ENCRYPTION CONSULTING

Windows Hello For Business

Introduction

Microsoft's most recent effort to do away with passwords in Windows enterprise contexts is Windows Hello for Business (WHfB). It features a new user interface and built-in support for biometric authentication techniques like fingerprint or facial recognition. It handles some of the frequent password issues like password leaks or phishing assaults.

In a survey, it was found that business users liked Windows hello more because it is more usable and secure than traditional Windows sign-in. Windows Hello was faster and perceived as more responsive than the traditional Windows login.

There are various deployment models offered by Windows Hello for Business. The optimal choice for you will depend on several variables, including your operating system version, whether you handle certificates on user devices, and if you have an on-prem, cloud-only, or hybrid environment.

Depending on your deployment model, our solution enables Windows for Business to interface with Azure Active Directory and on-premises domain controllers. Through a rapid pilot and rollout approach, it provides integration with Azure Multi-Factor Authentication for enhanced security.

Key Points of WhfB

• The basis for Windows Hello credentials is either a certificate or an asymmetric key pair. Both the token obtained with a Windows Hello credential and the credential itself can be tied to a device.

• During the registration phase, an identity provider verifies the user's identity and associates the Windows Hello public key with a user account. Active Directory, Azure AD, and a Microsoft account are a few examples of providers.

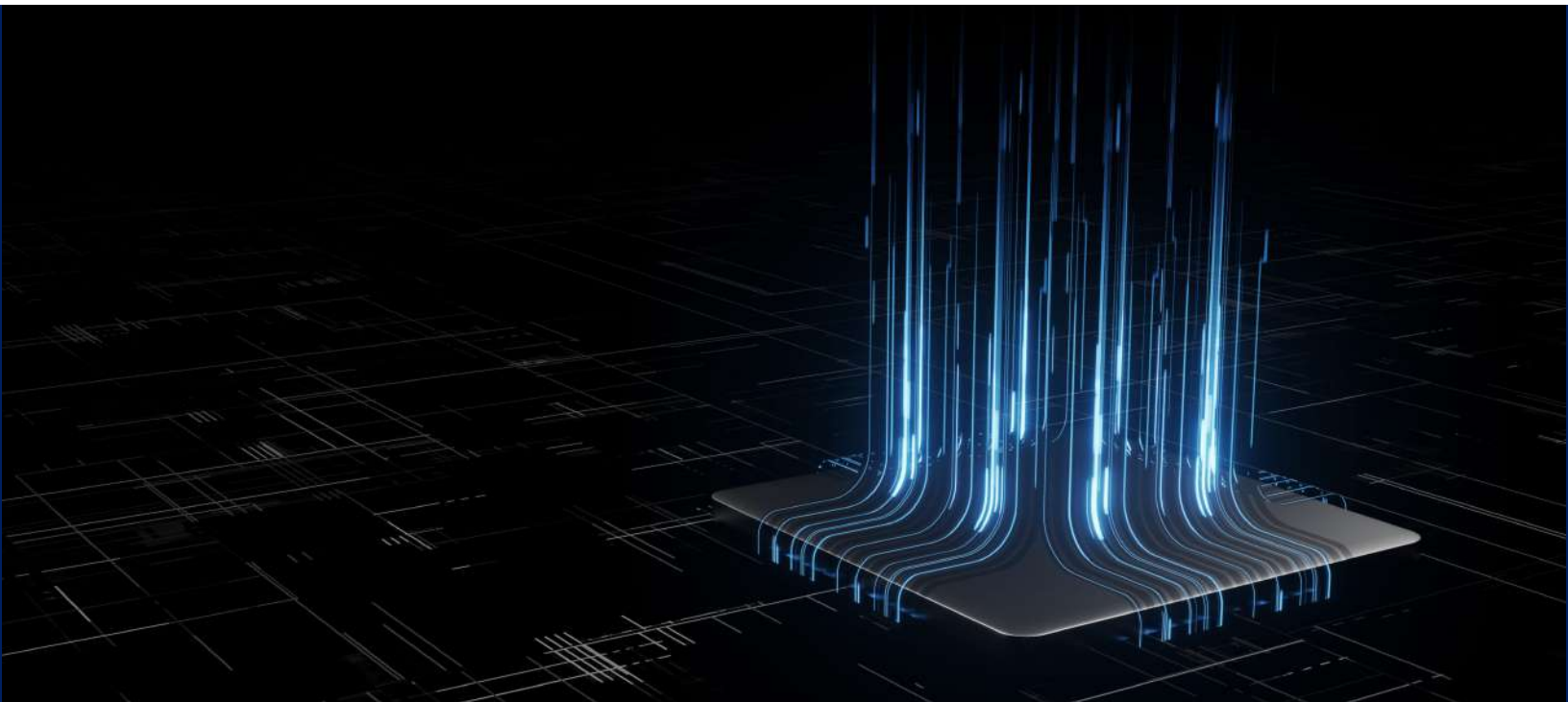
• Depending on the policy, keys can be generated in either hardware (TPM 1.2 or 2.0 for corporations, and TPM 2.0 for consumers) or software. You must establish a policy in order to ensure that keys are produced in hardware.

• When employing TPM, the private key never leaves a device. During the registration procedure, the user account is mapped to the authenticating server's public key.

• Windows 10 and later employ the private key to cryptographically sign data before sending it to the identity provider upon PIN enter and biometric gesture, respectively. The identity provider authenticates and confirms the user's identity.

• Keys are stored in a single container for both individual (Microsoft account) and business (Active Directory or Azure AD) accounts. To assist in protecting user privacy, all keys are separated by the domains of identity providers.

• Both the Windows Hello container and the Windows Hello gesture can protect certificate private keys.



Implementation Plan

The EC team will first carry out a quick pilot and advise your teams on how to embrace Windows Hello for Business technology. After this, they will integrate the solution with the current Enterprise infrastructure while keeping your future state in mind.

WEEK 01 - 03

We help collect details pertaining to existing IT Infrastructure, Azure Licensing, and MFA needs and develop an approach for deployment and setup configurations for deployment.

WEEK 04 - 09

We assist in rolling out the pilot deployment and test with supported infrastructure, gather feedback from the workforce (on-site & remote) and Ops teams (new processes), and capture analytics and then expand capabilities piloted & build a rollout plan.

WEEK 10

We work together to finalize the phased rollout plan for your organization.

Why Encryption Consulting LLC?

ENCRYPTION CONSULTING

Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized accees. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security for organizations.

Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates that provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure.

Hardware Security Module - HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.

Certificate Lifecycle Management

Certificates typically have a 4-phase lifecycle -Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases.

Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environment? Do you want to protect data without disruptive changes to applications or business practices?

Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations.

See it in action

Encryption Consulting LLC is a customer-focused cyber security consulting firm providing an array of services in all aspects of data protection.

Contact Us

encryptionconsulting.com

linkedin.com/company/encryptionconsulting

facebook.com/encryptionconsulting

twitter.com/encryptioncons

Strategic Technology Partnerships

We work with the industry's best technology providers and have broad experience deploying, managing, and integrating our integrating our solutions with their products and services. We also pride ourselves on our flexibility and are always open to help our clients achieve their data security success with the technology of their choice. If you have products and services already deployed or are considering, we'd be glad to help you evaluate these to get the most out of your investment.

ENTRUST

nCipher Security, a leader in the general purpose hardware security module market, is now an Entrust Datacard company, delivering trust, integrity and control to business critical information and applications.

THALES

Thales-e-Security is a leader in encryption, advanced key management, tokenization, priveleged user control and meets the highest standards of certification for high assurance solutions.

Fortanix

Fortanix is a leader in runtime encryption and it protects applications even when the infrastructure is compromised.

KEYFACTOR

Keyfactor has its roots in the trenches of IT security, deployment and operations. We understand how companies work because of our deep industry experience - we know firsthand the challenges of competing agendas, budget constraints and time pressures.

Microsoft

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington.

MICRO FOCUS

Micro Focus and HPE Software have joined to become one of the largest pure-play software companies in the world.

CRYPTOMATHIC

Cryptomathic is a global provider of secure server solutions to business across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile.

gemalto

For those shaping the digital interactions of tomorrow, we provide the digital security that enables the trusted connections of today.

FORNETIX

Fornetix Key Orchestration TM is a scalable and Aexible solution designed to simpligy key management. Granular ploicy tools, user access controls, and powerful automation enable organiza-tions to manage hundreds of millions of encryption keys while integrating seamlessly with existing technology investments.

appviewX

AppviewX is revolutionizing the manner in which NetOps and SecOps team.

PrimeKey

PrimeKey's technology is used by organizations and enterprses to securely implement PKI solutions used for ePassports, eBanking, ePayment, mobile/Internet security, IoT and more.

UNBOUND

Unbound protects secrets such as cryptographic keys, credentials or private data by ensuring they never exist in complete form.

Venafi

Venafi Cloud helps organizations prevent outages and secure their keys and certificates.

PrimeFactors

Prime Factors software products help business leaders implement and manage enterprise-wide data protection policies to secure sensitive information being used by or stored in virtually any application or system.

utimaco

Utimaco is a leading manufacturer of Hardware Security Modules(HSMs) that provide the Root of Trust to all industries, from financial services and payment to the automotive industry, cloud services to the public sector.

PROTEGRITY

The Only Data-First Security Solution. Protect sensitive enterprise data at rest, in motion, and in use with Protegrity's best-in-class data discovery, de-identification and governance capabilities.

comforte

Secure your data, minimise risk, and meet compliance and regulation requirements. Find out more about Comforte's Data Security Services.