Friedrich-Heinrich-Allee 130, D-47475 Kamp-Lintfort

Europaweite Ausschreibung im Offenen Verfahren

„DMS mit Workflowengine“

Leistungsbeschreibung - Allgemein

Dieses Dokument ist urheberrechtlich geschützt.

Die unbefugte Vervielfältigung, Umgestaltung, Bearbeitung, Verbreitung oder öffentliche Wiedergabe dieses Dokuments oder eines Teils davon ist unzulässig. Ein Verstoß wird sowohl straf- als auch zivilrechtlich verfolgt.

1. Ausgangssituation

Die Kreise Kleve, Viersen und Wesel sowie die Städte Bottrop und Krefeld bilden den Zweckverband Kommunales Rechenzentrum Niederrhein (KRZN) nach dem Gesetz über kommunale Gemeinschaftsarbeit in der Fassung der Bekanntmachung vom 01.10.1979 (GV NRW S. 621), zuletzt geändert durch Art. V des Gesetzes zur Stärkung der kommunalen Selbstverwaltung – GO Reformgesetz- vom 09.10.2007 (GV NRW S. 389). Weiter sind die bestehenden öffentlich-rechtlichen Vereinbarungen zwischen dem Kreis Kleve und seinen Städten und Gemeinden vom 18.11.1977, zwischen dem Kreis Viersen und seinen Städten und Gemeinden in der Änderungsfassung vom 20.01.1978 und zwischen dem Kreis Wesel und seinen Städten und Gemeinden vom 28.03.1979 zu berücksichtigen. Gemäß § 2 Abs. 2 der Satzung des KRZN hat der Zweckverband die Aufgabe, Technikunterstützte Informationsverarbeitung für seine Mitglieder und Anwender zu entwickeln oder zu beschaffen und anzubieten. Ferner kann der Zweckverband Leistungen im Rahmen seines Aufgabenbereiches für Dritte erbringen.

Seit 16 Jahren wird im KRZN IBM Domino zusammen mit Notes als eGovernment-Basisinfrastruktur eingesetzt. Hierauf wurden vom KRZN ein Dokumentenmanagement, ein Webcontentmanagement und eine Workflow-Engine entwickelt.

2. Beschreibung des IST-Zustands

Momentan wird die vom KRZN entwickelte eGovernment-Suite in den Versionen 2.X bzw. 3.X auf den Dominoservern der Anwender eingesetzt. Die eGovernment-Suite beinhaltet die Komponenten Dokumentenmanagement, Workflow-Engine und Webcontentmanagement.

Bei den folgenden genannten Werten bzgl. Nutzern, Ablagen, Speicherplatz und Dokumentengröße handelt es sich um unverbindliche Orientierungsgrößen (Schätzmengen).

3. Dokumentenmanagement

Flächendeckend wird das Modul Dokumentenmanagement bei der Gemeinde Schwalmtal (62 Nutzer, 18 DMS-Ablagen, 200 GB), dem Kreis Wesel (bis Ende 2017 laufender flächendeckenden Rollout bislang 855 Nutzer, 301 DMS-Ablagen, 260 GB) und der Stadt Rheinberg (120 Nutzer, 165 DMS-Ablagen, 288 GB) eingesetzt.

In ausgewählten organisatorischen Bereichen wird das Dokumentenmanagement bei dem KRZN (200 Nutzer, 251 DMS-Ablagen, 382 GB), der Stadt Krefeld (40 Nutzer, 18 DMS-Ablagen, 24 GB), der Stadt Kalkar (20 Nutzer, 10 DMS-Ablagen, 7 GB), der Gemeinde Kranenburg (8 Nutzer, 14 DMS-Ablagen, 9 GB) und der Stadt Kleve (100 Nutzer, 33 DMS-Ablagen, 25 GB) eingesetzt.

Weitere geringfügige Dokumentenmanagement-Umgebungen, z.B. Stadt Emmerich am Rhein (4 Nutzer, 4 DMS-Ablagen, <0,5 GB), sind im Verbandsgebiet vorhanden.

Die Anzahl und das Volumen der Dokumente ist sehr heterogen. Es sind Dokumente mit Größen von mehreren Gigabyte bis wenigen Byte vorhanden. Die Schätzung des KRZN geht davon aus, dass die ungefähre durchschnittliche Dokumentengröße bei 25 KB liegt und ein Gesamtdatenbestand von ca. 1,2 Terrabyte vorhanden ist. Daher beläuft sich die geschätzte Anzahl an Dokumenten auf ca. 4,4 Mio. Dokumente. Die vorhandenen Dokumente sind in das neue Verfahren vollständig zu migrieren. Es ist davon auszugehen, dass die Dokumentenmenge weiterhin steigend ist und zum Migrationszeitpunkt noch höher liegen wird.

4. Workflow-Engine

Die vom KRZN entwickelten Prozesse sind als Anlage beigefügt. Fallzahlen zu den Workflows werden nicht erfasst und sind nur schwer abschätzbar. Es muss davon ausgegangen werden, dass insbesondere einige der externen Workflows mehrere tausendmal jährlich initiiert werden (bspw. „Anmeldung zur Belehrung nach Infektionsschutzgesetz“). Andere Workflows wie „Beschwerdemanagement“ werden kaum 100 Fälle jährlich aufweisen.

Weiter ist zu berücksichtigen, dass auch einige Anwender selbst Workflows mittels der eGovernment-Suite erstellt haben. Zu den Anwendern, die dies selbst entwickelt haben, gehören u.a. Stadt Rheinberg, Stadt Kleve, Stadt Moers und Stadt Krefeld.

Die Architektur des Workflows muss so angelegt sein, dass die Initiierung von Prozessen auch aus dem Internet möglich ist und (Teil-)Ergebnisse mit entsprechender Internettechnologie verfügbar gemacht werden können. Der Zugriffsschutz auf ggf. vertrauliche Informationen ist zu gewährleisten.

5. Systemumfeld im KRZN

5.1 Netzwerkstruktur

Das neue Verfahren muss sich in die aktuelle Weitverkehrsinfrastruktur (WAN), das Primärnetz des KRZN, integrieren. Die WAN-Verbindungen sind nicht mit den Spezifikationen der lokalen Netzwerke (LAN) zu vergleichen und haben deshalb grundlegende Anforderungen an das Kommunikationsdesign der Anwendungen.

Das WAN des KRZN besteht aus einer Kombination von unterschiedlichen WAN-Technologien. Werden für die Anbindung der Kommunalverwaltungen Clearchannel SDH und ATM-DSL Verbindungen genutzt, stehen für die Verbindung der nachgelagerten Lokationen (Bauhöfe, Feuerwehren, Außenstellen usw.), im sog. Sekundärnetz die DSL Konsumerprodukte der Telekom zur Verfügung. Diese Endkundenprodukte unterscheiden sich nochmals durch Übertragungsqualität und Verfügbarkeit von den hochwertigen Leitungen im Primärnetz.

Diese Topologie hat teilweise ein sehr heterogenes Übertragungsprofil zur Folge, die eine Anwendung durch hohe Flexibilität und Stabilität bei der Datenübertragung ausgleichen muss.

Latenzzeiten und Delay

Neben den Restriktionen bei der Übertragung von großen Datenmengen ist auch die Art und Weise der Kommunikation zwischen Client und Server zu berücksichtigen. So ist die Verweildauer eines IP-Pakets bei einer WAN-Übertragung bedingt durch Router, IPSec, NAT, Priorisierung um den Faktor 100 bis 1.000 mal größer, als dies bei reiner LAN-Kommunikation der Fall wäre.

LAN: Delay zwischen Client und Server = 0,02 ms

WAN: Delay zwischen Client und Server <= 3 ms

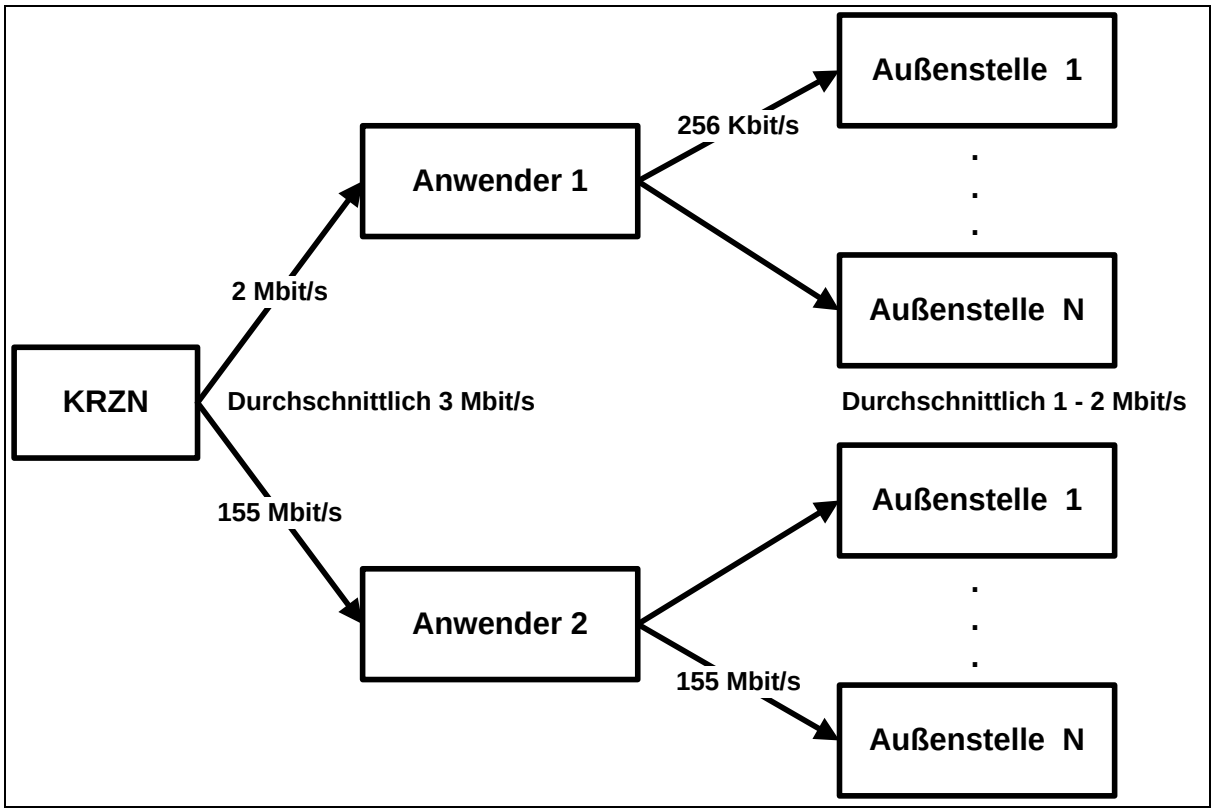
Bei LAN-Lösungen ist der Einfluss des Leitungsdelays vernachlässigbar klein. Bei Übertragung der gleichen Kommunikationsstruktur über eine WAN-Lösung macht sich dies dann in der Anwendung bemerkbar, wenn es sich um bestätigungsintensive Kommunikation zwischen dem Client und dem Server handelt. In der weitgespannten WAN Umgebung ist also eine Kommunikation mit niedriger Bandbreite, geringen Lastspitzen und einer geringen Bestätigungsrate im Netzwerkprotokoll unabdingbar.

IP- und Domainkonzept

Innerhalb des WAN und der angeschlossenen LAN-Strukturen wird ein privates IP-Adresskonzept verwandt. Alle Kommunalverwaltungen verfügen über einen Class-B Adressraum aus dem 10er Adressbereich. Direkte Kommunikation zu öffentlichen IP-Adressen ist nur mittels NAT über das KRZN möglich.

Bei Überschneidungen in den Adresskonzepten im Zusammenhang mit dem Anschluss neuer Kunden und Anwender werden NAT-Pools eingesetzt, die eine Beibehaltung der jeweiligen Strukturen ermöglichen. An das IP-Konzept angelehnt, existiert ein durchgängiges Domainkonzept für die Kommunalverwaltungen.

Das vorhandene WAN (Niederrheinnetz) ist wie folgt strukturiert:



Durch den Auftragnehmer ist sicherzustellen, dass alle angebotenen Funktionalitäten der neuen Anwendungen einwandfrei und ohne Einschränkungen in der Infrastruktur des KRZN und seiner

Anwender betrieben werden können. Dies gilt sowohl für die LAN- als auch für die WAN-Topologien.

Sollten zusätzliche Anforderungen an die Leistungsfähigkeit der Netzwerktopologie existieren, die über die aktuellen verfügbaren Kapazitäten hinausgehen, ist dies vom Bieter in seinem Angebot aufzuzeigen.

5.2 Internetkommunikation und -dienste

Bis auf die Stadt Bottrop verfügt kein Anwender über einen eigenen Zugang zum Internet. Alle Internetdienste werden zentral durch das KRZN zur Verfügung gestellt. Die klassischen Kommunikationsbeziehungen wie Mail, Internetrecherche (http, https), Filetransfer (ftp) usw. werden über Proxy-Systeme ermöglicht. Der Mailverkehr wird zentral über SPAM- und Antivirenfilter geleitet (bis auf Stadt Bottrop), bevor er auf die dezentralen Mailsysteme verteilt wird.

Direkte ausgehende NAT Verbindungen zu Servern im Internet unterliegen strengen Auflagen und müssen einzeln auf den zentralen Sicherheitssystemen freigeschaltet werden. Eingehende NAT Verbindungen sind nicht gestattet.

Dienste (z.B. http-Server), die für andere Internetnutzer weltweit zur Verfügung gestellt werden, sind in einer DMZ des KRZN zu installieren. Die Kommunikationsbeziehungen sind vor der Installation dem Datenschutzbeauftragten und dem Fachpersonal des KRZN mitzuteilen. Die Vergabe der öffentlichen IP-Adressen und die Freischaltung erfolgt durch das KRZN.

6. Zielsetzung

Das KRZN beabsichtigt, eine komplette Umgebung im Bereich Dokumentenmanagement mit Workflow-Engine seinen Anwendern auf Basis eines am Markt befindlichen Produkts (der Beschaffungsgegenstand) offerieren zu können. Auch zukünftig wird das KRZN im Bereich der Anwendungsentwicklung tätig sein und für seine Anwender elektronische Akten und komplexe Workflows erstellen sowie notwendige Schnittstellen entwickeln.

Es muss möglich sein, dass Anwender des KRZN auf Wunsch das zu beschaffende Produkt auch dezentral betreiben können. Evtl. entstehende Mehrkosten für Serverlizenzen und zusätzliches Consulting werden durch den jeweiligen Anwender getragen.

Jeder Benutzer muss einen Einzelplatzscanner nutzen können. Ein Rendition-Service für die Dokumente muss für alle Benutzer in dem neuen Verfahren enthalten sein.

6.1 Zeitplanungen

Die Einhaltung folgender Meilensteine ist zwingende Grundlage für die Projektrealisierung und Vertragsausführung:

06/2017: Einrichtung der Systemumgebung im KRZN

07/2017: Installation des neuen Verfahrens durch den Auftragnehmer und Schulungen der KRZN-Mitarbeiter

10/2017: Abschluss der Installationsleistung durch den Auftragnehmer und Beginn des KRZN-internen Testbetriebs vor der Freigabe für die produktive Nutzung

01/2018: Aufnahme des Echtbetriebs für die erste betreue Anwenderverwaltung

Danach: voraussichtlich sukzessive Produktionsaufnahmen für alle betreuten Anwendern während der ersten fünf Jahre (Roll-out).

6.2 Mengengerüst

Grundlage für die technischen Rahmenbedingungen ist das folgende geschätzte Mengengerüst im Endausbau:

Betreute Anwenderverwaltungen:	42 (gemäß Anlage)
Betreute Arbeitsplätze:	ca. 12.500
Umgebungen:	Produktionsumgebung, QS-Umgebung, Entwicklungsumgebung

In der Produktionsumgebung befinden sich die produktiven Daten für alle im KRZN betriebenen Mandanten. Die QS-Umgebung dient der Qualitätssicherung. Die Entwicklungsumgebung dient der Wartung, Pflege und Weiterentwicklung.

Die zu vereinbarende (Verbands-)Lizenz umfasst alle gegenwärtigen und zukünftigen Mitarbeiter der Kreise, Städte und Gemeinden im KRZN-Verbandsgebiet (vgl. Anlage der Kommunalverwaltungen) sowie alle Beteiligungen, die ausgelagert Aufgaben dieser Kommunen wahrnehmen, mit mehr als 50 % Beteiligungsanteil der beteiligten Kommunen.

6.3 Zentraler / dezentraler Betrieb

Die ausgeschriebene Software für das Dokumentenmanagement inkl. Workflow-Komponente soll zentral im KRZN eingesetzt werden. Die benötigten Datenbank- und Applikations-Server haben dabei ihren Standort im KRZN. Alternativ muss ein dezentraler Betrieb der Software für das Dokumentenmanagement incl. Workflow-Komponente bei den einzelnen Anwendern des KRZN möglich sein. Für den Fall, dass ein Mandant einen dezentralen Betrieb wünscht, ist vom Bieter **eine Preisliste für die notwendigen Serverkomponenten und Dienstleistungen dem Angebot beizulegen**.

Zu einem zentralen Betrieb gehören u.a.:

- Bereitstellung und Überwachung der Serverhardware bzw. virtueller Server,
- Durchführen und Überwachung der Datensicherung,
- Durchführen und Überwachen von Batch-Läufen,
- Durchführung und Überwachung des Datenaustauschs mit anderen Verfahren,
- Bereitstellung der Kommunikationsverbindungen für den Datenaustausch mit externen Organisationseinheiten,
- Pflege und Updates der Betriebs- und Anwendungssoftware,
- Organisation von Produktions-, QS- und Entwicklungsumgebung und
- Unterstützung der Mandanten.

Teilaspekte dieser Auflistung gelten auch für den dezentralen Betrieb.

Unabhängig vom zentralen und dezentralen Betrieb werden alle Schulungen zentral über das KRZN (dem Auftraggeber) organisiert und in der Regel auch dort durchgeführt.

7. Anforderung an die Fernwartung

Über eine Zugangslösung muss sichergestellt werden, dass Softwareprodukte von Fremdfirmen entsprechend den Richtlinien der Security Policy des KRZN und der technischen Infrastruktur gewartet werden können.

Fernwartungszugänge im Rahmen von Remote Access:

- Einzelplatzlösung: OpenVPN Softwareclient mit personalisiertem e-Token. Mit den personalisierten e-Token erfolgt die Einwahl über das KRZN.
- Mehrplatzlösung: IPsec-VPN Verbindung mit einem zentralen VPN-Concentrator
- Desksharing: Im Einzelfall kann eine Team-Viewer-Session oder ein vergleichbares Produkt genutzt werden. Generell dürfen diese Verbindungen nur von einem internen Mitarbeiter (KRZN) initiiert werden. Ein direkter Zugriff von extern ist nicht gestattet. Über diesen Weg kann dem externen Dienstleister (Auftragnehmer) Zugriff auf das zentrale System ermöglicht werden.

Es ist Folgendes zu beachten:

- Die Zugänge werden restriktiv durch Firewall-Systeme überwacht und eingeschränkt.
- Das Wartungspersonal des Auftragnehmers muss sich zu Beginn der Wartung authentisieren. Werden dabei Passwörter unverschlüsselt übertragen, sollten Einmalpasswörter benutzt werden.
- Alle Tätigkeiten bei der Durchführung der Fernwartung müssen auf dem zu wartenden IT-System protokolliert werden.
- Die Fernwartung ist im Normalbetrieb gesperrt und wird nur für eine genau definierte Zeitspanne freigegeben.
- Der Aufbau der Verbindung für eine Fernwartung wird immer vom lokalen KRZN IT-System initiiert bzw. zugelassen.
- Das Wartungspersonal des Auftragnehmers sollte nicht mit vollen Admin-Rechten arbeiten; auf keinen Fall werden mit dem Admin-Account Wartungsarbeiten durchgeführt.
- Auf dem System existiert für das Wartungspersonal des Auftragnehmers eine eigene Nutzerkennung, unter der möglichst alle Wartungsarbeiten durchgeführt werden.
- Die Fernwartung durch den Auftragnehmer muss vom Fachpersonal des KRZN beobachtet werden, bzw. es ist ein detaillierter Arbeitsnachweis am Ende eines Wartungsfensters durch den Auftragnehmer zu erstellen und dem Anwendungsbetreuer zeitnah zuzusenden.
- Mit dem Wartungspersonal des Auftragnehmers werden vertragliche Regelungen über die Geheimhaltung von Daten vereinbart. Insbesondere sind Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig vom Auftragnehmer zu löschen.