

Vergabe-Nr. ZE 2026.41

Hardwarebasierte FIDO2-Token



Inhaltsverzeichnis

I. Leistungsbeschreibung.....	3
1. Ausgangslage.....	3
2. Ziel der Beschaffung.....	3
3. Gegenstand der Leistung / Abgrenzung.....	4
4. Liefer- und Ausstattungsumfang.....	4
5. Anforderungen.....	4
5.1 MUSS-Anforderungen (Ausschlusskriterien).....	5
6. Service, Support und Garantieleistungen.....	10
7. Qualitätssicherung, Vertragsgemäßheitsprüfung und Dokumentation.....	10
8. Datenschutz und Informationssicherheit.....	10
9. Begriffe / Definitionen.....	11

I. Leistungsbeschreibung

1. Ausgangslage

Der Auftraggeber, die Investitions- und Förderbank Niedersachsen (NBank), bedient aktuell die Anforderung an eine starke Authentifizierung der Benutzerkonten mittels physischer SmartCards, auf denen personenbezogene Benutzerzertifikate gespeichert sind. Diese SmartCards werden in Verbindung mit geeigneten Lesegeräten zur Anmeldung an IT-Systemen und Anwendungen eingesetzt.

Der Betrieb der SmartCard-Infrastruktur erfordert den Einsatz einer Public-Key-Infrastruktur (PKI) sowie aufwändige Prozesse zur Ausstellung, Verwaltung, Sperrung und Erneuerung von Zertifikaten. Zudem ist die Nutzung der SmartCards an spezifische Hardware und Treiber gebunden, was insbesondere bei mobilen Endgeräten und modernen Cloud-Diensten zu Einschränkungen führt.

Vor dem Hintergrund steigender Anforderungen an Benutzerfreundlichkeit, Sicherheit und Flexibilität soll die bestehende Authentifizierungslösung perspektivisch modernisiert werden. Ziel ist es, eine alternative, phishing-sichere Hardware-Authentifizierung einzuführen, die ohne Benutzerzertifikate auskommt und sich nahtlos in aktuelle IT-Umgebungen integrieren lässt.

2. Ziel der Beschaffung

Ziel dieser Ausschreibung ist die Beschaffung von hardwarebasierten FIDO2-Security-Keys zur starken Mehrfaktor-Authentifizierung (MFA) von Benutzerkonten in einer modernen IT-Umgebung. Die Keys sollen insbesondere zur Anmeldung an Cloud- und Web-Diensten (z. B. Microsoft Entra ID / Microsoft 365) sowie an kompatiblen lokalen Systemen eingesetzt werden.

- Ermöglichung einer phishing-resistenten, passwortlosen Anmeldung
- Stärkung der internen Sicherheitsstandards
- Anbindung der Entra-Infrastruktur der NBank
- Senkung der Komplexität der Anmeldevorgänge innerhalb der NBank

3. Gegenstand der Leistung / Abgrenzung

Gegenstand dieser Ausschreibung ist die Beschaffung von hardwarebasierten FIDO2-Security-Keys zur Nutzung als starkes, phishing-sicheres Authentifizierungsmerkmal für Benutzerkonten. Die Security-Keys sollen die bislang eingesetzten SmartCards mit Benutzerzertifikaten ergänzen bzw. perspektivisch ersetzen und eine passwortlose oder mehrstufige Authentifizierung ermöglichen.

Die verbindlichen technischen, funktionalen und sicherheitsbezogenen Mindestanforderungen ergeben sich ausschließlich aus Abschnitt 5.1 „MUSS-Anforderungen (Ausschlusskriterien)“. Anforderungen außerhalb dieses Katalogs begründen keine zusätzlichen Ausschlusskriterien.

Out of Scope (nicht Bestandteil der Leistung):

- Die Einführung, der Betrieb oder die Pflege einer Public-Key-Infrastruktur (PKI)
- Die Ausstellung, Verwaltung oder Migration von Benutzer- oder Gerätezertifikaten
- Konfigurations- oder Einrichtungsleistungen an Zielsystemen oder Identitätsdiensten
- Schulungen, Betriebs- oder Supportleistungen über die reine Hardwarelieferung hinaus

- die Bereitstellung von optionalen Hersteller-Cloud-Diensten oder zusätzlichen Softwarelizenzen.

4. Liefer- und Ausstattungsumfang

Der Lieferumfang umfasst die nachfolgend aufgeführten Mengen als einmalige Lieferung. Eine mengenmäßige Erweiterungsoption ist nicht Gegenstand dieser Ausschreibung.

Pos.	Beschreibung	Menge	Einheit	Zeitraum	Anmerkung
P-01	FIDO2 Hardware Token	1.000	Token	Einmalige Lieferung	Verbindlicher Lieferumfang
P-02	Schutz- bzw. Etui-Lösung passend zum angebotenen Security-Key; geeignet für einen sicheren Transport und eine sichere Aufbewahrung. Die Schutzlösung darf die bestimmungsgemäße Nutzung des Security-Keys nicht beeinträchtigen.	1.000	Etui	Einmalige Lieferung	Verbindlicher Lieferumfang; passend zum angebotenen Token

5. Anforderungen

Die nachfolgenden MUSS-Anforderungen sind zwingend zu erfüllen. Die Nichterfüllung einer MUSS-Anforderung führt zum Ausschluss des Angebots.

5.1 MUSS-Anforderungen (Ausschlusskriterien)

Pos.	Funktion	Anforderung	Nachweis / Prüfung
M-01	Bauform Hardware	/ Der angebotene Security Key muss die Schnittstellen USB-A, USB-C und NFC in einem einzelnen physischen Gerät bereitstellen. Hintergrund ist die heterogene Arbeitsplatz- und Endgeräteumgebung des Auftraggebers sowie das Ziel eines einheitlichen, supportarmen und ohne Adapter nutzbaren Authentifizierungsverfahrens	Produktdatenblatt
M-02	Bauform Hardware	/ Die geforderten Schnittstellen USB-A, USB-C und NFC müssen unmittelbar am Security Key nutzbar sein. Der Einsatz	Produktdatenblatt oder technische Produktbeschreibung mit Abbildung bzw.

Pos.	Funktion	Anforderung	Nachweis / Prüfung
		zusätzlicher Adapter, Zwischenstücke oder externer Hilfsmittel zur Erfüllung dieser Schnittstellenanforderung ist nicht zulässig.	Beschreibung der Schnittstellen
M-03	Standardisierung	Der Security Key muss FIDO2 nach Maßgabe der FIDO Alliance unterstützen, insbesondere die Standards WebAuthn und CTAP2. Die Nutzung als hardwarebasierter Authenticator für passwortlose bzw. phishing-resistente Authentifizierung muss möglich sein.	Nachweis der FIDO2-Konformität, z. B. FIDO-Zertifizierung, Produktdatenblatt oder technische Herstellerdokumentation
M-04	Sicherheit	Die im Security Key erzeugten oder gespeicherten privaten Schlüssel müssen hardwarebasiert geschützt und nicht exportierbar sein. Ein Auslesen, Kopieren oder Exportieren privater Schlüssel aus dem Security Key darf nicht möglich sein.	Technische Herstellerdokumentation oder Sicherheitsbeschreibung mit Angaben zum Schutz und zur Nicht-Exportierbarkeit privater Schlüssel
M-05	Sicherheit	Der Security Key muss für Authentifizierungsvorgänge eine aktive lokale Benutzerinteraktion zur Bestätigung unterstützen, z. B. durch Berührung oder Taste. Für den vorgesehenen Einsatz muss mindestens ein nicht-biometrischer Bestätigungsmechanismus verfügbar sein; die Nutzung biometrischer Verfahren darf nicht erforderlich sein.	Produktbeschreibung, Produktdatenblatt oder technische Herstellerdokumentation mit Angaben zur lokalen Benutzerinteraktion und zum verfügbaren nicht-biometrischen Bestätigungsmechanismus

M-06	Sicherheit Datenschutz	/ Der Security Key muss eine PIN- oder Passwort-basierte Benutzerverifikation unterstützen. Die Prüfung muss lokal und offline auf dem Security Key erfolgen. Biometrische Verfahren dürfen hierfür nicht erforderlich sein.	Produktbeschreibung, Produktdatenblatt oder technische Herstellerdokumentation mit Angaben zur PIN- oder Passwort-basierten Benutzerverifikation und lokaler Prüfung
M-07	Sicherheit	Der Security Key muss einen technischen Schutzmechanismus gegen Brute-Force-Angriffe auf die PIN-basierte Benutzerverifikation unterstützen. Unbegrenzte PIN-Eingabeversuche dürfen nicht möglich sein; nach einer begrenzten Anzahl fehlerhafter Eingaben muss eine Sperre, Verzögerung, Rücksetzung oder ein gleichwertiger Schutzmechanismus greifen.	Technische Herstellerdokumentation oder Sicherheitsbeschreibung mit Angaben zum Fehlversuchs- und Brute-Force-Schutz
M-08	Sicherheit	Phishing-resistente Authentifizierung gem. FIDO2-Standard. Die Authentifizierung muss auf asymmetrischer Kryptografie und dienstgebundenen Zugangsdaten beruhen, sodass keine wiederverwendbaren oder übertragbaren Authentifizierungsgeheimnisse an den Zieldienst übermittelt werden.	FIDO2-Zertifizierung der FIDO Alliance oder gleichwertiger Nachweis der FIDO2-Konformität
M-09	Kompatibilität	Der Security Key muss unter Microsoft Windows 11 als FIDO2-Security-Key ohne zusätzliche herstellerspezifische Treiberinstallation nutzbar sein.	Produktdatenblatt, Herstellerdokumentation oder Kompatibilitätsmatrix mit Angabe zur Unterstützung von Microsoft Windows 11
M-10	Kompatibilität	Der Security Key muss unter aktuellen, vom Hersteller unterstützten Versionen von macOS als FIDO2-Security-Key ohne zusätzliche herstellerspezifische Treiberinstallation nutzbar sein.	Produktdatenblatt, Herstellerdokumentation oder Kompatibilitätsmatrix mit Angabe zur Unterstützung von macOS

M-11	Kompatibilität	Der Security Key muss über NFC als FIDO2-Security-Key mit aktuellen, vom jeweiligen Hersteller unterstützten Versionen von iOS und Android nutzbar sein. Die Nutzung darf keine zusätzliche herstellerspezifische App oder Registrierung bei einem Herstellerdienst voraussetzen.	Produktdatenblatt, Herstellerdokumentation oder Kompatibilitätsmatrix mit Angabe zur NFC-Nutzung unter iOS und Android
M-12	Kompatibilität	Der Security Key muss als FIDO2/WebAuthn-Authenticator mit aktuellen, vom jeweiligen Hersteller unterstützten Versionen marktüblicher Browser nutzbar sein; mindestens mit Microsoft Edge, Google Chrome und Mozilla Firefox.	Produktdatenblatt, Herstellerdokumentation oder Kompatibilitätsmatrix mit Angaben zur WebAuthn-/FIDO2-Nutzung in Microsoft Edge, Google Chrome und Mozilla Firefox
M-13	Integration	Der Security Key muss als FIDO2-Security-Key in Microsoft Entra ID registrierbar und für die FIDO2-basierte Anmeldung an Microsoft 365 sowie weiteren Microsoft-Entra-ID-angebundenen Diensten nutzbar sein.	Herstellerdokumentation, Produktdatenblatt, Kompatibilitätsmatrix oder Referenzangabe zur Nutzung mit Microsoft Entra ID
M-14	Betrieb	Der Security Key muss auf den in dieser Leistungsbeschreibung geforderten unterstützten Plattformen als FIDO2-Security-Key ohne zusätzliche herstellerspezifische Treiber- oder Softwareinstallation nutzbar sein.	Produktbeschreibung, Produktdatenblatt oder technische Herstellerdokumentation mit Angaben zur treiberfreien Nutzung
M-15	Betrieb / Provisionierung	Der Security Key muss eine interne Vorabregistrierung durch den Auftraggeber als FIDO2-Security-Key in Microsoft Entra ID vor Ausgabe an die Benutzer ermöglichen. Hierfür darf keine verpflichtende Nutzung herstellerspezifischer Cloud-Dienste, zusätzlicher kostenpflichtiger Lizenzen oder personenbezogener Vorbelegung durch den Auftragnehmer erforderlich sein.	Produktbeschreibung, Herstellerdokumentation oder technische Beschreibung zur internen Vorabregistrierung bzw. Vorabinitialisierung als FIDO2-Security-Key in Microsoft Entra ID

M-16 Datenschutz	Auf dem Security Key dürfen keine Benutzeridentitäten, Passwörter, biometrischen Merkmale oder sonstigen personenbezogenen Inhalts- oder Profildaten im Klartext gespeichert werden. Die Speicherung technisch erforderlicher kryptografischer bzw. protokollbezogener Daten ist nur zulässig, soweit sie für die FIDO2-Funktion erforderlich, hardwarebasiert geschützt und nicht exportierbar sind.	Herstellererklärung, Produktbeschreibung oder technische Datenschutz-/Sicherheitsdokumentation
M-17 Qualität	Der Security Key muss vom Hersteller für den regelmäßigen mobilen und stationären Einsatz vorgesehen sein. Gehäuse und Anschlüsse müssen für den bestimmungsgemäßen wiederholten Anschluss an Endgeräte sowie den üblichen Transport im Arbeitsalltag ausgelegt sein.	Produktdatenblatt oder technische Herstellerdokumentation, aus der der bestimmungsgemäße mobile und stationäre Einsatz sowie die Auslegung von Gehäuse und Anschlüssen hervorgehen
M-18 Garantie	Für die angebotenen Security Keys muss ab Lieferung für mindestens 24 Monate eine Herstellergarantie oder eine gleichwertige, für den Auftraggeber kostenfreie Austauschzusage bei Defekt oder Funktionsstörung bestehen. Die gesetzlichen und vertraglichen Mängelrechte des Auftraggebers, insbesondere nach den EVB-IT Kauf-AGB, bleiben hiervon unberührt.	Garantiebedingungen, Herstellerangabe, Produktbeschreibung oder Eigenerklärung des Auftragnehmers
M-19 Verwaltung	Der Security Key muss durch den Auftraggeber mit standardkonformen Mitteln initialisiert und verwaltet werden können, insbesondere für PIN-Vergabe bzw. PIN-Änderung, Zurücksetzen des Tokens und Auslesen einer eindeutigen Geräteerkennung. Hierfür darf keine verpflichtende Nutzung herstellereinspezifischer Cloud-	Produktbeschreibung, technische Herstellerdokumentation oder Administrationsbeschreibung zu Initialisierung, PIN-Verwaltung, Zurücksetzen und Geräteerkennung

Dienste oder zusätzlicher
kostenpflichtiger Lizenzen
erforderlich sein.

M-20 Betrieb	Der Security Key muss die Speicherung und Nutzung mehrerer unabhängiger FIDO2-/WebAuthn-Credentials für unterschiedliche Anwendungen und Dienste auf einem einzelnen Token unterstützen.	Herstellerangabe, Produktdatenblatt oder technische Herstellerdokumentation zur Anzahl bzw. Unterstützung mehrerer FIDO2-/WebAuthn-Credentials
M-21 Kennzeichnung	Der Security Key muss über eine eindeutige und dauerhaft zuordenbare Geräteerkennung verfügen, die eine Inventarisierung und eindeutige Identifizierung des Tokens ermöglicht.	Produktbeschreibung, Produktdatenblatt oder technische Herstellerdokumentation mit Angaben zur Geräteerkennung

6. Service, Support und Garantieleistungen

Für die angebotenen Security-Keys gelten die gesetzlichen und vertraglichen Mängelrechte, insbesondere die EVB-IT Kauf-AGB. Ergänzend ist die in M-18 geforderte Herstellergarantie oder gleichwertige kostenfreie Austauschzusage für mindestens 24 Monate sicherzustellen.

Der Auftragnehmer ist gegenüber der NBank für die Abwicklung von Garantie- und Austauschfällen verantwortlich. Er stellt ein strukturiertes RMA- bzw. Austauschverfahren bereit und benennt der NBank spätestens mit Lieferung die hierfür vorgesehenen Kontaktwege und Verfahrensschritte. Der Austausch ist für die NBank kostenfrei abzuwickeln.

Für Meldungen zu Defekten, Funktionsstörungen und Austauschfällen sind mindestens elektronische Kontaktmöglichkeiten (z. B. E-Mail oder Webportal) bereitzustellen. Weitergehende Service-Level-Vereinbarungen, insbesondere garantierte Reaktions- oder Entstörzeiten, sind nicht Gegenstand dieser Ausschreibung. Die gesetzlichen und vertraglichen Rechte der NBank bei Mängeln, insbesondere das Recht zur Setzung einer angemessenen Frist zur Nacherfüllung, bleiben unberührt.

7. Qualitätssicherung, Vertragsgemäßigkeitsprüfung und Dokumentation

Der Auftragnehmer stellt sicher, dass die gelieferten Security-Keys den in dieser Leistungsbeschreibung definierten Anforderungen vollständig entsprechen. Es sind ausschließlich neue, unbenutzte und funktionsfähige Geräte zu liefern.

Nach Lieferung führt die NBank eine Wareneingangs- und Vertragsgemäßigkeitsprüfung durch. Diese umfasst insbesondere die Prüfung von Menge, äußerlich erkennbaren Beschädigungen und der Übereinstimmung der gelieferten Geräte mit der vertraglich geschuldeten Produktvariante. Die NBank ist berechtigt, die Vertragsgemäßheit der gelieferten Geräte bei Bedarf durch geeignete Stichproben zu überprüfen. Die Unterzeichnung eines Lieferscheins bestätigt lediglich den Erhalt der Lieferung und stellt weder eine Bestätigung der Vollständigkeit oder Mangelfreiheit noch eine Abnahme im werkvertraglichen Sinne dar. Festgestellte Abweichungen oder Mängel sind nach Maßgabe der vertraglichen Regelungen, insbesondere der EVB-IT Kauf-AGB, zu beseitigen. Die gesetzlichen und vertraglichen Mängelrechte der NBank bleiben unberührt.

Der Auftragnehmer hat eine angemessene Produktdokumentation bereitzustellen. Diese umfasst mindestens technische Spezifikationen, Angaben zur Nutzung (z. B. Inbetriebnahme, PIN-Verfahren) sowie Hinweise zur Kompatibilität und Unterstützungsumgebungen. Die Dokumentation kann elektronisch in deutscher oder englischer Sprache bereitgestellt werden.

8. Datenschutz und Informationssicherheit

Die angebotenen Security-Keys müssen die in dieser Leistungsbeschreibung festgelegten Anforderungen an Datenschutz und Informationssicherheit erfüllen. Soweit bei der Nutzung personenbezogene Daten verarbeitet werden, sind die einschlägigen datenschutzrechtlichen Vorschriften, insbesondere die Datenschutz-Grundverordnung (DSGVO), einzuhalten.

Auf den Security-Keys dürfen keine Benutzeridentitäten, Passwörter, biometrischen Merkmale oder sonstigen personenbezogenen Inhalts- oder Profildaten im Klartext gespeichert werden. Die Speicherung technisch erforderlicher kryptografischer bzw. protokollbezogener Daten ist nur zulässig, soweit sie für die FIDO2-Funktion erforderlich, hardwarebasiert geschützt und nicht exportierbar sind. Die im Rahmen der Authentifizierung erzeugten oder verwendeten privaten Schlüssel müssen hardwarebasiert geschützt sein und dürfen nicht ausgelesen, kopiert oder exportiert werden können.

Der Auftragnehmer hat sicherzustellen, dass durch die Nutzung der angebotenen Security-Keys keine zusätzlichen datenschutzrechtlichen Risiken entstehen, insbesondere keine unkontrollierte Datenübertragung an Dritte oder den Hersteller erfolgt. Eine Nutzung der Geräte muss ohne verpflichtende Registrierung bei Herstellerdiensten oder cloudbasierten Plattformen möglich sein.

Die angebotenen Security-Keys müssen dem Stand der Technik entsprechende Sicherheitsmechanismen aufweisen, insbesondere Schutz vor Manipulation, unbefugtem Zugriff sowie gängigen Angriffsszenarien (z. B. Phishing, Replay-Angriffe).

Der Auftragnehmer hat auf Anforderung geeignete Nachweise zur Informationssicherheit bereitzustellen, beispielsweise Herstellerangaben, Zertifizierungen oder technische Dokumentationen.

9. Begriffe / Definitionen

Die nachfolgenden Definitionen dienen der eindeutigen Auslegung dieser Leistungsbeschreibung und gelten für das gesamte Dokument sowie für alle vertraglichen Anlagen, sofern dort nicht ausdrücklich abweichende Definitionen getroffen werden.

Begriff	Definition
FIDO2	Offener Authentifizierungsstandard der FIDO Alliance zur passwortlosen und phishing-resistenten Anmeldung auf Basis asymmetrischer Kryptografie (WebAuthn / CTAP2)
Security-Key / Hardware-Token	Physisches Authentifizierungsgerät zur sicheren Anmeldung an IT-Systemen, das kryptografische Schlüssel in einem geschützten Hardware-Element speichert
Kombinations-Token	Security-Key, der die Schnittstellen USB-A, USB-C und NFC in einem einzelnen Gerät vereint und ohne Adapter nutzbar ist
WebAuthn (Web Authentication)	Webstandard des W3C zur Integration von FIDO2-basierter Authentifizierung in Browser und Webanwendungen
CTAP (Client to Authenticator Protocol)	Protokoll zur Kommunikation zwischen Endgerät (Client) und Authenticator (z. B. Security-Key) im Rahmen von FIDO2
NFC (Near Field Communication)	Kontaktlose Kommunikationsschnittstelle zur Nutzung des Security-Keys insbesondere mit mobilen Endgeräten
Microsoft Entra ID	Cloudbasierter Identitäts- und Zugriffsverwaltungsdienst (ehemals Azure Active Directory) zur Authentifizierung und Autorisierung von Benutzern in Cloud- und Hybridumgebungen
Multi-Faktor-Authentifizierung (MFA)	Authentifizierungsverfahren, bei dem mindestens zwei unterschiedliche Faktoren (z. B. Besitz, Wissen, Biometrie) zur Anmeldung verwendet werden.
Phishing-resistente Authentifizierung	Authentifizierungsverfahren, bei dem Anmeldeinformationen nicht durch Täuschung (z. B. gefälschte Webseiten)

Begriff	Definition
	abgegriffen werden können, da keine übertragbaren Geheimnisse (z. B. Passwörter) übermittelt werden.
Public-Key-Kryptografie	Kryptografisches Verfahren mit einem Schlüsselpaar aus öffentlichem und privatem Schlüssel, wobei der private Schlüssel das Gerät niemals verlässt