HIRSCH

SOLUTIONS BRIEF



LÖSUNGEN FÜR DIE

MULTI-FAKTOR-AUTHENTIFIZIERUNG

Mit Hirsch bleiben Organisationen vertrauenswürdig und bieten Mitarbeitenden wie Kunden ein hervorragendes Erlebnis – ohne sich um Cybersicherheit sorgen zu müssen.

GRUNDLAGEN

Was ist Multi-Faktor-Authentifizierung?

Bei der Multi-Faktor-Authentifizierung (MFA) muss der Benutzer zwei oder mehr Verifizierungsfaktoren nachweisen, um Zugriff auf eine Ressource wie eine Anwendung, ein Online-Konto oder ein virtuelles privates Netzwerk (VPN) zu erhalten.

MFA ist ein zentraler Bestandteil einer starken Richtlinie für das Identitäts- und Zugriffsmanagement.

ZWEI ODER MEHR FAKTOREN

1. **Etwas, das Sie wissen**
   Passwort, Passphrase oder persönliche Identifikationsnummer (PIN)
2. **Etwas, das Sie besitzen**
   Sicherheitsschlüssel oder Smartcard
3. **Etwas, das Sie sind**
   Biometrisches Merkmal wie ein Fingerabdruck

BEISPIEL: ANMELDUNG MIT DREI FAKTOREN

SCHRITT 1
Benutzername und Passwort
werden eingegeben

→

SCHRITT 2
PIN aus der Smartphone-App
wird eingegeben

→

SCHRITT 3
Fingerabdruck
wird verifiziert

01 Warum brauchen Sie Multi-Faktor-Authentifizierung?

Mehr als Benutzername und Passwort

Statt nur Benutzername und Passwort abzufragen, verlangt MFA zusätzliche Verifizierungsfaktoren und senkt so die Wahrscheinlichkeit eines Cyberangriffs. Dazu kommen weitere Vorteile:

Schutz vor Datenschutz-verletzungen

Der wichtigste Grund für MFA: Ihre geschäftskritischen Informationen werden vor möglichen Datenschutzverletzungen geschützt.

Wird ein Benutzer nur per Passwort authentifiziert, bleibt ein unsicherer Angriffsweg offen. Ist das Passwort schwach oder wurde es an anderer Stelle offengelegt – woher wissen Sie dann, ob sich tatsächlich der Benutzer mit diesen Anmeldedaten anmeldet und nicht ein Angreifer?

Mit einer zweiten Form der Authentifizierung erhöhen Sie die Sicherheit, denn ein Angreifer kann den zusätzlichen Faktor nicht ohne Weiteres beschaffen oder duplizieren.

39 %

der analysierten Datenschutzverletzungen enthielten an irgendeiner Stelle der Angriffskette den Missbrauch von Zugangsdaten.

18 %

der Unternehmen in Deutschland waren von Angriffen auf Passwörter betroffen.

160–206

Mrd. €

Schaden durch Cyberangriffe für die deutsche Wirtschaft – 76 % des Gesamtschadens.

Quellen: Verizon 2026 Data Breach Investigations Report (DBIR); Bitkom, Wirtschaftsschutz-Studie 2026 (n = 1.003 Unternehmen)

Schutz Ihrer digitalen Werte

MFA ist einer der kosteneffizientesten Mechanismen, mit denen Unternehmen ihre digitalen Werte schützen können. In einer Welt, in der Angriffe zum Abgreifen von Anmeldedaten zunehmen, wird eine bessere Authentifizierung von einer wünschenswerten zu einer absolut unverzichtbaren Technologie.

Ein starkes Passwort ist für die Cybersicherheit unerlässlich, aber nur ein Teil des Puzzles. Wenn Sie MFA für alle Konten aktivieren, hat Ihr Passwort immer eine Absicherung, die Sie schützt.

Gestohlene Anmeldedaten vermeiden

Passwörter sind wohl die gängigste Methode, die eigene Online-Identität nachzuweisen – bieten aber nur sehr wenig Schutz. Ist ein Passwort erst einmal gestohlen, können Hacker mit Ihren Anmeldedaten auf Anwendungen und Geschäftssysteme zugreifen, andere Zugangskontrollen umgehen und erheblichen Schaden anrichten.

Ein MFA-Tool entschärft die Folgen übermäßiger Passwort-Wiederverwendung, weil Benutzer zur Authentifizierung mehr als nur ein Passwort benötigen. MFA-Methoden wie FIDO-Sicherheitsschlüssel und Smartcards bzw. Tokens erhöhen die Sicherheit und halten potenzielle Bedrohungen fern.

Sicherheit und Gelassenheit

Online-Konten und -Dienste gehören in vieler Hinsicht unvermeidlich zum modernen Leben. Sie sind bequem – wir halten über soziale Medien Kontakt zu Freunden oder kaufen in unseren Lieblingsgeschäften ein. Die Kehrseite: Cyberkriminelle erhalten mehr Gelegenheiten, Ihre Daten zu stehlen.

Schlimmer noch: Wird eines Ihrer Konten kompromittiert, sind auch die anderen gefährdet. Verschafft sich ein Hacker beispielsweise Zugang zu Ihren sozialen Medien, kann er Informationen stehlen, mit denen er weitere Konten angreift.

Multi-Faktor-Authentifizierung gibt Ihnen Sicherheit: Selbst wenn Sie Opfer eines Angriffs werden, schützt Sie eine zusätzliche Sicherheitsebene.

Den sich wandelnden Cyber-bedrohungen voraus

Cyberbedrohungen werden immer ausgefeilter. Cyberkriminelle nutzen inzwischen raffinierte Phishing- und Smishing-Techniken, auf die selbst versierte Nutzer hereinfallen. Um cybersicher zu bleiben, brauchen Sie jede verfügbare Verteidigungslinie.

Mit aktivierter MFA bleiben Sie diesen Bedrohungen einen Schritt voraus. Angenommen, Sie werden Opfer eines raffinierten Phishing-Angriffs und das Passwort für ein wichtiges Konto wird gestohlen: MFA schützt Sie, denn der Cyberkriminelle bräuchte zusätzlich Zugriff auf ein weiteres Gerät – etwa Ihr Mobiltelefon – oder eine weitere Information, um sich anzumelden.

Mit Multi-Faktor-Authentifizierung haben Sie ein weiteres Mittel gegen Cyberkriminelle, die beim Datendiebstahl immer geschickter vorgehen.

02 Anwendungsfälle für Multi-Faktor-Authentifizierung

Branchen mit hohem Risiko

Multi-Faktor-Authentifizierung ist für Unternehmen eine der wirksamsten Methoden, ihre Systeme und die Online-Konten ihrer Kunden vor Hacking, Spam, Datendiebstahl und mehr zu schützen.

Hier einige typische Anwendungsfälle in Branchen mit hohem Risiko, die von MFA in ihren Sicherheitsprotokollen profitieren:

REGULATORISCHE TREIBER FÜR MFA IN DEUTSCHLAND UND DER EU

Regelwerk	Gilt für	Bezug zur Authentifizierung
NIS-2-Umsetzungsgesetz (BSIG), in Kraft seit 6.12.2025	Besonders wichtige und wichtige Einrichtungen, u. a. Energie, Gesundheit, Finanzwesen, digitale Infrastruktur	§ 30 Abs. 2 Nr. 10 BSIG: Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung
DORA (EU) 2022/2554, anwendbar seit 17.1.2025	Finanzunternehmen in der EU, z. B. Banken, Versicherungen, Zahlungsinstitute	Richtlinien und Protokolle für starke Authentifizierungsmechanismen auf Basis anerkannter Standards und der IKT-Risikobewertung
PCI DSS v4.0.1 verbindlich seit 31.3.2025	Alle, die Kartenzahlungsdaten verarbeiten, speichern oder übertragen	Anforderung 8.4.2: MFA für jeden Zugriff auf die Karteninhaberdatenumgebung (CDE)
PSD2 Zahlungsdiensterichtlinie	Zahlungsdienstleister in der EU	Starke Kundenauthentifizierung mit mindestens zwei unabhängigen Faktoren beim Online-Banking und bei Online-Zahlungen
DSGVO	Alle, die personenbezogene Daten verarbeiten	Art. 32: technische und organisatorische Maßnahmen nach dem Stand der Technik; Art. 9: besonderer Schutz z. B. von Gesundheitsdaten

Stand: November 2026. Diese Übersicht dient der Orientierung und ersetzt keine Rechtsberatung.

Finanzwesen

Finanzinstitute wie Banken gehören zu den bevorzugten Zielen von Cyberangriffen. Banken müssen so viel Sicherheit wie möglich bieten, um Kundendaten zu schützen.

Verschafft sich ein Hacker Zugang zum Bankkonto einer Person, erbeutet er weit mehr als nur Geld: Er erhält auch Zugriff auf Kartendaten und persönliche Identitätsdaten – mit Identitätsdiebstählen, deren Aufklärung Jahre dauern kann.

Seit dem 17. Januar 2025 gilt in der gesamten EU der Digital Operational Resilience Act (DORA). Er verpflichtet Finanzunternehmen, Richtlinien und Protokolle für starke Authentifizierungsmechanismen umzusetzen – auf Basis anerkannter Standards und ihrer IKT-Risikobewertung.

Wer Kartenzahlungsdaten verarbeitet, speichert oder überträgt – auch Banken –, muss zudem den Payment Card Industry Data Security Standard (PCI DSS) einhalten. Seit dem 31. März 2025 verlangt PCI DSS v4.0.1 mit Anforderung 8.4.2 MFA für jeden Zugriff auf die Karteninhaberdatenumgebung – nicht mehr nur für Administratoren und Fernzugriffe.

Gegenüber Kunden schreibt die EU-Zahlungsdiensterichtlinie PSD2 beim Online-Banking und bei Online-Zahlungen bereits eine starke Kundenauthentifizierung mit mindestens zwei unabhängigen Faktoren vor. MFA ist damit im Finanzwesen keine Kür mehr, sondern Pflicht – und zugleich ein Baustein für das Vertrauen und die Loyalität, auf die Banken für langfristige Kundenbeziehungen angewiesen sind.

SO HILFT HIRSCH

- FIDO-Schlüssel als sicherer Authentifizierungsfaktor für den Zugriff auf Ihr Kryptowährungskonto über eine FIDO-fähige Anwendung
- Zutritt zum Gebäude mit Smartcard und kontaktlosem Leser
- Sicherer Zugang zur Bank mit einem Smartcard-Dienstausweis
- Sicherer Netzwerkzugriff auf Finanzinformationen und private Kundendaten mit Smartcard-Technologie

Gesundheitswesen

Mit dem erweiterten Datenzugriff steigt im Gesundheitswesen das Risiko von Datenschutzverletzungen. Portale und digitale Akten sind heute ein gängiger Weg, Befunde und Dokumente auszutauschen – und bieten Hackern mehr Gelegenheiten, Patienten- wie Anbieterkonten zu infiltrieren. Gesundheitsdaten lassen sich nicht wie eine gestohlene Kreditkartennummer sperren. Das macht Gesundheitseinrichtungen zu einem bevorzugten Ziel.

Gesundheitsdaten gehören nach Art. 9 DSGVO zu den besonders geschützten Kategorien personenbezogener Daten, und Art. 32 DSGVO verlangt Schutzmaßnahmen nach dem Stand der Technik. Viele Krankenhäuser und weitere Einrichtungen des Gesundheitssektors fallen zudem unter das NIS-2-Umsetzungsgesetz, das MFA ausdrücklich als Risikomanagementmaßnahme nennt. Dennoch verlassen sich viele Einrichtungen beim Zugriff auf ihre Systeme noch allein auf Passwörter – angesichts zunehmender Angriffe reicht das nicht mehr aus.

Angriffe zielen oft auf die Anmeldedaten von Beschäftigten, um Zugang zu einem System zu erhalten. Interne MFA sollte für Gesundheitseinrichtungen daher hohe Priorität haben. Sie ist zudem ein wirksamer Baustein, um den Zugriff auf elektronische Gesundheitsdaten auf berechtigte Personen zu beschränken und dies nachweisen zu können.

SO HILFT HIRSCH

- Schneller und sicherer Zugriff auf Patientendaten mit kontaktloser Smartcard und kontaktlosem Leser
- Sicherer Zugriff per MFA auf ein medizinisches Gerät, nachdem bei einer Röntgenaufnahme oder einem Eingriff Patientendaten erfasst wurden, die geprüft und zur Speicherung übertragen werden

E-Commerce

Der Onlinehandel wächst – der Betrug wächst mit. Laut dem Merchant Risk Council verloren Onlinehändler 2025 weltweit schätzungsweise 48 Milliarden US-Dollar durch Betrug. Kontoübernahmen sind dabei eine der größten Gefahren: Im Digital Trust Index von Sift (Q1 2026) gaben 21 % der befragten Verbraucher an, im vergangenen Jahr eine Kontoübernahme erlebt zu haben.

Viele Onlinehändler zögern, MFA einzuführen, weil sie fürchten, Kunden abzuschrecken. Doch das Betrugsrisiko wird für Unternehmen zu einer immer größeren Bedrohung. Die PSD2 sichert zwar den Zahlungsvorgang mit starker Kundenauthentifizierung ab – das Kundenkonto im Shop selbst ist damit aber noch nicht geschützt.

Hacker müssen für Onlinebetrug nicht physisch anwesend sein, und E-Commerce-Websites können in großem Umfang angegriffen werden. Betrug wie unberechtigte Bestellungen ist für Unternehmen sehr teuer – am Ende zahlen die Händler, wenn sie betrogenen Kunden Geld erstatten müssen.

Mit MFA für Online-Konten lässt sich E-Commerce-Betrug wirksam eindämmen. Das gibt Kunden die Gewissheit, dass ihre Daten geschützt sind, und schreckt Hacker ab, die schwächere Websites bevorzugen. Wer das Betrugsrisiko mit MFA senkt, kann sein Ergebnis verbessern und sich einen Ruf für den Schutz von Kundendaten aufbauen.

SO HILFT HIRSCH

- FIDO-Sicherheitsschlüssel schützen Einkäufe bei eBay vor Kontoübernahmen

Öffentliche Verwaltung

Beschäftigte in Behörden sind bevorzugte Ziele von Cyberangriffen, weil sie Zugang zu sensiblen Daten wie Finanz-, Wirtschafts- und Sicherheitsinformationen haben. Angreifer nehmen sie typischerweise mit Phishing ins Visier und geben sich als vertrauenswürdige Quellen aus, um an Anmeldedaten zu gelangen.

Ein bekanntes Beispiel für Zwei-Faktor-Authentifizierung in Deutschland ist die Online-Ausweisfunktion des Personalausweises: Sie verbindet den Besitz der Karte mit der Kenntnis der PIN und ermöglicht so eine sichere Anmeldung bei Verwaltungsportalen.

Seit dem 6. Dezember 2025 ist das NIS-2-Umsetzungsgesetz in Kraft. Es modernisiert das BSI-Gesetz und verpflichtet besonders wichtige und wichtige Einrichtungen in § 30 BSIG ausdrücklich zur Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung. Einrichtungen der Bundesverwaltung müssen ihr Informationssicherheitsmanagement auf Basis des IT-Grundschutzes umsetzen und die BSI-Mindeststandards einhalten.

Die Folgen eines Cyberangriffs reichen über ein kompromittiertes Netzwerk hinaus: Angriffe auf Verwaltungen können Dienstleistungen für Bürgerinnen und Bürger über Wochen lahmlegen und private Daten offenlegen. MFA stellt sicher, dass nur berechtigte Benutzer auf Verwaltungsdaten zugreifen, und verringert die Möglichkeit für Angreifer, in ein System einzudringen.

SO HILFT HIRSCH

- Smartcard-basierte Dienstausweise in Kombination mit Smartcard-Lesern: Die Karte ist der Authenticator, der Leser

wird im Authentifizierungsprozess genutzt

- Konten in Verwaltungs- und Fachportalen mit einem FIDO-Sicherheitsschlüssel absichern – sofern das Portal FIDO2/WebAuthn unterstützt –, damit Phishing-Angriffe keine Konten übernehmen und keine Anmeldedaten kompromittieren

Webdienste

MFA kann auch als Identitätsanbieter für einen Webdienst wie Google Docs oder Salesforce-Cloud-Anwendungen eingesetzt werden. Dabei nutzt eine Anmeldeanfrage die Security Assertion Markup Language (SAML) und vertrauenswürdige Zertifikate zwischen der Anwendung und dem MFA-Server für den zusätzlichen Authentifizierungsschritt.

Auf diese Weise ergänzen Google und Apple die Google-Konten bzw. Apple-IDs ihrer Nutzer um einen zweiten Faktor. MFA ist ein wirksamer Weg, Online-Konten vor Cyberkriminellen zu schützen.

03 Multi-Faktor-Authentifizierung per Smartcard

Was sind Smartcards?

Smartcards sind Karten oder kryptografische USB-Tokens für verschiedene Authentifizierungszwecke: physischer Zutritt (Gebäude, Räume), Computer- und Netzwerkzugang sowie bestimmte Lösungen für den sicheren Fernzugriff (virtuelle private Netzwerke, Portale).

Sicheres Identifikationsmittel

Dank fortschrittlicher kryptografischer Funktionen ist die Smartcard-Authentifizierung sicherer als Passwörter, RFID oder Magnetstreifenkarten. Die PIN zur Smartcard bietet eine zusätzliche Sicherheitsebene: Selbst wenn eine Smartcard gestohlen wird, muss der Dieb die PIN kennen, um sie zu nutzen.

Smartcards sind zudem manipulationssicher und schwer zu hacken, zu klonen oder zu fälschen. Sie verfügen über integrierte Sicherheitsfunktionen wie Metallschichten, Sensoren gegen Angriffe mit Wärme und UV-Licht sowie Software- und Hardwareschaltungen, die Angriffe per differenzieller Stromverbrauchsanalyse (DPA) abwehren.

Außerdem enthalten Smartcards kryptografische Elemente, die die gespeicherten Informationen schützen und sichere Verfahren für deren Abruf erfordern.

Vielseitig einsetzbar

Smartcards sind praktisch, weil eine einzige Karte mehrere Zwecke erfüllen kann – Benutzer müssen nicht mehrere Identifikationsmittel mitführen. Eine Smartcard kann zum Beispiel

gleichzeitig für den Gebäudezutritt, den sicheren Computer- und Netzwerkzugang und als Ausweis (für Mitarbeitende, Patienten, Besucher, Behörden usw.) dienen.

Datenspeicherung

Die in Smartcards eingebetteten Chips ermöglichen es, Informationen auf der Karte hinzuzufügen, zu speichern und zu aktualisieren – etwa Gesundheitsdaten von Patienten –, auch nachdem die Karte ausgegeben wurde.

Einfache Nutzung

Smartcards sind leicht, gut mitzuführen und ermöglichen einen schnellen Zugang. Da Smartcards bereits vielfach genutzt werden, etwa als Kreditkarten, sind die meisten Menschen mit ihnen und ihrer Funktionsweise vertraut.

Sind Smartcards das Richtige für Ihre Organisation?

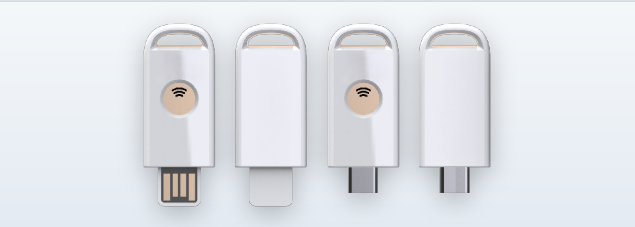
Smartcards sind eine vielseitige Option für Organisationen, die physischen und digitalen Zugang verbinden möchten. Zudem bieten sie eine höhere Sicherheit als viele andere Arten von Identifikationsmitteln.

Beschaffung, Anpassung und Einführung der Smartcard-Authentifizierung sind jedoch mit höheren Kosten und mehr Aufwand verbunden. Je nach Bedarf Ihrer Organisation gibt es daher möglicherweise günstigere und dennoch sichere Alternativen.

Passen Smartcards zu den Prioritäten Ihrer Organisation, ist die Wahl einer Lösung mit den richtigen Funktionen entscheidend, um Zeit, Aufwand und Kosten gering zu halten. Wir empfehlen eine vollständig integrierte Smartcard-Management-Lösung, die:

- die Erstellung und das Lebenszyklusmanagement von Smartcard-Geräten und PKI-Zertifikaten sofort einsatzbereit abdeckt,
- kontaktbehaftete und kontaktlose Smartcard-Technologie in Karten- und Token-Form umfassend unterstützt,
- alle Komponenten für die erfolgreiche Einführung, Verwaltung und Nutzung von Smartcard-Technologie mit Public-Key-Infrastruktur (PKI) liefert – darunter Smartcards, Smartcard-Leser, Smartcard-Management, PKI-Zertifikatsmanagement und professionelle Dienstleistungen.

04 MFA-Lösungen von Hirsch



SecureKey FIDO2-NFC-Sicherheitsschlüssel

Mit den FIDO2-NFC-Sicherheitsschlüsseln von Hirsch ersetzen Privatpersonen, Unternehmen, Behörden und Auftragnehmer Passwörter durch eine sichere, schnelle, skalierbare und kosteneffiziente Anmeldelösung. Sie unterstützen kontaktbehaftete (USB-A/-C) und kontaktlose (NFC) Anwendungsfälle, die Protokolle FIDO U2F, FIDO2, Smartcard und OTP und sind kompatibel mit Windows, Linux, macOS, Android und iOS.

IDENTIFIKATIONSMITTEL

uTrust SmartID Secure Access Credentials

Eine Familie von Multi-Applikations-Identifikationsmitteln für konvergenten Zugang, die Datenintegrität und Authentizität sichert. Sie schützen die Identität der Karteninhaber von der Tür (physische Zutrittskontrolle) bis zu den Daten (logische Zugangskontrolle). Auf Basis digitaler Zertifikate ermöglicht das Portfolio vertrauenswürdige Authentifizierung, digitale Signaturen, sicheren Fernzugriff, Desktop-Anmeldung und Datenverschlüsselung.

TOKENS

uTrust Token-Familie

Die uTrust Tokens bieten sichere Mobilität für Desktop-Anwendungen im PC-verbundenen Modus und dienen im autonomen Modus als kontaktloser Smartcard-Token für zahlreiche kontaktlose Anwendungen. Alle uTrust Tokens ermöglichen eine starke Zwei-Faktor-Authentifizierung aus etwas, das Benutzer besitzen (dem Token), und etwas, das sie wissen (ihrer PIN).

KONTAKT-LESER

SCR3310 v2.0 USB-Kontakt-Smartcard-Leser

Der CAC- und PIV-zugelassene SCR3310 v2.0 ist ein kleiner, robuster, PC-gebundener USB-Kontakt-Smartcard-Leser nach ISO/IEC 7816 mit Befestigungslöchern auf der Rückseite – ideal für eine Vielzahl sicherer Anwendungen. Dank voller Konformität mit allen wichtigen Branchenstandards wie ISO/IEC 7816, USB CCID, PC/SC und Microsoft WHQL arbeitet er reibungslos mit praktisch allen Kontakt-Smartcards und PC-Betriebssystemen.



uTrust 3720 F Smartcard-Leser/-Schreiber-Familie

Die Familie vereint Multi-Technologie- und Multi-ISO-Optionen für kontaktlose Schnittstellen und unterstützt so eine Vielzahl von Identifikationsanwendungen – darunter elektronische Ausweise und E-Pässe, E-Banking und E-Commerce.

KONTAKT-LESER

uTrust SmartFold SCR3500 Familie

Die CAC- und PIV-zugelassenen, PC-gebundenen USB-Kontakt-Smartcard-Leser erfüllen ISO/IEC 7816, CCID, PC/SC, EMV 2011 und GSA FIPS 201. Einsatzbereiche sind u. a. elektronische Ausweise, Sozialversicherungs- und Kundenbindungsprogramme, E-Couponing, sichere Netzwerkanmeldung, E-Banking, Onlineshopping und Gaming.

Die MFA-Lösungen von Hirsch schützen die Daten Ihrer Mitarbeitenden und Kunden.

Bereit, Ihr Unternehmen abzusichern? Sprechen Sie noch heute mit unseren Experten.

KONTAKT
info@hirschsecure.de
+49 6142 4811950

Hirsch ist ein weltweit führendes Technologieunternehmen und revolutioniert Lösungen für physische Sicherheit, Videoanalyse und digitale Identifikationssysteme.

fpr_SB_MFA - DE - 20/11/2026 - Unverbindliche Angaben, Änderungen vorbehalten.