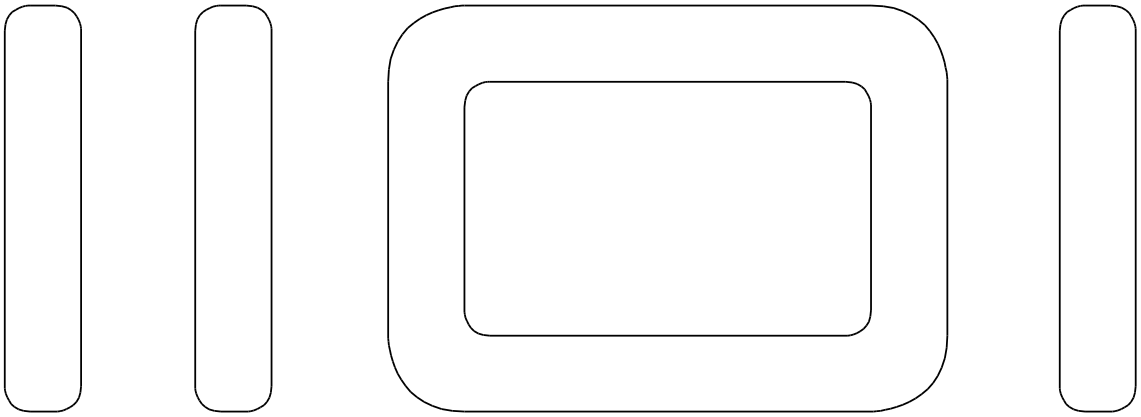
Rahmenanforderungen Softwarearchitektur V4.0



Dokumenteninformation	
Verantwortliche Stelle:	Dataport
Datum:	12.10.2015
Status des Dokumentes:	Entwurf

Inhaltsverzeichnis

1 VORWORT 4

2 SCHICHTEN UND KOMPONENTEN 4

3 TECHNOLOGISCHE BASIS 4

4 FACHLICHE ADMINISTRATION UND STEUERUNG 4

5 MANDANTENFÄHIGKEIT 5

6 SOFTWAREERGONOMIE 5

7 BARRIEREFREIHEIT 6

8 TECHNOLOGISCHE UND ANWENDUNGSRELEVANTE NORMEN UND STANDARDS 6

8.1 ZEICHENSATZ UNICODE 6

9 DATENSCHUTZANFORDERUNGEN 6

10 SERVICEORIENTIERTE ARCHITEKTUREN 8

11 SCHNITTSTELLEN ZU ANDEREN SYSTEMEN UND VERFAHREN 9

11.1 INTEGRATION INS GOVERNMENTGATEWAY 9

11.2 IDENTITÄTS- UND ZUGRIFFSMANAGEMENT (IAM) 9

11.2.1 Unterstützung von Identitätsprovisionierung 9

11.2.2 Unterstützung von Authentisierung beim Zugriff 10

11.2.3 Unterstützung von Autorisierung beim Zugriff 11

11.3 KASSENSCHNITTSTELLE, EIN- UND AUSZAHLUNGEN 11

11.4 MICROSOFT OFFICE 11

11.5 ELEKTRONISCHE AKTE 11

Dokumentenverwaltung

Ansprechpartner und Ort der Ablage

Ansprechpartner: Dataport

Ort der Ablage:

Änderungsübersicht

Version	Datum	Veränderungen/ Bemerkungen	Autor(en)
	03.08.2015	Absatz zu UNICODE und Fußnote zur Barrierefreiheit ergänzt	Dataport
	18.08.2015	Redaktionelle Änderungen	Dataport
	25.08.2015	Redaktionelle Änderungen	Dataport
	26.08.2015	Redaktionelle Änderungen	Dataport
	01.10.2015	Version auf 4.0 erhöht	Dataport
	12.10.2015	Vorwort ergänzt	Dataport

Dokumentenverweise

Dokumentenname	Bemerkungen	Ort der Ablage

Hinweis zur Abnahme des Dokumentes

Software Architektur

1 Vorwort

Im Rahmen einer Vergabe soll dieses Dokument Bietern eine valide Lösungsfindung und Kostenschätzung erleichtern. Es hat in diesem Rahmen ausschließlich informellen Charakter und wird unabhängig von den einzelnen Formulierungen nicht in die Vergabeentscheidung mit einbezogen. Insbesondere stellen die einzelnen Aspekte ausdrücklich keine Bewertungs- oder Ausschlusskriterien dar und haben insoweit keine vergaberechtliche Relevanz.

2 Schichten und Komponenten

Die Architektur der Software sollte aus einzelnen Komponenten bestehen und in drei Schichten aufgebaut sein, so dass Präsentation, Logik und Datenhaltung auf getrennten Systemen betrieben werden können.

Änderungen der Anwendungslogik sollten grundsätzlich nicht zur Aktualisierung der Software auf den Clients führen (Vermeidung von Softwareverteilung durch Beschränkung auf Präsentation).

Die Applikation sollte clusterfähig sein, so dass die Anwendung bei einem Ausfall der betriebenen Datenbank- oder Applikationsserver auf einem anderen Rechner weiter betrieben werden kann.

Dataport bietet an, dass Clients evtl. als Terminal-Service zur Verfügung gestellt werden können.

3 Technologische Basis

Um die Heterogenität der bei Dataport eingesetzten Technologien zu reduzieren, werden für eine Softwareentwicklung die Plattformen .NET mit seinem Framework oder Java EE (ehemals J2EE) in der im Dokument „Rahmenanforderungen Systemarchitektur, Anlage Basissoftware“ angegebenen Version bevorzugt.

4 Fachliche Administration und Steuerung

Soweit die Einstellung fachlicher Parameter fachlich/logisch sinnvoll durch eine getrennte organisatorische Betreuung übernommen werden kann, ist neben der zentralen technischen Administration des Verfahrens auch ein Modul für eine fachliche Administration und Pflege des Verfahrens - sowohl für eine zentrale Stelle bei Dataport als auch für dezentrale Stellen bei Kunden - bereitzustellen. Dies gilt insbesondere für

- die Einstellung fachlicher Parameter,
- die Pflege von Referenzwerten,
- die Aktualisierung von Benutzer- und Organisationsdaten (sofern erforderlich, siehe 11.2 Identitäts- und Zugriffsmanagement),

- die Festlegung von Berechtigungen und Zuständigkeiten,
- Programmfunktionen, die eine Batch-Verarbeitung, Datenübermittlung oder Auswertung auslösen und nicht Bestandteil der allgemeinen Benutzerschnittstelle sein sollen.

Für die Steuerung von Datenübermittlungen, Auswertungen und (anderen) regelmäßigen Batch-Verarbeitungsläufen muss ein Werkzeug zur Verfügung gestellt werden, über das die erforderlichen Parameter für die Datenverarbeitung (z.B. Gültigkeitszeiträume für Auswertungen oder Datenabzüge, häufig gewählte Selektionsmerkmale) mitgegeben werden. Es muss auch sichergestellt werden, dass zu Start- und Endzeitpunkt sowie zum Ergebnis (z.B. Anzahl verarbeiteter Datensätze, Status, ggf. aufgetretene Fehlerfälle) der erfolgten Datenverarbeitung informiert wird.

5 Mandantenfähigkeit

Wenn vorgesehen ist, dass eine einzelne Instanz (installierte Kopie) des Verfahrens gleichzeitig von mehreren Mandanten (Kunden, Auftraggebern, Organisationseinheiten, Fachbereichen,..) genutzt wird, die keine gegenseitige Einblicke in ihre Daten haben dürfen, muss zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterschieden werden können („Mandantenfähigkeit“).

Mandantenübergreifende Daten sollen – vorrangig aus wirtschaftlichen Gründen - nur einmal zur gemeinsamen Nutzung durch alle Mandanten gehalten und gepflegt werden.

Mandantenabhängige Daten sollen zum einen eine mandantenspezifische Konfiguration des Systemverhaltens ermöglichen. Vor allem aber müssen sie eine zuverlässig sichere Separation („Abschottung“) der Daten und Objekte eines Mandanten gegen Einblicke und Zugriffe aus anderen Mandanten gewährleisten.

Die Art der Separation der mandantenabhängigen Daten (logisch, physisch,...) ist passend zu den Sicherheitsanforderungen am für die Applikation vorgesehenen Einsatzort zu realisieren.

6 Softwareergonomie

An das ausgeschriebene Verfahren wird eine Reihe von Anforderungen bezüglich der Softwareergonomie gestellt:

- Das Verfahren muss die Ergonomie seiner Benutzerschnittstelle nach den Regeln der ISO EN 9241 Teil 11-17 und 110 gestalten.
- Eine deutschsprachige Benutzeroberfläche muss lieferbar sein.
- Eingabe- und Bedienungsfehler sollen vom Verfahren abgefangen werden und dürfen nicht zu undefinierten Zuständen oder Abstürzen des Systems führen.
- Die Schriftgröße soll 4mm bei 17“ - TFT – Monitoren nicht unterschreiten.
- Das Verfahren soll alternativ vollständig mit Hilfe der Tastatur bedienbar sein.

- Das Verfahren soll Fehlermitteilungen mit genauer und verständlicher Beschreibung ausgeben. Bei Eingabe-/Bedienungsfehlern durch den Anwender soll das Verfahren einen Hinweis auf die korrekte Durchführung des Vorganges in verständlicher Form liefern (Bearbeitungshinweis).
- Die Bildschirmauflösung soll wahlweise zwischen 1024x768 bis zu 1680x1050 Bildpunkten betragen können.

7 Barrierefreiheit[1]

Das Verfahren muss für öffentlich zugängliche Dialogteile die rechtlichen Vorschriften zur Barrierefreiheit erfüllen, die im vorgesehenen Einsatzgebiet gelten.

8 Technologische und anwendungsrelevante Normen und Standards

Soweit technische oder fachliche Standards oder Normen für Leistungen oder Datenformate der ausgeschriebenen Lösung existieren, sind diese zu berücksichtigen.

8.1 Zeichensatz UNICODE

Für öffentlich übermittelte Daten und Registerwerte soll das Verfahren grundsätzlich lateinische Zeichen in UNICODE verwenden.

Für bestimmte Übermittlungen und Register ist diese Codierung lt. Entscheidung 2014/04 des IT-Planungsrats verbindlich.

9 Datenschutzanforderungen

- Das Verfahren muss die gesetzlichen Bestimmungen einhalten.
- Personenbezogene Daten sind vor unbefugtem Zugriff zu schützen.
- Personenbezogene Daten dürfen zu statistischen Zwecken nur anonymisiert genutzt werden; ein Rückschluss auf einzelne Personen oder Gruppen darf nicht möglich sein.

---

[1]BGG §4 Barrierefreiheit
Gesetz zur Gleichstellung behinderter Menschen (Behindertengleichstellungsgesetz - BGG)

Barrierefrei sind bauliche und sonstige Anlagen, Verkehrsmittel, technische Gebrauchsgegenstände, Systeme der Informationsverarbeitung, akustische und visuelle Informationsquellen und Kommunikationseinrichtungen sowie andere gestaltete Lebensbereiche, wenn sie für behinderte Menschen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar sind

- Werden sensible personenbezogene Daten im Rahmen der Bearbeitung über öffentliche Netze geleitet, so muss dafür Sorge getragen werden, dass kein unbefugter Zugriff auf die Daten möglich ist. Die Maßnahmen sind zu beschreiben.

10 Serviceorientierte Architekturen

Umfangreichere Applikationen sind über das übliche Strukturierungsmittel der Komponentenbildung hinaus nach dem Muster von „serviceorientierten Architekturen“ (SOA) zu entwerfen. Hierzu sind fachlich strukturierte und verteilt nutzbare Dienste als plattformunabhängige Webservices zu realisieren. Für die Webservice-Realisierungen bestehen folgende Anforderungen:

- Die Webservices sind konform zum Basic Profile V.1.1 der Web-Service-Interoperability-Organization (WS-I) zu realisieren.
- Authentizität, Integrität und Vertraulichkeit sind nach dem Standard WS-Security (V.1.1) zu gewährleisten.
- Eine formale Beschreibung einschließlich aller technischen Richtlinien (WS-Policy, insb. WS-SecurityPolicy) in Form von WSDL 1.1 existiert für jeden Service.
- Dienstnutzer müssen in der Lage sein, die Services auf Basis der WSDL dynamisch einzubinden (z.B. über ein Service-Verzeichnis).

Neben diesen technischen Vorgaben sollten die Services dem SOA-Paradigma folgend fachlich strukturiert und grob-granular entworfen sein. Die Schnittstellen sollten dokumentenorientiert sein, d.h. Input- und Output-Nachrichten sollten durch explizite XML-Schemata definiert sein.

11 Schnittstellen zu anderen Systemen und Verfahren

11.1 Integration ins GovernmentGateway

Am vorgesehenen Einsatzort der Applikation existierende Mandanten der Infrastruktur *GovernmentGateway* sind zu berücksichtigen.

Das heißt, sofern das Verfahren eine Internetschnittstelle umfasst, müssen die für den Einsatz geltenden spezifischen Anforderungen zur Integrationstiefe in diese Infrastruktur beachtet werden.

Wenn eine Integration gefordert ist, dann kann die Integrationstiefe von (minimal) der Nutzung der Webservice-Schnittstellen des GovernmentGateways für Authentifizierung und Autorisierung bis hin zur Nutzung des .NET-basierten Frameworks mit seinen Klassenbibliotheken gehen.

Bei jeder Integration sind spezifische Anforderungen der Infrastruktur zu erfüllen. Dazu gehören i.d.R. insbesondere die Bereitstellung von Schnittstellen zu anderen integrierten Fachverfahren und zu zentralen Diensten des GovernmentGateways.

Bei der Integration sind die Styleguides und die Programmierrichtlinien der relevanten Mandanten einzuhalten.

11.2 Identitäts- und Zugriffsmanagement (IAM)

Am vorgesehenen Einsatzort der Applikation wird kontinuierlich der Aufwand für das Management von Identitäten (elektronische Repräsentationen von Personen, Organisationseinheiten etc.) und den Zugriff auf Applikationen und andere Ressourcen (Identity and Access Management - IAM) durch Ausbau der Infrastruktur reduziert werden.

Vor diesem Hintergrund sollen neue Applikationen auf die Nutzung einer IAM-Infrastruktur durch standardisierte Schnittstellen insbesondere für Identitätsprovisionierung, Authentisierung und Autorisierung möglichst gut geeignet sein.

11.2.1 Unterstützung von Identitätsprovisionierung

Am vorgesehenen Einsatzort der Applikation wird kontinuierlich der Aufwand für die Pflege von gespeicherten Identitätsdaten (elektronische Repräsentationen von Personen, Organisationseinheiten etc.) und deren Konsistenz reduziert werden.

Werden im Verfahren Identitäten gespeichert, die bereits an anderer Stelle des Einsatzortes gepflegt werden, sollen sie von ihm auf standardbasierte Weise als Provisionierungssenke empfangen werden können.

Verfügt das Verfahren über Funktionalität, die in ihm gespeicherten Identitätsdaten zu pflegen (erzeugen, ändern, löschen), dann sollte es diese – andersherum - auf standardbasierte Weise als Provisionierungsquelle an andere Verfahren als am Einsatzort übergeben können.

Bevorzugte Provisionierungsstandards: SPML 1.0, SPML 2.0

11.2.2 Unterstützung von Authentisierung beim Zugriff

Die Überprüfung der Korrektheit der vom Benutzer beim Zugriffsversuch behaupteten Identität (Authentisierung) können Verfahren auf technisch unterschiedliche Weisen vornehmen, die Einfluss auf den Grad ihrer Eignung haben, eine IAM-Infrastruktur zu nutzen.

- Verfahren mit integrierter geschlossener Benutzerverwaltung: Verfahren mit Benutzerverwaltungen, die ein integrierter Teil sind, und deren Benutzer ausschließlich mithilfe dieses Verfahrens gepflegt werden können, sind *nicht* geeignet, IAM-Infrastrukturen für die Authentisierung zu nutzen.
- Verfahren mit Provisionierungs-Importschnittstelle für ihre integrierte Benutzerverwaltung: Verfahren, die über Schnittstellen - als Provisionierungssenken – Benutzerdaten in ihre internen Benutzerverwaltungen übernehmen können, *sind* geeignet, eine IAM-Infrastruktur indirekt für die Authentisierung zu nutzen.
- Verfahren, die auf Verzeichnisdienste (z.B. Active Directories) zurückgreifen: Verfahren, die für die Authentifizierung Einträge ihrer Benutzer in einem Verzeichnisdienst nutzen können (als Provisionierungsquelle für ihre eigene Benutzerverwaltung, durch Anfragen an den Verzeichnisdienst oder durch Akzeptierung einer bereits zuvor durch Login erfolgten Authentifizierung (SSO)), *sind* damit auch geeignet, eine IAM-Infrastruktur – nämlich diesen Verzeichnisdienst – zu nutzen.
- Verfahren die Zugriffstoken auswerten: Verfahren, die von Identityprovidern (IDPs) ausgestellte Token als Authentisierung akzeptieren, sind derzeit *am besten* geeignet, eine IAM-Infrastruktur zu nutzen.

Bevorzugte Authentisierungs-Standards: WS-Security, WS-Trust

11.2.2.1 Single-Sign-On (SSO) mit Windows Anmeldung

Der Anwender soll – soweit für das Fachverfahren sinnvoll und datenschutzrechtlich zulässig - nach einer einmaligen Authentifizierung auf alle Komponenten und Dienste des Verfahrens, für die er berechtigt ist, zugreifen können. Wann immer möglich, sollte der Login an der Microsoft Windows-Domäne (Active Directory) allen Komponenten und Diensten über das Netzwerkprotokoll Kerberos verfügbar gemacht werden. Windows-Accounts sind ggf. auf lokale Identitäten der Verfahren abzubilden.

Bei Windows-Domänen-übergreifenden Zugriffen sollten standardisierte Verfahren zur sicheren Übermittlung der Authentifizierungsinformationen verwendet werden. Webservice-basierte Komponenten sollten hierzu den Standards von WS-Security und ggf. WS-Trust/WS-Federation entsprechen.

11.2.3 Unterstützung von Autorisierung beim Zugriff

11.2.3.1 Nutzung spezieller IAM-Infrastruktur in Hamburg

Soll die Lösung im Intranet der Stadt (FHHNet) eingesetzt werden und verwendet sie ein rollenbasiertes Konzept zur Autorisierung der Anwender, dann soll sie die von Hamburg hierfür angebotene Infrastruktur nutzen. Hamburg bietet dazu mit der Kombination aus HamburgService Infosystem (HaSI) und Berechtigungskonzept Applikation (BeKA) die Möglichkeit, auf die Personendatenpflege in der Benutzer- und Rechteverwaltung von Fachverfahren zu verzichten. Die Zuweisung von Benutzerrollen, welche eine Person in einem Fachverfahren einnehmen soll, erfolgt über BeKA. Die für Fachverfahren relevanten von HaSI geführten Benutzerdaten werden in regelmäßigen Abständen per Export zur Verfügung gestellt. Benötigt eine Lösung Benutzerdaten, die nicht in HaSI sind, so ist zu klären, wie die Anwendung diese Daten erhält oder ob ggf. HaSI erweitert werden soll.

11.3 Kassenschnittstelle, Ein- und Auszahlungen

Ein- und Auszahlungen erfolgen über die Kassenverfahren der Länder, deren Schnittstellen zu bedienen sind.

11.4 Microsoft Office

Soweit aus dem Verfahren mit Hilfe von Vorlagen oder Textbausteinen komplette Dokumente erstellt werden sollen, müssen die Quelldokumente kompatibel zu den zum Zeitpunkt der Einführung oder Produktion gültigen Formaten und Versionen der Microsoft Office Pakete sein oder ein entsprechender Editor durch den Anbieter geliefert werden. Zusätzlich sind die – ggf. per Richtlinien – getroffenen Voreinstellungen der Versionen bezüglich Sicherheit und Funktionalität für die jeweilige Kundengruppe zu berücksichtigen.

11.5 Elektronische Akte

Elektronisches Schriftgut (Akte, Band, Vorgang, Dokument) wird über xdomea, das XML-Austauschformat für elektronisches Schriftgut – in der Version 2.1 oder höher - an die in den Ländern vorhandenen Systeme für elektronische Aktenführung (VISkompakt für Schleswig-Holstein und Bremen, ELDORADO für Hamburg) übergeben. Es sind dabei nur die xdomea-Nachrichtengruppen zu berücksichtigen, die für den konkreten Anwendungsfall benötigt werden.

Hiervon kann abgewichen werden, wenn spezifische Aktenführungssysteme der Anwendung einen deutlichen wirtschaftlichen Vorteil haben.

Bei landesspezifischen Anwendungen können die spezifischen Schnittstellen der vorhandenen Systeme für die Anbindung genutzt werden.