



Stadt Dortmund
Dortmunder Systemhaus

Projekt- und Verfahrensbeschreibung

Beschaffung und Einführung eines
gesamtstädtischen Identity & Access
Management-Systems

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Hinweise.....	4
1. Einleitung	5
1.1 Ziel des Dokuments	5
1.2 Informationen zur Auftraggeberin	5
1.2.1 Stadt Dortmund	5
1.2.2 Beschreibung des Dortmunder Systemhauses	5
1.2.3 Beschreibung der Aufgaben des FB 11.....	5
2. Projektbeschreibung und Ziele	6
3. Verfahrensbeschreibung	8
3.1 1. Stufe - Teilnahmewettbewerb	8
3.2 2. Stufe - Verhandlungsverfahren	8
3.3 Zuschlagskriterien.....	8
3.3.1 Zuschlagskriterium Preis	9
3.3.2 Zuschlagskriterium Qualität.....	9
4. Vorabinformation	12
4.1 Dokumentenwerk	12
4.2 Ausschlusskriterien	13
4.2.1 Mindestfunktion/-anforderung: [1075] Kein aktiver Internetzugang.....	13
4.2.2 Mindestanforderung: [1200] Verpflichtung des eingesetzten Personals	13
4.2.3 Mindestfunktion/-anforderung: [1201] Projektsprache	14
4.2.4 Mindestfunktion/-anforderung: [1202] Kundendokumentation	14
4.2.5 Mindestfunktion/-anforderung: [67] Der Betrieb und die Installation des IAM ist unter VMWARE möglich.....	14
4.2.6 Mindestfunktion/-anforderung: [541] Disaster-, Recovery und Restoremöglichkeit nach Systemausfall	14
4.2.7 Mindestfunktion/-anforderung: [10] Historisierung / Logging von IAM-Aktionen	

4.2.8	Mindestfunktion/-anforderung: [784] Protokolle: OAuth 2.0 (Open ID Connect) wird zur Authentisierung unterstützt.	15
4.2.9	Mindestfunktion/-anforderung: [785] Microsoft Public-Key-Infrastruktur (PKI) auf Basis des X.509-Standards (zertifikatsbasierendes Verfahren) muss unterstützt werden.	15
4.2.10	Mindestfunktion/-anforderung: [786] Framework: SAML 2.0 (Security Assertion Markup Language) wird unterstützt.	15
4.2.11	Mindestfunktion/-anforderung: [789] Protokolle: Kerberos Authentifizierung wird unterstützt.	15
4.2.12	Mindestfunktion/-anforderung: [917] Protokolle: LDAP wird zur Authentisierung unterstützt.	15
4.2.13	Mindestfunktion/-anforderung: [24] ID Zuordnungen über das IAM-Datenmodell soll n:1:m abbildbar sein (n Quellstammdaten zu einer Identität zu m Zielsystemaccounts).	15
4.2.14	Mindestfunktion/-anforderung: [25] Erweiterbares IAM-Schema.	15
4.2.15	Mindestfunktion/-anforderung: [582] Entkopplung des Benutzernamens von der E-Mail-Adresse.	16
4.2.16	Mindestfunktion/-anforderung: [810] Eindeutige, lebenslange, historisierbare Zuordnung einer natürlichen Person zu einer digitalen Identität im IAM.	16
4.2.17	Mindestfunktion/-anforderung: [408] Geschäftsprofil-Zuweisung/-Entzug auf Basis unterschiedlicher Regelwerke und Zusammenhänge auf Basis beliebiger Attribute 17	
4.2.18	Mindestfunktion/Mindestanforderung [322]: Verwendung von HTTPS.	17
4.2.19	Mindestfunktion/-anforderung: [2] Rollenbasierte Provisionierung.	17
4.2.20	Mindestfunktion/-anforderung: [16] Sicherstellung der bidirektionalen Datenübertragung.	17
4.2.21	Mindestfunktion/-anforderung: [1203] Transaktionsverwaltung.	17
4.2.22	Mindestfunktion/Mindestanforderung [956]: HR-Systemanbindung SAP HCM18	
4.2.23	Mindestfunktion/-anforderung: [1071] Wartungsvertragsende schränkt die IAM-Funktionalität / Nutzbarkeit / Betriebsfähigkeit nicht ein.	18
4.2.24	Mindestfunktion/-anforderung: [989] Eindeutige Nutzer- Zuordnung und Authentisierung.	19

4.2.25	Mindestfunktion/-anforderung: [998] Kryptographischer Schutz des Authentisierungsschlüssels und des Authentisierungsprotokolls	19
4.2.26	Mindestfunktion/ Mindestanforderung: [342] Austauschformat CSV	19
	Das IAM muss das CSV Austauschformat unterstützen. Bei Bearbeitung von CSV-Dateien muss der Bearbeitungsstatus hinterlegt und die CSV-Datei historisiert werden.	19
4.2.27	Mindestfunktion/ Mindestanforderung: [918] LDAP muss zum Austausch von Information und zur Abfrage von Informationen genutzt werden können.	19
4.2.28	Mindestfunktion/ Mindestanforderung: [333] AD-Provisionierungsschnittstelle	19
4.2.29	Mindestfunktion/ Mindestanforderung: [34] Anlage und Löschung von Accounts, sowie Zuweisung und Entzug von Berechtigungen in Zielsystemen mit verschiedenen Berechtigungsschemas.....	20
4.2.30	Mindestfunktion/-anforderung: [401] Unterstützung eines Vier-Augen-Prinzips	21

Hinweise

Im vorliegenden Dokument wird auf eine Geschlechterdifferenzierung verzichtet. Rollenbezeichnungen werden daher vereinfacht in der männlichen Form beschrieben. Dies dient ausschließlich der Vereinfachung der Formulierung und der Steigerung der Lesbarkeit.

1. Einleitung

1.1 Ziel des Dokuments

Dieses Dokument beschreibt im Rahmen des Teilnahmewettbewerbs das Projekt zur Beschaffung und Einführung eines stadtweiten Identity & Access Management Systems bei der Stadt Dortmund.

Es soll grundlegendes Verständnis für das Vorhaben schaffen und die Schwerpunkte des Projektes und des einzuführenden Systems inkl. der damit verbundenen Prozesse aufzeigen.

Das Dokument informiert des Weiteren vorab über die Ausschlusskriterien im anschließenden Bieterverfahren.

1.2 Informationen zur Auftraggeberin

1.2.1 Stadt Dortmund

Die Stadt Dortmund ist eine große kreisfreie Stadt im Bundesland Nordrhein-Westfalen. Mit rund 600.000 Einwohnern gehört sie zu den größten Städten Deutschlands und ist wirtschaftlich wie kulturell eine zentrale Metropole der Region.

Die Stadtverwaltung der Stadt Dortmund als Auftraggeberin gliedert sich in mehrere Dezernate, jedes Dezernat unterteilt sich in mehrere Fachbereiche und Eigenbetriebe. Insgesamt sind ca. 11.000 Mitarbeitende in der Stadtverwaltung tätig.

Die politische Steuerung erfolgt durch den Rat der Stadt Dortmund sowie den Oberbürgermeister bzw. die Oberbürgermeisterin als oberste Repräsentant(in) und Regierungssitz.

1.2.2 Beschreibung des Dortmunder Systemhauses

Das Dortmunder Systemhaus als Fachbereich (FB10) der Stadt Dortmund ist der zentrale IT-Dienstleister für die gesamte Stadtverwaltung. Neben dem Betrieb eines eigenen Rechenzentrums an 5 Standorten im Stadtgebiet werden insgesamt ca. 1.200 Serversysteme (Windows und Linux, größtenteils virtualisiert) betreut. Die Zahl der zu betreuenden Clients beträgt rund 9.000 Stück.

1.2.3 Beschreibung der Aufgaben des FB 11

Das Personal- und Organisationsamt (FB11) der Stadt Dortmund betreut die Beamt*innen, Beschäftigten und Ausbildungskräfte der Stadt Dortmund.

Zu den Aufgaben gehören u.a. Grundsatzfragen des Personalwesens, Arbeitszeitangelegenheiten, Dienstvorschriften, Personalcontrolling, Stellenplan- und Organisationsangelegenheiten, die Aus- und Fortbildung des Personals, die Personalentwicklung, die Personalplanung und die Personalbetreuung.

2. Projektbeschreibung und Ziele

Mit dem Projekt zur Einführung eines Identity & Access Management Systems (IAM, IAM-System) bei der Stadt Dortmund wird das Ziel verfolgt, die Erfassung und Bewirtschaftung von digitalen Identitäten der unterschiedlichen Identitätstypen zu verbessern. Das Projekt verfolgt dabei die folgende Vision:

„Ein zentrales IAM für alle Menschen und ihre digitale Identität im Umfeld der Stadtverwaltung Dortmund, welches einfach, transparent und sicher zu jedem Zeitpunkt genau die Zugänge & Berechtigungen bereitstellt, die benötigt werden.“

Die wesentlichen Schwerpunkte und Begriffe des Projektes lassen sich aus dieser Vision ableiten:

- **Zentral:** es soll ein System eingeführt werden, welches die Identitäten, also Benutzerinnen und Benutzer, und ihre Zugänge und Berechtigungen verwaltet und angebundene Systeme mit den erforderlichen Informationen beliefert.
- **Identity:** Eine natürliche Person wird durch genau eine (digitale) Identität repräsentiert. Im Umfeld der Stadt Dortmund betrachtet das Projekt die internen Identitäten, dies sind die Mitarbeitenden der Stadt Dortmund, und die hybriden Identitäten. Dies sind Menschen, die nicht im direkten Vertragsverhältnis mit der Stadt Dortmund stehen, jedoch ebenso wie interne Identitäten auf ihre Ressourcen zugreifen müssen. Im weiteren Verlauf des Projektes soll auch die Unterstützung von juristischen Personen sowie von technischen Usern ermöglicht werden.
- **Access:** Dieser Begriff beschreibt den Zugriff der Identitäten auf schützenswerte Ressourcen, Systeme und Informationen.
- **Einfach:** Die einzuführende Methodik und das zu beschaffende System müssen einfach in der Handhabung sein, um die Akzeptanz in der Stadtverwaltung sicherzustellen.
- **Transparent:** Jeder Vorgang und alle Entscheidungen rund um die Identitäten und ihren Zugriffsrechten wird dokumentiert und steht nachvollziehbar und auswertbar zur Verfügung.
- **Sicher:** Die zentrale Verwaltung von Identitäten und ihren Zugriffsrechten, die zugrunde liegenden Regelwerke und die angestrebte Transparenz der Aktivitäten erhöhen die Sicherheit und erschweren den Missbrauch.

- „Zu jedem Zeitpunkt...benötigt“: Die Vergabe von Zugängen und Berechtigungen erfolgt künftig auf Basis von Geschäftsprofilen. Dies sind systemunabhängige Beschreibungen von Tätigkeiten, für die Zugriffe erforderlich sind und die sich aus der Organisationszugehörigkeit, der Funktion und der Tätigkeit der digitalen Identität ableiten. Ändert sich etwas an diesen Merkmalen ändern sich auch möglichst automatisiert die Zugriffsrechte.

Externe natürliche Personen, z.B. Bürgerinnen und Bürger, werden in einer weiteren Ausbaustufe in das hier einzuführende IAM-System als digitale Identitäten integriert. Es muss grundsätzlich möglich sein, diese Identitätsart mit diesem einzuführenden System zu verwalten.

Mit einem zentralen IAM werden Prozesse vereinheitlicht, vereinfacht und automatisiert. Die Einführung von einheitlichen Prozessrollen und -verantwortlichkeiten, Geschäftsprofilen und der Bildung eines gemeinsamen Verständnisses rund um das Thema IAM unterstützt dieses Ziel.

Wesentliches Quellsystem für das einzuführende IAM ist das Personalwirtschaftssystem SAP HCM. Fokus dieses Projektes ist neben der Anbindung dieses Quellsystems die weitere Anbindung der Zielsysteme der ersten Stunde:

- Active Directory / Azure AD
- Call Manager / Cisco Jabber
- HCL Notes / Outlook
- SAP HCM (als Zielsystem)
- SAP S/4 HANA
- Dokumentenmanagementsystem (DMS)
- (Mobile) Device Management
- Lizenzmanagementsystem (USU LiMa)
- Ticket-System (ITSM)

Die Anbindung der Quell- und Zielsysteme erfolgt phasenweise.

3. Verfahrensbeschreibung

Die Stadt Dortmund beabsichtigt, auf Basis eines unbefristeten EVB-IT Systemvertrages einen Auftrag für die o.g. Leistung in einem zweistufigen Verhandlungsverfahren mit Teilnahmewettbewerb gemäß § 17 Abs. 1 VgV zu erteilen.

3.1 1. Stufe – Teilnahmewettbewerb

In einer ersten Stufe sind Firmen aufgerufen sich in einem Teilnahmewettbewerb für die o.g. Leistung zu qualifizieren.

Die Angebotsunterlagen dienen im Teilnahmewettbewerb dazu, Ihrem Unternehmen eine belastbare Entscheidung zu ermöglichen, ob die ausgeschriebenen Leistungen nach Art und Umfang in Ihr Produktportfolio fallen und es aus unternehmerischer Sicht sinnvoll ist, in den Teilnahmewettbewerb einzutreten, um die Chance zu erhalten, zur Abgabe eines Angebots aufgefordert zu werden.

Bitte reichen Sie für den Teilnahmewettbewerb die Bewerbungsunterlagen sowie die geforderten zusätzlichen Anlagen und Nachweise, wie z.B. Referenzen usw. ein.

Darstellungen, die über der in der Anlage dargestellten Form hinausgehen und nicht speziell angefordert werden, werden nicht bewertet.

Grundsätzlich werden keine Bewerbungsunterlagen zurückgegeben.

3.2 2. Stufe – Verhandlungsverfahren

In einer zweiten Stufe schließt sich ein Verhandlungsverfahren als Wettbewerb der geeigneten Firmen an, die gemäß den Bewerbungsbedingungen nach Abschluss des Teilnahmewettbewerbs den Eignungskriterien entsprechen.

In dieser zweiten Stufe erfolgt die Sichtung der eingereichten Erstangebote inklusive eines technischen Umsetzungsgrobkonzeptes (max. 100 Seiten).

Anschließend erfolgen ein oder ggf. mehrere Verhandlungsrunden, die vor Ort in Form einer Präsentation, per Videokonferenz oder schriftlich stattfinden können. Ausschließlich das endgültige Angebot wird bewertet.

Darüber hinaus behält die Auftraggeberin sich vor:

- das Umsetzungskonzept durch einen Dritten begutachten zu lassen,
- das Verfahren neu zu starten, sofern nur ein Angebot eingeht.

3.3 Zuschlagskriterien

Die geeigneten Unternehmen werden aufgefordert ein Angebot einzureichen. Anschließend wird mit den Bietern über die von ihnen eingereichten Erstangebote sowie alle

Folgeangebote verhandelt, mit dem Ziel, diese inhaltlich zu verbessern. Von einer weiteren Verhandlung ausgenommen sind die endgültigen Angebote.

Grundsätzlich darf über den gesamten Angebotsinhalt verhandelt werden mit Ausnahme der in den Vergabeunterlagen festgelegten Mindestanforderungen und der im Vorhinein festgelegten Zuschlagskriterien. Es wird sich zudem vorbehalten, den Auftrag auf der Grundlage der Erstantegebote zu vergeben, ohne in Verhandlungen einzutreten.

Bei der Zuschlagserteilung werden die Kriterien „Preis“ und „Qualität“ berücksichtigt.

Das Zuschlagskriterium „Preis“ (P) geht mit 40 % in die Wertung ein.

Das Zuschlagskriterium „Qualität“ (L) geht mit 60 % in die Wertung ein.

Der Zielwert ermittelt sich aus beiden Werten wie folgt:

$$\text{Gesamtpunkte } Z = (L) + (P)$$

Maximal können **13.296.667 Wertungspunkte** erreicht werden.

3.3.1 Zuschlagskriterium Preis

Kriterium in der Kategorie Preis ist der Gesamtpreis aller im Preisblatt aufgeführten Positionen. Das Angebot mit dem niedrigsten Angebotspreis erhält eine Punktzahl von **5.318.667 Wertungspunkten**. Der günstigste Angebotspreis erhält die maximale Preispunktzahl und ein fiktives Angebot mit einem Angebotspreis vom Zweifachen des günstigsten Angebotspreises 0 Preispunkte. Die Punktebewertung für die dazwischenliegenden Angebotspreise erfolgt über eine lineare Interpolation mit zwei Dezimalstellen. Angebote, die teurer als das fiktive Angebot sind, erhalten ebenfalls 0 Preispunkte.

Die Normierung erfolgt wie folgt: Preiswert (P) = $[(2P_{\min} - P) / P_{\min}] \times P_{\max}$ (für $P \leq 2P_{\min}$)

3.3.2 Zuschlagskriterium Qualität

Die Kategorie Qualität (Fachliche Anforderungen) wird anhand des Erfüllungsgrads und eines dedizierten Punktesystems bewertet. Dieses Kriterium geht mit 60 Prozent in die Wertung ein.

Das Lastenheft unterscheidet zwischen Mindestanforderungen/ Mindestfunktionen und Zusatzfunktionen.

Mindestanforderungen legen die grundlegenden Anforderungen an das IAM-System und den Auftragnehmer / Hersteller fest. Werden diese nicht in der geforderten Mindestausprägung erfüllt, führt dies zum Ausschluss vom Vergabeverfahren. Die Erfüllung der Mindestanforderungen selbst wird nicht bepunktet.

Anforderungen im Lastenheft, die als Zusatzfunktion definiert sind, sind mit einem bestimmten Punktwert je nach Erfüllungsgrad hinterlegt. Bei Erfüllung des Kriteriums wird der entsprechende Punktwert berücksichtigt und am Ende zu einer Gesamtpunktzahl aufaddiert.

Die Nichterfüllung von Zusatzfunktionen führt **nicht** zum Ausschluss vom Vergabeverfahren.

Die Punkte für die Zusatzfunktionen werden wie folgt vergeben:

1. Alle Anforderungen einer Kategorie wurden durch das Projektteam und weitere Experten miteinander verglichen und in eine Reihenfolge gebracht. Die Rangfolge wird in Prozenten der gewonnenen Paarvergleiche angegeben.
2. Alle Kategorien wurden durch das Projektteam und die operative Projektlenkung miteinander verglichen und in eine Rangfolge gebracht. Die Rangfolge wird in Prozenten der gewonnenen Paarvergleiche angegeben.

ID	Kategorie	Prozentual
1	Allgemeine Anforderungen an den Anbieter	35%
2	Administration und Betrieb	88%
3	Audit und Reporting	62%
4	Authentisierungsverfahren	54%
5	Datenmodell	71%
6	Einwilligungsmanagement	0%
7	Entwicklung und Konfiguration	48%
8	Geschäftsprofil-Entwicklung	48%
9	Geschäftsprofil-Funktion	75%
10	IAM Architektur	96%
11	IAM Funktionen	100%
12	Identitätenverwaltung B2C, B2B, B2G	69%
13	Interoperabilität	85%
14	KI	50%
15	Kosten	4%
16	LoA-Management	23%
17	Multifaktor	35%
18	Schnittstellen zu Services und Austauschformate	65%
19	Schnittstellen zur Provisionierung	92%
20	Schnittstelleneigenschaften	77%
21	Shop & Katalog für Geschäftsprofile, Services, Applikationen	23%
22	Support	19%
23	Unterstützte IDPs	38%
24	User Frontend	58%
25	User-/Passwort-Management	8%
26	Workflow Funktionen / Backend / Technologieorientiert	27%
27	Workflow-Dialog-Funktion - Ablauforientiert	31%

3. Alle Zusatzfunktionen erhalten grundsätzlich einen Basis-Wert von 10 Punkten. Bei Untieranforderungen werden die 10 Punkte aufgeteilt, so dass in Summe eine maximale Punktzahl von 10 erreicht werden kann. Die Rangfolge der Anforderung gilt gleichermaßen für die Untieranforderungen.

4. Ist die Anforderung voll erfüllt, wird der maximal zu erreichende Basis-Wert (max. 10 Punkte) vergeben, ist sie nicht erfüllt, werden 0 Punkte vergeben. Es gibt Anforderungen (keine Untieranforderungen), die teilweise erfüllt werden können, dann wird ein Teil der Punkte vergeben. Die Angabe „teilweise“ darf auch nur dann erfolgen, wenn dies in der Anforderung als möglich explizit angegeben wird.

5. Die Rangfolge der Anforderungen innerhalb der Kategorie bestimmen den **Hebesatz 1**. Gemäß der Rangfolge in Prozent aus Punkt 1 ergeben sich gemäß der logarithmische Skala folgende Faktoren:

$$> 75\% - 100\% = 200$$

$$> 50\% \leq 75\% = 32$$

$$> 25\% - \leq 50\% = 10$$

$$> 10\% - \leq 25\% = 3$$

$$0 - \leq 10\% = 1$$

6. Die Reihenfolge der Kategorien bestimmen den **Hebesatz 2**. Gemäß der Rangfolge in Prozent aus Punkt 2 ergeben sich folgende Faktoren:

$$> 75\% - 100\% = 50$$

$$> 50\% \leq 75\% = 40$$

$$> 25\% - \leq 50\% = 30$$

$$> 10\% - \leq 25\% = 20$$

$$0 - \leq 10\% = 10$$

7. Der Gesamtwert der Anforderung ergibt sich nun gemäß folgender Formel:

$$\text{Gesamtwert der Anforderung} = \text{Basis-Wert} \times \text{Hebesatz 1} \times \text{Hebesatz 2}$$

Basis für die Bewertung ist die vom Bieter auszufüllende Wertungsmatrix. Maximal können **6.978.000 Wertungspunkte** erreicht werden.

Weitere **1.000.000 Wertungspunkte** können für das technischen Umsetzungsgrobkonzept erreicht werden.

Alle Wertungspunkte addiert, ergeben den **L-Wert**, der in die Gesamtwertung einfließt.

4. Vorabinformation

Sofern zur Abgabe eines Angebotes aufgefordert wird, erhalten Sie in diesem Kapitel vorab Informationen zum Dokumentenwerk, welches die Auftraggeberin zur Verfügung stellen wird und zu den zu Ausschlusskriterien.

4.1 Dokumentenwerk

Im Verlauf des Projektes wurden Dokumente erstellt, die aufeinander referenzieren. Die Schwerpunkte der Dokumente sind im Folgenden beschrieben:

Dokument	Inhalt	Voraussichtlicher Umfang
Big Picture / Grobkonzept	Das Dokument beinhaltet die Grundlagen und Rahmenbedingungen zur Einführung eines IAM, beschreibt den sogenannten Happy Path anhand der Lebenszyklen der Identitäten, Organisationseinheiten und weiteren Elementen.	Ca. 400 Seiten
Fachliche Feinkonzepte	Aufbauend auf dem Grobkonzept werden die wesentlichen Prozesse im Detail und mit den relevanten Ausnahmen modelliert.	20 – 25 modellierte Prozesse
Geschäftsprofil-Methode	Dieses Dokument beschreibt die grundsätzliche Funktionsweise der Geschäftsprofil-Methode und erläutert die wesentlichen Begrifflichkeiten und Verantwortlichkeiten. Es beschreibt die Rahmenbedingungen und das Vorgehen für den Aufbau des Rollenkataloges und den Rollout in der Stadtverwaltung.	Ca. 60 Seiten
Masterplan	Der Masterplan beschreibt das phasenweise Vorgehen im Rahmen der Implementierung	Ca. 60 Seiten

	und den Umfang der Funktionalitäten, Schnittstellen und Prozesse für die Inbetriebnahme des IAM.	
Anforderungskatalog / Lastenheft	Der Anforderungskatalog enthält die einzelnen priorisierten Anforderungen und ist Bestandteil des Lastenheftes für das Vergabeverfahren.	Ca. 200 Seiten

Tabelle 1 - Überblick Projektdokumentation

Die finalen Vergabeunterlagen (Leistungsbeschreibung, Lastenheft, EVB IT Vertrag und seine Anlagen, Bewertungsmatrix, Vertrag zur Auftragsverarbeitung, Teleservicevereinbarung) werden erst in der Angebotsphase zur Verfügung gestellt.

4.2 Ausschlusskriterien

Das Lastenheft wird mindestens die im folgenden genannten Mindestanforderungen enthalten. Mindestanforderungen legen die grundlegenden Anforderungen an den IT-Dienst und die Implementierungsleistungen fest. Werden diese nicht in der geforderten Mindestausprägung erfüllt, führt dies zum Ausschluss vom Vergabeverfahren.

4.2.1 Mindestfunktion/-anforderung: [1075] Kein aktiver Internetzugang

Es darf kein aktiver Internetzugang der IAM On-Prem Lösung zum Softwarehersteller notwendig sein, um den vollen IAM-Funktionsumfang nutzen zu können. Für die Provisionierung von Cloud-Applikationen wird zwar ein aktiver Internetzugang benötigt, eine Kommunikation oder Datenübertragung zum Softwarehersteller ist aber auch bei einem vorhandenen Internetzugang nicht notwendig.

4.2.2 Mindestanforderung: [1200] Verpflichtung des eingesetzten Personals

Mindestanforderungen an das einzusetzende Personal des Auftragnehmers ergeben sich wie folgt: Gemäß Punkt 7.1 der EVB-IT System-AGBs erfolgt die Kommunikation mit dem Auftraggeber in deutscher Sprache. Der Auftragnehmer verpflichtet sich, für die Wahrnehmung der geschuldeten Leistungen und Aufgaben nur Personal einzusetzen, welches bereit ist, sich aufgrund des § 1 des Verpflichtungsgesetzes verpflichten zu lassen. Wenn der Auftraggeber, das vom Auftragnehmer eingesetzte Personal aufgrund gesetzlicher Regelung selbst verpflichten muss, wird durch den Auftragnehmer deutschsprachiges Personal eingesetzt. Wenn in diesen Fällen nicht deutschsprachiges Personal durch den Auftragnehmer eingesetzt werden soll, ist für die Verpflichtung nach dem

Verpflichtungsgesetz ein entsprechender Dolmetscher durch den Auftragnehmer zu beauftragen und zu bezahlen. Der Vorgang der Verpflichtung mit dem Auftragnehmer ist durch den Dolmetscher zu begleiten. Dabei ist sicherzustellen, dass der Inhalt der Verpflichtungserklärung sowie die maßgeblichen gesetzlichen Regelungen der zu verpflichtenden Person ordnungsgemäß in der Muttersprache des zu Verpflichtenden übersetzt werden. Dies ist entsprechend zu dokumentieren. Es ist ein beim Oberlandesgericht allgemein beeidigter Dolmetscher/Übersetzer einzusetzen. Über die bundesweite Dolmetscher- und Übersetzerdatenbank der Justiz können diese aufgefunden werden: <https://www.gerichts-dolmetscher.de/Recherche/de/Suchen>.

4.2.3 Mindestfunktion/-anforderung: [1201] Projektsprache

Die Projektsprache im Projekt zur Beschaffung und Einführung eines IAM-Systems bei der Stadt Dortmund muss Deutsch (mind. Sprachniveau ist C2) sein. Die Projektdokumentation muss vollständig auf Deutsch erstellt werden.

4.2.4 Mindestfunktion/-anforderung: [1202] Kundendokumentation

Zum Zeitpunkt der Abnahme des IAM muss eine Kundendokumentation des IAM-Systems inklusive der durchgeführten Installations- und Konfigurationsleistungen vorliegen. Diese muss in einem Format zur Verfügung gestellt werden, welches durch den Kunden pflegbar ist.

4.2.5 Mindestfunktion/-anforderung: [67] Der Betrieb und die Installation des IAM ist unter VMWARE möglich

Das IAM System muss vollständig (mit allen Komponenten), ohne Einschränkungen, unter VMWARE (Version 8.0.3 oder höher) betrieben werden können.

4.2.6 Mindestfunktion/-anforderung: [541] Disaster-, Recovery und Restoremöglichkeit nach Systemausfall

Recovery und Restore muss über alle angebundenen Systeme hinweg die konsistente User- Berechtigung und Record-Matching aus dem Backup unter Berücksichtigung der Historie und Zielsystemen wiederherstellen können.

Recovery und Restore müssen dabei objektbasiert oder komplett durchgeführt werden können.

4.2.7 Mindestfunktion/-anforderung: [10] Historisierung / Logging von IAM-Aktionen

Alle IAM-Aktionen (wie Erstellung/Änderung von Aktivitäten, Berechtigungen und Workflows) müssen gelogged und historisiert werden können.

Dadurch muss die Nachvollziehbarkeit aller IAM-Aktionen möglich sein.

4.2.8 Mindestfunktion/-anforderung: [784] Protokolle: OAuth 2.0 (Open ID Connect) wird zur Authentisierung unterstützt.

Das OAuth 2.0 (Open ID Connect) Protokoll muss vom IAM-System als Authentisierungsverfahren unterstützt werden.

4.2.9 Mindestfunktion/-anforderung: [785] Microsoft Public-Key-Infrastruktur (PKI) auf Basis des X.509-Standards (zertifikatsbasierendes Verfahren) muss unterstützt werden.

Das IAM-System muss Public-Key-Infrastruktur (PKI), von Microsoft, auf Basis des X.509-Standards (zertifikatsbasierendes Verfahren) unterstützen.

4.2.10 Mindestfunktion/-anforderung: [786] Framework: SAML 2.0 (Security Assertion Markup Language) wird unterstützt.

SAML-Format auf XML-Basis zur Authentisierung und Autorisierung von Benutzern muss vom IAM-System unterstützt werden.

4.2.11 Mindestfunktion/-anforderung: [789] Protokolle: Kerberos Authentifizierung wird unterstützt.

Kerberos Authentifizierung muss vom IAM-System als Authentisierungsverfahren unterstützt werden.

4.2.12 Mindestfunktion/-anforderung: [917] Protokolle: LDAP wird zur Authentisierung unterstützt.

LDAP muss vom IAM-System als Authentisierungsverfahren unterstützt werden.

4.2.13 Mindestfunktion/-anforderung: [24] ID Zuordnungen über das IAM-Datenmodell soll n:1:m abbildbar sein (n Quellstammdaten zu einer Identität zu m Zielsystemaccounts)

Jede digitale Identität muss aus zuzuliefernden Attributen / Werten der Stammdaten gebildet werden. Dabei muss es möglich, mehrere Stammdaten aus unterschiedlichen Quellen (n) zu mappen und die digitale Identität vielen Accounts in unterschiedlichen Systemen (m) zuzuordnen.

(n: Stammdaten, 1:Identität, m:Accounts)

4.2.14 Mindestfunktion/-anforderung: [25] Erweiterbares IAM-Schema

Das IAM-Schema muss gut dokumentiert und durch die Stadt Dortmund beliebig erweiterbar sein.

Folgende Eigenschaften müssen bereits im Rahmen der Initialimplementierung vorhanden sein:

- Änderungen sind versionierbar für Objekt- und Attributklassen
- Jede IAM-Objekt-Klasse kann mit einem Gültigkeitszeitfenster (Start- und Enddatum) versehen werden. Dies ermöglicht eine Lebenszyklusverwaltung z.B. Ressourcen, Laufwerke, Software inkl.
- vom Hersteller erlaubte und dokumentierte Änderungen und Erweiterungen am Schema müssen Upgrade-stabil sein.
- Zur Verwaltung und Konfiguration steht ein Entwicklungswerkzeug zur Verfügung

4.2.15 Mindestfunktion/-anforderung: [582] Entkopplung des Benutzernamens von der E-Mail-Adresse

Das Datenmodell muss dem User ermöglichen, nicht zwingend die E-Mail-Adresse als Benutzername zum Anmelden am IAM zu verwenden. Der Benutzername muss von der E-Mail-Adresse entkoppelt werden können.

4.2.16 Mindestfunktion/-anforderung: [810] Eindeutige, lebenslange, historisierbare Zuordnung einer natürlichen Person zu einer digitalen Identität im IAM

Eine natürliche Person muss unabhängig von Ihren Stammdaten bzw. der Quellen (z.B. unterschiedliche HR-Systeme, Anstellungsarten, Typen von Identitäten (Interner und / oder externer Mitarbeiter, Kunde, usw.)) eineindeutig, lebenslang und historisierbar einer digitalen Identität zugeordnet mit den folgenden Eigenschaften sein:

- Ein eindeutiger, einzigartiger, lebenslang verfügbare Primärschlüssel für die digitale Identität ist im IAM-System hinterlegt
- Ein n:1 Mapping der Personenstammdaten einer natürlichen Person aus Drittapplikationen (z.B. HR-Systemen) über deren Primär- oder einen eindeutigen Sekundär-Schlüssel anwendbar
- Paralleles (gleichzeitiges) Mapping zu mehreren Personenstammdaten einer natürlichen Person ist möglich
- Die digitale Identität einer natürlichen Person ist mit beliebigen anderen natürlichen Personen zum Zweck einer Vertretungs- und Delegations-Steuerung befristet verknüpfbar

- Historisierung der digitalen Identität einer natürlichen Person und der Mappings bei gleichbleibender digitaler Identität (Primärschlüssel hat Ewigkeitscharakter)

4.2.17 Mindestfunktion/-anforderung: [408] Geschäftsprofil-Zuweisung/-Entzug auf Basis unterschiedlicher Regelwerke und Zusammenhänge auf Basis beliebiger Attribute

Das IAM-System muss in der Lage sein, Geschäftsprofilzuweisung/-entzug auf Basis unterschiedlicher Regelwerke und Zusammenhänge und auf Basis beliebiger Attribute automatisch durchzuführen.

4.2.18 Mindestfunktion/Mindestanforderung [322]: Verwendung von HTTPS

Das HTTPS Kommunikationsprotokoll muss unterstützt werden.

4.2.19 Mindestfunktion/-anforderung: [2] Rollenbasierte Provisionierung

Accounts und Berechtigungen können in Zielsystemen auf Basis von IAM Rollen (Geschäftsprofilen) provisioniert werden.

4.2.20 Mindestfunktion/-anforderung: [16] Sicherstellung der bidirektionalen Datenübertragung

Die Sicherstellung der bidirektionalen Datenübertragung zwischen dem IAM und den Quell- und Zielsystemen:

- Active Directory (Domain Functional Level 2016)
- Call Manager V 15 / Cisco Jabber V 15
- HCL Notes V 14.5
- SAP HCM (Quell- und Zielsystem)
- SAP S/4 HANA
- Dokumentenmanagementsystem (DMS) Doxis CSB V 12.3
- (Mobile) Device Management MECM V 2509 / Microsoft Intune / JAMF Pro V 11.29

muss gewährleistet werden. Dabei muss die Verarbeitung der Rückmeldung zur Übermittlung der Daten erfolgen.

4.2.21 Mindestfunktion/-anforderung: [1203] Transaktionsverwaltung

Die Sicherstellung der Datenübertragung innerhalb des IAM und zu den Quell- und Zielsystemen:

- Active Directory (Domain Functional Level 2016)
- Call Manager V 15 / Cisco Jabber V 15

- HCL Notes V 14.5
- SAP HCM (Quell- und Zielsystem)
- SAP S/4 HANA
- Dokumentenmanagementsystem (DMS) Doxis CSB V 12.3
- (Mobile) Device Management MECM V 2509 / Microsoft Intune / JAMF Pro V 11.29

muss dadurch gewährleistet werden, dass die Transaktionen im IAM bis zur erfolgreichen Umsetzung am Ziel (kein Fire & Forget) vorgehalten werden.

Dies darf nicht nur im "Standard"-Betrieb, sondern muss auch in nachfolgenden Fällen erfolgen:

- Nicht-Erreichbarkeit (z.B. Netzwerk) des Quell- oder Ziel-Systems
- zeitliche Verzögerung (Belastbarkeit, Qualität) des Quell- oder Ziel-Systems.

Hinweis: Sicherheit der Datenübertragung ist nicht dadurch gewährleistet, dass das IAM als Ersatz mehrfach versucht die Daten zu übertragen, ohne eine Rückmeldung zu erwarten und zu verarbeiten.

4.2.22 Mindestfunktion/Mindestanforderung [956]: HR-Systemanbindung SAP HCM

Das IAM-System muss einen Konnektor zur Anbindung der HR-Plattform SAP HCM für personalwirtschaftliche Aufgaben besitzen.

Das IAM-System muss die Funktionalität besitzen, mittels des verfügbaren Konnektors Stamm- und Organisationsdaten aus dem HR System zu importieren und zu verarbeiten.

Der Stamm- und Organisationsdatenimport beinhaltet:

- Statusinformationen
- Abgrenzungen
- Zeitstempel
- Maßnahmen

Ein Rückfluss von Kommunikationsdaten (E-Mail und Telefonnummer) ins HR-System SAP HCM muss über den Konnektor möglich sein.

4.2.23 Mindestfunktion/-anforderung: [1071] Wartungsvertragsende schränkt die IAM-Funktionalität / Nutzbarkeit / Betriebsfähigkeit nicht ein

Das Wartungsvertragsende darf die IAM-Funktionalität / Nutzbarkeit / Betriebsfähigkeit nicht einschränken.

4.2.24 Mindestfunktion/-anforderung: [989] Eindeutige Nutzer-Zuordnung und Authentisierung

Das Authentisierungsmittel Multi-Protokoll-Sicherheitstoken muss eindeutig einer Identität zugeordnet werden.

Das Authentisierungsverfahren muss eindeutig den berechtigten Besitzer des Authentisierungsmittels authentifizieren.

4.2.25 Mindestfunktion/-anforderung: [998] Kryptographischer Schutz des Authentisierungsschlüssels und des Authentisierungsprotokolls

Der Authentisierungsschlüssel muss durch das Authentisierungsprotokoll geschützt sein. Das Authentisierungsprotokoll zwischen MFA-Applikationen und Endgeräten muss kryptographisch geschützt sein.

Hierzu stehen verschieden Verschlüsselungsverfahren wie RSA (asymmetrisch), DLIES und ECIES (hybride Verschlüsselungsverfahren) zur Verfügung (siehe BSI TR-02102-1).

4.2.26 Mindestfunktion/ Mindestanforderung: [342] Austauschformat CSV

Das IAM muss das CSV Austauschformat unterstützen. Bei Bearbeitung von CSV-Dateien muss der Bearbeitungsstatus hinterlegt und die CSV-Datei historisiert werden.

4.2.27 Mindestfunktion/ Mindestanforderung: [918] LDAP muss zum Austausch von Information und zur Abfrage von Informationen genutzt werden können.

Das IAM-System muss per LDAP mit anderen LDAP-fähigen Systemen kommunizieren können, um Datenaustausch zu ermöglichen. Unterschiedliche LDAP-Standards müssen dabei unterstützt werden.

4.2.28 Mindestfunktion/ Mindestanforderung: [333] AD-Provisionierungsschnittstelle

Das IAM-System muss eine native Active Directory Schnittstelle (ADSI) zur Verfügung stellen. Dabei müssen folgende Eigenschaften/Attribute/Funktionen provisioniert werden können:

- Useraccounts mit Start/Ende Datum
- Gruppenmitgliedschaften (mit Start/Ende Datum)
- Gruppen (anlegen/modifizieren/löschen)
- beliebige Attribute (Vorname, Nachname, Mail, Führungskraft, Organisationseinheit)
- Passwort verschlüsselt
- Environment (Homedirectory, Loginscript)
- AD-Profile

Die Verknüpfung / Assoziation zwischen IAM Identität und AD Account muss dabei über den Primärschlüssel des UID Objektes im AD und nicht über den distinguished name/ common name erfolgen.

Die Verknüpfung / Assoziation zwischen Berechtigungsrolle und AD Gruppenobjekt muss dabei über den Primärschlüssel des UID Objektes im AD und nicht über den distinguished name/ common name erfolgen.

Das IAM muss eine Placement Policy für Accounts und Gruppenobjekte unterstützen.

4.2.29 Mindestfunktion/ Mindestanforderung: [34] Anlage und Löschung von Accounts, sowie Zuweisung und Entzug von Berechtigungen in Zielsystemen mit verschiedenen Berechtigungsschemas.

Das IAM-System muss Accounts anlegen und löschen, Berechtigungen zuweisen und entziehen.

Es müssen dabei verschiedene Zielsystemstrukturen der Zielsysteme:

- Active Directory (Domain Functional Level 2016)
- Call Manager V 15 / Cisco Jabber V 15
- HCL Notes V 14.5
- SAP HCM (als Zielsystem)
- SAP S/4 HANA
- Dokumentenmanagementsystem (DMS) Doxis CSB V 12.3
- (Mobile) Device Management MECM V 2509 / Microsoft Intune / JAMF Pro V 11.29

unterstützt werden.

Das IAM-System muss dabei auch die verschiedenen Strukturen gleicher Systeme abbilden können (AD-Stadt Dortmund, AD-Feuerwehr Stadt Dortmund, AD-Theater Stadt Dortmund).

4.2.30 Mindestfunktion/-anforderung: [401] Unterstützung eines Vier-Augen-Prinzips

Das System muss bei jeder Genehmigung mindestens ein Vier-Augen-Prinzip unterstützen können. Dabei muss sichergestellt werden können, dass der Beantragende nicht sein eigener Genehmiger ist.