ICT POWER.IT

Microsoft

#POWERCON2023

Windows Hello for Business è la MFA di Windows!

Riccardo Corna

MVP Security – Senior Consultant

@riccardocorna

/riccardocorna

Agenda

- La domanda ricorrente che tutti fanno
- I problemi delle password
- Cos'è Windows Hello for Business (WHfB) ?
- Come funziona WHfB ?
- Tipologie di trust
- Perché WHfB è passwordless e multi-factor
- DEMO

È possibile avere la MFA al login di Windows?

*"Sì, implementando **Windows Hello for Business**"*

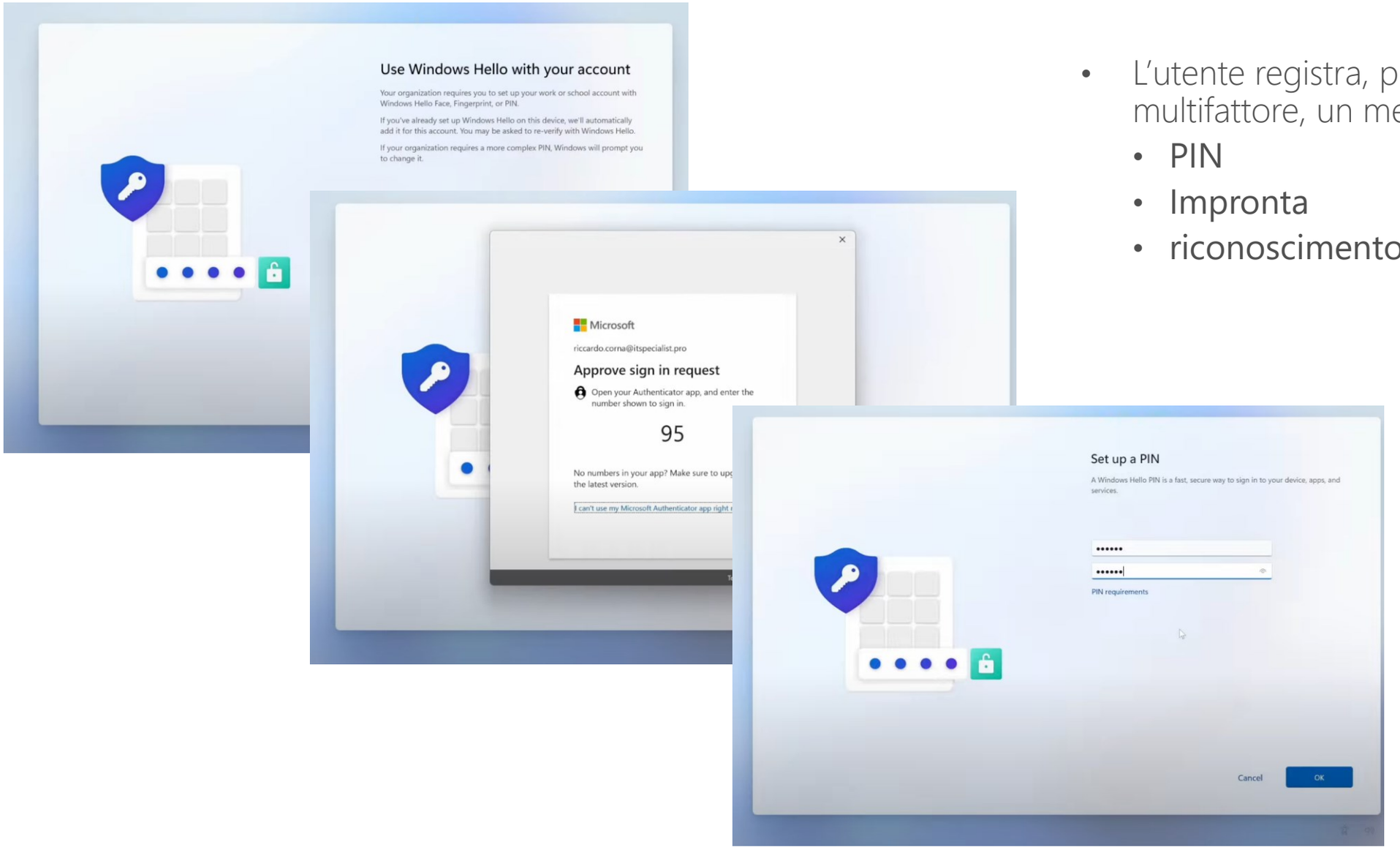
I problemi delle password

- Le password complesse sono difficili da ricordare
- Riutilizzo su più servizi
- Violato uno, violati tutti
- Phishing

Cos'è Windows Hello for Business?

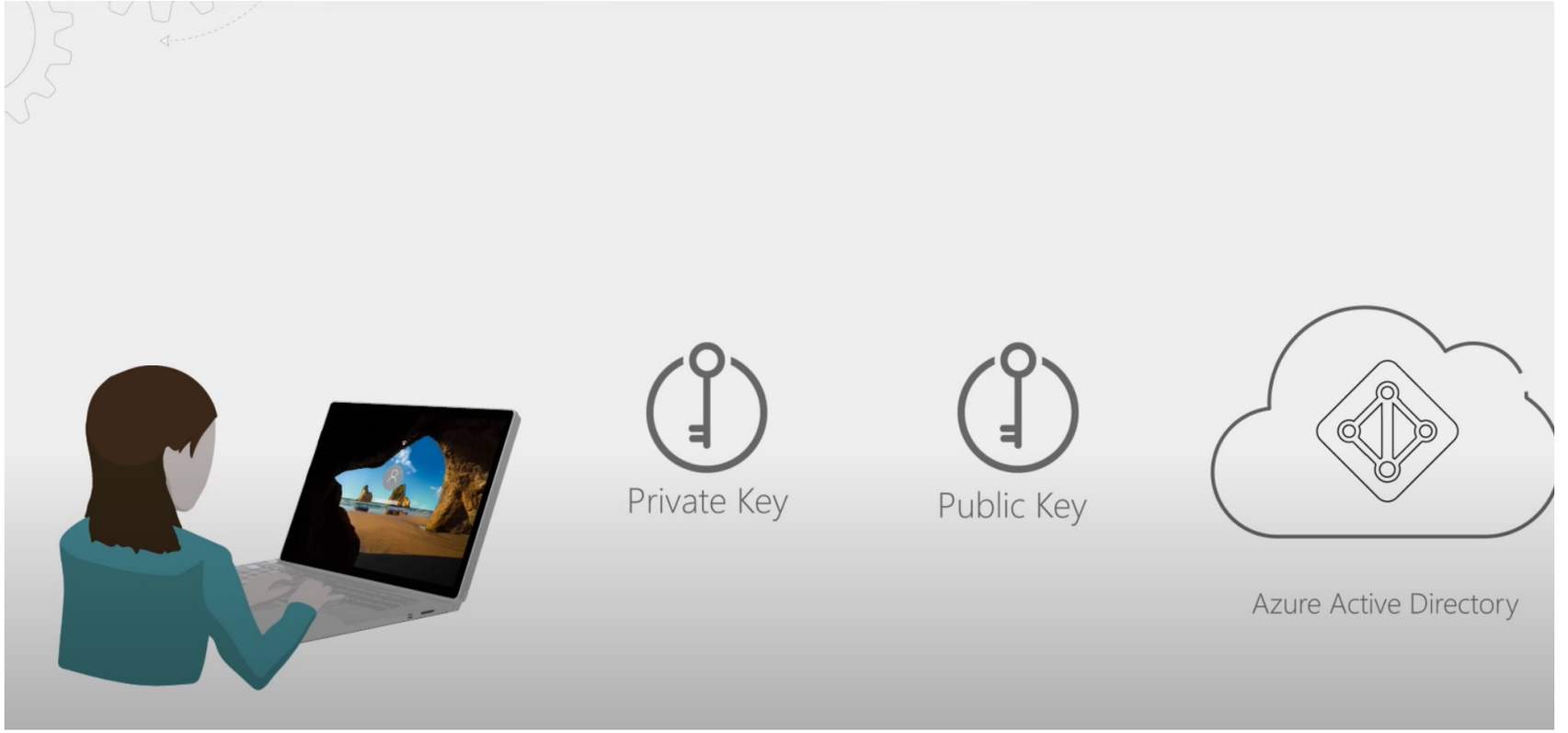
- È una funzionalità avanzata di sicurezza di Windows
- Sostituisce la password con un'autenticazione forte a due fattori sui dispositivi
- L'autenticazione consiste in una credenziale utente legata al singolo dispositivo (PIN o biometrica)

Come funziona WHfB? - Registrazione



- L'utente registra, previa autenticazione multifattore, un metodo di verifica:
  - PIN
  - Impronta
  - riconoscimento facciale

Come funziona WHfB? - Registrazione



Le credenziali di Windows Hello sono basate su certificato o su una coppia di chiavi asimmetriche

Come funziona WHfB? - Registrazione

Un identity provider convalida l'identità dell'utente mappa la chiave pubblica di Windows Hello sull'utente. Esempi:

- Microsoft account
- Active Directory account.
- Azure Active Directory (Azure AD) account
- Identity Provider Services or Relying Party Services che supporti autenticazione Fast ID Online (FIDO) v2.0

Come funziona WHfB? - Registrazione

- Le chiavi possono essere generate via TPM o via software
- Quando generata via hardware (TPM chip), la chiave privata viene memorizzata lì dentro e non lascia MAI il dispositivo

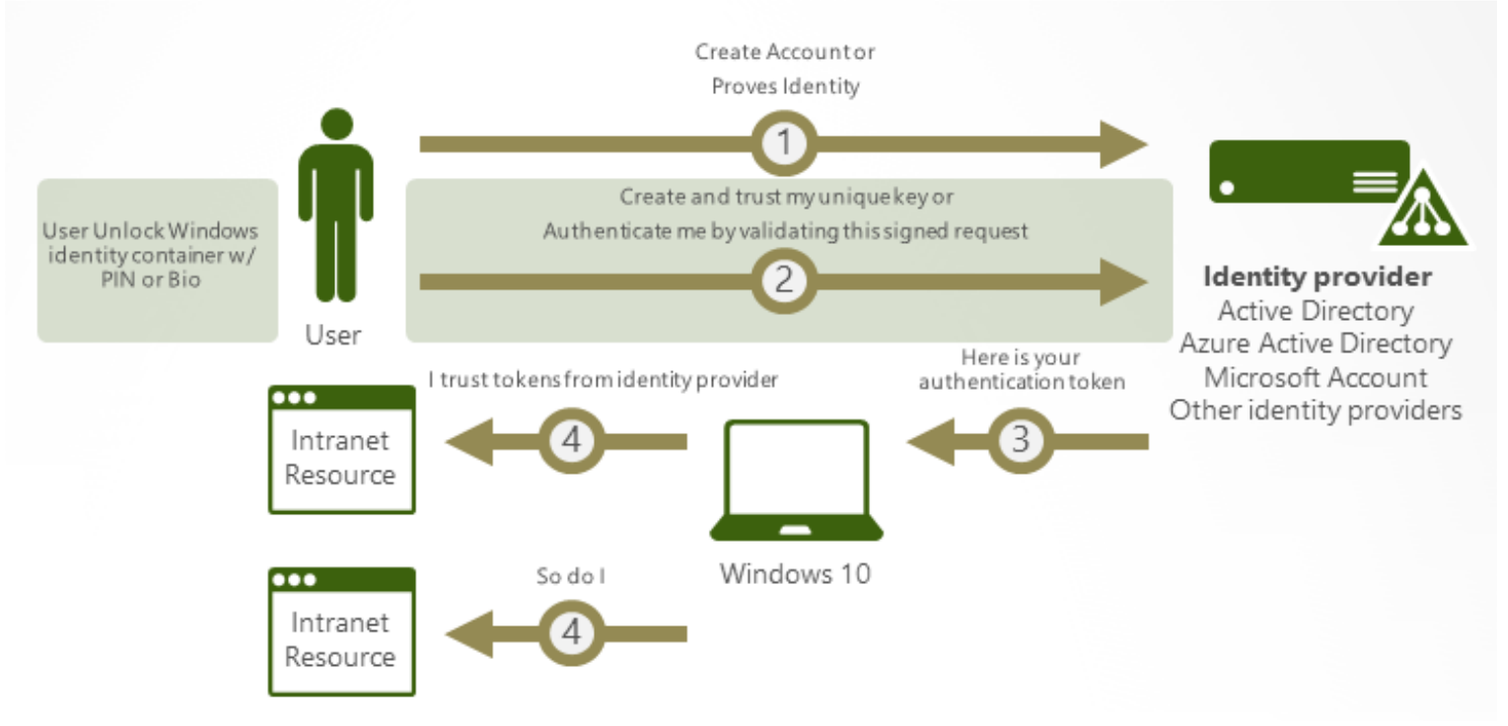
Come funziona WHfB? - Autenticazione

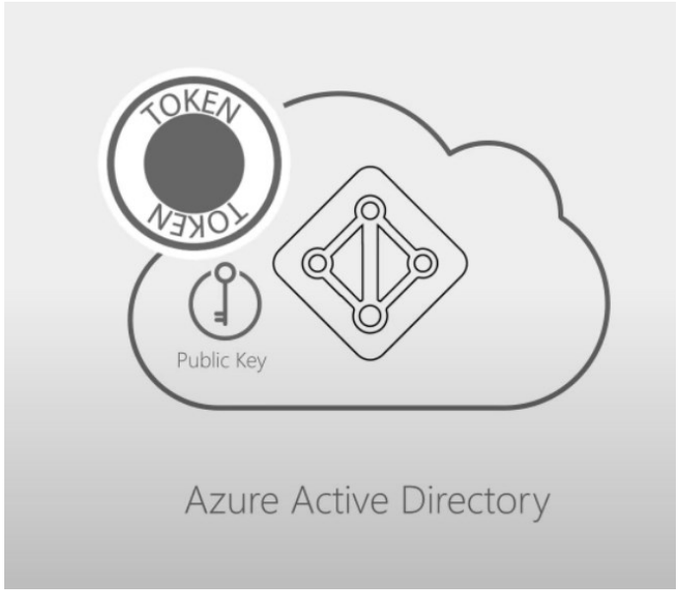
- Il PIN, l'impronta o il viso, servono solo per sbloccare l'utilizzo della chiave privata
- La chiave privata viene usata per firmare digitalmente i dati che vengono inviati per l'autenticazione

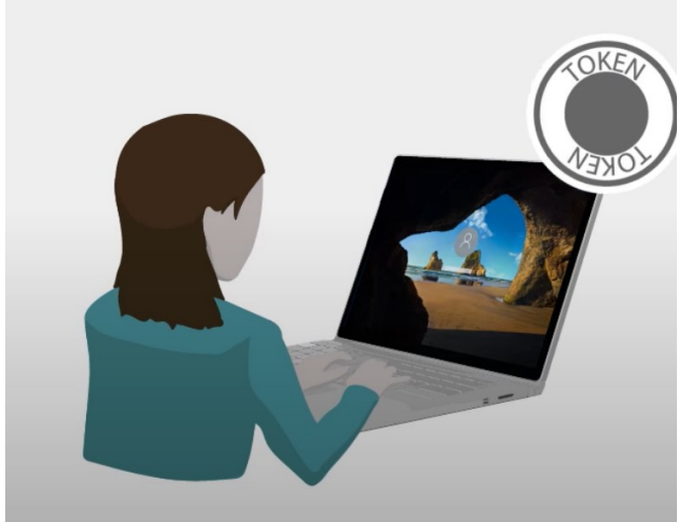
Come funziona WHfB? - Autenticazione

Se tutto va come deve andare,
l'identity provider rilascia un token

😀







Perché WHfB è passwordless e multi factor?

- È passwordless perché: avete visto usare la password da qualche parte? ☺
- È MFA perché, per autenticarci, dobbiamo usare
  1. Un certificato o una chiave, legate ad uno specifico dispositivo
  2. Qualcosa che sappiamo (PIN) o che siamo (impronta, viso)

- Altri takeaway
  - Le credenziali sono legate al dispositivo
  - Il token ottenuto per accedere è anch'esso legato a quel dispositivo
  - Nessun PIN, nessuna impronta, nessuna scansione facciale lasciano il dispositivo
  - Queste credenziali non sono valide su altri dispositivi e non vengono condivise con nessun server

Perché il PIN è importante?

- Un PIN è legato ad uno specifico dispositivo
- Un PIN è locale su uno specifico dispositivo
- Il tutto è gestito dal chip TPM → Sicurezza hardware
- Il PIN è un metodo di backup in caso di infortunio che renda indisponibile il metodo biometrico

Tipi di deployment e di trust

Deployment - Trust	Join	Per chi?
Cloud-Only	AADJ	- Ha un mbiente full-cloud
Hybrid **Cloud Kerberos trust**	AADJ Hybrid AADJ	- Non intende rilasciare certificati utente - Dispone di DC Win Srv 2016 nei siti AD - Non intende usare Certificate Services - **Metodo raccomandato al posto di Key trust**
Hybrid **Key trust**	AADJ Hybrid AADJ	- Non intende rilasciare certificati utente - Dispone di DC Win Srv 2016 nei siti AD - Richiede AD Certificate Services
Hybrid **Certificate trust**	AADJ Hybrid AADJ	- Usa e/o intende rilasciare certificati utente - Non è pronto a rilasciare DC Windows Server 2016 - Richiede AAD Certificate Services
On-premises **Key trust**	Domain join	- Intende sostituire username e password con WHfB - Non intende rilasciare certificati utente - Dispone di DC Win Srv 2016 nei siti AD - Richiede AD Certificate Services
On-premises **Certificate trust**	Domain join	- Intende sostituire username e password - Non è pronto a rilasciare DC Windows Server 2016 - Richiede AAD Certificate Services

E il Remote Desktop?

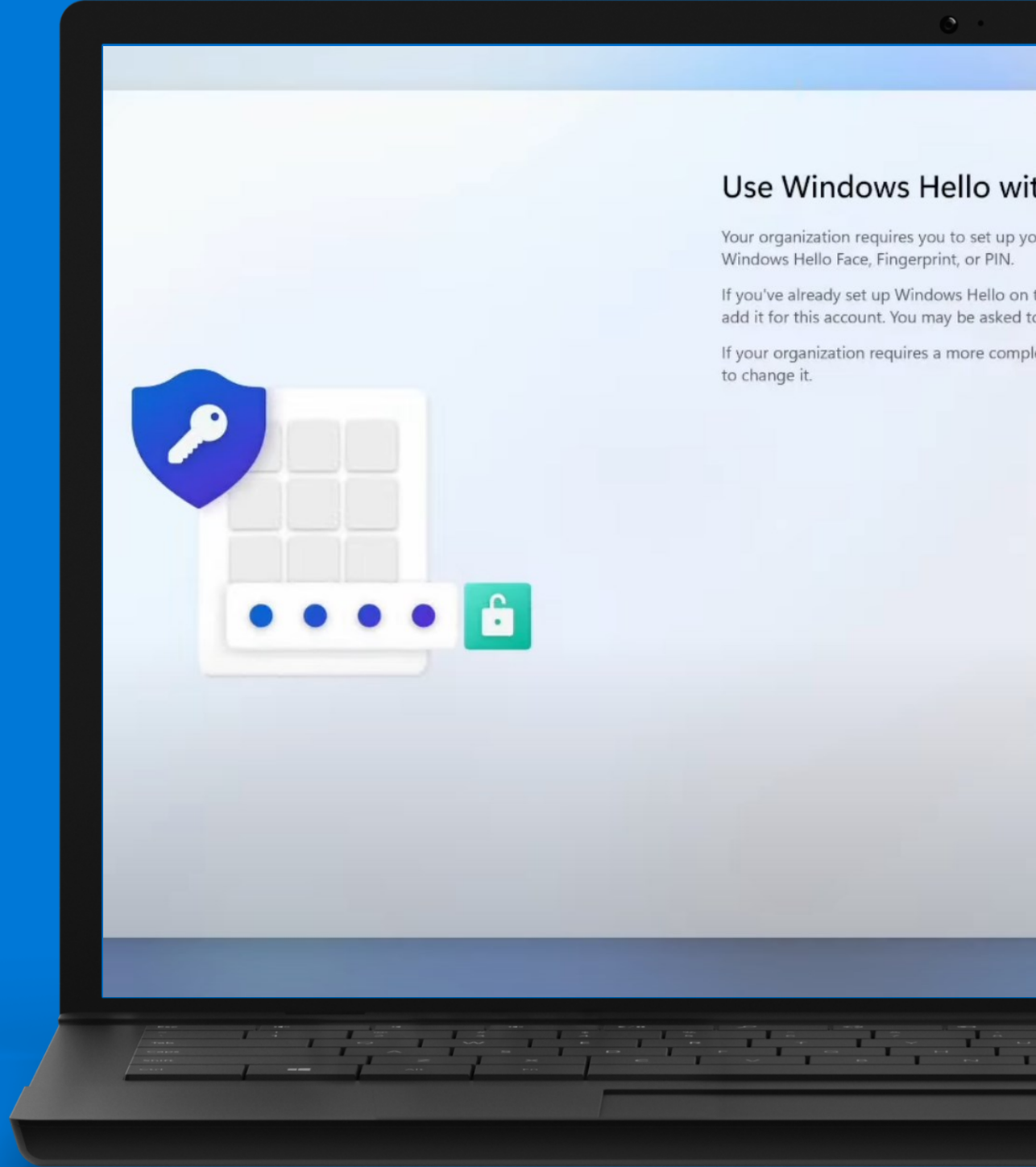
> **Note**
>
> RDP does not support authentication with Windows Hello for Business Key Trust or cloud Kerberos trust deployments as a supplied credential. RDP is only supported with certificate trust deployments as a supplied credential at this time. Windows Hello for Business Key Trust and cloud Kerberos trust can be used with **Windows Defender Remote Credential Guard**.

Cloud Kerberos Trust

- È un modello di distribuzione di WHfB
- Ne semplifica la distribuzione:
  - Non c'è necessità di una PKI o di modifiche ad una PKI esistente
  - Nessuna necessità di sincronizzare le chiavi pubbliche tra AAD e AD on-prem, per accedere a risorse on-prem
  - Supporta il SSO con chiave di sicurezza FIDO2
- Come funziona?
  - Anziché usare l'autenticazione Kerberos basata su certificato che viene usata negli altri modelli di distribuzione, viene usata Azure AD Kerberos
  - Viene richiesto un ticket TGT «particolare» ad AAD Kerberos
  - Il ticket restituito, ulteriormente «lavorato» da AD on-prem, può essere usato per autenticarsi su risorse on-prem
  - Viene creato un computer account di nome «AzureADKerberos» in AD che appare come un RODC

DEMO

Windows Hello for Business Cloud Kerberos Trust



Administrator: Windows PowerShell ISE

MVP-VM-DC-01.itspecialist.local

File Edit View Tools Debug Add-ons Help

Run Script (F5)

Untitled1.ps1* Untitled2.ps1* Untitled3.ps1*

```
1  # First, ensure TLS 1.2 for PowerShell gallery access.
2  [Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor [Net.SecurityProtocolType]::Tls12
3
4  # Install the Azure AD Kerberos PowerShell Module.
5  Install-Module -Name AzureADHybridAuthenticationManagement
```

PS C:\>

Ln 5 Col 59 100%

Type here to search

ITA 12:57 AM 2/26/2023

Microsoft Edge File Edit View History Favourites Tools Profiles Tab Window Help

Mon 27 Mar 19:31

windows hello for business - S | Windows Hello for Business cl | MVP M365 E5 Lab (itspecialist

https://intune.microsoft.com/#home

Office 365 | Office Personal | Mastodon | LinkedIn | Feedly | Banking & Invest... | I Miei Siti | Un caffè con | World Webcams | Altri portali MS | Software Library:... | Lofi Girl | LinkedIn Live | Other Favourites

Microsoft Intune admin center

rcadmin@itspecialistlab.... MVP M365 E5 LAB (ITSPECIALIS...

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

MVP M365 E5 Lab (itspecialist.pro)

Home | Microsoft Managed Desktop

Status

Errors/failures **0**

Healthy **6**

Account status	Active
Client apps	No installation failures
Connector status	Healthy
Device compliance	All in compliance
Device configuration	No policies with error or conflict
Service health	Healthy

News

Intune add-ons

Intune add-ons offer advanced endpoint management functionality.

Explore

Intune Customer Success blog See all >

New Microsoft Intune Devices experience

Configuring BitLocker via Microsoft Intune settings catalog

Announcing support of the new Microsoft Store apps during Windows Autopilot

Cloud PC

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Explore

Guided scenarios See all >

Deploy Edge for mobile

Configure Edge for use at work and deploy it to the iOS and Android devices managed by your organization.

Start

What's happening in Intune

What's new in Microsoft Intune

MVP M365 E5 Lab (itspecialist

https://intune.microsoft.com/#home

Microsoft Intune admin center

rcadmin@itspecialistlab....
MVP M365 E5 LAB (ITSPECIALIS...

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

MVP M365 E5 Lab (itspecialist.pro)

Home | Microsoft Managed Desktop

Status

Errors/failures **0**

Healthy **6**

Account status	Active
Client apps	No installation failures
Connector status	Healthy
Device compliance	All in compliance
Device configuration	No policies with error or conflict
Service health	Healthy

News

Intune add-ons

Intune add-ons offer advanced endpoint management functionality.

Explore

Intune Customer Success blog See all >

New Microsoft Intune Devices experience

Configuring BitLocker via Microsoft Intune settings catalog

Announcing support of the new Microsoft Store apps during Windows Autopilot

Cloud PC

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

Explore

Guided scenarios See all >

Deploy Edge for mobile

Configure Edge for use at work and deploy it to the iOS and Android devices managed by your organization.

Start

What's happening in Intune

What's new in Microsoft Intune

Features in development

UI updates for Intune end-user apps

Bibliografia

- Windows Hello for Business Overview - Windows Security | Microsoft Learn
- Why a PIN is better than an online password - Windows Security | Microsoft Learn
- Windows Hello for Business Deployment Overview - Windows Security | Microsoft Learn
- How Windows Hello for Business works - Windows Security | Microsoft Learn
- How Azure AD device registration works - Microsoft Entra | Microsoft Learn
- How Windows Hello for Business works - Provisioning - Windows Security | Microsoft Learn
- How Windows Hello for Business authentication works - Windows Security | Microsoft Learn
- Planning a Windows Hello for Business Deployment - Windows Security | Microsoft Learn
- Windows Hello for Business Deployment Prerequisite Overview - Windows Security | Microsoft Learn
- Windows Hello for Business cloud-only deployment - Windows Security | Microsoft Learn
- Windows Hello for Business cloud Kerberos trust deployment - Windows Security | Microsoft Learn
- Windows Hello for Business hybrid key trust deployment - Windows Security | Microsoft Learn
- Windows Hello for Business hybrid certificate trust deployment - Windows Security | Microsoft Learn
- Windows Hello for Business deployment guide for the on-premises key trust model - Windows Security | Microsoft Learn
- Windows Hello for Business deployment guide for the on-premises certificate trust model - Windows Security | Microsoft Learn

Volete quotidianamente contenuti come questi?

Siete appassionati di security e di tecnologie Microsoft?

SEGUITECI! 😉

Microsoft Security Italian Users Group

ITSpecialist.cloud

ICT POWER.IT

Microsoft

Grazie

Riccardo Corna
MVP Security – Senior Consultant

@riccardocorna

/riccardocorna