swissbit®

Made in Germany

Hardware Authentifizierung für Behörden

Der universelle Security Key für digitalen und physischen Zugang

Behörden und Ministerien generieren große Datenmengen, darunter geheime Informationen. Damit wird der öffentliche Sektor weltweit zum Ziel von Cyberangriffen. Allein im Jahr 2025 wurden rund 1.000 Cybervorfälle registriert, bei welchen sensible Daten offengelegt wurden. Behörden sind wegen ihrer E-Mail-zentrierten Bürokratie Ziele für Phishing. Cyberkriminelle nutzen Phishing, um Zugang zu Anmeldedaten oder E-Mails zu erhalten. Um die öffentliche Verwaltung aufrechtzuerhalten, müssen Behörden ihre Sicherheit und Resilienz verbessern. Sie müssen globale Vorschriften wie ISO/IEC 27001:2022, EO 14028, NIST, OMB M-22-09, CER, CISA, NIS2 und DSGVO (EU), BSiG & IT-SiG 2.0 (Deutschland) einhalten.

fido CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID

www.swissbit.com/iShield-Key

Herausforderungen

- **Phishing:** Angreifer versuchen, Zugriff auf wertvolle Daten (wie Entwürfe von Richtlinien oder Bürgerakten) und IT-Systeme zu erlangen.
- **Use Cases:** Sicherung wertvoller Daten, IT- und Verwaltungssysteme sowie des Zugriffs auf Mitarbeiterzugangsdaten, Gebäude, Büros und den Datenaustausch mit Drittanbietern.
- **Vorschriften:** ISO/IEC 27001:2022, EO 14028, NIST, OMB M-22-09, CER, CISA, NIS2 und DSGVO (EU), BSIG & IT-SiG 2.0 (Deutschland).

Der "Threat Landscape 2025" Report zeigt, dass die digitale Infrastruktur der EU weiterhin Ziel von Cyberangriffen ist.

Source: enisa.europa.eu, 2025

FIDO Passkeys und Security Keys werden bis 2027 der Goldstandard für die Authentifizierung.

Source: 2025 HYPR State of Passwordless Identity Assurance

Lösung

- **Digitaler & physischer Zugang mit einem Gerät:** Da alle gängigen physischen Zugangssysteme (MIFARE, HID, LEGIC) unterstützt werden, lässt sich jede öffentliche Verwaltung nahtlos integrieren.
- **Zertifizierte Sicherheit:** Der Smartcard-Chip garantiert mit FIPS 140-3 Level 3 & CC EAL6+ Zertifizierung höchste Sicherheit.
- **Remote-Update-Fähigkeit:** Hält alle Protokolle aktuell, um höchste Sicherheitsanforderungen zu erfüllen.

Benefits

- **Einheitliche Authentifizierung über Systeme hinweg:** Der iShield Key 2 unterstützt nicht nur FIDO2, sondern kann aufgrund der Unterstützung von PKI- und OTP-Anwendungen flexibel & nahtlos in heterogenen Systemen eingesetzt werden.
- **Geringere Komplexität und Kosteneffizienz:** Der iShield Key 2 reduziert Sicherheitsvorfälle, Support-Aufwand und Kosten für das Gerätemanagement, in dem er den digitalen und physischen Zugang in einem Gerät verwendet.
- **Perfekt für den robusten Einsatz:** Der äußerst robuste iShield Key 2 ist ideal für Umgebungen im öffentlichen Sektor geeignet. Er kann dort eingesetzt werden, wo Smartphones nicht erlaubt sind.

Sie haben Fragen?
Kontaktieren Sie uns!

sales@swissbit.com
www.swissbit.com

iShield Key 2 – Key Features

- **Standards:** Unterstützt FIDO U2F, FIDO2 (CTAP 2.1), FIPS 140-3 Level 3 sowie optionale Enterprise Attestation
- **Remote-Updates:** Unterstützt sichere Remote-Firmware-Updates
- **Digitale Signaturen:** Ermöglicht digitales Signieren
- **Physischer Zugang:** Unterstützt MIFARE DESFire EV3 für sichere Zutritts- und Zahlungsanwendungen, optional mit HID Seos und LEGIC advant/neon
- **Passkey-Kapazität:** Speichert bis zu 300 Passkeys
- **Made in Germany:** Gefertigt mit Präzision und Qualität

Über Swissbit

Die Swissbit AG ist das führende europäische Technologieunternehmen für Speicherprodukte und Sicherheitslösungen. Unsere Vision ist eine vernetzte Welt, in der Daten und Identitäten jederzeit vertrauenswürdig sind, um die digitale Souveränität zu gewährleisten.