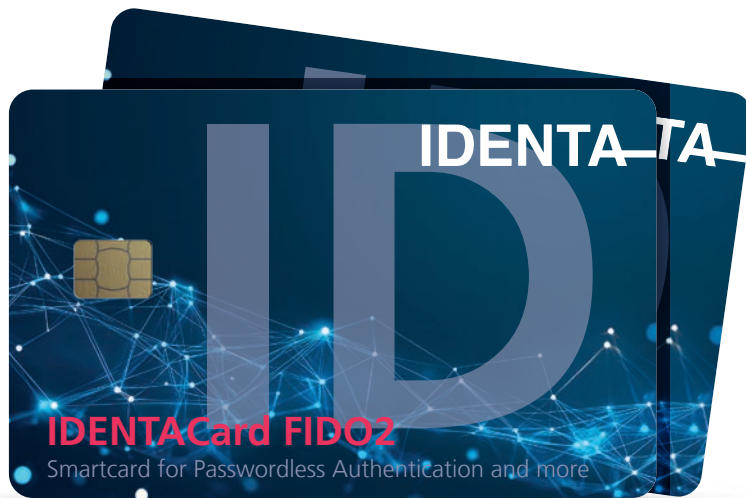


IDENTACard FIDO2

SMARTCARD FÜR PASSWORTLOSE AUTHENTIFIZIERUNG



EINSATZBEREICHE DER PRODUKTVARIANTEN

- **Standard:** Privacy-first, einfach integrierbar, skalierbar für breite Nutzergruppen
- **Enterprise:** Kontrollierte Authentifizierung für Asset Management, Gerätetransparenz, Governance, Compliance
- **Enterprise Premium:** Asset Management, erweitert um Supply-Chain-Kontrolle für hochsichere Infrastruktur-Anforderungen

	CONTACTLESS (CI)	DUAL INTERFACE (DIF)	CONTACT (6 PIN)
Commercial Chip Type	J3R452	J3R452	J3R452
Operating System	JCOP 4.5	JCOP 4.5	JCOP 4.5
NVM Size	450 kB	450 kB	450 kB
Delivery Form Factor Modul	MOB6	SOT658 (kann variieren)	SOT455 (kann variieren)
Input Capacitance	56 pF	56 pF	56 pF
FIDO	FIDO 2.1 (NXP) FIDO 2.X (GitHub OpenSource) FIDO 2.X (Custom)	FIDO 2.1 (NXP) FIDO 2.X (GitHub OpenSource) FIDO 2.X (Custom)	FIDO 2.1 (NXP) FIDO 2.X (GitHub OpenSource) FIDO 2.X (Custom)
MIFARE (Emulation)	MIFARE DESFire EV3 8K	MIFARE DESFire EV3 8K	N/A (MIFARE nur als Hybrid)
LEGIC Advant (Applet)	LEGIC Applikation auf DESFire (DESFire vorausgesetzt)	LEGIC Applikation auf DESFire (DESFire vorausgesetzt)	N/A (LEGIC nur als Hybrid)
Applets (Optionen)	SecID Applet (z. B. CV eDoc) Payment Applet VDV Applet (optional) Custom Applets*	SecID Applet (z. B. CV eDoc) Payment Applet VDV Applet (optional) Custom Applets*	SecID Applet (z. B. CV eDoc) Payment Applet Custom Applets*
Kombinationen (Auszug)	Kombinierbar mit klassischen RFID- / NFC-Technologien als Hybridausweis	Kombinierbar mit klassischen RFID- / NFC-Technologien als Hybridausweis	Kombinierbar mit klassischen RFID- / NFC-Technologien als Hybridausweis

*Weitere auf Anfrage

Die Marken und Logos FIDO CERTIFIED und FIDO2 sind Marken der FIDO Alliance.

#SICHER #BEQUEM #SKALIERBAR #KOMBINIERBAR #WIRTSCHAFTLICH

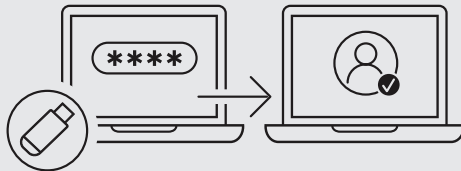
Die IDENTACard FIDO2 kombiniert moderne, passwortlose Authentifizierung mit klassischen RFID- / NFC-Funktionen und vereint so digitalen Login und physischen Zutritt in einem einzigen Medium. Im Unterschied zu reinen USB-Token bietet sie ein echtes One-Device-Konzept und stellt zugleich sicher, dass sensible Schlüsselinformationen vollständig in der geschützten Umgebung des Sicherheitschips verbleiben. Zudem ist sie eine wirtschaftlich attraktive Alternative zu token- oder hardwarebasierten Lösungen wie USB-Security-Keys. Für Wiederverkäufer steht die Karte auch als OEM- / Whitelabel-Variante zur Verfügung.

FIDO2

FAST IDENTITY ONLINE AUTHENTICATION



PASSWORDLESS authentication



SECOND FACTOR authentication



MULTI FACTOR authentication

WAS IST FIDO2?

FIDO2 ist ein offener Web Standard für sichere, passwortlose Authentifizierung mit hardwarebasierten Schlüsseln. Er ermöglicht schnelle, phishing resistente Logins auf Geräten, Desktop Systemen und Webanwendungen – plattformübergreifend und langfristig kompatibel.

WARUM FIDO2 FÜR UNTERNEHMEN SINNVOLL IST

- Schnelle, passwortlose Anmeldung für Nutzer
- Ein Medium für digitale und physische Zugänge
- Offen, standardbasiert und leicht integrierbar in bestehende Infrastrukturen

ZENTRALE SICHERHEITSVORTEILE

- Starker Phishing Schutz durch domaingebundene Schlüssel
- Private Schlüssel verbleiben ausschließlich in sicherer Hardware
- Erfüllt gängige Sicherheits- und Compliance-Standards
- Robuste Hardware für langfristige Nutzung

STANDARD

- Privacy-first Authentifizierung für breite, öffentliche oder skalierende Nutzergruppen
- Ideal für SaaS Plattformen, öffentliche Dienste und Anwendungen mit Fokus auf Datenschutz und einfachem Rollout

LEISTUNGSUMFANG

- Keine Geräteverfolgung
- Privacy by default
- Einfache Backend Integration
- Hoch skalierbar

ENTERPRISE

- Eindeutige Geräte-ID
- Kontrollierte Authentifizierung mit Geräteidentität, Governance und Unternehmens Policies
- Für Organisationen, die wissen müssen, welche Geräte und unter welchen Bedingungen auf ihre Systeme zugreifen

LEISTUNGSUMFANG

- Asset Management
- Geräteidentifikation und Nachvollziehbarkeit
- Asset Tracking und Kontrolle
- Policy basierter Zugriff
- Compliance Unterstützung



ENTERPRISE PREMIUM (OPTION)

- Erweitert die Produktvariante Enterprise um volle Kontrolle über Hardware Herkunft, PKI Bereiche und sicherheitskritische Grenzen einer Infrastruktur
- Für besonders regulierte oder sicherheitskritische Umgebungen

ZUSATZFUNKTIONEN:

- Asset Management
- Supply Chain Kontrolle
- Kundenspezifische PKI Segmentierung
- Hardware Level Admission Control
- Infrastruktur Governance

