



Leistungsbeschreibung

zur Beschaffung eines Rahmenvertrages über den Bezug von Lizenzen für eine Clientmanagement-Software zzgl. Wartung, Pflege und Support sowie von Dienstleistungen für den Zweckverband Südwestfalen-IT, seine 100-prozentige Tochtergesellschaft SIT GmbH und für seine Verbandsmitglieder/Kunden

Südwestfalen-IT
Sonnenblumenallee 3
58675 Hemer

Inhalt

1. Allgemeines	3
1.1. Auftraggeber	3
1.2. Struktur von Zweckverband und Verbandsmitgliedern	3
2. Leistungsgegenstände	4
3. Bewertung	5
4. Beschreibung Leistungsgegenstand I (MUSS- und KANN-Kriterien)	6
4.1. Funktion.....	6
4.2. System	11
4.3. Usability	13
5. Beschreibung Leistungsgegenstand II	15
6. Beschreibung Leistungsgegenstand III	15

1. Allgemeines

1.1. Auftraggeber

Der Zweckverband Südwestfalen-IT (SIT) plant die Vergabe einer Rahmenvereinbarung zur Beschaffung von Lizenzen inkl. Wartung, Pflege und Support sowie Einführungsunterstützung einer Clientmanagement-Software für sich, ihre Tochtergesellschaft SIT GmbH sowie ihre Verbandsmitglieder/Kunden.

Die aktuell eingesetzte Clientmanagement-Software Lösung wird für das Client-Management, die automatisierte Verteilung von Software und Windows Betriebssystemen sowie das Patch-Management eingesetzt. Die aktuelle Lösung erreicht am 31. Dezember 2026 ihr End-of-Life (EOL). Daher muss eine Migration zu einer neuen Lösung bis zum EOL umgesetzt werden. Anschließend werden für diese Software kein Support sowie keine Updates mehr bereitgestellt. Eine Migration soll der Auftraggeber selbst durchführen können, nachdem der Auftragnehmer ihm gegenüber Einführungsunterstützung, geleistet hat (siehe Leistungsgegenstand III.b)

Im Falle der Zuschlagserteilung kommt eine Rahmenvereinbarung zwischen dem bezuschlagten Bieter einerseits als Auftragnehmer (AN) und der SIT andererseits als Auftraggeber (AG) zustande. Die beabsichtigte Abnahmemenge wird in Nummer 2 dieser Leistungsbeschreibung aufgeführt.

1.2. Struktur von Zweckverband und Verbandsmitgliedern

Die SIT ist ein Zweckverband für kommunale IT-Dienstleistungen. Sie ist u.a. IT-Dienstleister für 72 Kreise, Städte und Gemeinden. Sie betreut rund 22.000 Arbeitsplätze sowie zusätzliche Arbeitsplätze im schulseitigen Bereich und bietet umfassende IT-Services – von der Basisinfrastruktur über Netzwerke über den Betrieb von Rechenzentren, der Bereitstellung von virtuellen Arbeitsumgebungen für Verbandsmitglieder und Dritte auf eigenen Rechenzentrumressourcen, zu technischer Unterstützung und dem Lizenzmanagement.

Die SIT entstand 2018 aus dem Zusammenschluss der KDZ Citkomm (Kommunale Datenverarbeitungszentrale Citkomm) und der KDZ Westfalen-Süd (Kommunale Datenzentrale Westfalen-Süd).

Die SIT betreibt verschiedene Betriebsumgebungen für Anwendungslösungen, die für spezielle Fachverfahren durch Verbandsmitglieder und/oder Dritte eingesetzt werden.

Die im Rahmen dieser Ausschreibung zu beschaffende Clientmanagementsoftware wird in folgenden, klar abgegrenzten Einsatzszenarien genutzt:

1. **Eigenbetrieb durch und für den Zweckverband SIT:** Die Software wird zur Verwaltung und Steuerung der SIT-eigenen Endgeräte eingesetzt und im Rechenzentrum der SIT betrieben.
2. **Betrieb für Kunden des Zweckverbands:** Die Software wird im Rechenzentrum der SIT betrieben und den Kunden des Zweckverbands zur Nutzung bereitgestellt. In diesem Zusammenhang werden den Kunden entsprechende Nutzungsrechte eingeräumt.

3. **Lizenzweitergabe an Kunden:** In dieser Konstellation können die Lizenzen an Verbandsmitglieder – soweit diese nicht die Konstellation nach 2. Nutzen, übertragen werden, die die Software eigenständig auf eigenen Servern und zu eigenen Zwecken betreiben.

Bei allen vorgenannten Konstellationen handelt es sich um GOV-Lizenzen (öffentliche Auftraggeber).

Für die EDU-Lizenzen (für den Schulbereich) findet ausschließlich die unter Ziffer 2 und 3 beschriebene Konstellation Anwendung.

Bitte beachten Sie hierzu auch das Dokument „Eigenerklärung zur Nutzungsrechteübertragung“ (Vordruck 6).

2. Leistungsgegenstände

Die Leistung gliedert sich im Folgenden in drei Leistungsgegenstände. Durch den Bieter sind alle drei Leistungsgegenstände anzubieten.

Leistungsgegenstand I: Lizenzen für eine Clientmanagement-Software (sowohl GOV- als auch EDU-Lizenzen).

Achtung: Es werden zwei separate Preisblätter zur Verfügung gestellt, je nachdem ob ein Angebot für reine Kauflizenzen oder für reine Mietlizenzen zur Verfügung abgegeben wird. Sollten bei Kauflizenzen zusätzliche Funktionen als Mietbestandteil angeboten werden (Mischmodell), sind die Angaben im Preisblatt für Kauflizenzen abzugeben.

Leistungsgegenstand II: Wartung, Pflege und Support

Leistungsgegenstand III:

- a. Einführungsunterstützung für Erstinstallation und Konfiguration (bei Bedarf pro Instanz), ggf. auch direkt für Kunden/Verbandsmitglieder
- b. Onboarding Workshops, ggf. auch direkt für Kunden/Verbandsmitglieder

Der Bieter kann für Leistungsgegenstand I und dem damit zusammenhängenden Leistungsgegenstand II entweder reine Mietlizenzen, reine Kauflizenzen oder Kauflizenzen mit zusätzlichen Funktionen als Mietbestandteil (Mischmodell) anbieten; dies jeweils für einen Zeitraum von 48 Monaten (Hinweis: Dieser Zeitraum dient der Vergleichbarkeit von Miet- und Kauflizenzen; siehe hierzu auch das Dokument „Erläuterung zur Angebotsbewertung“) In jedem Fall muss der Auftragnehmer die Berechtigung erhalten, die Lizenzen bzw. die Nutzungsrechte daran an die Zugangsberechtigten weiterzugeben.

Bei gleicher Wertungskennzahl zweier Angebote wird das „Mischmodell“ (Kauflizenzen mit zusätzlichen Funktionen als Mietbestandteil) vor reinen Kauflizenzen vor reinen Mietlizenzen bevorzugt (s. Nr. 5 der Erläuterungen zur Angebotsbewertung). In den Lizenzmodellen kommt die beigefügte Rahmenvereinbarung zustande. Für die jeweiligen Einzelabrufe gelten entweder – bei reinen Kauflizenzen – die AGB zu EVB-IT-Überlassung Typ A (Kauf gegen Einmalvergütung), bei

reinen Mietlizenzen – die AGB zu EVB-IT-Überlassung Typ B (dauerhafte Überlassung), beim Mischmodell die jeweils entsprechenden AGB zu EVB-IT-Überlassung Typ A (gilt für die Kaufbestandteile) bzw. AGB zu EVB-IT-Überlassung Typ B (gilt für die Mietbestandteile) sowie in beiden Fällen die AGB zu EVB-IT-Pflege S und die AGB zu EVB-IT-Dienstleistungen .

Beim Einzelabruf einer Lizenz (Leistungsgegenstand I) wird gleichzeitig die Wartung, die Pflege und der Support (Leistungsgegenstand II) mit abgerufen.

Der Auftragnehmer hat auf Abruf im Wege der Einzelbeauftragung die oben genannten und nachfolgend tiefergehend beschriebenen Leistungen zu erbringen, die im Folgenden über den MUSS- und KANN-Kriterien (Nummer 4 dieser Leistungsbeschreibung) konkretisiert sind.

Der Grundumfang umfasst Lizenzen für 19.100 Systeme (Server oder Arbeitsplätze) wovon 7.100 Lizenzen für den Governmentbereich (öffentliche Auftraggeber im Folgenden „GOV“) und 12.000 Lizenzen für den Schulbereich (im Folgenden „EDU“) vorgesehen sind. Dies ist die Grundabnahmemenge (in den Vergabeunterlagen auch „Grundumfang“ genannt).

Da derzeit nicht alle Verbandsmitglieder/Kunden durch die SIT betreut werden, können die Verbandsmitglieder/Kunden Lizenzen und Dienstleistungen für maximal 12.000 weitere Systeme in variablen Stückzahlen beauftragen.

3. Bewertung

Die Bewertungskriterien zum für Leistungsgegenstand I gem. Nummer 4 dieser Leistungsbeschreibung sind in die Bereiche Funktion, System und Usability untergliedert, die wiederum jeweils in MUSS- oder KANN-Kriterien ausgestaltet sind. Sämtliche Kriterien sind in den Bieterangaben zur Leistungsbeschreibung (Anlage) mit „ja“ oder „nein“ zu beantworten.

MUSS-Kriterien (Grundfunktionen) (im nachfolgenden ROT gekennzeichnet)

Alle unter Nummer 4 dieser Leistungsbeschreibung aufgeführten MUSS-Kriterien bilden die Mindestanforderungen an den Leistungsgegenstand I und sind zwingend erforderlich sowie vollständig zu erfüllen, ohne dass hierfür über die im Angebot ausgewiesenen Preise hinaus zusätzliche Kosten entstehen. Wird auch nur ein MUSS-Kriterium mit „nein“ beantwortet, führt dies zwingend zum Ausschluss des Angebots.

Diese Funktionen bilden die Mindestanforderungen an den Leistungsgegenstand I. Diese Funktionen müssen sämtliche MUSS-Kriterien abdecken und diese vollständig erfüllen, ohne dass hierfür über die im Angebot ausgewiesenen Kosten hinaus zusätzliche Kosten entstehen.

KANN-Kriterien (im nachfolgenden GRÜN gekennzeichnet)

Alle unter Nummer 4 dieser Leistungsbeschreibung aufgeführten KANN-Kriterien können, bei Erfüllung in den angebotenen Lizenzen, zusätzliche Bewertungspunkte bringen, die in die Wertungskennzahl (s. Nr. 5 der Erläuterungen zur Angebotsbewertung) einfließen.

Die KANN-Kriterien werden gemäß dem Dokument „Bieterangaben zur Leistungsbeschreibung“ bepunktet; eine Beantwortung mit „nein“ führt hierbei nicht zum Ausschluss des Angebots, sondern ausschließlich zu einer Bewertung des jeweiligen Kriteriums mit 0 Punkten.

Alle Funktionen (MUSS- und KANN-Kriterien) werden nachfolgend näher beschrieben und sind durch entsprechende Verweise (Nummerierungsangaben z. B. 2.1, 2.2 etc.) eindeutig den „Bietangaben zur Leistungsbeschreibung“ (**im Folgenden Kriterienkatalog**) zuzuordnen. Grundsätzlich gelten alle MUSS- und KANN-Kriterien sowohl für GOV- als auch für EDU-Lizenzen mit Ausnahme des Kriteriums „Windows Defender Management“ (Kriterium 2.22 im Kriterienkatalog). Weitere Einzelheiten zur Bewertungssystematik ergeben sich aus dem Dokument „Erläuterung der Angebotsbewertung“.

4. Beschreibung Leistungsgegenstand I (MUSS- und KANN-Kriterien)

Mit dem Einzelabruf des Leistungsgegenstands I sind die Lizenzen der Client-Management-Software bereitzustellen.

Ziel ist die Bereitstellung einer lizenzierbaren Software zur zentralen Verwaltung von Clients und Servern in einer heterogenen, netzwerksegmentierten IT-Infrastruktur.

Der Betrieb erfolgt sowohl zentral im Rechenzentrum des Auftraggebers als auch in separierten Insellösungen (z. B. je Schule oder Organisationseinheit) sowie im parallelen Betrieb mehrerer logisch getrennter Instanzen zur Abbildung unterschiedlicher Mandanten und Sicherheitszonen. Die Software muss administrative Funktionen, Rollen- und Berechtigungskonzepte (nach Least-Privilege-Prinzip) sowie zentrale Steuerung und Überwachung unterstützen. Die Lizenzierung muss unabhängig von der Anzahl der Serverinstanzen flexibel auf verschiedene Instanzen und organisatorische Bereiche aufteilbar sein.

Die Software muss so konzipiert und konfigurierbar sein, dass der Auftraggeber mit ihrer Hilfe die rechtlichen Anforderungen (z. B. BSI-Grundschutz, ISO/IEC 27001) umsetzen kann. Sie muss dazu geeignete Funktionen, Schnittstellen und Konfigurationsmöglichkeiten bereitstellen, die eine nachvollziehbare und dokumentierbare Umsetzung der Anforderungen ermöglichen.

Wie bereits oben beschrieben, können durch den Bieter entweder reine Miet- **oder** reine Kauflizenzen **oder** Kauflizenzen mit zusätzlichen Funktionen als Mietbestandteil (Mischmodell) angeboten werden. Die einzelnen Kriterien sind im Folgenden in die Rubriken Funktion, System und Usability sowie innerhalb der Rubriken in MUSS- und KANN-Kriterien unterteilt.

4.1. Funktion

Muss-Kriterien:

- **Ausführbare Skripte (Kriterium 2.2 im Kriterienkatalog)**

Gängige Scriptsprachen wie z.B. CMD(Batch), PS(Powershell), Python, Bash(Linux), etc., müssen über das Clientmanagement auf Endgeräte ausgeführt werden können. Zusätzlich zu einer ggf. vorhandenen/eigenen Scripting Engine | Rückmeldungen über Fehlercodes und Erfolgsmeldungen müssen in das Clientmanagement zurückgeführt werden können und für den Administrator in der Oberfläche visuell sichtbar sein (Stichwort: returncodes/errorcodes).

- **Feines Rechtemanagement (Kriterium 2.3 im Kriterienkatalog)**

Der Zugriff auf die einzelnen Module und der darin befindlichen Funktionen des Clientmanagement muss durch ein Berechtigungssystem anpassbar sein. Kunden müssen eigene Jobs/Pakete/Abfragen bauen können, ohne auf Daten von anderen Kunden zugreifen zu können. Ein administrativer Zugriff auf alle Module und Funktionen muss mandantenübergreifend möglich sein (Zentraler Administrator).

- **OS (Operating System) - Deployment (Kriterium 2.4 im Kriterienkatalog)**

Die Installation von Betriebssystemen (OS-Deployment - mindestens Windows OS) über einen Netzwerkboot (PXE) muss gewährleistet sein.

- **Softwareverteilung (Kriterium 2.5 im Kriterienkatalog)**

Es müssen Softwarepakete verteilt und der Status kontrolliert werden können. (Return Codes). Ein entsprechender Eintrag im Inventar des Endgerätes nach der Installation/Deinstallation muss vorhanden sein: Die Aktualisierungen (Updates) einzelner Softwares müssen in der Oberfläche des Clientmanagement nachvollzogen werden können. Es sollte möglich sein, ggf. eine Reparatur von Softwarepaketen durch weitere Versionen/Updates/Revisionen zu realisieren.

- **Dynamische Gruppen (Kriterium 2.6 im Kriterienkatalog)**

Es muss möglich sein, Dynamischen Gruppen anhand von frei wählbaren Kriterien wie z.B. Name des Gerätes, eigene definierte Variablen, Hardware aus dem Inventar, Installierter Software, etc., zu erstellen.

- **Inventarisierung Hardware (Kriterium 2.7 im Kriterienkatalog)**

Die Erfassung von einem Hardware-Inventar pro Endgerät (Beispiele: Angeschlossen Bildschirme, CPU, RAM, Festplatten, USB-Geräte, ggf. Drucker, andere Peripherie (Fingerabdruck-Sensoren, Scanner, ...), etc.) muss gewährleistet sein.

- **Inventarisierung Software (Kriterium 2.8 im Kriterienkatalog)**

Die Erfassung von einem Software-Inventar pro Endgerät (Beispiele: Menge Installierter Software, grobe Nutzung (nicht pro Client, sondern für gesamt Statistik), Version, Installationsstatus, ggf. noch verfügbare Lizenzen, etc.) muss gewährleistet sein.

- **Managed-Software (Kriterium 2.9 im Kriterienkatalog)**

Die Verteilung von vorpaketierter Software vom Hersteller/Clientmanagement muss möglich sein.

- **Updateverteilung & Überwachung (Kriterium 2.10 im Kriterienkatalog)**

Gefordert ist ein Updatemanagement (Verteilung von System-, Office-, ggf. Third-Party-Updates (Beispiel: Adobe Reader DC, 7-Zip, Keepass, Cisco Webex, usw.) als Modul integriert in das Clientmanagement. Eine zeitliche, bzw. Kriterien basierte Steuerung/Verteilung der Updates muss möglich sein (Beispiel: Systemupdates sollen bei einer kleinen Gruppe sofort installiert werden, Gesamtes Ausrollen erst nach 2-7 Tagen, ggf. Staffelung um Last auf das Netzwerk zu minimieren zum Microsoft Updatetag).

- **Wake on Lan (Kriterium 2.11 im Kriterienkatalog)**

Die Funktion „Wake on LAN“ (Aufwecken über Netzwerk) muss gegeben sein (Sicheres Aufwecken, nach aktuellem Stand der Technik).

- **Gateway Verfügbarkeit (Kriterium 2.12 im Kriterienkatalog)**

Endgeräte die durch z.B. einen Standortwechsel das direkte LAN (Local Area Network) zum Server verlassen, müssen fließend in eine Kommunikation über Gateways wechseln können. (auch ohne VPN-Tunnel)

- **Definierung von Testgruppen (Software/Update/Treiber/OS) (Kriterium 2.13 im Kriterienkatalog)**

Gefordert ist, eine Möglichkeit, Testgruppen für die Bereiche Software-, Betriebssystem-, Update- und Treiber -installationen zu definieren, damit Pakete vor dem vollständigen Ausrollen getestet werden können.

- **Auswertung / Reports (Kriterium 2.14 im Kriterienkatalog)**

Gefordert ist die Erstellung von Auswertungen/Reports über das Inventar (Software/Hardware), die Gerätedaten und ggf. über die Einstellungen der Endgeräte für entsprechend Berechtigte Administratoren. Die Auswertungen/Reports dürfen nur Daten enthalten, die der jeweilige Kunde/Administrator sehen darf (eigene Endgeräte). Übergeordnete Administratoren mit Zugriff auf mehrere Bereiche, müssen auch mehr Daten sehen können.

- **Zeitgesteuertes Ausführen von Befehlen (Kriterium 2.15 im Kriterienkatalog)**

Die Ausführung von zeitgesteuerten Befehlen wie z.B. Neustarten und Aufwecken (WOL) des Endgerätes, CMD/PS im Kontext des Endgerätes starten, Lokale Dienste/Eventmanager/Laufende Prozesse des Endgerätes anzeigen, Zugriff auf das Dateisystem des Endgerätes, Benutzer vom Endgerät abmelden, muss gegeben sein.

- **Anpassen der Windows Registry (Kriterium 2.16 im Kriterienkatalog)**

Einträge in der Windows Registry müssen erstellt/angepasst/gelöscht werden können (Diese Funktion muss in der Script-Engine oder in der Paketierung allgemein enthalten sein).

- **Softwarekiosk (Kriterium 2.17 im Kriterienkatalog)**

Endgerätebenutzern muss die Möglichkeit gegeben werden können, Pakete selbstständig, durch z.B. einen Softwarekiosk, auf dem Gerät zu installieren. Dabei muss flexibel gesteuert werden können, welche Pakete im Softwarekiosk hinterlegt sind (durch die Administratoren).

- **Treiber-Management & Verteilung (Kriterium 2.18 im Kriterienkatalog)**

Die Installation von Treibern für das OS-Deployment, WINPE und Geräteeinrichtung muss möglich sein.

- **Anbindung Linux (Kriterium 2.19 im Kriterienkatalog)**

Der Agent muss auf Debian, Ubuntu (LTS) und Redhat installiert werden können. Die Distributionen und die installierte Software müssen inventarisiert werden können.

- **Installations-Push und -Verzögerung (Kriterium 2.20 im Kriterienkatalog)**

Gefordert ist, dass auf dem Endgerät die Paketinstallation durch den Benutzer verschoben werden kann. Dabei muss eine maximale Anzahl an möglichen Verschiebungen angegeben werden können. Die Paketinstallationen müssen von zentralen Administratoren weiterhin erzwungen durchgeführt werden können.

- **Abhängigkeitsmanagement (Kriterium 2.21 im Kriterienkatalog)**

Abhängigkeiten zwischen verschiedener Software müssen definiert werden können, z.B. über Installationsreihenfolgen, erforderliche Vorinstallationen (z.B. .NET Framework).

- **Windows Defender Management (MUSS-Kriterium für Education-Lizenzen (EDU)/KANN-Kriterium für Government—Lizenzen (GOV)) (Kriterium 2.22 im Kriterienkatalog)**

Windows Defender Verwaltung (Ereignisse/Updates/Aktionen) | Automatisierte Abläufe steuern und einsehen | Zentrale Rückmeldung der Endgeräte in das Clientmanagement

Kann-Kriterien:

- **Einstellungen (Kriterium 2.23 im Kriterienkatalog)**

Dynamische Regelsätze sollen durch Administratoren angelegt werden können, um das Verhalten von Clients zu steuern (Beispiel: Energiemanagement, Bitlocker Verschlüsselung, Proxyeinstellungen, Default-Einstellungen für z.B. Internet-Browser)

- **Patchmanagement unabhängig von Microsoft WSUS (Kriterium 2.24 im Kriterienkatalog)**

Die Verteilung von Windowsupdates sollen ohne Microsoft WSUS (Windows Server Update Services) verteilt und gesteuert werden können.

- **Anbindung an Entra ID (Kriterium 2.25 im Kriterienkatalog)**

Gewünscht ist, dass cloudbasierte Active Directories wie Entra ID angebunden werden können.

- **Anbindung MacOS (Kriterium 2.26 im Kriterienkatalog)**

Gewünscht ist das Einbinden / Aktualisieren / Erfassen von MacOS Distributionen. Weiterhin soll ebenfalls Software-Pakete und Updates für MacOS verteilt und zur Verfügung gestellt werden können.

- **Aufzeichnungstool(s) für Installationen (Kriterium 2.27 im Kriterienkatalog)**

Tool(s) zur Aufzeichnung von komplizierten Installationen (Registry-Keys, Verschieben/Kopieren von Dateien, Erkennung von Klicks/Mausbewegungen)

- **Lizenzmanagement (Kriterium 2.28 im Kriterienkatalog)**

Gewünscht ist ein Modul zur Erfassung von Lizenzen (Bereits genutzte Lizenzen | Noch zur Verfügung stehende Lizenzen | Warnung vor Lizenzmangel und Ablauf von Lizenzen)

- **BIOS-Management (Kriterium 2.29 im Kriterienkatalog)**

Gewünscht ist, zentral Einstellungen im BIOS des Endgerätes zu verwalten, alternativ eine Schnittstelle zur Anbindung Herstellerspezifischer Tools. Auch um ggf. BIOS- und Firmware-updates durchführen zu können.

- **APPX-Überwachung (Kriterium 2.30 im Kriterienkatalog)**

Überwachung von Microsoft Store Applikationen (Installation/Deinstallation/Update/Erfassung)

- **Ereignisbasierte Aktionen (Kriterium 2.31 im Kriterienkatalog)**

Aktionen (z.B. Softwareverteilung, Scripting, Gruppenverschiebung) sollen auf definierbare Ereignisse reagieren können (z.B. Anmeldung, bestimmter Status, Inventarisierungswert)

- **Flexible Paketverknüpfung (Kriterium 2.32 im Kriterienkatalog)**

Pakete müssen verkettbar sein (z.B. Vorbereitungs-, Haupt-, Nachbereitungspaket), um komplexe Installationslogiken abzubilden.

- **Bitlocker Management (Kriterium 2.33 im Kriterienkatalog)**

Verwaltung der Bitlocker Funktionalität | Überwachen und Managen der Funktion | Einstellungen managen | Bitlocker Schlüssel Export | Die Verwaltung der BitLocker-Verschlüsselung muss die in TR-02102 empfohlenen Schlüssellängen und Verschlüsselungsverfahren (z.B. AES-256) unterstützen. Der Export von BitLocker-Schlüsseln muss sicher erfolgen und darf keine Schwachstellen aufweisen, die gegen TR-02102 verstoßen.

- **Fernwartung (Bildschirmfreigabe/Spiegelung) (Kriterium 2.34 im Kriterienkatalog)**

Es soll gewährleistet sein, dass eine Fernwartung (Bildschirmfreigabe/Spiegelung) auf Endgeräte über die Managementoberfläche gestartet werden kann. Es soll ein beaufsichtigter und unbeaufsichtigter Zugriff auf Endgeräte möglich sein. Die Dialoge der UAC (User Account Control) soll angezeigt werden können.

- Revisionssichere Datenlöschung (Kriterium 2.35 im Kriterienkatalog)

Gewünscht wird eine revisionssichere Datenlöschung (inkl. Protokoll für AUDIT-Zwecke) von Daten auf Festplatten der Endgeräte.

4.2. System

Muss-Kriterien:

- On-Premise (Kriterium 2.36 im Kriterienkatalog)

Das Clientmanagement muss On-Premise betrieben werden können.

- Anbindung AD / LDAP(S) / Multidomain Unterstützung (Kriterium 2.37 im Kriterienkatalog)

Eine Anbindung mehrerer Active Directorys (AD) über eine Managementoberfläche muss gewährleistet werden, genauso wie das Job-Basierte Auslesen von Objekt spezifischen über LDAP/LDAPS. Organisationseinheiten und Objekte müssen aus dem Active Directory synchronisiert werden können.

- Verwaltung von Geräten außerhalb der Domäne (Kriterium 2.38 im Kriterienkatalog)

Geräte ohne Domäne müssen ebenfalls aufgenommen und verwaltet werden können.

- Beachtung der Netzwerktopologie (Kriterium 2.39 im Kriterienkatalog)

Der gesamte Funktionsumfang muss über mehrere Subnetze/VLANs verfügbar sein.

- Datenschutz (Verarbeitung von Nutzerdaten) (Kriterium 2.40 im Kriterienkatalog)

Die aktuell geltenden Standards im Bereich Datenschutz müssen Anwendung finden. Die Verarbeitung von Nutzerdaten unter Berücksichtigung von aktuellen DSGVO-Richtlinien muss gegeben sein.

- DIPS / Depots (Kriterium 2.41 im Kriterienkatalog)

Es müssen mehrere Depots (Fileserver) flexibel genutzt, und die Daten-Last damit unter den Depots verteilt werden können. Weiterhin müssen die Depots über verschiedene Subnetze/VLANs hinweg angebunden werden können. Diese Funktionalitäten sollen zur Entlastung des Netzwerkes beitragen.

- Einfaches Updaten des Clientmanagements (ohne Hersteller-Support möglich) (Kriterium 2.42 im Kriterienkatalog)

Die Updates des Clientmanagementsystems müssen ohne Support des Herstellers durch einen Administrator durchführbar sein (maximal ein Manntag).

- **Informationssicherheit (Kriterium 2.43 im Kriterienkatalog)**

Die angebotene Clientmanagement-Lösung muss über ein Mehrfaktor-Authentifizierungsverfahren (MFA) verfügen, das explizit für alle Administrationszugänge des Clientmanagementsystems Pflicht ist. Die MFA-Implementierung muss den aktuellen Sicherheitsstandards entsprechen und eine sichere, nachvollziehbare Authentifizierung gewährleisten.

Zusätzlich muss die Software alle kryptografischen Verfahren und Schlüssellängen gemäß der aktuellen Ausgabe der BSI-Technischen Richtlinie TR-02102 unterstützen. Der Anbieter ist verpflichtet, im Rahmen des Angebots schriftlich nachzuweisen, welche Verschlüsselungsverfahren (z. B. AES, RSA, ECC), Hashfunktionen (z. B. SHA-256, SHA-3) und Schlüssellängen (z. B. mindestens 256 Bit für symmetrische Schlüssel, 3072 Bit für RSA) in der Software verwendet werden. Die Umsetzung muss den aktuellen Empfehlungen der TR-02102 entsprechen, insbesondere im Hinblick auf Verwendungszeiträume und die geplante Migration auf quantensichere Verfahren.

Die Konformität mit der TR-02102 muss jährlich durch den Auftragnehmer über einen schriftlichen Nachweis bestätigt werden, der dem Auftraggeber vorzulegen ist. Dieser Nachweis muss die technische Umsetzung, die verwendeten Algorithmen und die geplante Migration auf zukunftsichere Verfahren nachvollziehbar dokumentieren.

- **Eindeutiges Identifikationsmerkmal (Kriterium 2.44 im Kriterienkatalog)**

Die Identifikationsmerkmale für die Aufnahme eines Endgerätes ins Clientmanagement und zur Kommunikation mit einem Endgerät müssen mindestens UUID/SMBIOS GUID enthalten. Die Identifikationsmerkmale müssen im Clientmanagement (wenn mehrere vorhanden sind) hierarchisch anpassbar sein (wählbar).

- **Verwaltete Client- und Serverbetriebssysteme (Kriterium 2.45 im Kriterienkatalog)**

Gefordert sind alle Betriebssysteme ab Windows 11 und Windows Server 2016 aufwärts.

- **Einfache Installation der Infrastruktur (Kriterium 2.46 im Kriterienkatalog)**

Das Clientmanagement muss durch einen Administrator vor Ort aufgesetzt werden können. (maximal ein Personentag)

- **Aktuell angemeldeten Benutzer anzeigen (Kriterium 2.47 im Kriterienkatalog)**

Der angemeldete Benutzer am Endgerät muss in der Oberfläche sichtbar angezeigt werden können.

- **Skalierbarkeit für große Umgebungen (Kriterium 2.48 im Kriterienkatalog)**

Die Architektur muss skalierbar sein (Lastverteilung, horizontale Skalierung).

Kann-Kriterien:

- Gateway OS-Installation (Kriterium 2.49 im Kriterienkatalog)

Gewünscht ist, dass die OS-Installationen zwar durch einen Management Point(o.ä.) gesteuert werden können, das eigentliche Image für die OS-Installationen aber von dem nächstgelegenen Depot zum Client genommen wird | Optimal: Die OS-Installation kann auch ohne Netzwerkverbindung zum Hauptserver bzw. zur Hauptstruktur durchgeführt werden.

- Schwachstellenscan (Kriterium 2.50 im Kriterienkatalog)

Für das Updatemanagement, aber auch gesamt für das Endgerät ein Schwachstellenscan (offene CVE) | Schließung der CVE z.B. durch Updatemanagement oder durch Administrator vor Ort | Rückmeldung in das Clientmanagement System

- API-Schnittstelle (Kriterium 2.51 im Kriterienkatalog) (Kriterium 2.51 im Kriterienkatalog)

Eine Anbindung an andere Lösungen zur Übertragung von Daten (Beispiele: Ansible, MDM) ist wünschenswert.

- Integrationsschutz (Kriterium 2.52 im Kriterienkatalog)

Integrität der übertragenen Pakete muss überprüfbar sein (z.B. Hash-Prüfung, Signierung). Weiterhin sollten Pakete Revisionssicher erstellt werden können.

- CMDB-Anbindung (Kriterium 2.53 im Kriterienkatalog)

Synchronisierung von Asset-Daten mit einer zentralen CMDB (z.B. i-doit, ServiceNow)

- Endpoint Security-Schnittstellen (Kriterium 2.54 im Kriterienkatalog)

Austausch mit Antivirus/EDR/XDR-Systemen zur Statusauswertung oder Policy-Steuerung

4.3. Usability

Muss-Kriterien:

- GUI (Grafical User Interface) gestützte Paketierungs-Engine (Kriterium 2.55 im Kriterienkatalog)

Das Clientmanagementsystem muss die Erstellung von Software- und Konfigurationspaketen in einfacher und benutzerfreundlicher Weise unterstützen. Hierzu sind insbesondere Funktionen wie grafische Bedienkonzepte (z. B. Drag-and-Drop-Mechanismen), assistentengestützte Verfahren (Wizard) oder ein modular aufgebautes Bausteinprinzip bereitzustellen.

Darüber hinaus muss die Nachvollziehbarkeit erstellter Pakete jederzeit gewährleistet sein. Dies umfasst insbesondere eine transparente Darstellung der Paketbestandteile, Konfigurationsparameter sowie etwaiger Abhängigkeiten und Änderungen.

- **Systemüberwachung und Monitoring (Kriterium 2.56 im Kriterienkatalog)**

Das Clientmanagementsystem muss zusätzlich zur Ansicht innerhalb der Managementoberfläche über standardisierte Schnittstellen (z.B. Syslog, REST-API, SIEM-Adapter) in ein zentrales Monitoring- oder SIEM-System (z.B. CrowdStrike Falcon Next-Gen SIEM, Elastic Security, Splunk, Microsoft Sentinel) integrierbar sein. Alle administrativen Eingriffe müssen protokolliert werden. Die Protokolle müssen mindestens 90 Tage lang aufbewahrt werden und revisionssicher sein.

Sofern eine Schnittstelle derzeit nicht zur Verfügung steht muss diese in einem gemeinsamen Projekt im 1. Quartal 2027 angebunden werden können.

- **Lizenzen unabhängig von Anzahl der Serverinstanzen (Kriterium 2.57 im Kriterienkatalog)**

Die Software muss über zentrale, dynamische Lizenzpools pro Instanz lizenziert werden können, die unabhängig von der Anzahl der Instanzen und Server und ohne zusätzlichen Aufwand und Kosten eine flexible Lizenzverteilung auf alle angebundenen Clients ermöglicht.

- **Übersicht und Usability (Kriterium 2.58 im Kriterienkatalog)**

Das Clientmanagementsystem muss eine benutzerfreundliche und klar strukturierte Bedienoberfläche bereitstellen, die es Administratorinnen und Administratoren ermöglicht, die wesentlichen Funktionen des Systems nach einer Schulungsdauer von maximal drei Personentagen sachgerecht und eigenständig zu nutzen. Zur Unterstützung der Einarbeitung und des laufenden Betriebs muss eine geeignete Wissensdatenbank bzw. Dokumentation (z. B. in Form von Online-Dokumentation, Handbüchern oder Anwenderforen) verfügbar sein.

Die Systemoberfläche muss eine übersichtliche Darstellung der verwalteten Clients, Funktionen und Module gewährleisten und sowohl für Administratoren als auch für vertretungsweise eingesetzte Personen geeignet sein. Der Funktionsumfang der einzelnen Module (z. B. der Paketierungs-Engine) muss in einem angemessenen Verhältnis zur Übersichtlichkeit und Bedienbarkeit der Benutzeroberfläche stehen.

Kann-Kriterien:

- **Intelligente Suchfunktion (Kriterium 2.59 im Kriterienkatalog)**

Gewünscht ist: eine Suche, welche mit Teilbegriffen (Teilstring-Suche) bereits Einträge im Clientmanagement sichtbar machen kann.

- **Stammdatenpflege (Kriterium 2.60 im Kriterienkatalog)**

Das Clientmanagement (Eigenschaften der Clients/Inventar) soll erweiterbar um eigene (benutzte definierte) Felder sein | zusätzlich Langtextfelder für Bemerkungen | ggf. mehrere Bemerkungsfelder für verschiedene Zwecke

5. Beschreibung Leistungsgegenstand II

Mit Leistungsgegenstand II werden die Anforderungen an Wartungs-, Pflege- und Supportleistungen für die Clientmanagement-Software beschrieben. Gegenstand dieses Leistungsgegenstandes ist die Sicherstellung eines ordnungsgemäßen, aktuellen und störungsfreien Betriebs der eingesetzten Software.

Im Rahmen der Wartungs- und Pflegeleistungen muss dem Auftraggeber während der Vertragslaufzeit ein uneingeschränkter Zugang zu Aktualisierungen (wie bspw. Weiterentwicklungen und Fehlerkorrekturen) der Clientmanagement-Software zur Verfügung stehen.

Darüber hinaus wird ein zeitnahe und bedarfsgerechter Support bei Problemen, Störungen sowie bei allgemeinen technischen oder fachlichen Fragestellungen erwartet. Diese Supportleistungen müssen ohne zusätzliche Kosten im Rahmen der vereinbarten Wartungs-, Pflege- und Supportleistungen erbracht werden.

Ergänzend ist dem Auftraggeber der Zugang zu einem geeigneten Nutzerforum oder einer vergleichbaren Plattform bereitzustellen, die der Information, dem fachlichen Austausch mit anderen Anwendern sowie der transparenten Nachverfolgung von Funktionswünschen und Weiterentwicklungen (z. B. Feature-Requests) dient.

Die Wartungs-, Pflege und Supportleistungen sind unter Berücksichtigung der geltenden Sicherheitsanforderungen sowie der Vorgaben zur BSI-Konformität entsprechend den Regelungen zu Leistungsgegenstand I zu erbringen.

Muss-Kriterien

- **Support auf Deutsch (mind. C2-Niveau) (Kriterium 3.01 im Kriterienkatalog)**

Der Support beim Auftragnehmer muss mindestens das C2-Niveau erfüllen.

- **Support direkt vom Hersteller möglich (Kriterium 3.02 im Kriterienkatalog)**

Ist die Lösung eines Problems/Tickets innerhalb von 3 Werktagen durch den Auftragnehmer nicht zu realisieren, muss der Hersteller des Clientmanagementsystems mit einbezogen werden.

6. Beschreibung Leistungsgegenstand III

Leistungsgegenstand III.a umfasst die Einführungsunterstützung für die Clientmanagement-Software. Die Leistung ist als bedarfsorientierte Unterstützungsleistung ausgestaltet und muss jeweils auf Abruf durch den Auftraggeber erbracht werden. Abhängig vom Bedarf kann die Leistung während der Vertragslaufzeit mehrfach in Anspruch genommen werden.

Die Einführungsunterstützung dient der **fachlichen und technischen Begleitung** beim Aufbau und der Inbetriebnahme einer Clientmanagement-Instanz in der jeweiligen Systemumgebung des Auftraggebers oder der von ihm betreuten Bedarfsträger. Die Verantwortung für den Betrieb der Infrastruktur sowie für den eigentlichen Betrieb der Clientmanagement-Software verbleibt dabei beim Auftraggeber bzw. bei den von ihm eingesetzten Technikern.

Die Installationsunterstützung erfolgt **remote** und umfasst insbesondere die Anleitung, Beratung und Begleitung der vom Auftraggeber, ggf. auch direkt für Kunden/Verbandsmitglieder, benannten Techniker bei der Installation und Grundkonfiguration der Clientmanagement-Software. Ein dauerhafter administrativer Zugriff des Auftragnehmers auf die Systeme des Auftraggebers ist nicht geschuldet. Ein zeitlich begrenzter Fernzugriff kann, sofern erforderlich und vom Auftraggeber ausdrücklich freigegeben, ausschließlich zum Zweck der Leistungserbringung erfolgen.

Für den Leistungsgegenstand III.b hat der Auftragnehmer darüber hinaus Onboarding-Workshops durchzuführen. Diese dienen der Vermittlung der grundlegenden Funktionsweise der Clientmanagement-Software sowie der erforderlichen Kenntnisse zum eigenständigen Aufbau und zur Inbetriebnahme weiterer Instanzen durch den Auftraggeber. Die Workshops müssen die Schulung der Mitarbeitenden des Auftraggebers sowie ggf. weiterer beteiligter Techniker, ggf. auch direkt für Kunden/Verbandsmitglieder, umfassen und sind inklusive aller Nebenkosten sowie geeigneter elektronischer Schulungsunterlagen zu erbringen.

Ziel der Einführungsunterstützung und Workshops ist es, den Auftraggeber bzw. die Kunden/Verbandsmitglieder in die Lage zu versetzen, die Clientmanagement-Software nach Abschluss der Leistung **eigenständig** zu installieren, zu konfigurieren und in Betrieb zu nehmen.