

## Leistungsbeschreibung

**Die zu erbringende Leistung umfasst:**

### **A) Hardware**

**Die Hardware umfasst 5 containerfähige Hardware-Sicherheitsmodule auf mindestens 4 Container.**

#### ○ **Architektur:**



- **Logische Trennung der Container:** Das physische Hardware-Sicherheitsmodul ist in mindestens 4 logisch unabhängig voneinander Container aufgegliedert
- **Skalierbarkeit:** Die Anzahl der Container kann bei Bedarf zu einem späteren Zeitpunkt ohne Neubeschaffung der Hardware realisiert werden
- **Multi-Mandanten-Fähigkeit:** Die Struktur des Hardware-Sicherheitsmoduls ermöglicht es, verschiedene Anwendungen aus unterschiedlichen Netzen so zu trennen, dass jeder Mandant sein eigenes Schlüsselmaterial verwendet
- **Timestamp-Modul:** Das Hardware-Sicherheitsmodul verfügt über ein Zeitstempelmodul, welches zur Durchführung von Signaturen verwendet wird
- **Notstromversorgung:** Das Gerät verfügt über eine eigene Batterie, die auch bei Ausfall der Stromversorgung oder längerer Nichtbenutzung das Schlüsselmaterial vor Verlust schützt

#### ○ **Einsatzbereiche und Algorithmen**

- Das Hardware-Sicherheitsmodul muss PKCS#11 unterstützen
- Post-Quantenkryptographie: Das Hardware-Sicherheitsmodul muss für spätere Anwendungsfälle im Bereich der Postquantenkryptographie vorbereitet sein.
  - Dazu gehört, dass das angebotene Hardware-Sicherheitsmodul über Krypto-Agilität und Firmware-Aktualisierbarkeit verfügen muss. Dies erfordert, dass es zwingend möglich sein muss, neue kryptografische Algorithmen ausschließlich über signierte Firmware-Updates nachzurüsten. Ein Austausch oder physischer Umbau der Hardware darf für die Implementierung von Post-Quanten-Kryptografie (PQC) nicht erforderlich sein.
  - Unterstützung von PQC-Standardalgorithmen: Das System muss die mathematische und speicherseitige Verarbeitung von

quantenresistenten Algorithmen gemäß den aktuellen Vorgaben von NIST (z. B. ML-KEM, ML-DSA) und/oder BSI (z. B. XMSS, LMS) nativ unterstützen oder über ein direkt verfügbares Software-/Firmware-Erweiterungspaket des Herstellers abbilden können.

- Verarbeitung großer Schlüsselweiten und Signaturen: Die Hardware und der kryptografische Coprozessor müssen architektonisch für die im Vergleich zu klassischen Verfahren (RSA/ECC) signifikant größeren PQC-Schlüsselweiten und PQC-Signaturen ausgelegt sein, ohne dass es zu Systemabstürzen oder unzulässigen Timeouts in den angebundenen Applikationen kommt.
- Erstellung von eIDAS-konformen Signaturen: Die Hardware-Sicherheitsmodule müssen geeignet sein für den Einsatz in Infrastruktur zur Erstellung qualifizierter elektronischer Signaturen nach eIDAS. Die eIDAS-Konformität ist durch einschlägige ETSI Normen oder gleichwertige Nachweise belegbar.
- **Sicherheit und Zertifizierung**
  - Physische Sicherheit: Schutz vor Manipulation durch Zertifizierung nach FIPS 140-2 Level 4
  - Verschlüsselung: Alle innerhalb der Container gespeicherten Schlüssel sind hardwareseitig geschützt und verlassen das Modul niemals im Klartext.
- **Hardwareform**
  - Eigenständiges Gerät für den Einbau im 28" Serverschrank inkl. notwendigem Befestigungsmaterial (z. B. Rails)
- **Anzahl der Signaturen**
  - Jeder Container muss mindestens 2.000 Signaturen pro Sekunde durchführen können
  - Die Leistung kann ohne den Erwerb neuer Hardware bei Bedarf durch Aufstockung der Anzahl der Container auf bis zu vier weitere Container erhöht werden
- **Netzwerkanbindung**
  - Das Hardware-Sicherheitsmodul können redundant im Netzwerk angebunden werden
- **Lifecycle**
  - Die Hardware-Sicherheitsmodule müssen mindestens eine Laufzeit von 7 Jahren unterstützen



	<p style="text-align: center;">Lotto Thüringen 198/26 – Beschaffung von Hardware-Sicherheitsmodulen mit Wartungsvertrag und Implementierungsunterstützung BC1_Leistungsbeschreibung Offenes Verfahren gem. § 15 VgV</p>	
---	---	---

- **Bedienung**
  - **Remote-Management:** Das Hardware-Sicherheitsmodul muss vollständig Remote administriert werden können
  - **Zugriffsschutz:** Der Nutzerzugriff ist mittels Mehrfaktor-Authentifizierung durch die Verwendung von Smartcards abgesichert
- **Lieferumfang**
  - 5 x Hardware-Sicherheitsmodul
  - 5 x Einbaumaterial
  - Mind. 2 Lesegeräte für Smartcards
  - Pro Gerät mind. 10 Smartcards
  - Software zur Administration der Hardware-Sicherheitsmodule über die Kommandozeile der Hardware-Sicherheitsmodule
  - Software zur Administration (Windows- und Linuxversion als Installationspaket)
  - Anwenderhandbücher (auch digital möglich)
  - Einrichtung aller Komponenten, die zum Betrieb des Timestamp-Moduls und zur Programmierung auf Firmwareebene notwendig sind
  - Software für die Verwendung des Timestamp-Moduls
  - Erteilung aller Lizenzen für die Verwendung der Hardware-Sicherheitsmodule und des Timestamp-Moduls

## B) Wartungsvertrag

**Zur Leistung gehört ein Wartungsvertrag für 60 Monate mit folgenden Leistungsinhalten:**

- **Software-Wartung:** Zugang zu den neuesten Software-Updates, Firmware-Releases, Feature-Packs und Sicherheits-Patches.
- **Technischer Support:** Unterstützung bei der Fehlerdiagnose und Fehlerbehebung durch Experten
- **Servicezeiten:** Support während der **Standard-Geschäftszeiten** (Montag bis Freitag, 9:00 bis 17:00 Uhr Ortszeit)
- **Reaktionszeiten:** Reaktion auf Störungen spätestens innerhalb von 12 Stunden
- **Hardware-Reparatur/Austausch:** Im Fehlerfall ist die Reparatur oder der Austausch der Hardware (RMA-Prozess) abgedeckt.
- **Online-Ressourcen:** Unbeschränkter Zugriff auf die Wissensdatenbank (Knowledge Base) und das Kundenportal für Downloads und Ticketerstellung

	<p style="text-align: center;">Lotto Thüringen 198/26 – Beschaffung von Hardware-Sicherheitsmodulen mit Wartungsvertrag und Implementierungsunterstützung BC1_Leistungsbeschreibung Offenes Verfahren gem. § 15 VgV</p>	
---	---	---

- **Verlängerung:** Der Wartungsvertrag muss optional auch über die 60 Monate hinaus bis zum End-of-Life um jeweils ein Jahr bis maximal um weitere 60 Monate verlängert werden können

### **C) Einrichtungs- und Inbetriebnahmeunterstützung**

Für die Ersteinrichtung (Anlegen von Nutzern, Erstellen von Schlüsselmateriale, Einbindung in unsere Umgebungen (3 x Live und 2 x Testsystem) der Hardware-Sicherheitsmodule wird entsprechende Vor-Ort-Unterstützung benötigt. Ebenso unterstützt der Auftragnehmer den Auftraggeber bei der Inbetriebnahme der Hardware-Sicherheitsmodule. Dazu gehört das Anlegen von Nutzern, Einrichten von Backups, Anbindung des Netzwerkes im HSM und Konfiguration zur Verwendung des Timestamp-Moduls.