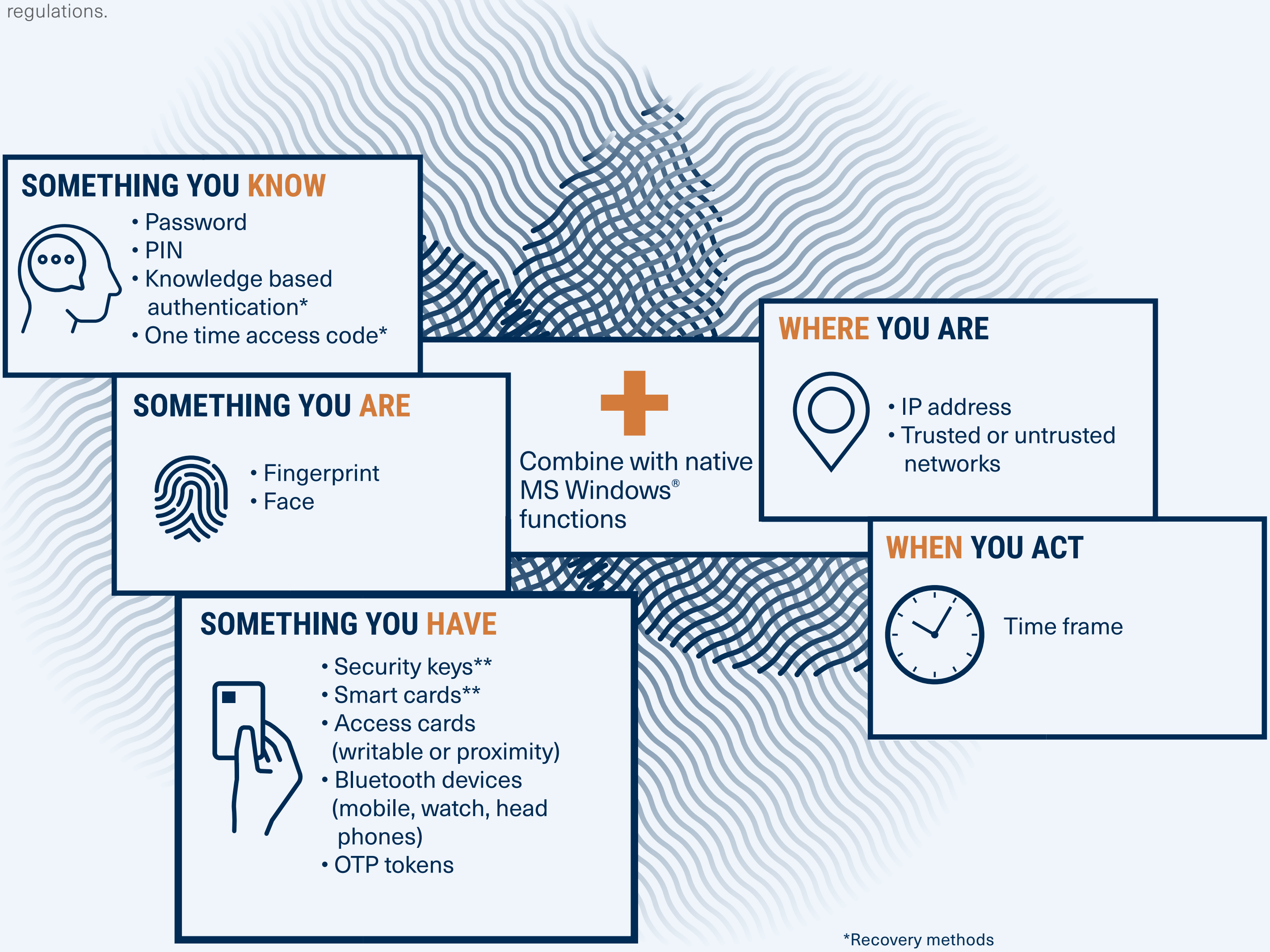
HID DigitalPersona®

Flexibility and convenience when wanted, strength and security where needed

HID DigitalPersona transforms the way an organization protects the integrity of digital assets and applications by providing easy-to-deploy, adopt and manage multi-factor authentication (MFA) that eliminates siloed security processes with cost-efficiency. Designed for today's border-less organization, this MFA solution enables rapid and secure login to Windows, networks and applications via biometrics, mobile devices, physical access badges, smart cards and security keys – delivering a seamless user experience with the strongest protection available in the industry.

Combining security and usability, DigitalPersona employs one of the widest arrays of authentication methods and form factors in the industry, including Personal Identifiable Number (PIN), One-Time Passwords (OTP), mobile push notifications, FIDO, PKI, fingerprint and face recognition – enabling a Zero Trust security approach that evolves with security standards, technologies and industry regulations.



SOMETHING YOU KNOW

- Password
- PIN
- Knowledge based authentication*
- One time access code*

SOMETHING YOU ARE

- Fingerprint
- Face

SOMETHING YOU HAVE

- Security keys**
- Smart cards**
- Access cards (writable or proximity)
- Bluetooth devices (mobile, watch, head phones)
- OTP tokens

+

Combine with native MS Windows® functions

WHERE YOU ARE

- IP address
- Trusted or untrusted networks

WHEN YOU ACT

Time frame

*Recovery methods
**Supported technologies: PKI, FIDO2, OATH

KEY BENEFITS

Complete coverage

With DigitalPersona, organizations can rest assured that they are taking a holistic approach to access security by enforcing strong MFA to all applications (cloud, custom made and legacy), systems and networks – all while securing access for all identities, including employees, customers, suppliers and partners.

In addition to the traditional set of authentication factors — something you have, something you are, or something you know — DigitalPersona can be combined with Microsoft Sites and Services adding authentication for the contextual risk factors of time, velocity, and location. The latter cover what you do, where you are and when you act, allowing you to precisely match your risk exposure to the optimal security posture for your organization.

Versatile authentication

DigitalPersona's wide array of supported authentication methods and factors eliminate both the reliance and burden on users enabling organizations to adopt strong authentication best practices without compromising user experience and productivity. This growing range of authentication options provides unprecedented freedom of choice empowering organizations to combine convenience and security, now and in the future.

Rapid deployment and scalability

Deploy quickly and be up and running in days. With its native support for Active Directory®, Azure® AD and Microsoft 365®, DigitalPersona enables you to easily integrate with your existing IT infrastructure using current IT tools and resources and achieve staffing flexibility and lower up-front and ongoing overhead costs — all while gaining peace of mind with a future-proof solution that scales with growing business needs, security requirements and industry regulations.

	HID DIGITALPERSONA
	FEATURES
Centralized Management	Active Directory – Set security policies for domain users and computers using Group Policy Objects Azure Active Directory – Set DigitalPersona security policies for domain users and computers
Web Administration Console	Web based user and authenticator management console
Multi-factor Authentication for Windows Logon	**AUTHENTICATION FACTORS** **Something you KNOW:** Windows Password, PIN as user knowledge authenticators **Something you ARE:** Fingerprint, Face Recognition biometrics as user inherent authenticators **Something you HAVE:** One Time Password (OTP) tokens; Smart credentials (Smart Cards and/or Security Keys (USB-A, USB-C, NFC), such as HID Crescendo®) with support for FIDO2, PKI, OATH; Physical Access (PACS) credentials (Contactless Access Cards, Contactless Writeable Cards, Mobile ID); Bluetooth Devices (mobile, watch, headphones) as user possession authenticators
Fast Kiosk Access	Shared-User Workstation ("Kiosk") Logon Control: Enforce advanced authentication policies for shared workstations (such as walk-up kiosks) where people use their individual credentials to unlock Windows and log into applications. Support for multiple kiosks and share workstation environments.
Self-Service Password Recovery	User password recovery via question challenge at Windows logon or web based self-service portal. Questions may be uniquely created by users or predetermined by administrator.
Identity Provider Federation	Identity Provider (IdP) supports WS-FED and OpenID Connect to Federate to applications such as Azure AD for Microsoft 365, Salesforce, SharePoint, and ADFS.
	CLIENTS & COMPONENTS
DigitalPersona Client	Connects to DigitalPersona server for Windows Login, enrollment, authentication, and policy enforcement
DigitalPersona Console with Attended Enrollment	Provides user enrollment or attended enrollment for both desktop and WEB tools
DigitalPersona RADIUS Plugin	RADIUS Plugin for Microsoft Network Policy Server (NPS) to provide 2FA for remote access
DigitalPersona ADFS Extension	Enables Multi-factor authentication capabilities for users that are logging on using Microsoft Active Directory Federation Services (ADFS)
	TECHNICAL SPECIFICATIONS
Client Software Operating Systems	Windows 11, Windows 10, Windows 8.1 (desktop mode), Windows Server 2016, 2019, 2022
Server Software Operating System	Windows Server 2022, 2019, 2016, and 2012 R2
VDI (Virtual Desktop Infrastructure)	RDP, ICA (Citrix), VMWare Horizon, VMWare Blast. NOTE: USB Virtualization and Authenticator Protocols vary by VDI product.

HID
hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800 | Latin America: +52 55 9171 1108
For more global phone numbers click here