based applications are used in retail, health care, green technology, automotive and education, as well as other markets.

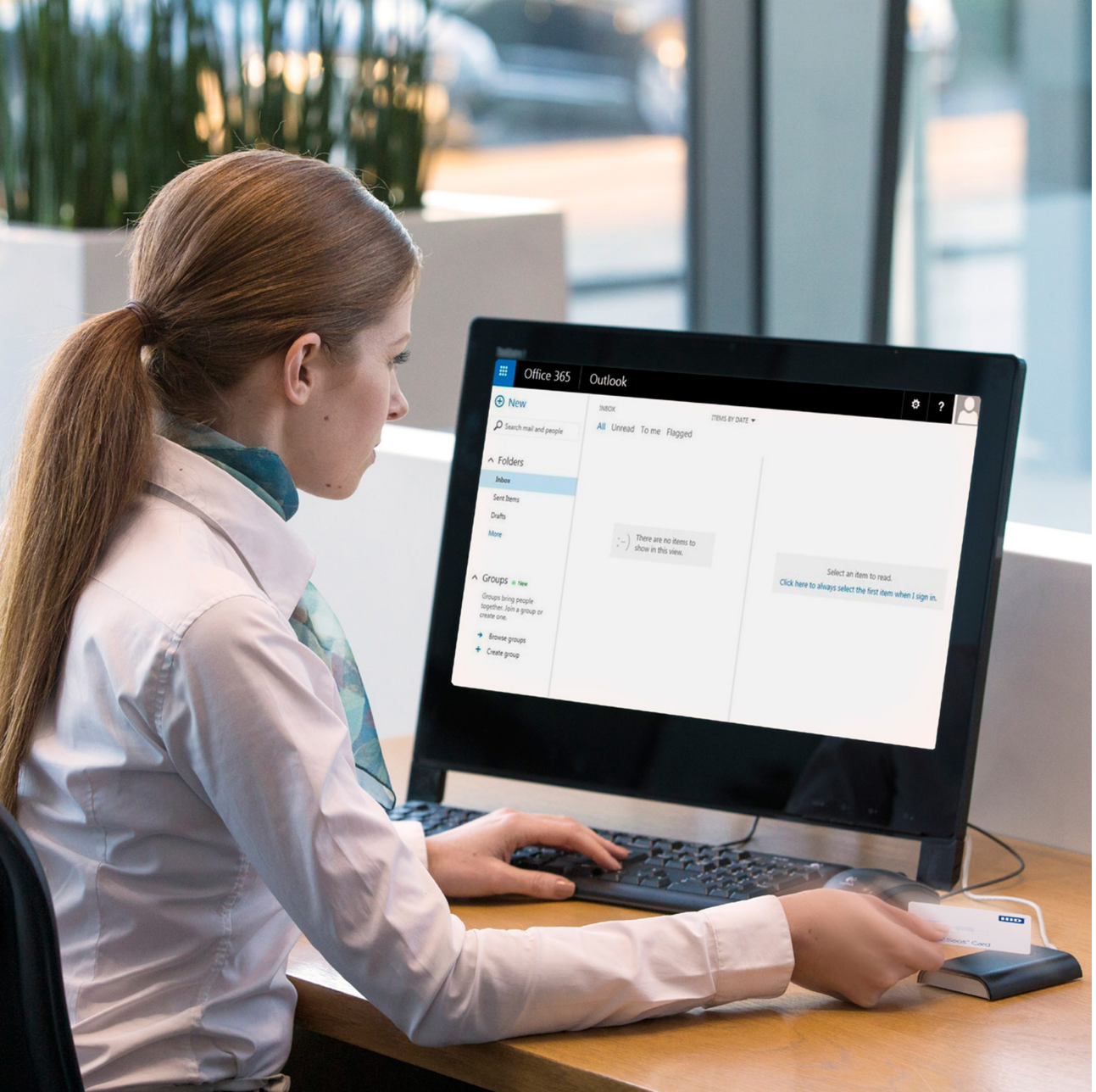
Friendly user experience

NFC chips are embedded in smart phones, mobile devices and laptops. According to RapidNFC, the top 10 phone manufacturers all sell mobile devices with built-in NFC technology. The experience is familiar and simple for end users. They only need to tap their phone against another device.

Designed for protection

NFC is fundamentally secure because it only works at extremely short ranges, from point of touch to a few centimeters. A hacker would have to stand uncomfortably close to piggyback on the signal of a nearby mobile device user. Furthermore, the integrated circuit in NFC devices are architected with security mechanisms beyond normal processors. Each circuit is designed with a unique digital signature for protection against both software and hardware attacks.





Security Solutions for the Mobile Workforce

ActivID® Tap Authentication™ from HID Global®

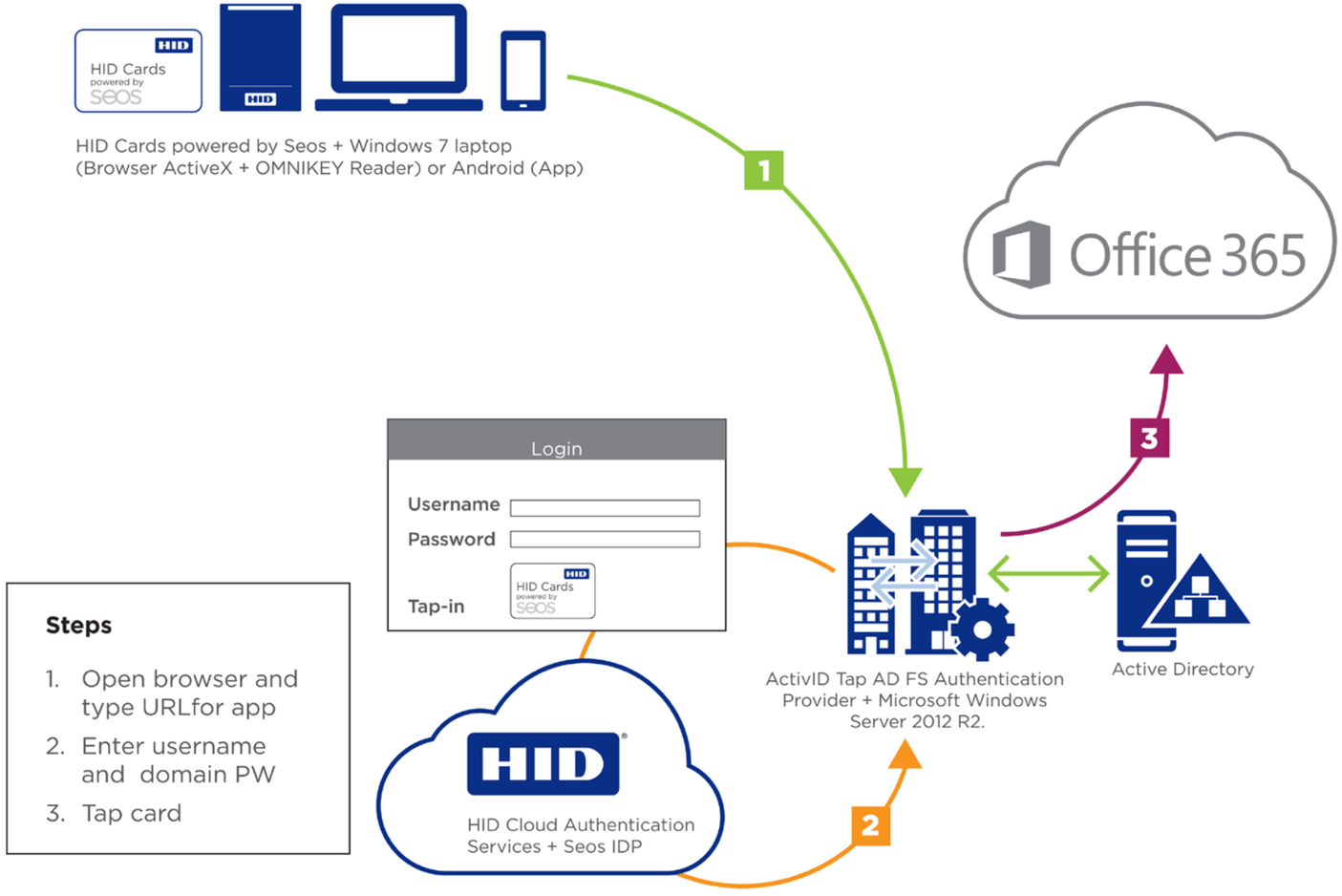
In the workplace, employees expect access to cloud applications, data and services anywhere and everywhere. HID Global, a leader in creating and managing secure identities, uses NFC technology to deliver a fast authentication experience that replaces two-factor, OTP passwords on mobile devices.

Simplifying the User Experience

The ActivID Tap Authentication solution confirms the identity of a unique user using the same card for both physical and virtual access. A user can access cloud applications and services on phones, tablets, and laptops in seconds with just a tap of the same card used to enter a building.

Delivering business value

For organizations already using smart cards for physical access, ActiveID Tap Authentication can save them the cost of investing and managing additional hardware. Because ActiveID Tap Authentication uses the cloud to authenticate users, organizations can move to a subscription-based model instead of the perpetual license model common with older authentication methods. Pricing for ActivID Tap Authentication is $2 per user per month with a minimum 12-month subscription, making security protection accessible for businesses of every size.



The HID and Microsoft Partnership

The ActivID Tap Authentication platform is integrated into the Microsoft® Active Directory® Federated Services environment and Microsoft® Windows Server® 2012 R2. It's a simple three-step process to connect, saving the expense of hiring professional services.

ActivID Tap Authentication works with Microsoft Office® 365, Salesforce.com and more than 2,200 other cloud applications. The solution is available in the My Apps portal, enabling users access to cloud applications with a single user account hosted in Microsoft Azure Active Directory.

Summary

Together, HID and Microsoft enable secure, real-time authentication for mobility users. ActivID Tap Authentication leverages the security features of NFC technology and works with Azure Authentication and the power of the Azure Active Directory to provide end users with safe and convenient access, no matter what device they happen to be using.

This unique solution gives IT managers better visibility and control of authenticated users and a single point of revocation, reducing security risks, enabling them to embrace BYOD, and realize cost savings through the use of existing cards and credentials.

For both the end user and IT manager, ActivID Tap Authentication makes security simpler, easier and faster.

READY TO LEARN MORE?

2015-08-31-hid-ms-azure-partnership-eb-en PLT-02547