

Kensington®

VeriMark™ Fingerprint- und Security Keys

Ihr zuverlässiger Partner für Multi-Faktor-
Authentifizierung und Cybersicherheit



Sicherer Zugang ohne Aufwand

Fingerprint Keys und NFC Security Key verändern die Art und Weise, wie wir unsere digitale Welt schützen. Fingerprint Keys bieten passwortlose, schnelle und zuverlässige Authentifizierung durch die Verwendung einzigartiger biometrischer Daten, die unbefugten Zugriff nahezu unmöglich machen. NFC Security Keys fügen eine weitere Ebene von Komfort und Flexibilität hinzu, insbesondere für Personen, die sowohl PCs als auch mobile Geräte verwenden. Sie sind einfach zu bedienen und oft preiswerter als biometrische Keys. Zusammen bieten diese Tools starken, mehrstufigen Schutz, der einfach zu bedienen, hochsicher und darauf ausgelegt ist, sensible Informationen sicher zu halten, ohne Sie zu verlangsamen.

Wichtige Fragen

- Was ist das **Hauptziel** im Anwendungsfall?
- Welche Geräte oder **Browsersversionen** müssen unterstützt werden?
- Wird **Windows Hello** oder **Windows Hello for Business** oder Web-Authentifizierung verwendet?
- Greifen die Benutzer auf **einzelne** oder **mehrere** Geräte zu?
- Werden **mehrere** Benutzer zu unterschiedlichen Zeiten am Tag auf dasselbe **Gerät** zugreifen?
- Welche **Dienste** werden genutzt?





Branchentrends und Forschungsergebniss

Aktuelle Landschaft der Gerätesicherheit

Kensington unterstützte eine Studie, die von dem unabhängigen Marktforschungsspezialisten Vanson Bourne durchgeführt wurde, mit 1.000 leitenden IT-Entscheidungssträgern, die für die physische Hardwaresicherheit ihrer Organisation verantwortlich sind. Eine wichtige Erkenntnis war, dass unbefugter Zugriff auf Unternehmensdaten auf Geräten die größte Sorge für 43 % der Befragten darstellt, gefolgt von 19 %, die sich um den Verlust sensibler Daten aufgrund unsicherer Heimnetzwerke sorgen. Organisationen wenden sich zunehmend der Multi-Faktor- Authentifizierung (MFA) als primärer Verteidigung zu, wobei 30 % der Befragten biometrische oder Multi-Faktor- Authentifizierung als entscheidend für die Minderung von Sicherheitsbedrohungen identifizieren.

Einsatz biometrischer Authentifizierung

Eine wachsende Zahl von Organisationen erkennt den Wert biometrischer Sicherheitslösungen. Laut unserer Marktforschung verwenden 71 % der befragten Organisationen derzeit Fingerprint und/oder Security Key für die Zwei-Faktor-Authentifizierung (2FA), während weitere 26 % planen, diese Maßnahmen in naher Zukunft umzusetzen. Kensingtons VeriMark™ Produktlinie steht für modernste biometrische Sicherheit und vereint passwortlosen Komfort mit Schutz auf Enterprise-Niveau. Als führender Anbieter für Workplace-Security liefert Kensington TAA- und DSGVO-konforme Lösungen, die sich reibungslos in bestehende Infrastrukturen integrieren und Unternehmen helfen, auf sich wandelnde Cybersecurity-Bedrohungen effektiv zu reagieren.

Quelle: Vanson Bourne , Gerätesicherheitsforschung, Oktober-November 2024.

Erhöhte Sicherheit und mehr Komfort mit VeriMark™ IT 2.0 & VeriMark™ Desktop 2.0



Biometrische Security Keys wie VeriMark™ IT 2.0 und VeriMark™ Desktop 2.0 integrieren sich nahtlos mit Windows Hello, um verbesserte Sicherheit und schnellen, bequemen Zugang zu bieten. Vollständig konform mit Microsofts Anforderungen an die verbesserte Anmelde-Sicherheit (ESS) kombinieren sie fortschrittliche Fingerabdruckerennung mit den neuesten Windows-Authentifizierungsstandards. VeriMark™ IT 2.0 und Desktop 2.0 gewährleisten sichere Anmeldungen, Verschlüsselung und Online- Schutz, ideal zum Schutz sensibler Daten, während der Zugang mit einem einfachen Touch vereinfacht wird, was sie perfekt für moderne Fachkräfte und IT-Umgebungen macht.

Starke Authentifizierung

Biometrische Authentifizierung verwendet den Fingerabdruck, der für jeden Benutzer einzigartig ist, was sie zu einer hochsicheren Methode der Authentifizierung macht.

Geringes Risiko des Vergessens oder Verlusts

Im Gegensatz zu Passwörtern können Benutzer ihre biometrischen Daten nicht vergessen oder verlieren.

Schneller und bequemer Zugang

Authentifizieren Sie sich in Sekunden mit nur einem Touch – kein Tippen, kein Aufwand.

Web-Sicherheit mit VeriMark™ Guard 2.1 durch MFA



Fingerprint- und Security Key wie VeriMark™ Guard 2.1 sind ideal für die Multi-Faktor-Authentifizierung (MFA) beim Zugriff auf Webdienste, die einen verbesserten Schutz erfordern. Als FIDO®-zertifizierte Lösung kombiniert sie biometrische Verifizierung oder PIN-Eingabe mit hardwarebasierter Authentifizierung, um starke, phishing-resistente Sicherheit zu bieten. Ideal für Finanzplattformen, Unternehmensanwendungen oder sensible Cloud-Konten bietet VeriMark™ Guard 2.1 robusten Schutz gegen Identitätsdiebstahl, während eine schnelle, nahtlose Benutzererfahrung aufrechterhalten wird.

Hochsicher

Security Keys verwenden starke kryptografische Authentifizierung, die extrem schwer zu duplizieren oder zu manipulieren ist, wodurch sie gegen Phishing- und Social-Engineering-Angriffe resistent sind. Als FIDO2-, U2F- und CTAP2.1-zertifizierte Geräte unterstützen sie moderne, hardwarebasierte Sicherheitsstandards, die Organisationen helfen, strenge regulatorische Anforderungen wie HIPAA und PCI DSS zu erfüllen.

Einfacher Austausch

Security Keys sind einfach zu bedienen und erfordern minimale Einrichtung, was sie zu einer bequemen Option für Benutzer macht.

Nutzen Sie Unternehmenssicherheit ohne Passwörter



Der VeriMark™ NFC+ Security Key bietet eine einfache, aber leistungsstarke Möglichkeit, den Zugriff über Geräte hinweg zu sichern. Sie kombinieren kabellosen Komfort mit robuster Verschlüsselung, sodass Benutzer sich authentifizieren können, indem sie einfach den Schlüssel einstecken oder den Schlüssel gegen einen NFC-Leser halten. Diese Keys beseitigen die Notwendigkeit einer biometrischen Registrierung, was sie perfekt für gemeinsam genutzte Arbeitsstationen oder schnelle Setups macht. Mit phishing-resistenter Technologie und FIDO®-Zertifizierung bieten sie Unternehmenssicherheit zu einem kosteneffektiven Preis, der sowohl Benutzerfreundlichkeit als auch Compliance gewährleistet.

Windows Hello-Integration

VeriMark™ Access ermöglicht schnelle, passwortlose Windows-Anmeldungen – mit einer einfachen Plug-and-Play-Einrichtung per Fingerprint-Key. Wenn der Security Key nicht verfügbar ist, dient die VeriMark™ Companion Mobile App als sichere Sicherung, die einen Einmalcode generiert, um einen unterbrechungsfreien Zugriff zu gewährleisten. Die Lösung unterstützt auch Umgebungen mit mehreren Benutzern, die schnelles und nahtloses Benutzerwechseln erfordern.

FIDO2-Funktionen

Zertifiziert für FIDO2 Level 2 und unterstützt CTAP2.1, funktionieren diese Keys auf allen wichtigen Plattformen und Browsern, einschließlich Windows, macOS, iOS und Android. Dieser Schlüssel bietet eine skalierbare, konforme Lösung für Unternehmen, die passwortlose Sicherheit annehmen.

Sicherheit wo, wann und wie Sie sie brauchen



Unternehmenslösung

VeriMark™-Produkte sind für eine skalierbare Bereitstellung in Unternehmen konzipiert und bieten eine einfache, kostengünstige Möglichkeit zur Implementierung passwortloser Authentifizierung. Mit umfassender Kompatibilität über Betriebssysteme, Browser und Identitätsplattformen integrieren sich VeriMark™-Produkte nahtlos in bestehende IT-Umgebungen. Sie unterstützen das zentrale Management, erfüllen die FIDO2- und Branchenkonformitätsstandards und bieten phishing-resistente Sicherheit, ohne die Komplexität zu erhöhen.

Unterstützt GDPR

Unterstützt Cyber-Sicherheitsmaßnahmen im Einklang mit Datenschutzgesetzen und -verordnungen wie z. B. DS-GVO, BIPA und CCPA.

Kompatibilität

VeriMark™ Fingerprint und Security Key sind für umfassende Kompatibilität konzipiert und bieten sichere, passwortlose Authentifizierung über mehrere Plattformen und Dienste. Diese plattformübergreifende Funktionalität macht VeriMark™ zu einer idealen Lösung für Unternehmen und Einzelpersonen, die starke, phishing-resistente Sicherheit suchen, ohne auf Komfort zu verzichten.

Zentrale Stärken von Fingerprint Security Keys



Biometrische Zugangskontrolle

Der herausragende Vorteil ist, dass der Besitz des Schlüssels allein nicht ausreicht; der Fingerabdruck des Benutzers muss übereinstimmen. Dies verringert das Risiko erheblich, falls der Schlüssel verloren geht oder gestohlen wird. Nur die Registrierten können die kryptografische Antwort des Schlüssels aktivieren.

Integrierte MFA in Einem Gerät

Ein Fingerprint Key kombiniert etwas, das Sie sind (biometrische Verifizierung), mit etwas, das Sie haben (ein physisches Sicherheitsgerät). In der Praxis ermöglicht dies, dass der Fingerabdruckscan als Schritt zur Benutzerverifizierung dient, wodurch die Notwendigkeit eines separaten PINs oder Passworts beim Login entfällt. Dies schafft ein optimiertes Anmeldeerlebnis, bei dem eine Aktion sowohl den Key entsperrt als auch authentifiziert, während gleichzeitig mehrere starke Authentifizierungsfaktoren durchgesetzt werden.

Benutzerfreundlichkeit und Geschwindigkeit

Für viele ist die Verwendung eines Fingerabdrucks schneller und bequemer als das Eingeben von Passwörtern oder das Greifen nach einem Telefon für einen OTP-Code. Bei einem gut durchdachten Key erfolgt der Fingerabdruck-Scan nahezu verzögerungsfrei.

Visuelles/Taktile Feedback

Biometrische Keys geben oft ein wenig Feedback (wie eine LED-Anzeige), wenn ein Fingerabdruck akzeptiert wird, was Vertrauen schaffen kann. Zu wissen, dass der Key aktiv überprüft hat, gibt ein Gefühl von Sicherheit.

Top-Vorteile der VeriMark™ Fingerprint Keys

Biometrische Sicherheit: Nur registrierte Benutzer können darauf zugreifen.

Schnelle Anmeldung: Berühren und loslegen – keine Eingabe erforderlich.

Phishing-Resistent: Hardwarebasierte Authentifizierung.

Portabel: Über mehrere Geräte hinweg nutzbar.

Regulatorisch: Unterstützt die DSGVO und ist TAA- konform



Zentrale Stärken von USB NFC Security Keys



Geräteübergreifende Kompatibilität

Der große Vorteil von NFC-fähigen Keys ist, dass sie nahtlos mit PCs und mobilen Geräten funktionieren. Sie können den Key in Standard-USB-Ports einstecken und ihn über NFC auf Handys oder Tablets tippen, um kabellos zu authentifizieren.

Benutzerfreundlichkeit auf Mobilgeräten

Die Verwendung eines Security Key auf einem Telefon kann schwierig sein, wenn das Telefon keinen USB-Port hat oder eine Hülle trägt, aber NFC löst das Problem. Das Antippen des Schlüssels am Smartphone ist schnell und intuitiv. Die Kommunikation erfolgt über eine sehr kurze Distanz (wenige Zentimeter) – komfortabel in der Anwendung und besonders sicher, da sie kaum abzufangen ist.

Ideal für Geteilte oder Rotierende Benutzer

NFC Keys speichern keine Fingerabdrücke und erfordern keine individuelle biometrische Einrichtung, was sie perfekt für Umgebungen macht, in denen mehrere Personen Zugang benötigen, wie z.B. Frontteams, Studentenlabore, oder Produktionsstätten.

Starke Sicherheit

NFC Keys halten das gleiche hohe Niveau an kryptografischer Sicherheit wie andere Hardware-Schlüssel. NFC selbst ist für die Nahbereichskommunikation konzipiert, was das Risiko des Abhörens erheblich einschränkt (ein Angreifer müsste während der Nutzung physisch in der Nähe sein).

Top-Vorteile der VeriMark™ NFC+ Security Key

Duale Schnittstelle: Funktioniert sowohl mit USB als auch mit NFC für flexiblen Gerätezugriff.

Phishing-Resistente Sicherheit: Hardwarebasierter Schutz gegen Phishing und Diebstahl von Anmeldeinformationen.

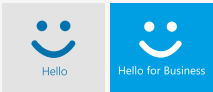
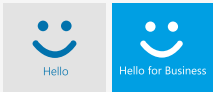
FIDO2 Level 2 Zertifiziert: Entspricht den höchsten Branchenstandards für passwortlose Authentifizierung und unterstützt CTAP2.1.

Plattformübergreifend: Kompatibel mit Windows, macOS, Android, iOS und wichtigen Diensten sowie Browsern.

Keine Biometrische Einrichtung Erforderlich: Schnell einsatzbereit – keine Fingerabdruckregistrierung erforderlich.



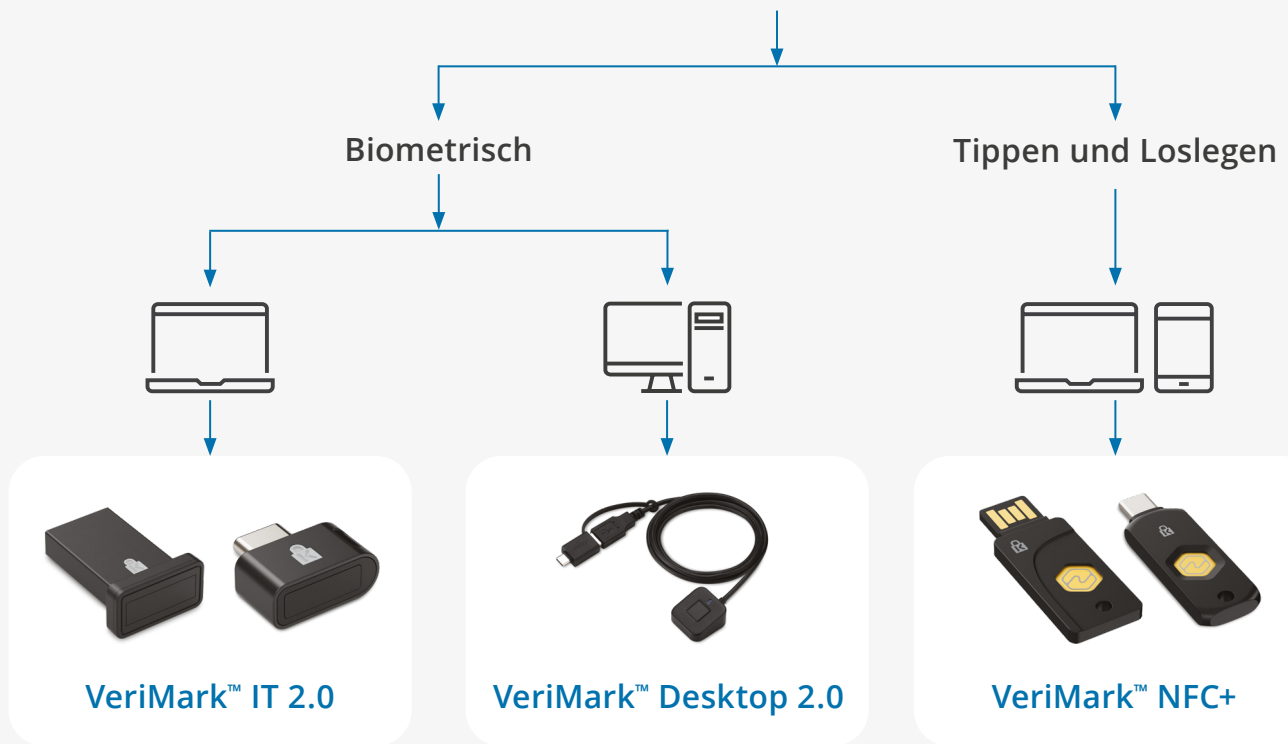


	VERIMARK™ IT 2.0 FINGERPRINT KEY	VERIMARK™ DESKTOP 2.0 FINGERPRINT KEY	VERIMARK™ GUARD 2.1 FINGERPRINT SECURITY KEY	VERIMARK™ NFC+ SECURITY KEY
Artikel #	USB-A - K64740WW USB-C® - K64705WW	K64741WW	USB-A - K65050WW USB-C® - K65051WW	USB-A - K64738WW USB-C® - K64739WW
Windows Hello			Nicht unterstützt	Nicht nativ unterstützt, kann jedoch über Software (VeriMark™ Access) Zugriff erhalten + Begleit-App
Microsoft Enhanced Sign-in Security (ESS)	Unterstützt durch Windows 11	Unterstützt durch Windows 11	Nicht unterstützt	Nicht unterstützt
FIDO2 & FIDO U2F	Nicht unterstützt WebAuthn-kompatibel	Nicht unterstützt WebAuthn-kompatibel		
CTAP	Nicht unterstützt	Nicht unterstützt	Unterstützt CTAP2.1 und ist abwärtskompatibel zu CTAP2.0	Unterstützt CTAP2.1 und ist abwärtskompatibel zu CTAP2.0
Gerät				
Betriebssystem				
Google, Amazon, Apple, und Microsoft- Dienste				
Webdienste				
Passwort Manager				

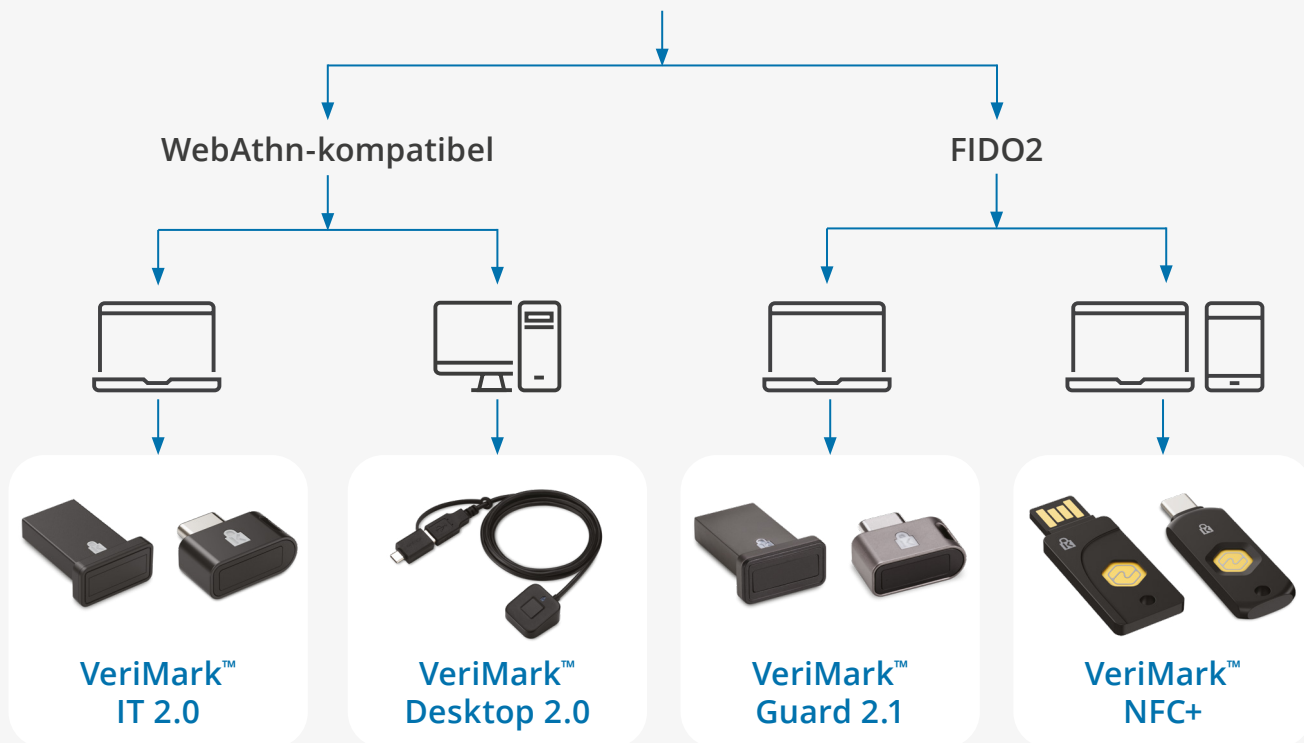


	VERIMARK™ IT 2.0 FINGERPRINT KEY	VERIMARK™ DESKTOP 2.0 FINGERPRINT KEY	VERIMARK™ GUARD 2.1 FINGERPRINT SECURITY KEY	VERIMARK™ NFC+ SECURITY KEY
Artikel #	USB-A - K64740WW USB-C® - K64705WW	K64741WW	USB-A - K65050WW USB-C® - K65051WW	USB-A - K64738WW USB-C® - K64739WW
Geeignet für	 	 	 	 
Schlüsseltyp				
Verbindungstyp	USB-C® oder USB-A	USB-A mit USB-C® Adapter	USB-C® oder USB-A	USB-A oder USB-C® und NFC
Passkey	Kompatibel über Biometrie	Kompatibel über Biometrie	Kompatibel über Biometrie	Kompatibel über NFC oder Tap-and-Go
Fingerprint- Authentifizierungstyp	Match-in-Sensor™	Match-in-Sensor™	Match-in-Sensor™	-
Datenpunktzahl	Fingerabdruck- Template lokal im Schlüssel gespeichert	Fingerabdruck- Template lokal im Schlüssel gespeichert	Fingerabdruck- Template lokal im Schlüssel gespeichert	-
False Rejection Rate (FRR)	2 %	2 %	2 %	-
False Acceptance Rate (FAR)	0,001 %	0,001 %	0,001 %	-
Lesbarkeit	365 Grad	365 Grad	365 Grad	-

Sicherer Login für Windows Hello



Sicherer Login für Webdienste





Der VeriMark™ NFC+ USB-C® Security Key wurde entwickelt, um die digitale Sicherheit bei webbasierten Diensten zu stärken. Dieser NFC-fähige USB-C® Security Key ist für FIDO2 Level 2 zertifiziert und bietet sichere, bequeme, plattformübergreifende Authentifizierung für Verbraucher und Unternehmensbenutzer. Durch die Eliminierung von Passwort-Schwachstellen mittels hardwarebasierter MFA bietet sie Schutz auf Enterprise-Niveau vor Phishing-Angriffen und Identitätsdiebstahl.

- FIDO2 Level 2 Zertifizierter Security Key
- FIDO CTAP2.1 Protokollunterstützung
- USB-C® + NFC Dual-Schnittstelle
- Einfachheit und ergänzende Software
- Plattformübergreifende Kompatibilität
- Kompakt & tragbar
- IP68 bewertet & stoßfest



Ebenfalls erhältlich -
USB-A



Jetzt mehr erfahren



Fingerprint Keys – Ideale Einsatzszenarien & Anwendungsbereiche

Fingerprint Keys kombinieren biometrische Authentifizierung mit hardwarebasierter Sicherheit. Sie sind am besten geeignet für Umgebungen, in denen die individuelle Identitätsverifizierung entscheidend ist.



Gesundheitswesen

- Sicherer Zugang zu Patientenakten (HIPA A-Konformität).
- Verhindert unbefugten Zugriff auf medizinische Geräte oder Terminals.
- Biometrische Anmeldung für Kliniker, die gemeinsam genutzte Arbeitsstationen verwenden.



Finanzen & Banken

- Sicherer Zugang zu Handelsplattformen oder Finanz-Dashboards.
- Verhindert den Diebstahl von Anmeldeinformationen in risikobehafteten Umgebungen.
- Erfüllt regulatorische Anforderungen (z. B. PCI-DSS, DSGVO).



Regierung & Öffentlicher Sektor

- Wird in Bundesinstitutionen für biometrische MFA verwendet.
- Unterstützt FIDO2 und Windows Hello for Business



Bildung

- Lehrer und Mitarbeiter verwenden Fingerprint Keys für eine sichere Anmeldung.
- Verhindert unbefugten Zugriff in gemeinsam genutzten Computerlaboren.



Enterprise IT

- Wird für das Management privilegierter Zugriffe verwendet.
- Reduziert die Belastung des Helpdesks durch Passwortzurücksetzungen.
- Unterstützt Prüfprotokolle und zentralisierte Zugriffskontrolle.



NFC Keys – Ideale Einsatzszenarien & Anwendungsbereiche

NFC keys ermöglichen eine einfache Tap-and-Go-Authentifizierung und eignen sich ideal für Mobile-First-Umgebungen, Multi-User-Szenarien sowie kundenorientierte Einsatzbereiche.



Retail- & POS-Umgebungen

- Tippen zur Authentifizierung für POS-Terminals.
- Schnelles Wechseln zwischen Mitarbeiterkonten.
- Unbefugte Transaktionen verhindern



Transport & Logistik

- Fahrer nutzen NFC-Keys, um auf Tools zur Routenplanung zuzugreifen.
- Sicherer Login zu Flottenmanagementsystemen.
- Ideal für raue Umgebungen (IP68 wasserdicht).



Bildung

- Schüler tippen, um sich an gemeinsamen Geräten anzumelden.
- IT-Administratoren verwalten den Zugriff, ohne biometrische Registrierung zu benötigen.



Endkunden & Kleine Sowie Mittelständische Unternehmen

- Passwortloser Login für persönliche Geräte.
- Einfache Einrichtung für nicht-technische Benutzer.
- Kompatibel mit Apple ID, Google, Microsoft und mehr.



Behörden & Öffentlicher Sektor – Außendienst

- Tippen und loslegen für mobile Mitarbeiter.
- Keine Notwendigkeit für Fingerabdruckregistrierung oder PIN-Merkwürdigkeit.
- Funktioniert offline und plattformübergreifend.



Alle Spezifikationen können ohne vorherige Ankündigung geändert werden. Kensington und der Name ACCO und das Design sind eingetragene Marken von ACCO Brands. Kensington The Professionals' Choice ist eine Marke von ACCO Brands. Alle anderen eingetragenen und nicht eingetragenen Markenzeichen sind Eigentum der jeweiligen Inhaber. Thunderbolt sowie das Thunderbolt-Logo selbst sind Marken der Intel Corporation in den USA und/oder anderen Ländern. © 2026 Kensington Computer Products Group, eine Abteilung von ACCO Brands. Alle Rechte vorbehalten. CBT54577DE

Kensington
The Professionals' Choice™

WEITERE INFORMATIONEN ERHALTEN SIE UNTER: +49 (0)800 - 72 38 49 | sales.dach@kensington.com