



Leistungsbeschreibung

**IT-Hardware: Mobile Datenträger, BSI-zugelassen bis Geheimhaltungsgrad
VS - Nur für den Dienstgebrauch**

ZIB 15.10 - 9935/25/VV : 1

Ihre Vergabestelle für das Vergabeverfahren

Beschaffungsamt des BMI

Referat ZIB15

Anschrift Beschaffungsamt des BMI
 Brühler Straße 3
 53119 Bonn

Inhaltsverzeichnis

1.	Allgemeines.....	3
1.1	Allgemeine Hinweise zu den Anforderungen in dieser Leistungsbeschreibung.....	5
1.2	Normative Verweisungen	5
2.	Gegenstand der Leistung	6
2.1	Allgemeine Leistungsanforderungen.....	6
2.2	Mechanische Konstruktion, allgemeine Umgebungsbedingungen	6
2.3	Gerätetypen und Speichergrößen	7
2.4	Kompatibilität/Anschlüsse	7
2.5	Verschlüsselung der Informationen.....	7
2.6	Schreibschutz	7
2.7	Zusätzliche Sicherheitsfunktionen	7
2.8	Nutzer- /Administratoranmeldung.....	7
2.9	Weitere Anwendungsfälle	7
2.10	Zulassung	7
2.11	Dokumentationen.....	7
2.12	Technischer Support / Hotline.....	7
2.13	Barrierefreiheit	8
2.14	Nachhaltigkeit.....	9
2.14.1	Materialanforderungen.....	9
2.14.2	Transparenz der Lieferkette	9
2.14.3	Soziale Aspekte.....	10
2.15	Firmware Update-Gerät.....	10

1. Allgemeines

Das Beschaffungsamt des Bundesinnenministeriums des Innern (BeschA) führt im Rahmen dieses Vergabeverfahrens eine Ausschreibung zum Zwecke der Beschaffung von mobilen Datenträgern die für die hardwarebasierte verschlüsselte Speicherung, den Transport und die Weitergabe von VS-eingestuften Informationen bis zum Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH geeignet und vom BSI zugelassen sind, durch.

Die Geräteklasse der mobilen Datenträger umfasst in dieser Ausschreibung die folgenden Gerätetypen:

- USB-(Daten)-Sticks
- Externe Solid State Festplatten (SSD)
- Externe Festplatten (HDD)

Die anzubietenden Produkte müssen gemäß dem Dokument BSI-VS-AP-0006 folgende Objekte im Datenträger schützen können:

- Die sensiblen Benutzerdaten (primäres Schutzobjekt)
- Die Authentisierungsdaten, z.B. Passwörter, PIN (sekundäres Schutzobjekt)
- Kryptographische Schlüssel (sekundäres Schutzobjekt)
- Firmware und Konfigurationseinstellungen (sekundäres Schutzobjekt)

Die anzubietenden Produkte müssen sicherstellen, dass die gemäß BSI-VS-AP-0006 Kapitel 2.3 definierten Bedrohungen erkannt und abgewendet werden können. Das sind im Wesentlichen die nachfolgend genannten Bedrohungen. Die komplette Beschreibung der Bedrohungen kann dem VS-Anforderungsprofil BSI-VS-AP-0006 entnommen werden. Die Notation des Bedrohungstyps entspricht dem VS-Anforderungsprofil.

Die detaillierten technischen Anforderungen an die zu liefernden Produkte, die notwendig sind, um den nachfolgenden Bedrohungen abzuwehren, sind in Kapitel 2 beschrieben.

- **T.Sensible_Benutzerdaten:** Hauptbedrohung, nicht autorisierte Offenlegung von sensible Benutzerdaten
- **T.AuthDaten:** nicht autorisierte Erlangung der Authentisierungsdaten
- **T.Schlüssel_AuthDaten:** nicht autorisierter Besitz von kryptografischen Schlüsseln, von Authentisierungsdaten oder anderen Werten, welche zur Generierung von

kryptographischen Schlüsseln oder
Authentisierungsdaten beitragen

- **T.Software:** nicht autorisierter Zugriff auf die Firmware inkl. Konfigurationsdaten des Datenträgers
- **T.Bypassing:** Umgehung der definierten Schnittstellen des Datenträgers um Zugriff auf die sensiblen Benutzerdaten, die Authentisierungsdaten oder die kryptografischen Schlüssel zu erhalten
- **T.Ersatz:** Den unbemerkten Ersatz eines Datenträgers gegen ein manipuliertes Gerät

Folgende Security Policies sind gemäß BSI-VS-AP-0006 einzuhalten:

- Es dürfen nur vom BSI akzeptierte kryptografische Verfahren und Protokolle eingesetzt werden
- Langzeitgeheimnisse müssen in einer entsprechend sicheren Hardware-Einheit gespeichert werden, so dass diese nicht kompromittiert werden können.

Alle in den nachfolgenden Kapiteln im Detail beschriebenen technischen Anforderungen dienen dazu die im VS-Anforderungsprofil beschriebenen Bedrohungen abzuwenden und die Security Policies des BSI für ein zugelassenes Produkt einzuhalten.

Dazu müssen die zu liefernden Produkte derart konstruiert, gefertigt und programmiert sein, dass:

- Eine ausreichende Verschlüsselung der zu speichernden Informationen gewährleistet ist
- Eine sichere Authentifizierung des Benutzers am Gerät über PIN oder Passwort erfolgen kann
- Mechanische Manipulationsversuche am Datenträger leicht erkannt werden können
- Mehrmalige erfolglose Anmeldeversuche dazu führen, dass der Datenträger gesperrt wird und nur durch eine Master-PIN oder Master-Passwort wieder entsperrt werden kann
- Mehrmalige Falscheingabe der Master-PIN oder des Master-Passwortes zum automatischen und unwiderruflichen Löschen der Verschlüsselungsschlüssel führen und damit die gespeicherten VS-eingestuften Informationen weiterhin gesichert bleiben

- Über eine Administrator-PIN oder ein Administrator-Passwort die mobilen Datenträger verwaltet werden können, ohne dass der Administrator dabei Zugang zu den VS- eingestuft Informationen erhält.

Die detaillierten Anforderungen an die oben genannten Eigenschaften werden im Kapitel 2 dieser Leistungsbeschreibung beschrieben.

Die dem Angebot der Bieterin zugrunde zu legenden geschätzten Stückzahlen für die einzelnen Gerätetypen und die unterschiedlichen Speicherkapazitäten sind dem Preisblatt (siehe Anlage „Preisblatt“) des Vergabeverfahrens zu entnehmen.

1.1 Allgemeine Hinweise zu den Anforderungen in dieser Leistungsbeschreibung

Die in dieser Leistungsbeschreibung genannten Leistungsmerkmale müssen zwingend angeboten werden.

Technische Anforderungen an den Leistungsgegenstand sind gemäß den vergaberechtlichen Vorgaben beschrieben.

Soweit besondere technische Anforderungen zu der Gesamtleistung oder Teilen der Leistung aufgrund gesetzlicher oder technischer Normen bzw. Regelungen bestehen, sind diese durch den Bieter eigenständig zu beachten und im Angebot entsprechend zu benennen und zu berücksichtigen. Gleiches gilt für den aktuell anerkannten Stand der Technik.

1.2 Normative Verweisungen

Sämtliche relevanten Vorgaben aus den dieser Ausschreibung zugrunde liegenden Rechtsgrundlagen sind einzuhalten. Hierzu zählen neben den anwendbaren gesetzlichen Vorgaben und EU-Verordnungen insbesondere die folgenden Dokumente:

- BSI TR-02102-1, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen vom 31.01.2025
- BSI TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS) vom 21.01.2025
- BSI-VS-AP-0006 VS-Anforderungsprofil Sicherer Mobiler Datenträger (SMD), Version 1.0.1 vom 30.08.2019
- Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlussachenanweisung - VSA) vom 13.03.2023
- DIN EN IEC 60721-3-3:2019 Klassifizierung von Umgebungsbedingungen, Teil 3-3: Klassen von Einflussgrößen und deren Grenzwerte – Ortsfester Einsatz, wettergeschützt

- Richtlinie 2011/65/EU zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten vom 8. Juni 2011

Die vorgenannten Richtlinien sind nicht abschließend.

2. Gegenstand der Leistung

In diesem Kapitel werden die allgemeinen und speziellen Anforderungen an die anzubietenden Produkte beschrieben.

Die grundsätzlichen Anforderungen an mobile Datenträger, die für die Speicherung von Daten bis zum Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH eingesetzt werden können, sind weitgehend identisch, unabhängig von der verwendeten Speichertechnologie.

Die genannten Mindestanforderungen sind als A-Kriterien zu verstehen und werden nachfolgend und im Dokument „Kriterienkatalog_Leistung“ beschrieben.

Alle nachfolgend beschriebenen Anforderungen gelten daher gleichermaßen für die Gerätetypen:

- USB-(Daten)-Stick
- Externe Solid State Festplatten (SSD)
- Externe Festplatten (HDD)

2.1 Allgemeine Leistungsanforderungen

Die gelieferten Produkte müssen fabrikneu sein und in einer Verpackung an die Bedarfsträgerin geliefert werden, die mechanische, thermische und chemische Manipulationsversuche an der Verpackung erkennen lässt, um eine Kompromittierung der Datenträger vor der ersten Verwendung auszuschließen.

Jeweils aktuell geltende Normen und Vorschriften insbesondere in Hinblick auf die Datensicherheit der zu liefernden Produkte sind einzuhalten, eventuell aus Zulassungen oder VS-Anforderungsprofilen gestellte Auflagen sind zu erfüllen.

Eine weitere detaillierte Anforderungsbeschreibung erfolgt in den nächsten Kapiteln.

2.2 Mechanische Konstruktion, allgemeine Umgebungsbedingungen

Die zu liefernden Datenträger müssen für den täglichen Einsatz unter normalen Betriebsbedingungen geeignet sein. Die Konstruktion der Datenträger soll so ausgeführt werden, dass mechanische Beschädigungen leicht zu erkennen sind, um mögliche mechanische Manipulationsversuche leicht erkennen zu können.

Es werden im Weiteren keine besonderen Anforderungen gestellt, die den Einsatz unter besonders rauen Bedingungen (Staub, Schmutz, hohe/niedrige Temperaturen,

explosionsgefährdete Umgebungen, besonders hohe Luftfeuchtigkeit (kondensierend)) ermöglichen sollen.

Die einzelnen Anforderungen werden im Dokument „Kriterienkatalog Leistung“ beschrieben.

2.3 Gerätetypen und Speichergrößen

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.4 Kompatibilität/Anschlüsse

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.5 Verschlüsselung der Informationen

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.6 Schreibschutz

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.7 Zusätzliche Sicherheitsfunktionen

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.8 Nutzer- /Administratoranmeldung

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.9 Weitere Anwendungsfälle

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.10 Zulassung

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.11 Dokumentationen

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.12 Technischer Support / Hotline

Diese Anforderungen sind im Dokument „Kriterienkatalog_Leistung“ beschrieben.

2.13 Barrierefreiheit

IT-Lösungen der Bundesverwaltung müssen gemäß § 4 BGG (Behindertengleichstellungsgesetz) für Menschen mit Behinderungen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe auffindbar, zugänglich und im Sinne der DIN EN ISO 9241 nutzbar sein. Dies erfordert gemäß § 3 Abs. 1 BITV 2.0, dass sie wahrnehmbar, bedienbar, verständlich und robust ist. Hierbei ist die Nutzung behinderungsbedingt notwendiger Hilfsmittel zulässig. Barrieren sind lediglich zulässig, wenn der aktuelle Stand der Technik vollumfängliche Barrierefreiheit nicht ermöglicht. Die Barrierefreiheit der IT-Lösung ermöglicht eine Nutzung durch folgende Gruppen:

- Menschen ohne Sehvermögen sowie Menschen mit eingeschränktem Sehvermögen
- Menschen ohne Farbwahrnehmung sowie Menschen mit eingeschränkter Farbwahrnehmung
- Menschen ohne Hörvermögen sowie Menschen mit eingeschränktem Hörvermögen
- Menschen ohne Sprachvermögen
- Menschen mit eingeschränkter Handhabung oder Kraft
- Menschen mit eingeschränkter Reichweite
- Menschen mit Anfälligkeit durch Lichtreize (Photosensibilität)
- Menschen mit kognitiven Einschränkungen

Nähere Ausführungen sind Abschnitt 4 der DIN EN 301 549 V3.2.1 zu entnehmen. Ihr Angebot hat alle zur Erfüllung der in der Leistungsbeschreibung enthaltenen Anforderungen an die Barrierefreiheit zu enthalten. Eine gesonderte Vergütung von Leistungen zur Herstellung der Barrierefreiheit erfolgt nicht. Barrierefreiheitsanforderungen gelten auch für Dokumente, die von der IT-Lösung automatisiert erzeugt werden, sowie für Hilfsfunktionen, Benutzungshandbücher und Schulungsunterlagen. Die Anforderungen an die Barrierefreiheit an die IT-Lösung müssen über die gesamte Vertragslaufzeit – das heißt sowohl über die Laufzeit einer Rahmenvereinbarung als auch über die Laufzeit eines jeden Einzelabrufs – erfüllt werden. Hierin eingeschlossen sind Pflege und Support der IT – Lösung, also insbesondere die Bereitstellung neuer Programmstände im Sinne der EVB-IT Verträge einschließlich Versionswechsel als auch die Störungsbeseitigung im Sinne der EVB-IT Verträge. Die Erfüllung der Anforderungen an die Barrierefreiheit ist mit der Vergütung der Nutzungsrechte und der Pflege- und Supportleistungen abgegolten. Der Auftragnehmer geht die Verpflichtung ein, verschuldensunabhängig die IT-Lösung nachzubessern, wenn die geforderten Anforderungen an die Barrierefreiheit nicht erfüllt werden (§ 443 BGB).“Die Erfüllung der Anforderungen an die Barrierefreiheit ist mit der Vergütung der Nutzungsrechte und der Pflegeleistungen abgegolten.

Die einschlägigen Barrierefreiheit-Bausteine umfassen im Einzelnen:

- Wenn IKT Anschlusspunkte für Eingabe- oder Ausgabegeräte von Benutzern bereitstellt, muss sie mindestens einen Eingangs- und/oder Ausgangsanschluss, der konform zu einem nicht-proprietären Industriestandardformat ist, durch direkten Anschluss oder durch die Verwendung im Handel erhältlicher Adapter zur Verfügung stellen.

ANMERKUNG 1: Die Anforderung zielt darauf ab, durch die Forderung der Verwendung von Standardanschlüssen bei IKT die Kompatibilität mit Assistenztechnologien sicherzustellen.

ANMERKUNG 2: Das Wort „Anschluss“ bezieht sich sowohl auf physische als auch auf kabellose Anschlüsse.

ANMERKUNG 3: Aktuelle Beispiele für nicht-proprietäre Industriestandardformate sind USB und Bluetooth.

D.h. die Notebooks müssen über Schnittstellen für das Anschließen von externen Peripherieprodukten für Menschen mit Behinderung verfügen.

- Die zusammen mit der IKT bereitgestellte Produktdokumentation muss in mindestens einem der folgenden elektronischen Formate verfügbar gemacht werden:

a) einem Webformat, das konform zu den Anforderungen von Abschnitt 9 "Web" der EN 301 549 ist; oder

b) einem Nicht-Web-Format, das konform zu den Anforderungen von Abschnitt 10 "Nicht-Web-Dokumente" der EN 301 549 ist.

ANMERKUNG 1: Dies schließt nicht die Möglichkeit des Bereitstellens der Produktdokumentation in anderen Formaten (elektronisch, gedruckt oder auditiv) aus, welche nicht barrierefrei sind.

ANMERKUNG 2: Dies schließt auch nicht die Möglichkeit des Bereitstellens alternativer Formate aus, welche auf die Erfordernisse bestimmter Benutzergruppen ausgerichtet sind (z. B. Braille-Dokumente für blinde Personen oder leicht lesbare Informationen für Personen mit eingeschränkten kognitiven, Sprach- und Lernfähigkeiten).

ANMERKUNG 3: Wenn Dokumentation in die IKT eingebunden ist, unterliegt die Dokumentation den Anforderungen zur Barrierefreiheit in der EN 301 549.

ANMERKUNG 4: Ein Benutzeragent, der automatische Medientumwandlung unterstützt, wäre für das Verbessern der Barrierefreiheit förderlich.

Ihr Angebot hat alle zur Erfüllung der in der Leistungsbeschreibung enthaltenen Anforderungen an die Barrierefreiheit zu enthalten. Eine gesonderte Vergütung von Leistungen zur Herstellung der Barrierefreiheit erfolgt nicht.

2.14 Nachhaltigkeit

2.14.1 Materialanforderungen

Die Kunststoffe der Gehäuse und Gehäuseteile dürfen bestimmte Stoffe nicht enthalten.

Die genauen Anforderungen sind im Dokument „Kriterienkatalog_Leistung*“ beschrieben.

2.14.2 Transparenz der Lieferkette

Die Lieferkette der vom Bieter angebotenen Geräte muss bis zur zweiten Stufe transparent dargelegt werden (auf Produktionsebene). Dabei sind die einzelnen Stufen der Lieferkette wie folgt definiert.

- Stufe 1: die Endproduktionsstätte und für den Fall, dass in der Endproduktionsstätte lediglich eine Produktveredelung stattfindet, auch auf deren direkte Zulieferbetriebe;
- Stufe 2: alle direkten Zulieferbetriebe der Produktionsstätte der Stufe 1 (Beschränkung

auf 3 im Rahmen der vorliegenden Ausschreibung);

- Stufe 3: alle direkten Zulieferbetriebe der Produktionsstätten der Stufe 2 (nicht für die vorliegende Ausschreibung relevant).

Hinweis: Darzustellen ist die Lieferkette bezogen auf die Produktion der angebotenen Speichermedien. Eine Rückverfolgung der Lieferkette auf „Händlerebene“ ist nicht ausreichend. Füllen Sie dazu mit Angebotsabgabe das Dokument „Transparenz_der_Lieferkette“ aus. Wenn die Abgabe der Anlage nicht bzw. nur unzureichend erfolgt, muss das Angebot ausgeschlossen werden.

2.14.3 Soziale Aspekte

Die ILO-Kernarbeitsnormen nach der beigefügten Mustererklärung müssen als Minimum der Anforderungen im Bereich der sozialen Aspekte der Nachhaltigkeit erfüllt werden. Dazu gibt der Anbieter die diesen Vergabeunterlagen beigefügte Dokument „Mustererklärung zur Einhaltung der ILO-Kernarbeitsnormen“ bei der Beschaffung von IT-Hardware und IT-Dienstleistungen ab.

2.15 Firmware Update-Gerät

Es ist vorgesehen bei Vorhandensein einer BSI-Zulassung zukünftig auch Firmware-Update-Geräte für die mobilen Datenträger in der Rahmenvereinbarung zu berücksichtigen.