swissbit®

Made in Germany

Hardware Authentifizierung für Städte

Der universelle Security Key für digitalen und physischen Zugang

Kommunalverwaltungen sind wichtige Datenzentren und kritische Infrastrukturen. Das macht sie anfällig für Cyberangriffe. Etwa 50 % der Städte sind stündlich oder mindestens einmal täglich Cyberangriffen ausgesetzt. Es wird erwartet, dass die Zahl der Angriffe bis 2026 weiter steigt. Aufgrund der vielen Bevölkerungsdaten sind Städte attraktive Ziele für Phishing & Ransomware.

Phishing wird genutzt, um die Vertrauenskette in der öffentlichen Verwaltung auszunutzen oder um sich Zugang zu kritischen Dienstleistungssystemen zu verschaffen. Städte müssen ihre Sicherheit und Resilienz verbessern sowie globale Vorschriften wie CIRCIA (USA), NIS2, DSGVO, CRA, DORA, CER (EU) und KRITIS (Deutschland) einhalten.

fido CERTIFIED FIDO2 L2

MIFARE

140-3 FIPS

HID

www.swissbit.com/iShield-Key

Herausforderungen

- **Phishing Attacks:** Angreifer geben sich als vertrauenswürdige Partner oder Behörden aus und kompromittieren per Phishing städtische IT-Konten, um anschließend weiter in verbundene Betriebssysteme von Lieferanten vorzudringen.
- **Use Cases:** Sicherung von Bevölkerungsdaten, IT-Systemen und Zugriff auf Mitarbeiterdaten, Gebäuden, Büros und Daten-austausch mit Drittanbietern sowie übergeordneten Behörden.
- **Vorschriften:** CIRCIA (US), NIS2, GDPR, CRA, DORA und CER (EU), NIS2 and KRITIS (Germany).

Rund 50% der Städte sind stündlich oder mindestens einmal täglich Cyberangriffen ausgesetzt.

Source: sciencedirect.com, 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:** Unterstützung aller wichtigen Zugangssysteme (MIFARE, HID, LEGIC), um jede lokale Verwaltungsumgebung nahtlos zu 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 kommunale Versorgungsbetriebe. Er kann dort eingesetzt werden, wo Smartphones nicht erlaubt oder un-geeignet 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.