

Vergabeverfahren

**Beschaffung und
Dienstleistung für Aufbau
eines Privileged Access
Managements (PAM)**

Vergabenummer

20263441277

Inhalt

1	Zuschlagskriterien.....	3
2	Preis	3
3	Technische Anforderungen	3
3.1	Beschreibung	3
3.2	Projektumfang	4
3.3	Produkt Kriterienkatalog	5
3.3.1	Muss-Kriterien.....	5
3.3.2	Bewertungskriterien	7
4	Dienstleistung.....	8
4.1	Kriterienkatalog.....	8
5	Projektteam	9

1 Zuschlagskriterien

Preis	70 Prozent
Produkt Bewertungskriterien	30 Prozent
Gesamt	100 Prozent

2 Preis

Der angebotene Festpreis enthält alle Kosten frei Verwendungsstelle. Eingeschlossen sind hier alle Kosten für Verpackung, Transport und Montage bis zur funktionsfähigen Übergabe, für Nebenleistungen, etwaige Auslösungs-, Fahrt-, Zehr- und Wegegelder, Lohnzulagen, Über- und Sonntagsstunden, welche aus Gründen, die der Auftragnehmer zu vertreten hat, geleistet werden müssen.

Die Ausführung der oben genannten Leistung wird zu den eingesetzten Preisen angeboten. Das Angebot gilt bis zum Ablauf der Bindefrist.

Die Angebotssumme ist der Leistungsbeschreibung / dem Leistungsverzeichnis / dem Preisblatt zu entnehmen.

3 Technische Anforderungen

3.1 Beschreibung

Die PAM-Lösung muss vollständig **on-premises** ohne Cloud-Abhängigkeiten betrieben werden können und privilegierte Zugriffe über ein **zentralisiertes, agentenloses Proxy-Gateway** bereitstellen. Sie hat **sämtliche RDP- und SSH-Sitzungen manipulationssicher aufzuzeichnen**, einschließlich Metadaten und integritätsgeschützter Speicherung (AES-256/SHA-256). Die Lösung muss in **streng segmentierten IT/OT-Netzen** funktionsfähig sein, Zielsystem-Passwörter im **AES-256-verschlüsselten Vault** verwalten und Benutzer über **rollenbasierte Rechte** sowie optionales 4-Augen-Prinzip steuern. Zusätzlich sind **LDAPS-Integration**, TLS-geschützte Kommunikation, **SIEM-Anbindung**, NTP-Synchronisation und lokale **MFA-Einbindung per RADIUS/LDAP** erforderlich.

3.2 Projektumfang

Der Auftragnehmer hat eine vollständige Lieferung, Bereitstellung und Implementierung einer On-Premises-PAM-Lösung entsprechend den technischen Anforderungen zu erbringen. Der Leistungsumfang umfasst insbesondere:

1. Lizenzbereitstellung

- Lieferung der für den Betrieb erforderlichen Jahreslizenzen inkl. initialem Support (z. B. Core-Ressourcen, Named-User-Komponenten, optionale Tunneling-Funktionen).
- Lizenzierung muss den im Projekt definierten Umfang (500 Zielsysteme und 100 berechnigte Nutzer) abdecken.
- Laufzeit 5 Jahre mit Verlängerungsoption.

2. Implementierungsleistungen

Der Bieter hat die vollständige Umsetzung der Lösung zu gewährleisten, u. a.:

- Projektkoordination, Workshops zur Anforderungsaufnahme und Feinkonzeption
- Erstellung eines Berechtigungs-, Rollen- und Betriebskonzepts
- Aufbau von QA- und Produktionsinstanzen inkl. Basisprozesse (Recovery, Audit, Break-Glass)
- Technische Umsetzung der definierten Use-Cases (Proxying, Session-Überwachung, Vault-Nutzung, Rollenmodell)
- Anbindung an bestehende Infrastruktur (Active Directory/LDAPS, NTP, Backup, Zertifikate, SIEM-Anbindung, MFA via RADIUS/LDAP)
- Onboarding von 500 Zielsystemen (IT-, OT- und Backend-Systeme)
- Umsetzung von Gruppen- und Policy-Konzepten für Assets
- Durchführung von Funktionstests, Pilotbetrieb und Wissenstransfer
- Begleitung der produktiven Inbetriebnahme

Der Gesamtaufwand beträgt 48 Personentage. (Abrufkontingent ohne Verpflichtung seitens ÜSTRA, diese aufzubrauchen)

3. Dokumentation & Übergabe

- Erstellung einer vollständigen Betriebs- und Administrationsdokumentation
- Übergabe an Betriebsteam, inkl. Know-how-Transfer
- Optional: HA-Einrichtung einschließlich Testszenarien

3.3 Produkt Kriterienkatalog

3.3.1 Muss-Kriterien

Muss-Kriterien sind zwingend vom Bieter in der vorgegebenen Weise zu erfüllen. Wird ein Muss-Kriterium nicht erfüllt, wird das Angebot ausgeschlossen.

	Parameter	Funktionalität	angeboten (Bieterangaben)
1	Privilegierte Zugriffs- und Sitzungsverwaltung		
1.1	Session Recording	Vollständige, manipulationssichere Aufzeichnung privilegierter RDP- und SSH-Sitzungen	☐ Ja ☐ Nein
1.2	Session-Metadaten	Erfassung von Befehlen, Aktionen, gestarteten Programmen	☐ Ja ☐ Nein
1.3	Live-Überwachung	Auditoren können Sitzungen live einsehen	☐ Ja ☐ Nein
1.5	Integritätsschutz der Aufzeichnungen	AES-256 & SHA-256 gesicherte Aufzeichnungen	☐ Ja ☐ Nein
2	OT- und KRITIS-Kompatibilität		
2.1	Betrieb in isolierten Netzen	Vollständige Funktionsfähigkeit ohne Internetzugang	☐ Ja ☐ Nein
2.2	Kein Agent auf Zielsystemen	Zugriff ausschließlich agentenlos	☐ Ja ☐ Nein
2.4	Strikte Netzwerk-segmentierung	Primary Domain, Target Domain, Admin Domain strikt getrennt	☐ Ja ☐ Nein
2.5	Kein direkter Zugriff Primary → Target	Verbindungen müssen zwingend über das PAM-Gateway laufen	☐ Ja ☐ Nein
2.6	Gängige Zertifizierungen der Lösung	Die Lösung ist von mind. einer gängigen Institution (BSI, ANSSI, TISAX...) geprüft und zertifiziert	☐ Ja ☐ Nein
2.7	Weiterentwicklung	Weiterentwicklung der Software findet innerhalb der EU statt	☐ Ja ☐ Nein
3	On-Premise Betrieb		
3.1	Vollständiger On-Prem Betrieb	Keine Cloud-Abhängigkeiten für Authentifizierung, Vault, Recording	☐ Ja ☐ Nein
3.2	Betrieb in virtualisierten Umgebungen	Kompatibel zu VMware ESXi	☐ Ja ☐ Nein
3.3	Keine externen Update-Server	Updates ausschließlich über signierte Offline-Pakete	☐ Ja ☐ Nein
3.5	Hardening	Die Lösung wird seitens des Herstellers als gehärtete Appliance bereitgestellt	☐ Ja ☐ Nein
4	Passwort- und Schlüsselmanagement		
4.1	AES-256 verschlüsselter Vault	Speicherung sämtlicher Zielkonten & SSH-Keys	☐ Ja ☐ Nein
4.2	Passwort-vertraulichkeit	Passwörter dürfen Nutzern niemals angezeigt werden	☐ Ja ☐ Nein
4.3	Credential Injection	Authentifizierung erfolgt automatisiert über den Proxy	☐ Ja ☐ Nein
4.4	Geschützter Schlüsselspeicher	Schutz aller privaten Schlüssel (RDP/SSH/HTTPS)	☐ Ja ☐ Nein

5	Privilegien- & Berechtigungsverwaltung		
5.1	RBAC	Rollenbasierte Zugriffskontrolle	☐ Ja ☐ Nein
5.2	Trennung Admin/User/Auditor	Dedizierte Rollen müssen vorhanden sein	☐ Ja ☐ Nein
5.3	Zielsystem-Zugriffslisten	Benutzergruppen + Zielsystemgruppen (ACL)	☐ Ja ☐ Nein
6	MFA-Integration		
6.1	On-Prem MFA	Nutzung lokaler MFA-Systeme (RADIUS/LDAP)	☐ Ja ☐ Nein
6.2	Keine Cloud-MFA-Pflicht	MFA-Funktionen müssen offline nutzbar sein	☐ Ja ☐ Nein
7	Kryptographie & Kommunikationssicherheit		
7.1	TLS-Versionsvorgabe	Mindestens TLS 1.2 / 1.3 auf allen Interfaces	☐ Ja ☐ Nein
7.2	Cipher Suites	AES-GCM (128/256), ECDHE, RSA ≥ 3072 Bit	☐ Ja ☐ Nein
7.3	Sicherer SSH-Transport	AES-GCM / AES-CTR, SHA-2	☐ Ja ☐ Nein
8	Logging & SIEM-Anbindung		
8.1	Syslog-Export	Export sicherheitsrelevanter Events via Syslog	☐ Ja ☐ Nein
8.2	TLS-gesicherte Logausgabe	Syslog muss TLS-verschlüsselt unterstützt werden	☐ Ja ☐ Nein
8.3	Fälschungsschutz der Logs	Integritätsschutz und konsistente Zeitstempel	☐ Ja ☐ Nein

3.3.2 Bewertungskriterien

Bewertungskriterien haben einen Wert, dessen Gesamtsumme am Ende zu 30% in die Zuschlagsbewertung einfließt.

	Parameter	Funktionalität	angeboten (Bieterangaben)
1	Privilegierte Zugriffs- und Sitzungsverwaltung		
1.4	Session-Termination	Auditoren können Sitzungen jederzeit beenden	☐ Ja ☐ Nein 15 Pt.
2	OT- und KRITIS-Kompatibilität		
2.3	Unterstützung industrieller Protokolle	RDP, SSH, Telnet, VNC (Proxy-basiert)	☐ Ja ☐ Nein 25 Pt.
3	On-Premise Betrieb		
3.4	Signierte Firmware	Updates müssen GPG-signiert sein	☐ Ja ☐ Nein 5 Pt.
5	Privilegien- & Berechtigungsverwaltung		
5.4	Genehmigungsprozesse	Optionales 4-Augen-Prinzip	☐ Ja ☐ Nein 25 Pt.
6	MFA-Integration		
6.3	Token-Unabhängigkeit	TOTP, Hardware-Token, Smartcards möglich	☐ Ja ☐ Nein 5 Pt.
7	Kryptographie & Kommunikationssicherheit		
7.4	RNG-Anforderungen	Nutzung eines sicheren RNG	☐ Ja ☐ Nein 5 Pt.
8	Logging & SIEM-Anbindung		
8.4	SIEM-Integration	Kompatibel zu Standard-SIEM-Systemen	☐ Ja ☐ Nein 20 Pt.
			Gesamt 100 Pt.

4 Dienstleistung

Die Leistung umfasst Konzeption, Implementierung und Integration der Lösung in bestehende Systeme (z. B. Verzeichnisdienste, Authentifizierung, SIEM), einschließlich Aufbau von Test- und Produktivumgebungen sowie Umsetzung von Berechtigungs- und Sicherheitskonzepten.

Weiterhin beinhaltet sie das Onboarding von Systemen und Accounts, die Einrichtung von Sicherheitsfunktionen (z. B. MFA, Logging, Monitoring) sowie die Durchführung von Tests, Pilotbetrieb und Wissenstransfer. Abschließend ist eine vollständige Dokumentation bereitzustellen.

4.1 Kriterienkatalog

Wird ein Kriterium nicht erfüllt, wird das Angebot ausgeschlossen.

	Parameter	Funktionalität	angeboten (Bieterangaben)
1	Koordination		
1.1	Projektkoordination / Planung		☐ Ja ☐ Nein
1.2	Projektmanagement / Meetings		☐ Ja ☐ Nein
1.3	Kick-Off Workshop		☐ Ja ☐ Nein
			Angeboten: ... PT
2	Konzepte		
2.1	Anforderungen / Feinkonzept		☐ Ja ☐ Nein
2.2	Berechtigungskonzept	Assets, User ...	☐ Ja ☐ Nein
2.3	Basisprozesse	Recovery, Audit, Update, ...	☐ Ja ☐ Nein
			Angeboten: ... PT
3	Umsetzung		
3.1	Produktiv-/QA-Umgebung	Init. Konfiguration gemäß Konzept	☐ Ja ☐ Nein
3.2	Technische Anbindung	E-Mail, Backup, Zertifikate, MFA, SIEM	☐ Ja ☐ Nein
3.3	Onboarding	Zielsysteme, Enduser, Berechtigungen	☐ Ja ☐ Nein
3.4	Umgebung Testen	Produktivumgebung testen	☐ Ja ☐ Nein
			Angeboten: ... PT
4	Einführung		
4.1	Pilotphase	Unterstützung, Troubleshooting	☐ Ja ☐ Nein
4.2	Wissenstransfer	Meeting, Workshop, o.ä.	☐ Ja ☐ Nein
4.3			Angeboten: ... PT
5	Abschluss		
5.1	Dokumentation		☐ Ja ☐ Nein
			Angeboten: ... PT

5 Projektteam

Der für das Projekt verantwortliche Mitarbeiter und dessen Vertretung sind namentlich sowie mit Kontaktdaten (Anschrift, Telefon, E-Mail) zu benennen. Der für das Projekt verantwortliche Mitarbeiter oder dessen Vertretung wird bei ggf. stattfindenden Terminen für Vergabeverhandlungen teilnehmen.

Die Qualifikationen dieser zwei Projektmitarbeiter sind je Mitarbeiter insbesondere durch mindestens zwei und bis zu fünf mitarbeiterbezogene Projektreferenzen, vorhandene Einzelqualifikation und berufliche Ausbildung nachzuweisen.

