D. Elektronische Verfahren und Datenschutz im IT-Bereich

1 Beschreibung der technischen Komponenten

1.1 Dienstleisterportal

Das Dienstleisterportal gliedert sich in wenige Hauptbereiche, die zielgruppengerecht positioniert wurden:

1.1.1 Anwendungsbereich

Der Anwendungsbereich besteht aus den Zugängen zur:

- Suche nach Einheitlichen Ansprechpartnern
- Suche nach Verwaltungsdienstleistungen
- Start Antragsverwaltung
- Start Antragsassistent

1.1.1.1 Modul Antragsassistent

Der Antragsassistent gliedert sich in Hauptfragestellungen zu:

- Persönlichen Angaben
- Angaben zu Gesellschafts- und Betriebsformen
- Angaben zu Betriebsstätten und Personal
- Abschluss

1.1.1.2 Modul Antragsverwaltung

Die Vorhabenverwaltung enthält folgende Bereiche:

- Registrierung (Abfrage persönlicher Daten)
- Vorhabenanlage und –ablage, Versand, Formularbearbeitung, Formularsuche, Anlagen hinzufügen, Bescheideingang
- Einladungsfunktion für den Zugriff weiterer Nutzer aus Zuständigen Stellen oder einheitliche Ansprechpartner auf die Einzelvorhaben
- Hilfe

1.1.2 Informationsbereich

Der Informationsbereich bildet den Rahmen. Er enthält:

- Nutzungs- und Datenschutzhinweise
- Impressum
- FAQ
- Tour durch das Portal (Video),
- weiterführende Links

1.2 Elektronisches Gerichts- und Verwaltungspostfach

Die Komponente elektronisches Gerichts- und Verwaltungspostfach (EGVP) besteht aus mehreren Infrastruktureinheiten:

1. Intermediär
2. Verzeichnisdienst
3. Backend

4. EGVP-Clients

Der Nachrichtenverkehr muss aus Gründen der IT-Sicherheit und der Rechtssicherheit über EGVP betrieben werden. Hierzu steht als zentraler Dienst im LSKN der Intermediär zur Verfügung. Er bildet die Vermittlungseinheit und stellt die EGVP- Postfächer bereit. Der Dienst ist an einen Verzeichnisdienst angeschlossen, der die Empfangsadressen sämtlicher an EGVP angeschlossenen Behörden enthält.

Jede eingehende und ausgehende Nachricht wird mit einem rechtssicheren Zeitstempel versehen.

Die EGVP-Clients und entsprechenden Backends werden jeweils in den Behörden, z.B. Kommune, betrieben. Über die Clients erfolgt der Zugriff auf die Inhalte der Postfächer.

Sämtlicher Datentransfer wird über ein Sicherheitsprotokoll namens OSCI vermittelt. Der OSCI-Nachrichtenverkehr ist verschlüsselt. Ein Datenzugriff durch Unbefugt kann somit erschwert werden.

Um die Software "Elektronisches Gerichts- und Verwaltungspostfach" korrekt ausführen und für qualifizierte elektronische Signaturen nutzen zu können, wird benötigt:

- Personalcomputer
    - mit Betriebssystem (Microsoft Windows: 2000, XP, Vista; Linux: RedHat 9.0, SuSE 10.x)
    - ein installierter Browser
    - ein Internetanschluss

für die Anwendung "Elektronisches Gerichts- und Verwaltungspostfach" selbst

- das Java™ Runtime Environment (beinhaltet Java™ Web Start)

für die qualifizierte elektronische Signatur

- eine Signaturkarte und ein Kartenlesegerät

Die Software "Elektronisches Gerichts- und Verwaltungspostfach" kann lizenzkostenfrei über das Internet bezogen werden.[1]

Im Rahmen der Umsetzung der EU-DLR wurden die zuständigen Stellen mit EGVP ausgestattet.

1.2.1 Strukturen der EGVP

Es gibt grundsätzlich drei Arten von EGV-Postfächern:

- die Backends,
- die Slaves und
- die Clients.

Alle Backends sind im öffentlichen EGVP-Adressbuch für jeden EGVP-Nutzer sichtbar. Umgekehrt kann ein Backend alle EGVP-Nutzer sehen. Die Slaves sind so genannte Unterpostfächer, die im Rahmen der EU-DLR derzeit nicht im Einsatz sind. Die EGVP-Clients sind für jeden frei zugänglich und stehen zum kostenlosten Download zur Verfügung. Mit einem

[1] http://www.egvp.de

EGVP-Client können alle Backends im Adressbuch erreicht werden, eine Kommunikation der Clients untereinander ist nicht möglich.

Für die Umsetzung der EU-DLR steht jedem Einheitlichen Ansprechpartner sowie jeder zuständigen Behörde ein EGVP-Backend zur Verfügung. Darüber hinaus ist das EGVP in das Dienstleisterportal integriert. Das hat den Vorteil, dass Antragsteller, die ein Verfahren elektronisch abwickeln wollen keinen Client auf ihrem PC installieren müssen. Der Versand der Anträge kann von einem registrierten User direkt aus dem Dienstleisterportal sicher und rechtsverbindlich erfolgen.

1.2.3 Schematische Darstellung (Schaubild)

Nachfolgend wird schematisch der Aufbau einer EGVP-Nachricht dargestellt, die aus dem Dienstleisterportal erzeugt wird:[2]

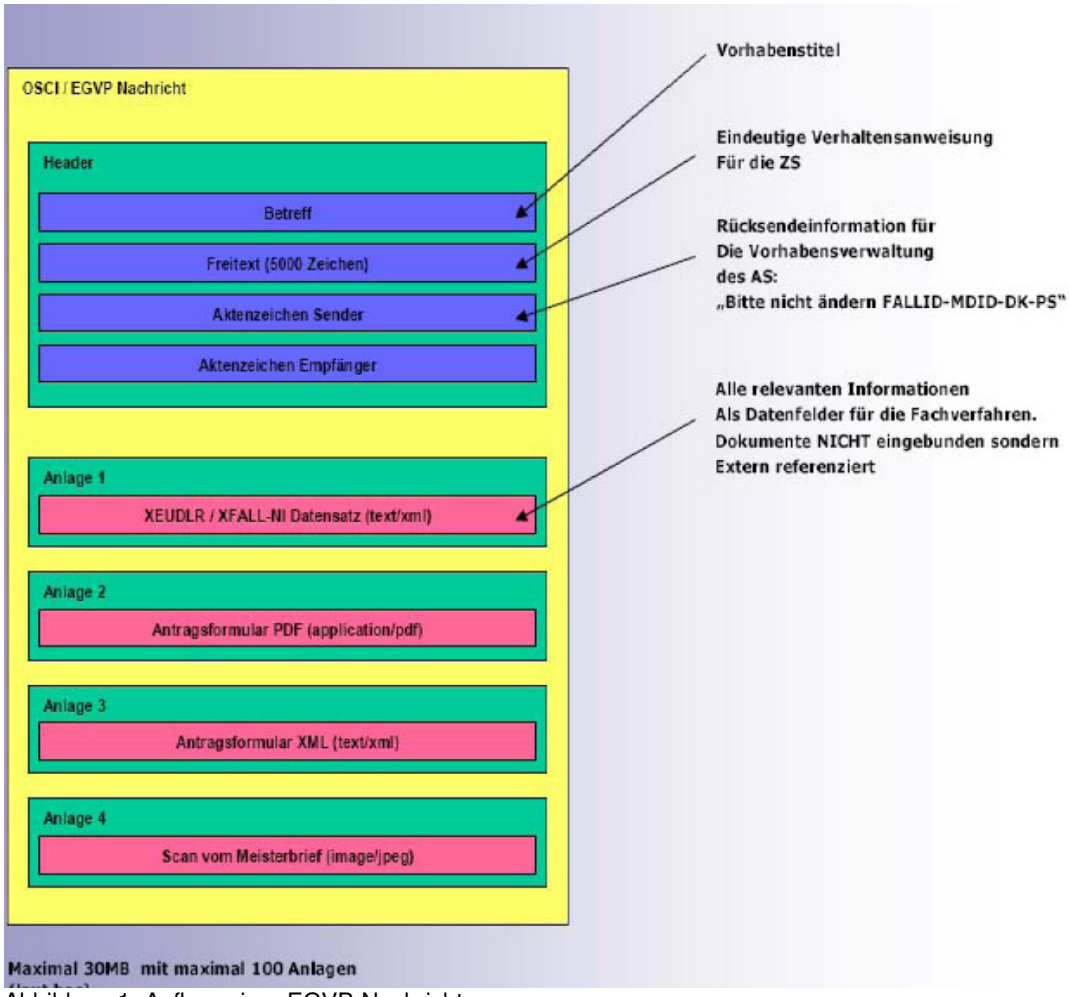

Abbildung 1: Aufbau einer EGVP-Nachricht

[2] Quelle: EA Landkreis Osnabrück, 23.04.2010

2. Elektronische Signaturen[3]

2.1 Verwendung der Signatur

Durch die Unterschriftenfunktion von Signaturkarten werden handschriftliche Unterschriften durch elektronische ersetzt, die in gleicher Weise rechtsverbindlich sind. Damit kann ein elektronisches Dokument, z. B. PDF, signiert werden und die Identität der Person, die das Dokument versandt hat, einwandfrei nachgewiesen werden.

Elektronische Dokumente mit Urkundencharakter, wie ein Bescheid, sollten grundsätzlich von der ausstellenden Behörde mit einer qualifizierten elektronischen Signatur versehen werden.

Des Weiteren können auch generell Meldungen über das elektronische Verwaltungs- und Gerichtsportfach signiert werden, dadurch sind diese Benachrichtigungen inklusive des enthaltenen Bescheids vor Gericht beweisfähig.

Dienstleistungserbringer können über die Signierfunktion der Antragsverwaltung unter Einsatz einer eigenen Signaturkarte deutscher Zertifizierungsdienste/Trustcenter elektronische Antragsformulare rechtsverbindlich signieren.

Nicht jedes Formular muss signiert werden. Die Signaturaufforderung wird vom Formularserver zu den betreffenden Formularen hinterlegt.

Signaturkarten erhält man über Zertifizierungsdiensteanbieter (Signaturkartenanbieter/Trustcenter).

Die Ausstellung einer Signaturkarte und das Vorhalten des ausgestellten Zertifikats durch den Zertifizierungsdiensteanbieter ist eine kostenpflichtige Dienstleistung. Ein Liste der Trustcenter und der Produkte, bei denen die Erfüllung der Anforderungen aus § 17 SiG und § 15, Anlage 1 SigV formal bestätigt ist, wird im Internetauftritt der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen bereitgestellt.[4]

Neben der Signaturkarte wird ein Kartenlesegerät benötigt. Das Kartenlesegerät liest im Signaturvorgang das Zertifikat der Signaturkarte aus. Über die Eingabe einer PIN wird der Signiervorgang abgeschlossen.

2.2 Rechtliche Vorgaben

Bezüglich Signatur wird die Behörde mit einer qualifizierten Signatur gemäß SigG zeichnen. Das Zertifikat muss über das jeweilige Trustcenter eindeutig zu identifizieren sein.

Rechtsbehelfe werden in der jeweiligen Information zum Verwaltungsverfahren benannt. Die Vorgaben zur Verwendung der Signatur ergeben sich aus § 3 a Abs. 2 VwVfG i. V. m. SigG und SigV. Im Übrigen gelten die Vorschriften des VwVfG und VwGO.

2.3 Technische Aspekte[5]

Zu unterscheiden sind rechtssicherer Kommunikationstransfer und rechtssichere elektronische Unterschrift (Signatur). Die EU-DLR Umsetzung in Niedersachsen bietet beides.

---

[3] Quelle: MI, CIO, 15.10.2010
[4] http://www.bundesnetzagentur.de
[5] Quelle: MI, CIO, 07.03.2011

Die Kommunikation, d. h. der Versand der Daten (elt. Formulare inkl. Anlagen, Bescheide), erfolgt über die elektronischen Gerichts- und Verwaltungspostfächer EGVP. Dieser Versand verschlüsselt die Daten und überträgt sich über das OSCI-Protokoll. Somit ist gewährleistet, dass kein unbefugter Datenabruf während des Datentransfers über das Internet erfolgen kann. Zudem werden die OSCI-Nachrichten mit einem Zeitstempel versehen, dieser ist einem Postausgangs- und Eingangsstempel gleichzusetzen. Das Webfrontend Antragsverwaltung im Dienstleisterportal ist nichts anderes als ein elektronisches Verwaltungs- und Gerichtspostfach. Unternehmen und Bürger müssen sich jedoch nicht mit der Installation und Bedienung der EGVP-Clientsoftware beschäftigen. Zuständige Stellen sind ebenfalls mit EGVP ausgestattet. Der elektronische Verkehr zwischen Dienstleisterportal/Antragsverwaltung und Formularserver sowie zuständigen Stellen erfolgt auf einer "Ende zu Ende Verschlüsselung", ein böswilliges Abändern oder Auslesen der Daten ist nicht möglich.

Falls Dienstleistungserbringer, die Bescheide in ihr persönliches Emailpostfach zugestellt bekommen, werden diese Bescheide in PDF-Format und dieses mit Passwortschutz versehen verschlüsselt zugestellt. Das Passwort muss ein Dienstleistungserbringer bei der Registrierung im Portal festlegen. Es wird verschüsselt im Identitymanagemenet bereitgehalten. Ein Auslesen der Daten ist auch bei der PDF nicht ohne weiteres möglich.

Die Signatur kommt dann ggf. zum Einsatz, wenn ein Antrag qualifiziert signiert werden muss. Dabei ist die elektronische Signatur der Unterschrift gleichgesetzt. Der Formularserver Niedersachsen bietet diese Signaturmöglichkeit an. Allerdings haben nur wenige Unternehmen und Bürger die persönliche Signaturmöglichkeit via eigener Signaturcard. Noch fataler ist die Lage im europäischen Kontext. Man konnte sich bislang noch auf keine europaweit gültige Signatur resp. Zertifikate und Prüfung derselben einigen. Durch eine dem EGVP hinterlegten Zertifikatbibliothek wäre es möglich, durchaus einige Signaturen anderer Länder abzuprüfen. Bisher kam es jedoch noch nicht zu einem entsprechenden Einsatz.

Als Ersatz kann zum Vorhaben ein Mantelbogen ausgedruckt, unterschrieben und im Nachgang mit Unterschrift versehen den Behörden postalisch übermittelt werden. Die Anträge können trotzdem elektronisch gestellt werden.

3 Fachverfahren für EA

3.1 EA-Fachverfahren

Das EA-Fachverfahren unterstützt die EA bei der Abwicklung der Fälle im Rahmen der EU-DLR. Es ist ein Fallmanagementsystem, über welches die einzelnen Vorhaben verwaltet werden.

3.2 Anbieter/Produkte

In Niedersachsen finden sich verschiedene Anbieter von EA-Fachverfahren wieder. Die am weitesten verbreiteten Verfahren werden von der Fabasoft Software GmbH (Fabasoft) und von der OPTIMAL SYSTEMS Vertriebsgesellschaft mbH Hannover (OPTIMAL SYSTEMS) angeboten.

3.2.1 Fabasoft[6]

Das Land bietet über den Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) die Nutzung eines EA-Fachverfahrens auf Basis von Fabasoft an.

Das EA-Fachverfahren liest die für den EA eingehenden EGVP-Nachrichten ein. Dabei werden Informationen zu dem Vorhaben, den Leistungen, dem Dienstleister sowie der zuständigen Stellen übergeben, welche in die Metadaten des EA-Fachverfahrens übernommen werden. Über das Fachverfahren lassen sich Nachrichten an die EGVP-Postfächer der zuständigen Stellen weiterleiten und Antworten an den Dienstleister verschicken.

3.2.2 OPTIMAL SYSTEMS[7]

Die Firma OPTIMAL SYSTEMS (OS) hat mit ihrem OS|EA-Fachverfahren ein speziell auf die EU-Dienstleistungsrichtlinie abgestimmtes Fallmanagementsystem entwickelt. In dem Verfahren können Kundendaten gepflegt, Vorhaben verwaltet und abgewickelt werden. Durch die Kommunikation zum EGVP und zum Bürger- und Unternehmensservice ist geplant, Daten auch direkt in das Programm einzulesen und auch wieder auszulesen. Das Fachverfahren archiviert die Akten in dem dazugehörigen digitalen Archiv.

3.3 Schnittstellen des Fachverfahrens zum Portal und zu den ZB

Das Dienstleisterportal nutzt als Kommunikationsmedium das EGVP (s. Kapitel 4.2 Elektronisches Gerichts- und Verwaltungspostfach (EGVP)). Ziel bei der elektronischen Verfahrensabwicklung ist es, dass Daten nicht mehrfach manuell in ein System eingegeben werden müssen, sondern nach der einmaligen Eingabe weiterverarbeitet werden können. Eingehende Nachrichten müssen beim Einheitlichen Ansprechpartner in das EA-Fachverfahren gelangen. Ebenso müssen diese Informationen an die zuständigen Behörden weitergebeben und das Ergebnis wieder angenommen werden und anschließend zurück in das Dienstleisterportal gelangen. Das EA-Fachverfahren ist dabei die Drehscheibe für die Informationen. Das OS | EA-Fachverfahren nutzt derzeit einen EGVP-Dunkel-Client um die Daten aus dem EGVP in das Fachverfahren zu bringen. Zukünftig soll zusätzlich ein automatisiertes Auslesen der xml-Datei, die als Anhang an der EGVP-Nachricht aus dem Dienstleisterportal hängt, möglich sein.

Um die ZB zu erreichen, wird aus dem EA-Fachverfahren das EGVP des Empfängers angesteuert. Als Ausbaustufe wird über eine Nutzung der unkomplizierten De-Mail nachgedacht, sobald diese Kommunikationsform freigegeben ist.

---

[6] Quelle: MI, CIO, 31.03.2011

[7] Quelle: EA Landkreis Osnabrück, 23.04.2010

Unabhängig von der Art des Datenaustausches und der Kommunikation zwischen den Beteiligten ist im EA-Fachverfahren ein Abgleich zu den Daten aus dem Bürger- und Unternehmensservice bzw. aus dem Portal äußerst wichtig. Es müssen regelmäßig die zur Verfügung stehenden Verfahren und Kontaktdaten über eine Schnittstelle abgeglichen werden können.

4 Datenschutz

Im Rahmen der Umsetzung der IT-Infrastruktur wurden die Vorgaben des Datenschutzes beachtet.

Verwendete Komponenten:

4.1 Dienstleisterportal allgemein

Bei dem Dienstleisterportal handelt es sich um einen Telemediendienst im Sinne des Telemediengesetzes (TMG), in dessen Rahmen personenbezogene Daten erhoben, verarbeitet und gespeichert werden. Die Nutzung der personenbezogenen Daten erfolgt allein zum Zwecke der Durchführung der Aufgaben der einheitlichen Stellen gemäß §§ 71a – 71e Verwaltungsverfahrensgesetz (VwVfG). Neben dem Vor- und Nachnamen inkl. des Geburtsnamen, dem Geschlecht, dem Geburtsdatum, dem Familienstand, der Staatsangehörigkeit, der Adresse und der E-Mail-Adresse werden auch die für die Durchführung der jeweils angeforderten Verwaltungsleistung für die Dauer des Verwaltungsverfahrens gespeichert.

Das Portal ist insgesamt als Teledienst einzuordnen, der den Regelungen des Telemediengesetzes (TMG) unterliegt. Eine gemäß § 13 Absatz 4 Nr. 3 TMG gegen Kenntnisnahme Dritter geschützte Nutzung des Portals kann durch einen Mausklick auf oben Verschlüsselte Datenübertragung eingeschaltet werden.

Zur Kontaktaufnahme steht ein Kontaktformular zur Verfügung, in das neben der E-Mail-Adresse auch weitere personenbezogene Daten des Absenders in ein Kommentarfeld eingegeben werden können. Die Verarbeitung dieser Daten unterliegt wie folgt gesetzlichen Bestimmungen. Für die eingegebenen Daten gelten die Bestimmungen des niedersächsischen Datenschutzgesetzes. Auch das Kontaktformular ist als Teledienst einzuordnen, der den Regelungen des Telemediengesetzes (TMG) unterliegt. Sofern Angaben im Kommentarfeld eingegeben werden, für die besondere Datenschutzbestimmungen gelten, werden diese beachtet.

Die mit der Verarbeitung von personenbezogenen Daten betrauten Mitarbeiter und Mitarbeiterinnen der kommunalen Behörden und Landesbehörden sind auf das Datengeheimnis verpflichtet.

Für statistische Zwecke und zur Qualitätssicherung werden bei jedem Zugriff auf die Webseiten des Portals folgende Zugriffsdaten anonymisiert protokolliert:

- Datum und Uhrzeit des Zugriffs;
- die gewünschte Zugriffsmethode/Funktion;
- die Eingabewerte des Zugriffs (zum Beispiel die Zieldatei);
- der Name der angeforderten Datei;
- die beim Zugriff verwendete Clientsoftware;
- die Statusmeldung des Web-Servers (zum Beispiel Datei übertragen, Datei nicht gefunden, Kommando nicht ausgeführt).

Die Protokolldaten werden für die Dauer von drei Monaten gespeichert und anschließend gelöscht. Die für den Zugriff verwendete IP-Adresse wird nicht protokolliert.

4.2 Registrierungskomponente

Es werden nur die nötigsten Daten eines Dienstleistungserbringers im System erfasst und vorrätig gehalten. Dienstleistungserbringer haben die Möglichkeit, diese Daten zu ändern oder zu löschen.

4.3 Antragsverwaltung

Dienstleistungserbringer können die Inhalte ändern und löschen. Weitere Personen erhalten nur durch den Dienstleistungserbringer Zugriff auf die Inhalte.

4.4 Antragsassistent

Es werden keine personenbezogenen Daten gespeichert. Die im Rahmen der Metaformularabfrage erhobenen Daten sind flüchtig, d. h. sie werden nur zur Ermittlung der korrekten Leistungen und Formulare herangezogen und dann verworfen.

Schutzstufen
Die Inhalte der Antragsverwaltung und des Registrierungsmoduls unterliegen Schutzstufen.

Registrierung
Adressangaben: Schutzstufe C
Kennung: Schutzstufe D

Antragsverwaltung
Alle Inhalte eines Vorhabens: Schutzstufe D

Begründung für die Einstufungen: Es handelt es sich um personenbezogene Daten, deren Missbrauch den Betroffenen in seiner rechtlichen sowie beruflichen Stellung erheblich beeinträchtigen kann.

Gewährleistung des Schutzes
Um den Schutz der insbesondere personenbezogenen Daten zu gewährleisten, werden alle Mitteilungen und Benachrichtigungen über die Antragsverwaltung nur verschlüsselt über EGVP übertragen.

Die zentralen Systeme befinden sich in einem gesondert geschützten Rechenzentrum. Netzinfrastrukturkomponenten wie Leitungswege, Server und Datenbanken sind gegen Zugriffe von außen abgesichert.

Daten sind vor Manipulationen aus dem Internet durch die Netzkomponente Application Security Gateway geschützt.

Weiterverwendung von Daten
Die Daten aus der Registrierung oder der eigentlichen Antragsstellung, z.B. Daten der Formulareingaben, werden aus der zentralen Infrastruktur heraus momentan keinem weiteren System zur Verfügung gestellt. Aus diesen Gründen unterbleibt z. B. auch ein automatisches Vorbefüllen der Formulare. Technisch wäre es durchaus möglich, einmal eingegebene Daten eines Dienstleistungserbringers auch in weitere Anträge automatisch einzufüllen. Hierfür wird jedoch eine Vorratsdatenhaltung benötigt, die aus Datenschutzgründen abzulehnen ist.

Lediglich fallbezogene Daten werden einmalig als rein beschreibende Daten (Fall-ID, Adressangaben) im XML-Format dem abgesendeten Formular als Metaangaben beigefügt. Hierbei handelt es sich um Daten aus dem Formular und einer Fall-ID (Vorhaben-ID), die den Vorgang zu identifizieren hilft.