

## F. Handlungsempfehlungen für zuständige Stellen und Träger des Einheitlichen Ansprechpartners

### Kurzüberblick

Der Projektbericht sieht als Zielarchitektur eine service-orientierte Architektur (SOA) vor. Diese Zielarchitektur ist jedoch nur langfristig zu erreichen, da die Prozesse in der Verwaltung mitunter sehr komplex sind und die IT Landschaften in den Ländern stark differieren. Es werden unterschiedliche Systeme zur Verfahrensabwicklung eingesetzt bzw. Abläufe sind unterschiedlich innerhalb und zwischen öffentlichen Verwaltungen geregelt. Vor diesem Hintergrund müssen die Prozesse in den einzelnen Ländern genauer untersucht werden. Erst nachdem die Prozesse klar identifiziert sind, können Überlegungen angestellt werden, wie diese durch eine Serviceorientierung konkret optimiert werden können. Durch genaue Kenntnis der Prozesse wird beispielsweise ersichtlich, welche Funktionalitäten aufgrund ihrer Wiederverwendbarkeit an zentraler Stelle als Dienst für unterschiedliche Organisationen bereitgestellt werden sollten. In Kapitel C, Abschnitt IV wird der Aufbau eines Prozessregisters vorgeschlagen, das beim Erreichen der Zielvorgaben unterstützen soll. Im Rahmen der Forschungs- und Entwicklungsprojekte des Hasso-Plattner-Instituts und der Humboldt Universität wurden bereits einige Prozesse zur Verfahrensabwicklung in verschiedenen Bundesländern betrachtet. Diese Untersuchungen werden auch zukünftig weitergeführt, da sie zwingend notwendig für ein sinnvolles und effizientes SOA-Design sind. Da die Arbeiten bezüglich der Prozessanalyse noch nicht in vollem Umfang vollzogen sind und demzufolge ein detailliertes SOA-Design noch bevorsteht, ist das beschriebene Architekturmodell als grobe Zielarchitektur zu verstehen.

In diesem Kapitel werden Handlungsempfehlungen gegeben, die aus den bisherigen Erkenntnissen der Untersuchungen abgeleitet werden können und dabei helfen, das langfristige Ziel einer SOA für die Umsetzungsstufe 2 zu erreichen. Beginnend mit Empfehlungen zur Sicherheit, werden Hinweise hinsichtlich der allgemeinen Kommunikation, der Ausgestaltung von Informationsportalen, der Datenspeicherung, des Prozessmanagements und der Nutzung von externen Diensten für die Verantwortlichen in den Umsetzungsprojekten zur DL-RL formuliert.

### I. Sicherheit

#### 1. Sicherheit ausreichend im SOA-Design berücksichtigen

- Sicherheit muss von Anfang an als ein zentrales Thema bei der Umsetzung von IT-Vorhaben angesehen werden und ist daher bereits beim SOA-Design speziell im Hinblick auf die Interoperabilität zu berücksichtigen. Performanceprobleme, die aufgrund einer ineffizienten oder fehlenden Sicherheitskonzeption zustande kommen, könnten somit verhindert werden. Um die Interoperabilität und sichere Kommunikation zwischen den verteilten Systemen und Diensten zu gewährleisten, sollten einzuhaltende Sicherheitsstandards von einer zentralen Koordinationsstelle oder Organisation verbindlich festgelegt werden (vgl. hierzu C.I.8. „Verbindlichkeit fachlicher und technischer Standards“ sowie E. III. 7 „vorgeschlagene Standards und Technologien“.) Durch eine Standardisierung könnten Mehrfachimplementationen oder zusätzliche Anstrengungen zur Herstellung der Interoperabilität vermieden werden. Bestimmte Sicherheitsfunktionalitäten wie z.B. die Verschlüsselung oder das Signieren von zu übertragenden Inhalten könnten ggf. zentral für verschiedene Verwaltungsebenen zur Verfügung gestellt werden.

#### 2. Neuen Schutzbedarf ermitteln

- Das Anbieten und Nutzen von Diensten im Internet stellt bestimmte Anforderungen an das zu gewährleistende Sicherheitsniveau. Aus diesem Grund ist es für die beteiligten Organisationen wichtig, zunächst den neuen Schutzbedarf zu bestimmen und daran anschließend die entsprechenden Sicherungsmaßnahmen zum Schutze der Vertraulichkeit, Verfügbarkeit und Integrität von Daten zu ergreifen. Speziell im Hinblick auf eine service-orientierte Architektur unterscheiden sich die Sicherungsmechanismen von den herkömmlichen Sicherungsfunktionen, die innerhalb einer Organisation

bisher zum Einsatz kamen. Da eine service-orientierte Architektur durch eine verstärkte domänenübergreifende Interaktion zwischen IT-Systemen und Diensten geprägt ist, müssen neue adäquate Sicherheitstechnologien und -techniken eingesetzt werden, die auch weiterhin die erforderliche Sicherheit bieten.

- **Vertraulichkeit:** Da zukünftig die Kommunikation der öffentlichen Verwaltung verstärkt elektronisch stattfinden soll, müssen ggf. weitere Maßnahmen zur Gewährleistung der Vertraulichkeit von Daten umgesetzt werden. Speziell bei der Kommunikation über öffentliche Netze, müssen sensible Daten verschlüsselt übertragen werden. Bei der Kommunikation im Web-Service-Umfeld kann OSCI 2.0 als eine Profilierung der Standards im Bereich WS-Security (s. vorgeschlagene Standards und Technologien im Kapitel E III. 7) zum Schutz der Vertraulichkeit eingesetzt werden. Für die Zukunft ist zudem mit einer verstärkten Nutzung von gemeinsamen Datenbanken und Informationssystemen zu rechnen, wodurch ein komplexes Identitäts- und Zugriffsmanagement erforderlich wird, das weiterhin die Vertraulichkeit sicherstellt. Es dürfen lediglich Personen oder Systeme Zugriff auf die Daten erhalten, die über die entsprechenden Berechtigungen verfügen.
- **Verfügbarkeit:** Die Verfügbarkeit von Diensten und Systemen ist zu gewährleisten, um einerseits ordnungsgemäß die elektronischen Verwaltungsprozesse zu unterstützen und andererseits dem Dienstleistungserbringer die Möglichkeit zu bieten, jederzeit Informationen zu erhalten bzw. Anträge zu stellen. Aus diesem Grund sind speziell Vorsorgemaßnahmen hinsichtlich der Ausfallsicherheit zu treffen.
- **Integrität:** Sicherstellung der Integrität zielt darauf ab, dass Daten vor Manipulation geschützt werden. Dies muss durch Umsetzung von geeigneten Zugriffsmechanismen sowie durch Identitäts- und Integritätsprüfungen erfolgen. Die Wahrung der Integrität von Daten kann über die Nutzung von elektronischen Signaturen gewährleistet werden. Im Hinblick auf eine Service-orientierte Architektur und für den Austausch von Nachrichten über Webservices bietet sich in diesem Zusammenhang der Gebrauch von XML-Signaturen an.

### 3. IT-Infrastruktur schützen

- Bei Einrichtung eines Webportals bzw. Aufbau eines Webangebots müssen je nach Ausgestaltung des Onlineangebots bestimmte Schutzmaßnahmen ergriffen werden. So gilt es durch geeignete Schutzmaßnahmen Angriffe wie bspw. Cross-Site Scripting, SQL-Injection, Buffer Overflows etc. zu verhindern. Speziell bei der Nutzung von dynamisch generierten Inhalten, wie es bspw. bei der dialogbasierten Erzeugung von Antragsformularen der Fall ist, muss von einem erhöhten Risiko ausgegangen werden.
- Unabhängig von der Ausgestaltung des Portals, sollte durch Einsatz von Sicherheits-Software und -Hardware sowie deren ordnungsgemäße Konfiguration das Portal abgesichert werden.
- Da als erste elektronische Kommunikationsform voraussichtlich verstärkt E-Mail eingesetzt wird, sollten effiziente Mailfilter zur Erkennung von SPAM- und Phishing-Mails sowie Mails mit Malicious Code zum Einsatz kommen.

### 4. Kommunikation und Zugriff auf Daten sichern

- Ermöglicht man dem Dienstleister eine Antragsstellung über ein Portal, muss eine gesicherte Verbindung zwischen dem Server und dem Client aufgebaut werden und die Daten verschlüsselt übertragen werden. In diesem Zusammenhang ist darauf zu achten, dass der Server stets über ein gültiges Zertifikat verfügt.
- Sollen Fachverfahren gekoppelt oder Wissensdatenbanken gemeinsam benutzt werden, muss eine Identitäts- und Zugriffssteuerung eingesetzt werden. Zu diesem Zweck ist zunächst festzulegen, wer auf welche Inhalte zugreifen darf und welche Daten an wen übertragen werden.

- Im Hinblick auf die Zielarchitektur sollte frühzeitig über ein föderiertes Identitäts- und Access-Management nachgedacht und im SOA-Design berücksichtigt werden. Dies ist notwendig, da in einer Service-orientierten Architektur Dienste und Systeme verteilt über verschiedene Trust-Domains genutzt werden, der Zugriff jedoch nur mit der jeweiligen Berechtigung erfolgen darf. Da innerhalb einer SOA der Verwaltungsaufwand von Identitäten aufgrund der komplexen und weitreichenden Kommunikationsbeziehungen schnell sehr ineffizient werden würde, ist ein föderiertes Identitäts- und Accessmanagement unabdingbar. Durch eine konsequente Umsetzung könnte sogar ein Single-Sign On realisiert werden, d.h. eine Kennung würde ausreichen, um komfortabel verschiedene Dienste nutzen zu können. An dieser Stelle wird deshalb nochmals auf das SAFE (Secure Access to Federated eJustice/eGovernment) Projekt der Justizverwaltungen der Länder und des Bundes hingewiesen, das sich speziell mit der Umsetzung eines föderierten Identitäts- und Access-Managements auseinandersetzt (vgl. E.III.4.).

#### **5. Regeln des Datenschutzes berücksichtigen**

- Neben den üblichen Datensicherungsmaßnahmen, die sich aus dem Betrieb von Informationssystemen ergeben, sind ggf. gesonderte Vorkehrungen bezüglich der Einhaltung datenschutzrechtlicher Regelungen zu treffen (vgl. C. I. 3.).
- Anbietern von Portalen oder Informationsdiensten wird aus Haftungsgründen empfohlen, relevante Zugriffe auf Daten oder Systeme innerhalb der Verwaltungsverfahren zu dokumentieren.

#### **6. IT-Sicherheitsmanagement**

- Zur dauerhaften Aufrechterhaltung der IT-Sicherheit erscheint der Aufbau eines effektiven IT-Sicherheitsmanagement auf allen Ebenen notwendig. Dabei sollte eine Orientierung an dem Standard ISO 27001 auf der Basis von IT-Grundschutz (BSI-Standards 100-1, 100-2 und 100-3) erfolgen. Die einzelnen IT-Sicherheitsmaßnahmen sollten in entsprechenden IT-Sicherheitskonzepten eingebettet sein.

#### **7. Schulung und Sensibilisierung von Mitarbeitern**

- Vor dem Hintergrund, dass Mitarbeiter in den Organisationen zukünftig verstärkt Informations- und Kommunikationstechnologien nutzen werden, müssen ausreichend Schulungen durchgeführt werden. Sensibilisierung der Mitarbeiter für Informationssicherheit ist eine wichtige Aufgabe, die frühzeitig erfolgen sollte. Durch ein angemessenes Sicherheitsbewusstsein können Sicherheitsvorfälle, die durch Unwissenheit, ungewolltes Fehlverhalten, Irrtum oder Nachlässigkeit entstehen, oftmals verhindert werden.

## **II. Allgemeine Kommunikation**

### **1. Verbindliche Kommunikationsstandards und Austauschformate festlegen**

- Die Art der Kommunikation hängt maßgeblich von dem im SOA-Design spezifizierten Diensten, Prozessen und involvierten IT-Systemen ab. Es ist festzulegen an welchen Stellen Adapter oder Schnittstellen zu bestehenden Systemen geschaffen werden müssen oder welcher Service komplett neu implementiert werden muss. Um jedoch allgemein eine standardisierte Kommunikation und damit Interoperabilität zu gewährleisten, sollten verbindliche Standards für die Kommunikation festgelegt werden (vgl. hierzu C.I.8. „Verbindlichkeit fachlicher und technischer Standards“ sowie E. III. 7 „vorgeschlagene Standards und Technologien“).
- Für eine für Stufe 2 vorgesehene automatisierte Kommunikation und Prozesssteuerung ist es wichtig, dass nach einer anfänglichen Kommunikation z.B. über E-Mail, frühzeitig Services bei den Einheitlichen Ansprechpartnern und den zuständigen Stellen implementiert werden, die gemeinsame Standards befolgen und somit die Interoperabilität zwischen unterschiedlichen IT-Systemen ermöglichen.

## 2. Frühzeitige Migration zu einer strukturierten Kommunikation

- Da die Umsetzung von E-Mail als elektronisches Kommunikationsmedium vermutlich am einfachsten ist, könnte die Kommunikation zwischen Dienstleistungserbringer und Einheitlichem Ansprechpartner bzw. EA und den zuständigen Stellen anfangs über E-Mail erfolgen. An dieser Stelle sollte aber auf die nicht zu vernachlässigen Nachteile hingewiesen werden: Der hohe manuelle Aufwand, der sich z.B. aufgrund der Verwaltung von E-Mails und Archivierung von Dokumentenanhängen ergibt, darf nicht unterschätzt werden. Zudem kann es mitunter bei vielen Bearbeitungsvorgängen sehr unübersichtlich werden. Aus diesem Grunde sollte frühzeitig über Alternativen zur strukturierter Kommunikation oder zumindest Optimierung nachgedacht werden. Empfehlenswert ist der Austausch über standardisierte Schnittstellen und die Übertragung in standardisierten Formaten (vgl. Kapitel E.III, 7.1 und 7.4). Von daher wird vorgeschlagen, zumindest darüber nachzudenken, ob der Datenaustausch zwischen den EA und den zuständigen Behörden nicht von vornherein über OSCl Transport erfolgen sollte. Hier wäre denkbar, zunächst asynchron über entsprechende Clients zu kommunizieren, anschließend dann das Protokoll in die Vorgangsbearbeitungssysteme zu integrieren, um dann schließlich synchrone Szenarien auch über Web-Services abzubilden. Um eine Übertragung von Informationen und Dokumenten strukturierter zu gestalten, könnten spezielle Programme (Clients) genutzt bzw. für Dienstleistungserbringer bereitgestellt werden. Diese Programme würden gewisse Funktionalitäten für die entsprechenden Verwaltungsaufgaben aufweisen und Daten in einem Standardformat übertragen. Über eine Schnittstelle auf Serverseite wäre dann ein automatischer Import in Vorgangsverwaltungssysteme oder Dokumentenmanagementsysteme realisierbar.
- Alternativ könnten bestimmte Dienste in ein Webportal integriert werden, so dass eine Übertragung und automatisierte Speicherung in einem standardisierten Format möglich wäre. Ein persönlicher Bereich für den Dienstleistungserbringer wäre denkbar und sollte zumindest zu einem späteren Zeitpunkt umgesetzt werden. Die Funktionalitäten, die dem Dienstleistungserbringer geboten werden, könnten z.B. ein persönliches Postfach oder ein Uploadbereich für Dokumente sein. Je nach Bedarf ist eine Erweiterung des Portals um zusätzliche Dienste denkbar. Neben einer komfortablen Dokumentenverwaltung und standardisierten Möglichkeit Daten zu speichern, lassen sich wichtige Zusatzfunktionen wie Signatur- und Zeitstempeldienst an zentraler Stelle leicht realisieren. Allerdings werden für ein solches Portal Authentisierungs- und Autorisierungsmechanismen erforderlich, so dass ein Dienstleistungserbringer jeweils nur auf seinen persönlichen Bereich zugreifen kann.

## 3. Existierende etablierte Kommunikationssysteme evaluieren und neue Technologien prüfen

- Für bestimmte Fachverfahren existieren bereits Software-Lösungen und IT-Systeme, die bestimmte Sicherheits- und Kommunikationsstandards implementieren und daher weiterhin für die Kommunikation eingesetzt werden können (s. verfügbare/integrierbare Systeme in Kapitel E.IV). Allgemein ist der Einsatz von bestehenden Lösungen zu evaluieren. In vielen Fällen ist ggf. durch Implementierung einer geeigneten Schnittstelle bzw. eines Dienstes die nötige Interoperabilität mit anderen Systemen zu erreichen. Bei der Neuanschaffung von IT Systemen sollte jedoch auf die Unterstützung von bestimmten Formaten bzw. Schnittstellen geachtet werden, so dass kein zusätzlicher Anpassungsaufwand anfällt.
- Für manche Organisationen könnte es hinsichtlich einer Service-Orientierung ggf. nützlich sein, einen Enterprise Service Bus (ESB) einzusetzen. Ein ESB ist eine leistungsfähige Infrastruktur, die hauptsächlich für den Austausch von Daten zwischen Webservices und IT-Systemen verantwortlich ist. Bestehende Systeme können mittels Adaptoren an den ESB angebunden werden. Neben der eigentlichen Datenübertragung kann ein ESB weitere Funktionalitäten besitzen wie bspw. Verschlüsselungsmechanismen, Datenkonvertierung, Orchestrierung etc.

## 4. Kommunikation effizienter gestalten durch Nutzung zentraler Informationssysteme

- Der Einheitliche Ansprechpartner soll eine allgemeine Beratungskompetenz haben und nicht lediglich als Weiterleitungsinstanz agieren. Allerdings ist es eine zentrale Aufgabe des EAs eingereichte

Unterlagen und Anträge der Dienstleistungserbringer an die zuständigen Stellen und somit Entscheidungsträger weiterzuleiten. In der Anfangsphase wird dies voraussichtlich per E-Mail geschehen, da diesbezüglich die jeweiligen Organisationen bereits über die nötigen Voraussetzungen verfügen. Allerdings sollte auch hier nach Möglichkeit ein rascher Wechsel hin zu einer effizienteren Kommunikation über standardisierte Schnittstellen erfolgen, wodurch bestimmte Kommunikationsabläufe leichter automatisiert werden könnten.

- Der Einheitliche Ansprechpartner ist dazu verpflichtet ordnungsgemäß Akten über alle seine Aktivitäten innerhalb der Verwaltungsverfahren zu führen. In einem Fallmanagementsystem sollte der EA somit u.a. festhalten an welche Behörden er bestimmte Unterlagen verschickt hat. Der Status muss nach Erhalt einer Empfangsbestätigung einer zuständigen Stelle aktualisiert werden. Dieser Prozess sollte nach Möglichkeit frühzeitig automatisiert werden, was wiederum durch Nachrichten in einem Standardformat und über definierte Schnittstellen realisiert werden kann. Analog zur Einführung eines zentralen Dokumentenspeichers, sollte langfristig ein zentralisiertes Fallmanagementsystem implementiert werden, das den beteiligten Organisationen Einsicht in die laufenden Verfahren ermöglicht und z.B. dabei hilft, Mehrfachanträge frühzeitig zu erkennen. Hierzu wird die Definition eines „XDienstleistung“ Standards vorgeschlagen (vgl. hierzu C.I.8. „Verbindlichkeit fachlicher und technischer Standards“.) Durch eine konsequente Prozessorientierung und Umsetzung einer SOA, könnte der EA nicht nur bei der Antragserstellung, sondern innerhalb des kompletten Prozess als einzige Kontaktstelle gegenüber dem Dienstleistungserbringer auftreten.

### III. Gestaltung von Informationsportalen

#### 1. Vollständige und verständliche Informationen bereitstellen

- Primäres Ziel eines Webportals sollte es sein, dem Dienstleistungserbringer alle gewünschten und benötigten Informationen anzubieten. Untersuchungen des Hasso-Plattner-Instituts haben gezeigt, dass Dienstleistungserbringer, die sich bereits im Vorfeld der Antragsstellung beraten ließen, deutlich weniger Probleme bei dem Ausfüllen von Antragsformularen hatten. An dieser Stelle könnten die Webportale einen wichtigen Beitrag leisten, indem kompetente Beratungshilfen auf den Webseiten angeboten werden. Neben Checklisten, die alle benötigten Antragsunterlagen auflisten, sollten die Anträge selbst als elektronische Dokumente online zur Verfügung stehen. Um Medienbrüche zu vermeiden, sollte der Wunsch der elektronischen Antragsabwicklung klar kommuniziert werden.

#### 2. Auf nutzerfreundliche Gestaltung und Bedienung achten

- Das Portal sollte eine klare Navigationsstruktur aufweisen und den Nutzer in wenigen Schritten zur gesuchten Information führen. D.h. es ist im besonderen Maße auf eine nutzerfreundliche Gestaltung und Bedienung (Usability) der Webseiten zu achten. Bezüglich der Gestaltung und Navigation sollten Mindestvorgaben gemacht werden, die zu berücksichtigen sind, um für ein möglichst einheitliches „Look & Feel“ bei den Nutzern zu sorgen. Falls Technologien wie z.B. Javascript zum Einsatz kommen, um die Bedienbarkeit komfortabler zu gestalten, muss darauf geachtet werden, dass die Seiten trotzdem die Anforderung der Barrierefreiheit erfüllen.

#### 3. Antragsabwicklung mit elektronischen Formularen und Diensten optimieren

- Um die Interoperabilität beim Austausch von Antragsdaten zu gewährleisten bzw. einfacher zu gestalten, wäre eine Standardisierung von Formularen wünschenswert. Durch eine einheitliche Benennung von Formularfeldern und strukturierte Speicherung, könnten Inhalte leicht von IT-Systemen weiterverarbeitet und importiert werden. Zur Datenrepräsentation der Daten bietet sich XML an.
- Untersuchungen hinsichtlich der Antragsstellung haben ergeben, dass häufig Probleme bei dem Ausfüllen von Formularen auftreten, weil die Formulare nicht ausreichend verständlich formuliert sind bzw. keine ergänzenden Hilfestellungen bei der Bearbeitung bieten. Es sollte daher über eine grundlegende Überarbeitung der Formulare nachgedacht werden.

- Als Alternative zu Formularen, die zum Download angeboten werden, kann auch ein Formularserver genutzt werden, der das Ausfüllen von Formularen direkt innerhalb des Portals ermöglicht. Vorteile bei dieser Variante sind, dass die Formulare auf jeden Fall elektronisch übermittelt und zudem auch sofort in strukturierter Form speicherbar sind. Eine dialoggesteuerte Formularerstellung könnte den Antragsprozess weiter unterstützen und optimieren. Durch geschickte Dialogführung werden nicht benötigte Felder im Antragsprozess ausgeblendet, wodurch bereits potentielle Bearbeitungsfehler auf Seiten des Antragsstellers ausgeschlossen werden können.

#### **4. Stufenweise Migration zu einem föderierten Informationsmanagement**

- In Kapitel D. wird die stufenweise Einführung eines föderativen Informationsmanagements vorgeschlagen, das zum Ziel eine effiziente Erstellung des Informationsangebots innerhalb der Portale hat. Bestimmte allgemeine Inhalte werden als EA-Modul gekapselt und können auf einfache Weise in die Portale der zuständigen Stellen integriert werden. Die zuständigen Stellen müssen somit nicht selbst diese allgemeinen Informationen erstellen und pflegen, da die Inhalte zentral vom Einheitlichen Ansprechpartner erstellt bzw. bereitgestellt werden. Desweiteren wird durch diesen Ansatz eine einheitliche Struktur und Darstellung innerhalb der unterschiedlichen Portale gewahrt. Das EA-Modul nimmt nur einen Teil des jeweiligen Portals ein, so dass die zuständigen Stellen weiterhin ihre eigenen Inhalte pflegen können. Bei der Realisierung des EA-Moduls muss darauf geachtet werden, dass die Daten in einem Format übertragen werden, das von den unterschiedlichen Content Management Systemen (CMS) der zuständigen Stellen unterstützt wird. Ggf. müssen verschiedene Formate bereitgestellt bzw. Schnittstellen implementiert werden, um einen Import in das jeweilige CMS der zuständigen Stellen zu ermöglichen.
- Neben dem Content Sharing mittels des EA-Moduls, könnte jedes Portal auf einfache Weise Funktionalitäten für die Wiederverwendung von Informationen bereitstellen. Nachrichten und Beiträge, die z.B. als RSS- oder ATOM-Feed veröffentlicht werden, bieten dem Dienstleistungserbringer, aber auch den zuständigen Stellen oder dem Einheitlichen Ansprechpartner die Möglichkeit, automatisiert in regelmäßigen zeitlichen Abständen die aktuellsten Nachrichten zu erhalten. Darüber hinaus besteht die Option, Beiträge, die in einem solchen XML-Format veröffentlicht werden und ggf. von unterschiedlichen Webportalen stammen, komfortabel und automatisiert innerhalb einer Webseite zu aggregieren.
- Die Realisierung eines zentralen Zuständigkeitsfinders könnte durch Aggregation der einzelnen regionalen Zuständigkeitsfinder vollzogen werden. Von Vorteil wäre bei dieser Variante, dass Zuständigkeiten dezentral gepflegt werden und somit auch an zentraler Stelle immer aktuell zur Verfügung stehen. Damit eine Integration der regionalen Zuständigkeitsinformationen an zentraler Stelle möglich ist, sollten diese in einem definierten Format vorgehalten werden.
- Da sich für kleinere Kommunen der Betrieb eines eigenen Webportals aus wirtschaftlichen Gründen ggf. nicht sinnvoll gestaltet, könnte ein integrierter Webaufritt innerhalb eines anderen Portals (z.B. eine Hierarchiestufe höher) stattfinden. Es sollte generell geprüft werden, ob eine bestehende Infrastruktur von mehreren Einrichtungen gemeinsam genutzt werden kann. Über einen Zugang zum Content Management könnten die beteiligten Organisationen ihre jeweiligen Seiten im Portal pflegen. Neben Effizienzvorteilen, würde eine solche Lösung durch Bündelung gleichartiger Organisationen die Übersichtlichkeit erhöhen und einen einheitlichen Auftritt gewährleisten.

#### **5. Zentrales SOA Informationsportal für die öffentliche Verwaltung aufbauen**

- Um über Entwicklungen der öffentlichen Verwaltungen auf dem Gebiet der service-orientierten Architekturen zu informieren, sollte die Einrichtung eines zentralen Webportals auf Bundes- oder Länderebene in Erwägung gezogen werden. Das Portal könnte in erster Linie als Plattform zum Austausch von Projekterfahrungen und zur Koordination von gemeinsamen SOA Aktivitäten eingesetzt werden. Veröffentlichte Ergebnisse und Erfahrungen könnten beispielsweise helfen, Mehrfachentwicklungen zu vermeiden und Hinweise hinsichtlich Problemlösungen zu bieten. Das Portal soll-

te weiterhin als Kollaborationsplattform konzipiert sein, so dass prinzipiell jede Person aus der öffentlichen Verwaltung seine Ideen und Erfahrungen aktiv einbringen kann. Aus technischer Sicht bieten sich für diesen Zweck, die typischen Web 2.0 Technologien wie Wikis oder Blogs an. Im Laufe der Zeit könnte das Portal zu einer SOA Wissensbasis reifen, die Synergien bei der Entwicklung von Lösungen in der öffentlichen Verwaltung schafft.

#### **6. Einsatz von aktuellen Portaltechnologien prüfen**

- Bei dem Neuaufbau eines Portals sollte der Einsatz von dedizierten Portalservern in Erwägung gezogen werden. Sie bieten bereits nützliche Features wie z.B. eine Nutzer- und Rechteverwaltung, Content Management, etc.

### **IV. Speicherung von Daten**

#### **1. Konsistenz von Daten sichern**

- Im Hinblick auf eine service-orientierte Architektur mit verteilten Systemen und Diensten, ist eine der größten Herausforderungen die Konsistenz von Daten zu gewährleisten. Es sollte überprüft werden, welche Informationen innerhalb der Geschäftsprozesse von mehreren Organisationen benötigt werden und daher zentral gespeichert werden sollten. Die Nutzung gemeinsamer Informationssysteme und –dienste schafft Synergieeffekte und verhindert Inkonsistenzen aufgrund verteilter Datenbestände.
- Zur effizienten (automatisierten) Weiterverarbeitung von Daten, sollten diese möglichst strukturiert abgespeichert werden. Es ist dabei sicherzustellen, dass über eine Schnittstelle komfortabel auf die Daten zugegriffen werden kann und ein Export in ein Standardformat möglich ist.
- Unter der Annahme, dass der Einheitliche Ansprechpartner sich zunächst hauptsächlich auf die Weiterleitung der Antragsinformationen und –dokumente an die zuständigen Stellen sowie allgemeine Antragsberatung beschränkt, müssten lediglich Grundinformationen zu dem Verwaltungsprozess in einem Vorgangsbearbeitungssystem/ CRM-System gespeichert werden. Antragsunterlagen, die von dem Dienstleistungserbringer übermittelt wurden, sind zumindest kurzfristig in einem Dokumentenmanagementsystem zu speichern. Durch das mehrfache Weiterleiten von Daten entstehen bei den beteiligten Organisationen jeweils Kopien, was letztlich zu Konsistenzproblemen führen kann. Eine zentrale Speicherung der Unterlagen würde dieses Problem vermeiden und zudem den Kommunikations- und Verwaltungsaufwand minimieren. Allerdings sind bei einer zentralen Datenspeicherung umfangreiche Zugriffsberechtigungen zu verwalten, um den Anforderungen an die Datensicherheit und den Datenschutz gerecht zu werden.

#### **2. Verwaltungsvorgänge ausreichend dokumentieren und Daten archivieren**

- Bei der Speicherung von Daten müssen gesetzliche Richtlinien beachtet werden. Der zu betreibende Aufwand hinsichtlich Aktenpflicht, Vorhaltepflcht und Schutz von elektronischen Daten hängt dabei auch stark von der Aufgabenerfüllung der einzelnen Organisationen ab. Besitzt der Einheitliche Ansprechpartner bspw. lediglich die Aufgabe, Anträge und Dokumente an die zuständigen Stellen weiterzuleiten, muss dieser nur wenige Daten speichern, dokumentieren und vorhalten. Ist der EA jedoch mit weitreichenden Kompetenzen ausgestattet, sind die Anforderungen deutlich höher, da prinzipiell jede Aktivität innerhalb des Verwaltungsvorgangs dokumentiert werden muss. Vor diesem Hintergrund ist für jede Organisation in Abhängigkeit ihrer Aufgabenerfüllung zu klären, welche individuellen rechtlichen Anforderungen bestehen.

#### **3. Verwaltung von Identitäten und Zugriffsrechten effizient gestalten**

- Zum sicheren Zugriff auf bestimmte Daten und IT-Systeme werden bereits Identitäts- und Zugriffsverwaltungen innerhalb der Organisationen eingesetzt. Bei Öffnung der Systeme für andere Organisationen, müssen zusätzliche Identitäten und Zugriffsregelungen verwaltet werden, was bei vielen Kommunikationsbeziehungen sehr komplex werden kann. Verfolgt man konsequent das Ziel einer

Service-orientierten Architektur, sollte ein föderiertes Identity- und Access-Management zum Einsatz kommen. Über die Definition von Vertrauensbeziehungen können Identitäten organisationsübergreifend genutzt werden, so dass eine zusätzliche Speicherung von externen Identitäten bei den Organisationen entfällt. An dieser Stelle wird deshalb auf das SAFE Projekt (vgl. E.III.4.) verwiesen, das sich mit der Konzeption und Umsetzung eines föderierten Identity Managements befasst.

## V. Prozessmanagement

### 1. Geschäftsprozesse modellieren und beschreiben

- Zunächst ist es wichtig, dass die Prozesse klar identifiziert und dokumentiert sind. Zu diesem Zweck bietet sich an, verfügbare Modellierungstools einzusetzen mit denen die Prozesse dargestellt werden können. Bei der Modellierung sollte eine Notation verwendet werden, die leicht verständlich ist, aber dennoch die Möglichkeit der Darstellung wichtiger Prozessdetails beinhaltet. In diesem Zusammenhang wird empfohlen, eine Notation zur Prozessbeschreibung zu wählen, die eine Transformation der Prozesse in eine maschinenlesbare Ausführungssprache erlaubt. Auf diese Weise können später Prozesse regelbasiert von einer Prozessmanagement Software automatisiert ausgeführt werden. Als Notation zur Modellierung von Prozessen könnte z.B. BPMN<sup>143</sup> (Business Process Modeling Notation) verwendet werden und als Ausführungssprache BPEL (Business Process Execution Language).
- Die Umsetzung einer Service-orientierten Architektur geht auch mit dem Ziel einher, zukünftig automatisiert Verwaltungsprozesse zu steuern und somit die Verfahren bei der Antragsabwicklung effizienter zu gestalten. Bevor mit der Umsetzung eines Prozessmanagements begonnen werden kann, muss als Grundvoraussetzung die Interoperabilität von Diensten gewährleistet sein. Es muss klar ersichtlich sein, welche Dienste welche Aufgaben erfüllen und wie diese aufgerufen werden können. Zu diesem Zweck sind die Dienste in einem standardisierten Format zu beschreiben (WSDL).

### 2. Frühzeitige Umsetzung einfacher Workflows

- Das Ziel, automatisiert ganze Geschäftsprozesse zu steuern, ist erst nach der Implementation aller notwendigen Dienste und somit langfristig (in Stufe 2) erreichbar. Dennoch könnten bereits frühzeitig bestimmte Abläufe über einfache Workflows abgewickelt werden. Das Fallmanagement des Einheitlichen Ansprechpartners sollte schon zu Beginn zumindest über eine (teil-)automatisierte Funktion verfügen, die komfortabel die relevanten Auftragsunterlagen an die zuständigen Stellen weiterleitet sowie alle Aktionen und Statusinformationen im Verwaltungsprozess protokolliert.

### 3. Möglichkeiten zur Orchestrierung von Diensten prüfen

- In Abhängigkeit der eingesetzten Systeme und geplanten Dienste, sollte über die Verwendung eines Enterprise Service Bus (ESB) innerhalb der Organisation nachgedacht werden. Ein ESB beschreibt eine Kommunikationsinfrastruktur, die hauptsächlich für den Austausch von Daten zwischen Webservices und IT-Systemen verantwortlich ist. Existierende Systeme können mittels Adapter an den ESB angebunden werden. In der Regel bieten heutige ESB Orchestrierungsfunktionen, so dass Prozesse als Folge von Service-Aufrufen automatisiert durchgeführt werden können. Ob und zu welchem Zeitpunkt der Einsatz eines Enterprise Service Bus sinnvoll ist, ist individuell für die jeweilige Organisation zu überprüfen.

<sup>143</sup>Die vom Forschungsvorhaben der Humboldt Universität verwendete Modellierung als ePK mit dem Tool „ARIS“ unterstützt die Prozessdarstellung gemäß der BPMN-Notation

## VI. Nutzung von externen Diensten

### 1. Nutzung über standardisierte Schnittstellen

- Um die Kommunikation und damit die Interoperabilität mit externen, organisationsübergreifenden Diensten zu gewährleisten, müssen Standards hinsichtlich der Kommunikation, Sicherheit und Datenformate eingehalten werden. Damit die externen Dienste aufgerufen werden können, müssen diese in einem standardisierten Format beschrieben werden. Bei Webservices findet eine Beschreibung der Dienste in WSDL (Web Services Description Language) statt. Die Beschreibung der Dienste muss dem potentiellen Dienstekonsumenten bereitgestellt werden, z.B. über ein Dienstverzeichnis.

### 2. Gemeinsame Nutzung von Diensten

- Bei dem SOA Design sind u. a. Prozessfunktionalitäten zu identifizieren, die aufgrund ihres hohen Wiederverwendbarkeitsgrads durch einen Dienst realisiert werden sollten. Diese sogenannten „shared services“ könnten dann gemeinsam von anderen Diensten bzw. Organisationen genutzt werden. D.h. es sollte jeweils geprüft werden, inwieweit bereits bestimmte Dienste von anderen Organisationen bereitgestellt werden, um Mehrfachentwicklungen zu vermeiden und Synergieeffekte zu nutzen. Desweiteren sollte erörtert werden, inwieweit eine Nutzung von bestehenden Diensten von externen, ggf. kommerziellen Dienstleistungserbringer aus wirtschaftlichen Gesichtspunkten sinnvoll ist. Ein bundes- bzw. landesweites Dienstverzeichnis bzw. Informationsportal ist zu empfehlen, um den Organisationen eine Übersicht über die verfügbaren Dienste zu ermöglichen (s. Handlungsempfehlung „Informationsportal“).
- Ein elektronischer Bezahlendienst (e-Payment) ist beispielsweise ein idealer Kandidat für einen wiederverwendbaren Dienst, da zukünftig eine Online-Bezahlung der Verwaltungsgebühren unterstützt werden soll und diese Funktionalität häufig innerhalb der Verwaltungsprozesse benötigt wird. Nach Möglichkeit sollte der e-Payment Dienst mit den Haushaltssystemen der Organisationen koppelbar sein, so dass eine effiziente Abwicklung des Bezahlvorgangs stattfindet.

## G. Weiteres Vorgehen

### I. Fortführung des Vorhabens

Der Projektbericht des Deutschland-Online Vorhaben Dienstleistungsrichtlinie enthält eine Reihe von länderübergreifend gültigen Handlungsempfehlungen und Vorschlägen. Die Federführer schlagen vor diesem Hintergrund für das weitere Vorgehen folgendes vor:

1. Das Deutschland-Online Projekt Dienstleistungsrichtlinie begleitet bis Ende 2009 als prioritäres Vorhaben die weitere IT-Umsetzung der Richtlinie durch die Länder.
2. Das Projekt wird die in den Umsetzungsprojekten einzelner Länder gewonnenen Erkenntnisse allen Ländern, Kommunen und Kammern und dem Bund in geeigneter Weise zur Verfügung stellen und den fachlichen Austausch unterstützen.
3. Es wird vorgeschlagen, geeignete Teilprojekte unter Federführung und Beteiligung weiterer Länder (länderoffene Gruppen) zu bilden. Als Teilprojekte kommen beispielsweise in Betracht:
  - Planung und Umsetzung eines „Föderativen Informationsmanagements“
  - Interoperabilität/Standardisierung
  - Recht, Organisation und Prozesse

### II. Vorlage an die Regierungschefs von Bund und Ländern

Die Federführer schlagen vor, den Projektbericht den Regierungschefs von Bund und Ländern für die Sitzung am 18.12.2008 mit folgendem Beschlussvorschlag vorzulegen:

*Die Bundeskanzlerin und die Regierungschefs der Länder nehmen den Bericht des Projektes „Nationale IT-Umsetzung der EG-Dienstleistungsrichtlinie“ zur Kenntnis und empfehlen, die Ergebnisse des Projekts bei der weiteren Umsetzung in den Ländern zu berücksichtigen. Die weitere Begleitung der IT-Umsetzung der Richtlinie bis Ende 2009 durch das Projekt wird befürwortet.*