

Wichtiger Hinweis:

Muster - Der Inhalt der Leistungsbeschreibung kann sich bis zur Aufforderung der Angebotsabgabe ändern.

Lieferung eines elektronischen Schließsystems für technische Objekte des Auftraggebers in Bochum

Technische Vorbemerkungen und Mindestanforderungen

1. Gegenstand der Beschaffung / Leistungsabgrenzung

1.1 Gegenstand der Beschaffung ist die Lieferung eines elektronischen Schließsystems einschließlich der hierfür erforderlichen Systemkomponenten frei Lieferadresse des Auftraggebers.

1.2 Montage- und Einbauleistungen, insbesondere der Einbau von Zylindern in Türen, Tore, Schränke oder sonstige Elemente, sind nicht Bestandteil der ausgeschriebenen Leistung, soweit im Leistungsverzeichnis nicht ausdrücklich etwas Abweichendes geregelt ist.

1.3 Sämtliche angebotenen Komponenten müssen systemkompatibel sein und sich innerhalb einer einheitlichen Systemarchitektur verwalten, programmieren und dokumentieren lassen.

2. Herstelleranforderungen: Managementsysteme und Zertifizierungen

2.1 Der Hersteller der angebotenen Systemlösung muss

- aufgrund der sensiblen Einsatzgebiete der elektronischen Schließzylinder nach DIN ISO 9001 zertifiziert sein.
- Ein ganzheitliches Informationssicherheits-Managementsystem (ISMS) nach DIN EN ISO27001 verfügen und entsprechend zertifiziert sein (Entwicklung, Vertrieb, Betrieb, Pflege von Produkten, Servicedienstleistungen sowie Softwareplattformen).
- Ein zertifiziertes Umweltmanagementsystem nach DIN EN ISO 14001 nachweisen.

2.2 Ein Zertifikat nach DIN EN 15684 muss für das Schließsystem vorliegen

2.3 Für die Schließanlage muss eine VdS-Anerkennung der Klasse BZ+ gemäß VdS 2156-2 sowie für Schalteinrichtungen von Einbruchmeldeanlagen gemäß VdS 2119 vorhanden sein.

2.4 Die Nachweise gemäß den Ziffern 2.1 bis 2.3 sind in geeigneter Form, z. B. durch Vorlage gültiger Zertifikate, mit dem Angebot einzureichen.

2.5 Beim elektronischen Schließsystem muss es sich um ein am Markt etabliertes und bewährtes Produkt handeln. Aus diesem Grund muss das Produkt mindestens 5 Jahre am Markt vorahnden sein

3. Projektierungs- und Feinplanungsphase nach Zuschlag

3.1 Schließplan sowie Berechtigungs- und Rechtekonzept werden nach Zuschlag im Rahmen einer Projektierungs- und Feinplanungsphase erarbeitet. Der Schließplan wird hierbei grundsätzlich nicht vollständig für das Gesamtprojekt im Voraus festgelegt, sondern jeweils für die anstehende Roll-out-Stufe erarbeitet, abgestimmt, freigegeben und fortgeschrieben.

3.2 Der Auftragnehmer erstellt die hierfür erforderlichen Unterlagen eigenverantwortlich in Abstimmung mit dem Auftraggeber.

3.3 Sämtliche Dokumente sind in deutscher Sprache auszufertigen.

3.4 Die Abstimmungen erfolgen grundsätzlich per Videokonferenz. Der Auftraggeber behält sich vor, zusätzlich bis zu sechs Abstimmungstermine in Präsenz vor Ort durchzuführen. Etwaige Reise-, Fahrt-, Neben- und Übernachtungskosten des Auftragnehmers sind mit den Einheitspreisen bzw. Pauschalen abgegolten und werden nicht gesondert vergütet.

3.5 Die Projektierungsergebnisse, insbesondere Schließplanstände, Berechtigungsstrukturen, Zylinderlisten und sonstige Systemparameter, sind dem Auftraggeber je Roll-out-Stufe in digitaler Form zur Prüfung und Freigabe vorzulegen.

3.5 Eine verbindliche Umsetzung sowie die finale Zuordnung von Komponenten, Berechtigungen und Parametern erfolgt jeweils erst nach ausdrücklicher Freigabe der Unterlagen für die betreffende Roll-out-Stufe durch den Auftraggeber.

4. Festlegung der konkreten Zylinder

4.1 Die endgültige Festlegung der Zylindertypen, Zylinderlängen und der Zuordnung zu Türen bzw. Schließpunkten wird im Rahmen der Projektierung in Abstimmung mit dem Auftraggeber festgelegt. Verbindliche Stückzahlen ergeben sich je Roll-out-Stufe aus dem freigegebenen Berechtigungs-, Roll-out- und Umsetzungskonzept.

5. Ermittlung der Identmedien / Schlüssel

5.1 Die Anzahl und Ausprägung der Identmedien bzw. elektronischen Schlüssel wird im Rahmen der Projektierung in Abstimmung mit dem Auftraggeber festgelegt. Verbindliche Stückzahlen ergeben sich je Roll-out-Stufe aus dem freigegebenen Berechtigungs-, Roll-out- und Umsetzungskonzept.

6. Roll-out in Stufen

6.1 Die Ausbringung bzw. Inbetriebnahme des Systems sowie die Erarbeitung, Fortschreibung und Freigabe des Schließplans erfolgen abschnittsweise in mehreren Roll-out-Stufen.

6.2 Die konkrete Roll-out-Planung inkl. der jeweils zugehörigen Schließplanstände und Berechtigungsstrukturen, wird nach Zuschlag in der Projektierungsphase gemeinsam durch Auftraggeber und Auftragnehmer erarbeitet, dokumentiert und durch den Auftraggeber freigegeben.

6.3 Der Auftragnehmer stellt die termingerechte Bereitstellung von Komponenten, Parametrierungen und softwareseitigen Strukturen entsprechend den abgestimmten Roll-out-Stufen sicher. Dies umfasst auch die rechtzeitige Erstellung, Fortschreibung und Vorlage der für die jeweilige Roll-out-Stufe erforderlichen Schließplan- und Berechtigungsunterlagen.

7. Mengenansätze

7.1 Die im Leistungsverzeichnis genannten Mengen sind unverbindliche Orientierungs- bzw. Schätzmengen. Wir verpflichten uns nicht die Mengen komplett abzunehmen.

7.2 Die endgültigen Mengen sowie die konkrete Zuordnung zu Schließpunkten ergeben sich erst aus der freigegebenen Projektierungs- und Feinplanung gemäß den Ziffern 4 bis 6 sowie aus dem abgestimmten Roll-out-Konzept gemäß Ziffer 7.

8. Technische Mindestanforderungen – Systemkomponenten

8.1 Elektronische Schließzylinder

8.1 Die elektronischen Zylinder sind ohne Verkabelung auszuführen.

8.2 Die Zylinder dürfen keine interne Spannungsversorgung besitzen; die Energieversorgung erfolgt ausschließlich über den Schlüssel bzw. das jeweilige Identmedium, soweit die betreffende Bauart dies vorsieht.

8.3 Elektronische Zylinder müssen ohne An- und Aufbauten liefer- und montierbar sein; sämtliche Elektronik ist innerhalb des geschützten Zylindergehäuses unterzubringen.

8.4 An den Bestandstüren sind unterschiedliche Schutzbeschläge bzw. Schutzrosetten mit Zylinderabdeckung und zentrischem, schmalem Schließkanal verbaut, welche auch in Zukunft genutzt werden sollen. Zum Einsatz kommende elektronische Schließzylinder müssen damit kompatibel sein.

8.4 Profilzylinder sind modular aufzubauen, sodass die Zylinderlänge vor Ort an wechselnde Einbausituationen angepasst werden kann.

8.5 Profilzylinder sind grundsätzlich mit verstellbarem Schließbart anzubieten. Der Schließbart ist aus bruchfestem, korrosionsbeständigem Edelstahl auszuführen.

8.6 Zylinder müssen mit gebräuchlichen Sonderausstattungen lieferbar sein, insbesondere mit erhöhtem Anbohrschutz, Freilauf und Gefahreineinrichtung.

8.7 Der Betrieb der Zylinder muss im Temperaturbereich von mindestens - 25 °C bis +85 °C gewährleistet sein.

8.9 Die Zylinder müssen wartungsfrei sein.

9. Elektronische Schlüssel / Identmedien

9.1 Die elektronischen Schlüssel müssen die für die Systemfunktion erforderliche Energie bereitstellen und diese aus handelsüblichen Batterien beziehen.

9.2 Alle Schlüssel sind mindestens in Schutzart IP67 auszuführen. Hierbei muss der einfache Austausch von Batterie oder Akku jederzeit gewährleistet sein.

9.3 Es müssen Schlüsselvarianten verfügbar sein, die eine optische und akustische Signalisierung, insbesondere zu Batterie- und Berechtigungsstatus, bereitstellen.

9.5 Nachbestellte Schlüssel, die einer bestehenden elektronischen Gruppe zugeordnet werden, müssen ohne erneute Programmierung an allen bestehenden Zylindern schließberechtigt sein, an denen die betreffende Gruppe berechtigt ist.

9.6 Es müssen Schlüssel mit integriertem Bluetooth-Modul zur mittelbaren Kommunikation mit der Systemsoftware verfügbar sein.

9.7 Die elektronischen Schlüssel müssen so ausgeführt sein, dass die zur Betätigung des Schließsystems erforderlichen Drehmomente dauerhaft und sicher übertragen werden können.

Hierbei darf bei bestimmungsgemäßem Gebrauch keine erhöhte Bruchgefahr des Schlüssels bestehen.

10. Berechtigungslogik, Zeitmodelle, Revalidierung, Kryptografie

10.1 Alle Schließkomponenten sind ab Werk fest einer bestimmten Schließanlage zugewiesen und dauerhaft mit einer eindeutigen Schließanlagennummer versehen. Eine nachträgliche Neukodierung oder freie Konfiguration ist nicht möglich.

10.2 Elektronische Schließberechtigungen müssen sowohl an den Schließzylindern als auch an den Nutzerschlüsseln änderbar bzw. umprogrammierbar sein.

10.2 Es muss möglich sein, Zeitpläne und Gültigkeitszeiträume einzurichten, um zeitlich begrenzte Zutrittsberechtigungen abzubilden.

10.3 Eine Revalidierung elektromechanischer Schlüssel muss auch bei fehlender Verbindung zwischen Server und Remote-Programmiergerät möglich sein (Offline-Validierung).

10.4 Kryptografische Verfahren, Konfigurationen und Schlüssellängen müssen dem Stand der Technik entsprechen.

10.5 Für alle administrativen Zugriffe, für Remote-Zugriffe sowie für Zugriffe auf sicherheitsrelevante Funktionen ist eine Mehrfaktor-Authentifizierung bereitzustellen.

10.6 Sämtliche sicherheitsrelevanten Vorgänge sind manipulations- und revisionssicher zu protokollieren. Hierzu zählen insbesondere:

- An- und Abmeldungen,
- fehlgeschlagene Anmeldeversuche,
- Änderungen an Rollen und Berechtigungen,
- Ausgabe, Sperrung, Löschung und Reaktivierung von Identmedien,
- Änderungen von Zeitprofilen und Schließgruppen,
- Firmware-Updates,
- Konfigurationsänderungen,
- administrative Exporte und Auslesevorgänge.

10.6.1 Die Protokolle müssen mindestens Benutzerkennung, Zeitstempel, betroffene Objekte, Art der Änderung und Ergebnis enthalten.

10.6.2 Protokolldaten müssen in einem exportierbaren Standardformat bereitgestellt werden; soweit möglich, ist eine Anbindung an ein SIEM-/Syslog-/Web-Service-Verfahren zu unterstützen.

11. Software und Programmiermittel

11.1 Für die Verwaltung und Programmierung der elektronischen Schließanlage sind mindestens bereitzustellen:

- Verwaltungs- bzw. Programmiersoftware,
- Programmiergerät,
- Programmierschlüssel.

11.2 Mindestfunktionen der Verwaltungssoftware

11.2.1 Verwaltung von Zylindern, Schlüsseln/Identmedien, Personen sowie Schlüsselausgaben und Schlüsselrückgaben.

11.2.2 Verwaltung von Berechtigungen über einen Schließplan.

11.2.3 Programmierung zeitlich eingeschränkter Zutrittsberechtigungen.

11.2.4 Unterstützung von Auswertungen, Protokollen, Quittungen und Druckfunktionen.

11.2.5 Benutzermanagement sowie Verwaltung von Programmierschlüsseln und PIN-/PUK-Codes zur Softwareanmeldung.

11.2.6 Import- und Export-Schnittstellen zur Datenübernahme.

11.2.7 DSGVO-unterstützende Funktionen, insbesondere Anonymisierung, Deaktivierung und permanente Löschung.

11.2.8 Unterstützung eines virtuellen Netzwerkes sowie Administration von Remote-Programmiergeräten.

11.2.9 Die Verwaltung der Zutritts-Berechtigungen, die Ausgabe neuer Medien und die Vergabe von temporären Berechtigungen für externe Dienstleister soll in einem übergeordneten Managementsystem von mehreren Standorten (FIT) erfolgen können.

11.3 Strukturierung, Schnittstellen und Auditfunktionen

11.3.1 Es muss möglich sein, Domains und Tags einzurichten.

11.3.2 Die Software muss über eine Web-Service-Schnittstelle verfügen.

11.3.3 Das Auslesen von Ereignislisten aus Schlüsseln und Zylindern muss über eine Genehmigerfunktion steuerbar sein.

11.4 Bereitstellungsmodelle / Rechenzentrum / Sicherheitstests

11.4.1 Datenspeicherung, Programminstallation und Netzwerkverbindungen dürfen ausdrücklich nicht als Cloud-Service vorgenommen werden. Das System muss aufgrund des Datenschutzes und der Datensicherheit in der virtuellen Serverumgebung von Stadtwerke Bochum Netz GmbH lauffähig sein.

11.4.3 Die Softwarelösung ist nachweislich zu jedem Hauptrelease oder mindestens jährlich einem externen Penetrationstest zu unterziehen und Ergebnisse sind dem Kunden bei Bedarf zur Verfügung zu stellen.

11.4.4 Schließanlagendaten, Firmware und Sicherheitszertifikate sind über einen zentralen Datenserver automatisiert und grundsätzlich durchgängig verfügbar bereitzustellen.

12. Einweisung / Schulung und Betreiberbefähigung

12.1 Der Auftragnehmer weist das technische Personal des Betreibers in die Systemstruktur und Funktionsweise der elektronischen Schließanlage ein.

12.2 Der Auftragnehmer unterweist den zuständigen Personenkreis in der Bedienung der Programmiergeräte und der Verwaltungssoftware.

12.3 zusätzlich zur funktionalen Einweisung ist eine IT-Sicherheitsdokumentation bereitzustellen. Diese muss insbesondere enthalten:

- Systemarchitektur,
- Rollen- und Rechtekonzept,
- Netz- und Schnittstellenübersicht,
- Backup-/Restore-Verfahren,
- Update- und Patchverfahren,
- Notfall- und Eskalationswege.