

Gegenstand der Beschaffung

Hardware-Sicherheitstoken zur phishing-resistenten Multi-Faktor-Authentifizierung (MFA) über physische und kontaktlose Schnittstellen.

Technische Anforderungen & Schnittstellen

Beiden technischen Anforderungen handelt es sich um Mindestanforderungen. Die angebotene Sicherheitstoken müssen die Kriterien mindestens gleichwertig erfüllen. Angebote, die diese Anforderungen nicht erfüllen, können für den Zuschlag nicht berücksichtigt werden. Es könne auch höherwertigen Modelle angeboten werden.

physische Merkmale & Formfaktor	
Schnittstelle (kabelgebunden)	USC-C (USB 2.0)
Schnittstelle (kontaktlos)	NFC (Near Field Communication), voll kompatibel nach ISO/IEC 14443-3 Type A.
Gehäuse/Bauform	kompaktes, spritzgegossenes Kunststoffgehäuse ohne Batterien, Akkus oder externe Knopfbatterien (Wartungsfrei)
Robustheit	Wasser- und staubgeschützt nach Schutzart IP68 sowie bruchsicher (Crush Resistance bis mindestens 25 Nm)
Sensor	Kapazitiver Touch-Sensor zur Anwesenheitsüberprüfung (Presence Detection / Touch-Verifikation) im Gehäuse integriert
unterstützte Sicherheitsprotokolle	
Das angebotene Hardware-Token muss zwingend alle nachfolgenden Protokolle und Standards parallel auf einem einzigen Chip/Chipset unterstützen.	
FIDO-Standards	FIDO2 / WebAuthn (inkl. CTAP 2.0 & CTAP 2.1) sowie FIDO U2F
OATH-Einmalpasswörter	Unterstützung für OATH-TOTP (Time-Based) und OATH-HOTP (Event-Based) mit Speicherkapazität für mindestens 64 OATH-Konten
Kryptografische Spezifikationen & Kapazitäten	
Hardware Security Element	Ausführung kryptografischer Operationen direkt auf einem zertifizierten Hardware-Sicherheitschip (kein Auslesen von Private Keys möglich)
Passkey-Speicher	Integrierter Speicher für mindestens 100 FIDO2 Passkeys
Kryptografische Algorithmen	Unterstützte Schlüsselweiten von RSA-2048, RSA-3072, RSA-4096 sowie Elliptic Curve (ECC P-256, P-384)
Kompatibilität & Software	
Betriebssysteme	Nativer Plug-and-Play-Betrieb ohne Herstellertreiber unter Microsoft Windows, Linux, Android und iOS (sowohl über USB-C als auch NFC)
Zentrales Management	Das Token muss die Möglichkeit bieten, einzelne Schnittstellen oder Protokolle (z. B. NFC oder

	OTP) über ein Konfigurationstool administrativ abzuschalten oder einzuschränken.
--	--

Das Referenzmodell ist der Yubikey 5C NFC (GTIN: 5060408462331). Es werden insgesamt 900 Sicherheitstoken benötigt. Die Lieferung und Rechnungsstellung müssen bis spätestens zum 01.12.2026 erfolgen.