Kensington®

VeriMark™ Fingerprint and Security Keys

Your Trusted Partner in Multi-Factor Authentication and Cybersecurity

Secure Access Without the Hassle

Fingerprint keys and NFC security keys are transforming the way we protect our digital world. Fingerprint keys offer passwordless, fast, reliable authentication by using unique biometric data making unauthorized access nearly impossible. NFC security keys add another layer of convenience and flexibility, especially for people who use both PCs and mobile devices. They're simple to use and are often more budget-friendly than biometric options. Together, these tools deliver strong, multi-factor protection that's easy to use, highly secure, and designed to keep sensitive information safe without slowing you down.

Key Questions

- What is the **key objective** in the use case?
- What devices or **browsers** need to be supported?
- Is **Windows Hello** or **Windows Hello for Business** or web authentication being utilized?
- Are users accessing **single** or **multiple** devices?
- Will **multiple** users access the **same device** at different times in a day?
- What **services** are being used?

Industry Trends and Research Insights

Current Landscape of Device Security

Kensington sponsored a study, conducted by independent market research specialist Vanson Bourne, of 1,000 senior IT decision-makers responsible for their organization's physical hardware security. One key finding was that unauthorized access to company data on devices is the top concern for 43% of respondents, followed by 19% who worry about sensitive data loss due to insecure home networks. Organizations are increasingly turning to multi-factor authentication (MFA) as a primary defense, with 30% of respondents identifying biometric or multi-factor authentication as critical for mitigating security threats.

Adoption of Biometric Authentication

A growing number of organizations recognize the value of biometric security solutions. According to our market research, 71% of responding organizations currently use fingerprint and/or security keys for two-factor authentication (2FA), while an additional 26% plan to implement these measures in the near future. Kensington's VeriMark™ lineup exemplifies cutting-edge biometric security, combining passwordless convenience with enterprise-grade protection. As a leader in securing the modern workplace, Kensington delivers TAA and GDPR compliant solutions that integrate into existing infrastructures, enabling organizations to address evolving cybersecurity threats effectively.

Source: Vanson Bourne, Device Security Research, October-November 2024.

Enhanced Security and Convenience with VeriMark™ IT 2.0 & VeriMark™ Desktop 2.0

Biometric keys like VeriMark™ IT 2.0 and VeriMark™ Desktop 2.0 seamlessly integrate with Windows Hello to deliver enhanced security and fast, convenient access. Fully compliant with Microsoft's Enhanced Sign-In Security (ESS) requirements, they combine advanced fingerprint recognition with the latest Windows authentication standards. VeriMark™ IT 2.0 and Desktop 2.0 ensure secure logins, encryption, and online protection, ideal for safeguarding sensitive data while streamlining access with a simple touch, making them a perfect fit for modern professionals and IT environments.

Strong Authentication

Biometric authentication uses the fingerprint which is unique to each user, making it a highly secure method of authentication.

Low Risk of Forgetting or Losing

Unlike passwords, users cannot forget or lose their biometric data.

Fast and Convenient Access

Authenticate in seconds with just a touch—no typing, no hassle.

Elevate Web Security with VeriMark™ Guard 2.1 through MFA

Fingerprint & security keys such as VeriMark™ Guard 2.1 are ideal for multi-factor authentication (MFA) when accessing web services that require enhanced protection. As a FIDO® certified solution, it combines biometric verification or PIN entry with hardware-based authentication to deliver strong, phishing-resistant security. Perfect for financial platforms, enterprise applications, or sensitive cloud accounts, VeriMark™ Guard 2.1 provides robust defense against credential theft while maintaining a fast, seamless user experience.

Highly Secure

Security keys use strong cryptographic authentication that is extremely difficult to duplicate or manipulate, making them resistant to phishing and social-engineering attacks. As FIDO2, U2F, and CTAP2.1 certified devices, they support modern, hardware-based security standards that help organizations meet strict regulatory requirements such as HIPAA and PCI DSS.

Easy to Use

Security keys are simple to use and require minimal setup, making them a convenient option for users.

Tap Into Enterprise Grade Security Without Passwords

The VeriMark™ NFC+ security key offers a simple yet powerful way to secure access across devices. They combine wireless convenience with robust encryption, allowing users to authenticate by simply tapping the key when inserted, or by tapping the key against a NFC reader. This keys eliminate the need for biometric enrollment, making them perfect for shared workstations or quick setups. With phishing-resistant technology and FIDO® certification, they deliver enterprise-grade security at a cost-effective price point, ensuring both usability and compliance.

Windows Hello Integration

VeriMark™ Access enables fast, password-free Windows sign-ins with a simple plug-and-play fingerprint key setup. When the key isn't available, the VeriMark™ Companion mobile app serves as a secure backup, generating a single-use code to ensure uninterrupted access. The solution also supports multi-user environments requiring quick and seamless user switching.

FIDO2 Capabilities

Certified for FIDO2 Level 2 and supporting CTAP2.1, these keys work across major platforms and browsers, including Windows, macOS, iOS, and Android. This key provides a scalable, compliant solution for enterprises embracing passwordless security.

Security Where, When, and How You Need It

Enterprise Deployment

VeriMark™ products are built for scalable enterprise deployment, offering a simple, cost-effective way to implement passwordless authentication. With broad compatibility across operating systems, browsers, and identity platforms, VeriMark™ products integrate seamlessly into existing IT environments. They support centralized management, meet FIDO2 and industry compliance standards, and provide phishing-resistant security without adding complexity.

Supports GDPR and TAA Compliant

Can be used to support cybersecurity measures consistent with (but not limited to) such privacy laws and regulations as GDPR, BIPA, and CCPA. Ready for use in U.S. Federal Government institutions and organizations.

Compatibility

VeriMark™ fingerprint and security keys are designed for broad compatibility, delivering secure, passwordless authentication across multiple platforms and services. This cross-platform functionality makes VeriMark™ an ideal solution for enterprises and individuals seeking strong, phishing-resistant security without sacrificing convenience.

Core Strengths of Fingerprint Security Keys

Biometric Access Control

The standout benefit is that possession of the key alone is not enough, the user's fingerprint must match. This dramatically reduces the risk in case the key is lost or stolen. Only the registered can activate the key's cryptographic response.

Integrated MFA in One Device

A fingerprint key combines something you are (biometric verification) with something you have (a physical security device). In practice, this allows the fingerprint scan to serve as the user-verification step, eliminating the need for a separate PIN or password at login. This creates a streamlined sign-in experience where one action both unlocks the key and authenticate while still enforcing multiple strong authentication factors.

User Convenience and Speed

For many, using a fingerprint is quicker and more convenient than typing passwords or grabbing a phone for an OTP code. With a well-designed key, the fingerprint scan is almost instantaneous.

Visual/Tactile Feedback

Biometric keys often give a bit of feedback (like an LED indicator) when a fingerprint is accepted, which can be confidence-inspiring. Knowing that the key actively verified you adds a sense of security. .

Top Benefits of VeriMark™ Fingerprint Keys

Biometric Security: Only registered users can access.

Fast Login: Touch and go—no typing required.

Phishing Resistant: Hardware-based authentication.

Portable: Use across multiple devices.

Regulatory: Supports GDPR and is TAA compliant

Core Strengths of USB NFC Security Keys

Cross-Device Compatibility

The big benefit of NFC-enabled keys is that they work with both PCs and mobile devices seamlessly. You can plug the key into standard USB ports and tap it on phones or tablets via NFC to authenticate wirelessly.

Ease of Use on Mobile

Using a security key on a phone can be tricky if the phone has no USB port available or has a case on it, but NFC solves that. Tapping the key on the phone is quick and intuitive and communicates over a very short range (within a few centimeters), which is convenient and secure (difficult to intercept).

Great for Shared or Rotating Users

NFC keys don't store fingerprints or require individual biometric setup, making them perfect for environments where multiple people need access, such as frontline teams, student labs, or manufacturing floors.

Strong Security

NFC keys maintain the same high level of cryptographic security as other hardware keys. NFC itself is designed for close-range communication, which greatly limits any risk of eavesdropping (an attacker would have to be physically inches away during use).

Top Benefits of VeriMark™ NFC+ Security Keys

Dual Interface: Works with both USB and NFC for flexible device access.

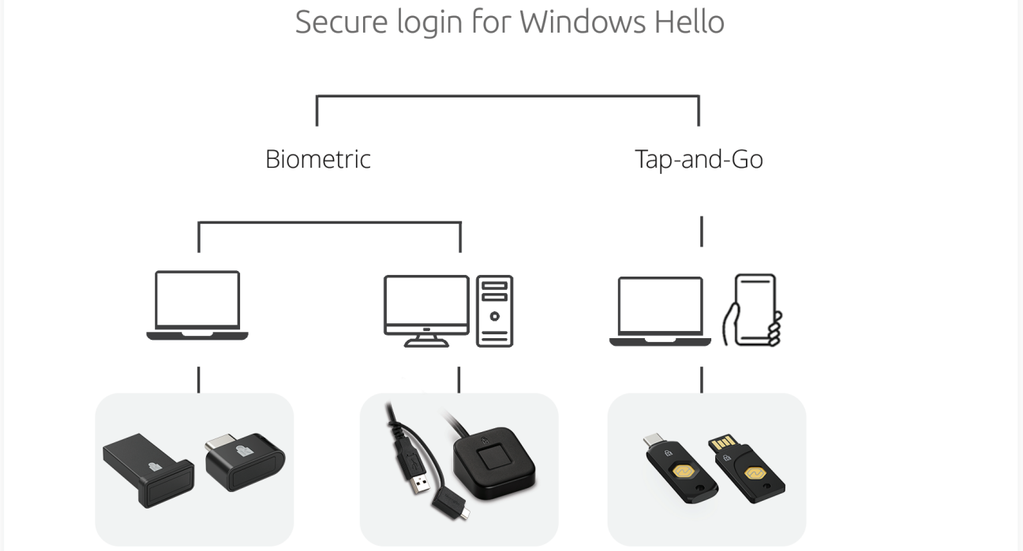
Phishing-Resistant Security: Hardware-based protection against phishing and credential theft.

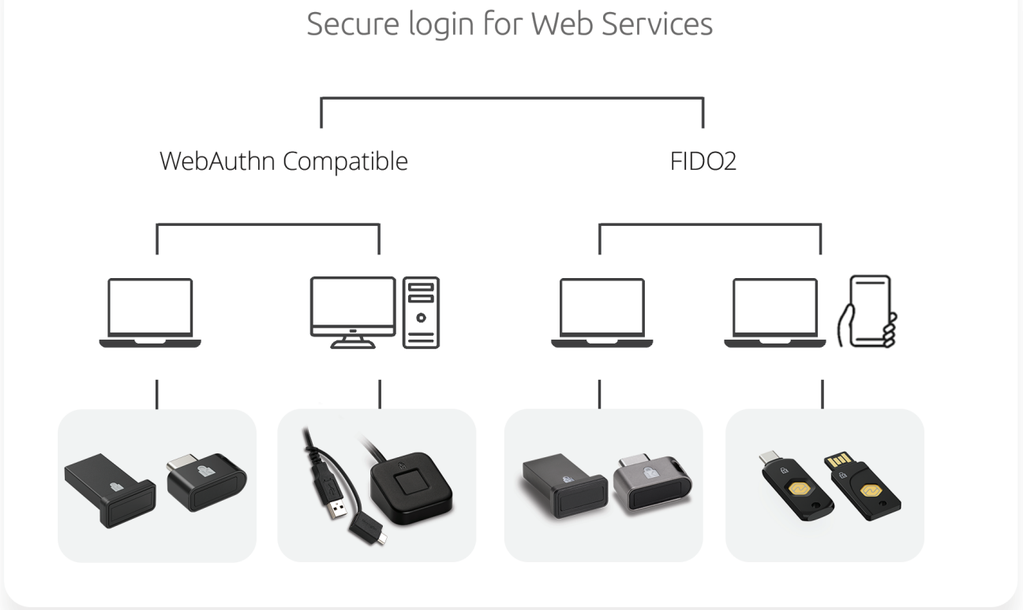
FIDO2 Level 2 Certified: Meets top industry standards for passwordless authentication and supports CTAP2.1.

Cross-Platform: Compatible with Windows, macOS, Android, iOS, and major services major services and browsers.

No Biometric Setup Needed: Quick to deploy—no fingerprint registration required.

	 **VeriMark™ IT 2.0 Fingerprint Key**	 **VeriMark™ Desktop 2.0 Fingerprint Key**	 **VeriMark™ Guard 2.1 Fingerprint Security Key**	 **VeriMark™ NFC+ Security Key**
Windows Hello	Windows Hello for Business	Windows Hello for Business	Not Supported	Not natively supported but can gain access through software (VeriMark™ Access) + Companion mobile App
Microsoft Enhanced Sign-in Security	Supported through Windows 11	Supported through Windows 11	Not Supported	Not Supported
FIDO2 & FIDO U2F	Not Supported	Not Supported	FIDO2 Level 1	FIDO2 Level 2
CTAP	Not Supported	Not Supported	Supports CTAP2.1 and backwards compatible to CTAP2.0	Supports CTAP2.1 and backwards compatible to CTAP2.0
Device				
Operating System				
Google, Amazon, Apple, and Microsoft Services		Microsoft Services	aws	
Web Services			okta	
Password Managers	DASHLANE	1Password	LastPass	NordPass





	 **VeriMark™ IT 2.0 Fingerprint Key**	 **VeriMark™ Desktop 2.0 Fingerprint Key**	 **VeriMark™ Guard 2.1 Fingerprint Security Key**	 **VeriMark™ NFC+ Security Key**
Item #	USB-C® : K64705WW USB-A : K64740WW	K64741WW	USB-C® : K65051WW USB-A : K65050WW	USB-C® : K64739WW USB-A : K64738WW
Certified For	Windows Hello Microsoft Enhanced Sign-In Security (ESS)	Windows Hello Microsoft Enhanced Sign-In Security (ESS)	FIDO CERTIFIED U2F L1 FIDO CERTIFIED FIDO2 L1	FIDO CERTIFIED U2F L2 FIDO CERTIFIED FIDO2 L2
Operating System				
Key Type				
Connection Type	USB-C® or USB-A	USB-A with USB-C® Adapter	USB-C® or USB-A	USB-C® or USB-A and NFC
Windows Hello	Supported	Supported	Not Supported	Not natively supported but can gain access through software (VeriMark™ Access)
FIDO	WebAuthn compatible	WebAuthn compatible	FIDO U2F and FIDO2 Level 1 Certified	FIDO U2F and FIDO2 Level 2 Certified
CTAP	N/A	N/A	Supports CTAP2.1 Protocol	Supports CTAP2.1 Protocol
Passkey	Compatible through biometrics	Compatible through biometrics	Compatible through biometrics	Compatible through NFC or Tap-and-Go
Fingerprint Authentification Type	Match-in-Sensor™	Match-in-Sensor™	Match-in-Sensor™	N/A
Data Score	Fingerprint Template Data in Key	Fingerprint Template Data in Key	Fingerprint Template Data in Key	N/A
False Rejection Rate	2%	2%	2%	N/A
False Acceptance Rate	0.001%	0.001%	0.001%	N/A
Readability	365 Degrees	365 Degrees	365 Degrees	N/A

The VeriMark™ NFC+ USB-C® Security Key is designed to strengthen digital security across web-based services. This NFC-enabled USB-C® security key is certified for FIDO2 Level 2 and offers secure, convenient, cross-platform authentication for both consumers and enterprise users. By eliminating password vulnerabilities with hardware-based MFA, it provides enterprise-grade protection against phishing and identity theft.

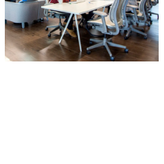
- FIDO2 Level 2 Certified Security
- FIDO CTAP2.1 Protocol Support
- USB-C® + NFC Dual Interface
- Simplicity and Complementary Software
- Cross-Platform Compatibility
- Compact & Portable
- IP68 Rated & Crush Resistant

Also available

Learn more by visiting
kensington.com/solutions/product-category/why-biometrics/

Fingerprint Keys – Ideal Use Cases & Purposes

Fingerprint keys combine biometric authentication with hardware-based security. They are best suited for environments where individual identity assurance is critical.



Healthcare

- Secure access to patient records (HIPAA compliance).
- Prevent unauthorized access to medical devices or terminals.
- Biometric login for clinicians using shared workstations.

Finance & Banking

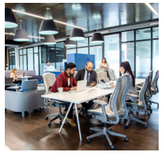
- Secure access to trading platforms or financial dashboards.
- Prevent credential theft in high-risk environments.
- Meet regulatory requirements (e.g., PCI-DSS, GDPR).

Government & Public Sector

- Used in federal institutions for biometric MFA.
- Supports FIDO2 and Windows Hello for Business.
- Ideal for agencies requiring TAA-compliant hardware.

Education

- Teachers and staff use fingerprint keys for secure login.
- Prevents unauthorized access in shared computer labs

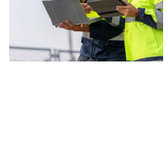


Enterprise IT

- Used for privileged access management.
- Reduces helpdesk burden from password resets.
- Supports audit trails and centralized access control.

NFC Keys – Ideal Use Cases & Purposes

NFC keys offer tap-and-go authentication and are ideal for mobile-first, multi-user, or consumer-facing environments.



Retail & Point-of-Sale

- Tap-to-authenticate for POS terminals.
- Quick switching between staff accounts.
- Prevent unauthorized transactions

Transportation & Logistics

- Drivers use NFC keys to access route planning tools.
- Secure login to fleet management systems.
- Ideal for rugged environments (IP68 waterproof rating).

Education

- Students tap to log into shared devices.
- IT admins manage access without needing biometric enrollment.

Consumer & SMB

- Passwordless login for personal devices.
- Easy setup for non-technical users.
- Compatible with Apple ID, Google, Microsoft, and more.

Public Sector - Field Work

- Tap-and-go login for mobile workers.
- No need for fingerprint enrollment or PIN memorization.
- Works offline and across platforms.

FOR MORE INFORMATION CONTACT: 1-855-692-0054 | sales@kensington.com

Kensington
The Professionals' Choice™