Detlef Rätz [et. al.] (Hrsg.): Digitale Transformation:
Methoden, Kompetenzen und Technologien für die Verwaltung
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 137

Implementierungsvarianten elektronischer Signaturen für E-Government-Systeme

Alexander Teich[1], Andreas Hartmann[2], Jürgen Anke und Marcel Rothe[3]

Abstract: Elektronische Signaturen können als Alternative zur eigenhändigen Unterschrift die Effizienz von Vorgängen zwischen Bürgern und Verwaltung verbessern. Für die technische Umsetzung der Unterstützung von elektronischen Signaturen in Internetportalen gibt es verschiedene Varianten. In diesem Beitrag stellen wir diese Varianten vor, vergleichen sie und leiten daraus Handlungsempfehlungen ab, die Verantwortlichen als Entscheidungshilfe dienen können.

Keywords: E-Government, elektronische Signatur, De-Mail

1 Einleitung und Motivation

Durch Teilautomatisierung von Prozessen kann die Abwicklung von Vorgängen verbessert und somit Kosten reduziert werden. Derzeit führen Abläufe in der Verwaltung zum Einreichen von Dokumenten des Kunden zu Medienbrüchen, welche in der Schriftformbedürftigkeit begründet liegen. Damit der Ablauf für die Erstellung bzw. Versendung auf Kundenseite vereinfacht werden kann, gilt es die Schriftform zu ersetzen. Damit Verträge mit den Kunden auch rechtssicher abgewickelt werden können, ist die Umsetzung einer digitalen Signatur erforderlich. Sie kann die Authentizität des Absenders und die Integrität des Inhalts sichern und damit papierbasierten Datenaustausch ersetzen.

Um eine Unterstützung bei Gestaltung von E-Government-Diensten zu geben, haben wir folgende Forschungsfrage untersucht: *Welche Implementierungsvarianten zur Einbindung elektronischer Signaturen in Internetportale gibt es und welche Vor- und Nachteile weisen diese auf?*

Dazu ist dieser Beitrag wie folgt gegliedert: Zunächst erläutern wir verschiedene Varianten der elektronischen Signatur und stellen die rechtlichen Rahmenbedingungen für die Einbindung der elektronischen Signatur vor. Anhand eines Beispiels der Förderfallbearbeitung zeigen wir die Vorteile, die eine Signatureinbindung bringen kann. Anschließend stellen wir Varianten De-Mail, Online-Ausweisfunktion des neuen Personalausweises und sign-me vor und vergleichen diese. Auf dieser Basis leiten wir Handlungsempfeh-

[1] T-Systems Multimedia Solutions GmbH, Riesaer Str. 5, 01129 Dresden, alexander.teich@t-systems.com
[2] Hochschule für Telekommunikation Leipzig, G.-Freytag-Str. 43-45, 04227 Leipzig, {hartmann|anke}@hft-leipzig.de
[3] easy-soft GmbH Dresden, Fetscherstraße 32/34, 01307 Dresden, MRothe@easy-soft.de

lungen für Behörden ab. Der Beitrag schließt mit einer Zusammenfassung und einem Ausblick.

2 Grundlagen

2.1 Elektronische Signaturen

Elektronische Signaturen können in drei Kategorien eingeordnet werden, die technisch unterschiedliche Anforderungen stellen und verschiedene Sicherheitsaspekte erfüllen. Die Daten der **einfachen elektronischen Signatur** werden den zu signierenden Daten beigefügt oder logisch mit ihnen verbunden. Gemäß § 2 SigG [Bu01] dient diese Verknüpfung der Authentifizierung, d.h. dass die Daten werden durch die Signatur als echt bestätigt. So stellt die Angabe des Namens als Absender in einer E-Mail bereits eine einfache elektronische Signatur dar [Ni01]. Die **fortgeschrittene elektronische Signatur** verfolgt darüber hinaus das Ziel, die Integrität der Daten zu gewährleisten. Dazu ist nach §2 SigG u.a. erforderlich, dass die Signatur zum Signaturschlüsselinhaber eindeutig zugeordnet werden kann, nachträgliche Datenänderungen erkennbar sind sowie die Signatur nur durch den Signaturschlüsselinhaber erzeugt werden kann. Die **qualifizierte elektronische Signatur (QES)** muss zum Zeitpunkt der Erstellung auf ein gültiges qualifiziertes Zertifikat basiert sein. Ein **qualifiziertes Zertifikat** ist eine elektronische Bescheinigung, dessen Signaturprüfschlüssel genau einer Person zuordenbar ist und die Identität dieser Person beglaubigt wurde. Das Zertifikat wird gemäß §2 SigG von einem Zertifizierungsdiensteanbieter (ZDA) ausgestellt. Der ZDA hat gemäß § 5 Abs. 1 SigG weiterhin zu gewährleisten, dass die geschaffene Zuordnung für jeden nachprüfbar ist. Zudem muss ein QES mit einer sicheren Signaturerstellungseinheit erzeugt werden (§ 2 SigG). Dies kann eine Signaturkarte in Verbindung mit einer Persönlichen Identifikationsnummer (PIN) oder einem Passwort sein (§ 17 SigG). Damit eine QES akzeptiert wird, müssen alle, die sich auf die Signatur berufen wollen, einem unabhängigen Dritten vertrauen können. Diese Rolle übernehmen ebenfalls ZDA [Gr07].

2.2 Neuer Personalausweis

Den neuen Personalausweis (nPA) gibt es seit dem 1. November 2010. Neben seiner üblichen Ausweisfunktion als akzeptiertes Legitimationspapier wird mit ihm durch seinen integrierten Chip ein digitaler Identitätsnachweis im Internet möglich [Bu16d] [Bu16b]. Der nPA bietet die Online-Ausweisfunktion an und unterstützt die Signaturfunktion.

2.3 Rechtsgrundlagen für den Einsatz elektronischer Signaturen

Die **Schriftform** erfordert, dass die Urkunde oder Erklärung nur mit einer eigenhändigen Namensunterschrift des Erklärenden gültig ist §37 VwVfG [Bu03]. Die **elektronische Form** kann die Schriftform ersetzen, wenn das Dokument in elektronischer Form vorliegt und mit einer QES versehen ist (§3a Abs. 2 VwVfG).

Im Gesetzes zur Förderung der elektronischen Verwaltung werden Bundesbehörden zum 24. März 2016 verpflichtet, einen elektronischen Zugang zur Verwaltung zu errichten (§ 2 EGovG) [Bu13]. Dieser dient der Übermittlung elektronischer Dokumente, die mit einer QES versehen sind (§2 Abs. 1 EGovG). Weiterhin muss die Bundesbehörde einen Zugang zur De-Mail eröffnen, um De-Mails empfangen zu können, sofern sie nicht an das zentrale IT-Verfahren der Bundesverwaltung angeschlossen ist (§2 Abs. 2 EGovG). Zudem wird ermöglicht, eine vorgeschriebene Identifizierung der Person im Verwaltungsverfahren, mit einem elektronischen Identitätsnachweis durchzuführen (§2 Abs. 3 EGovG). Dieser Nachweis wird durch den nPA möglich gemacht.

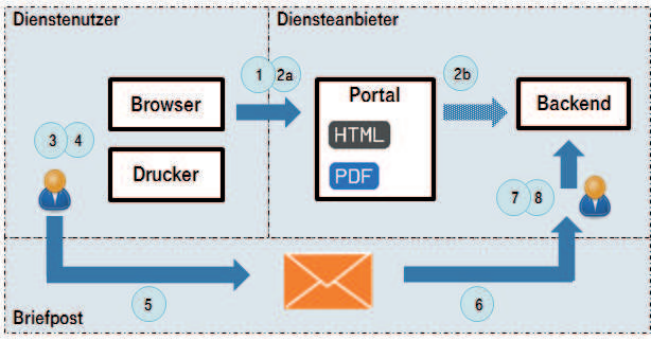

Abb. 1: schematischer Ablauf, aktuell[4]

2.4 Anwendung im E-Government am Beispiel Förderbeantragung

Förderbanken unterstützen Vorhaben ihrer Kunden durch Zuschüsse bzw. Darlehen. Das große Aufkommen von Förderanträgen verursacht einen hohen Verwaltungsaufwand der Förderfallbearbeitung. Ein online Förderportal dient hierbei zur Vereinfachung der Förderfallbearbeitung und der Kommunikation mit dem Kunden. Beim derzeitigen Förderportal ohne Signaturlösung kommt es zu Medienbrüchen. Das vom Kunden im Förderportal gespeicherte elektronische Dokument ist zwar für den Bearbeiter sofort sichtbar, muss jedoch vom Kunden erst ausgedruckt, unterschrieben und mit der Post zur Förderbank gesendet werden. Dem Kunden entsteht hierdurch ein Mehraufwand und ein zeitlicher Verzug (vgl. Abb. 1, Schritte 3-5). Auf der Seite der Förderbank entsteht Aufwand durch die Prüfung des unterschriebenen Dokuments und der Ablage des Doku-

[4] (1) Ausfüllen, (2) Datenübertragung, (3) Drucken, (4) Unterzeichnen, (5) Post, (6-8) manuelle Bearbeitung

ments in Papierform. Verfügte das Förderportal jedoch über eine adäquate Signaturlösung, kann der Kunde das ausgefüllte Dokument im Förderportal rechtsverbindlich signieren und das Dokument steht dem Bearbeiter anschließend sofort zur Bearbeitung bereit. Der Verwaltungsvorgang wird nicht durch Medienbrüche gestört und der Kunde profitiert von einer kürzeren Bearbeitungszeit. Die Förderbank kann Verwaltungsarbeit für die Förderfallbearbeitung und die Datenerhaltung effizienter gestalten. Darüber hinaus öffnen sich neue Möglichkeiten der ad-hoc Bearbeitung von Vorgängen, die bisher auf die Briefform angewiesen waren. Das Förderbankgeschäft auf Landesebene - wie die Förderbank im Freistaat Sachsen - wird von Landesgesetzen geregelt. Die Landesgesetzgebung muss der Bundesgesetzgebung folgen, um den Ersatz der Schriftform durch die elektronische Form zu erlauben. Für die nachfolgenden Betrachtungen wird davon ausgegangen, dass dies gegeben ist.

3 Vergleich der Signaturtechnologien

3.1 Technische Varianten für die Realisierung elektronischer Signaturverfahren

Dieser Abschnitt beschreibt den Postfach- und Versanddienst von De-Mail, die Online-Ausweisfunktion und die elektronische Signaturfunktion des nPA als Varianten für elektronische Signaturverfahren. Für jede Variante werden die vom Dienstenutzer und Diensteanbieter zu erbringenden Voraussetzungen, der technische Ablauf und die Integration in Backend-Systeme des Diensteanbieters skizziert.

Postfach- und Versanddienst von De-Mail

De-Mail ist ein an E-Mail orientierter elektronischer Nachrichtendienst, mit dem Nachrichten und Dokumente vertraulich, sicher und nachweisbar über das Internet versendet und empfangen werden können. De-Mail wurde von der deutschen Bundesregierung initiiert, um eine elektronische Entsprechung zur Briefpost zu schaffen. Die tatsächliche Leistungserbringung erfolgt durch zertifizierte Unternehmen, den sogenannten De-Mail-Anbietern. Im Regelfall meldet sich der Nutzer sicher (bzw. “hoch”) an seinem De-Mail-Postfach an. Bei der **hohen Anmeldung** wird eine Zwei-Faktoren-Authentifizierung durchgeführt, d.h. der Nutzer muss etwas wissen (z.B. Nutzername und Passwort) und im Besitz von etwas sein (z.B. nPA). Der De-Mail-Anbieter muss dem Nutzer mindestens zwei Verfahren zur sicheren Anmeldung anbieten, von denen eines die Online-Ausweisfunktion des nPA ist (§ 4 Abs. 2 De-Mail-G [Bu11]). Bei der **normalen Anmeldung** genügt die Eingabe von Nutzername und Passwort. Je nach Art der Anmeldung stehen dem Nutzer unterschiedliche Empfangs- und Versandoptionen zur Verfügung. Zum Beispiel kann er mit normaler Anmeldung eine einfache De-Mail (analog: Brief), mit hoher Anmeldung eine als ‘persönlich’ gekennzeichnete De-Mail (analog: eigenhändiges Einschreiben) versenden [MS11]. Einen Schriftformersatz stellen gemäß VwVfG §3a nur De-Mails mit der Versandoption ‘absenderbestätigt’ dar, für die eine hohe Anmeldung erforderlich ist. Ein Dienstenutzer benötigt neben einem aktiven De-

Mail-Konto einen nPA mit aktivierter Online-Ausweisfunktion (oder ein anderes, von seinem De-Mail-Anbieter akzeptiertes Token, z.B. ein Mobilfunkgerät zum Empfang von Mobile TAN)[5]. Bei der Eröffnung eines De-Mail-Kontos wird die Identität des Nutzers geprüft und seiner De-Mail-Adresse zugeordnet. Beim Diensteanbieter gelten im einfachsten Fall die gleichen Voraussetzungen. Für eine effizientere Verarbeitung werden die Abbildung der Organisationsstruktur auf De-Mail-Unterkonten bzw. -domains und der Einsatz eines De-Mail-Gateways empfohlen. Dieses ist in die existierende E-Mail-Infrastruktur integriert, hält eine Zuordnung zwischen De-Mail- und E-Mail-Adressen und 'übersetzt' De-Mails bzw. E-Mails. De-Mail-Gateways existieren als Hard- und Software-Lösungen mit unterschiedlichen Betriebsoptionen (z.B. In-house, Cloud-basiert). Eine mit der Gateway-Anbindung implementierte Signatur kann eine dauerhafte Authentifizierung gewährleisten.

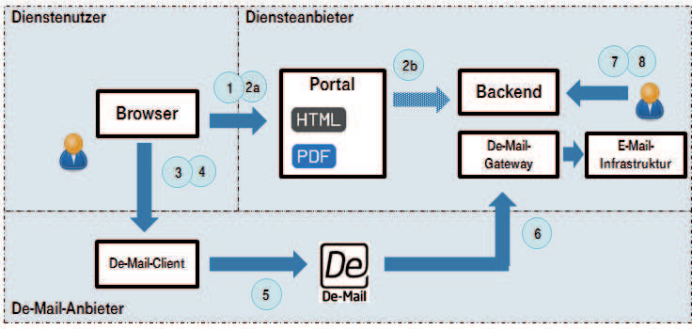

Abb. 2: schematischer Ablauf, De-Mail

Im Einzelnen sind folgende Schritte notwendig (vgl. Abb. 2): (1) Dienstenutzer füllt Formular im Portal aus (HTML) und erhält ein PDF-Dokument zum Versand mit De-Mail. Optional erfolgt eine elektronische Einreichung über das Portal (2a) und die Übernahme ins Backend (2b); Datenvalidierung erfordert Abgleich mit der eingereichten Schriftform (vgl. 6). (3) Dienstenutzer meldet sich am De-Mail-Client sicher an (mit nPA oder mTAN). (4) Dienstenutzer verfasst und sendet eine absenderbestätigte De-Mail an die De-Mailadresse des Diensteanbieters (manuell); Formulardokument als Anhang. (5) De-Mail übermittelt Nachricht. (6) De-Mail Empfang bei Diensteanbieter; Weiterleitung in dessen Infrastruktur. (7) Diensteanbieter ordnet De-Mail manuell dem zuständigen Sachbearbeiter zu. (8) Sachbearbeiter prüft und überträgt (manuell) strukturierte Daten von De-Mail ins Backend-System.

Online-Ausweisfunktion des nPA

Die Online-Ausweisfunktion (auch Identitäts- oder eID-Funktion) ermöglicht dem Inhaber eines Personalausweises sich gegenüber einem elektronischen Dienst (z.B. einer Anwendung im Internet) auszuweisen und ausgewählte Identitätsattribute an den Dienst

[5] Der beim Diensteanbieter beschriebene De-Mail-Gateway kann auch beim Dienstenutzer eingesetzt werden (insbesondere für Unternehmen sinnvoll).

zu übertragen. Die Online-Ausweisfunktion ermöglicht im technischen Sinne keine elektronische Signatur, stellt aber in Kombination mit der Abgabe einer Erklärung in einem vom Diensteanbieter bereitgestellten elektronischen Formular eine Alternative zur Schriftform dar (§3a VwVfG). Ein Dienstenutzer benötigt einen Personalausweis mit aktivierter Identitätsfunktion und muss die persönliche PIN für diese Funktion kennen. Er benötigt außerdem ein geeignetes Kartenlesegerät (hier genügt ein Basislesegerät) und einen lokal installierten eID-Client (z.B. die vom Bund bereitgestellte AusweisApp2) zur Unterstützung der sicheren Kommunikation zwischen Ausweis, Lesegerät und Dienst. Der Diensteanbieter benötigt ein Zertifikat, das ihn zum Zugriff auf Identitätsdaten des Personalausweises berechtigt. Dafür beantragt er zunächst eine Berechtigung für den Zugriff auf bestimmte Identitätsattribute bei der Vergabestelle für Berechtigungszertifikate (VfB) und bezieht dann das technische Zertifikat von einem Berechtigungszertifikate-Anbieter. Der Diensteanbieter muss außerdem seinen Dienst mit einem eID-Service integrieren. Der eID-Service dient der gegenseitigen Authentifizierung von Dienstenutzer und Diensteanbieter. Er übernimmt die Kommunikation mit dem eID-Client, stellt die Authentizität und Gültigkeit des Personalausweises sicher und übermittelt die ausgelesenen Daten an den Dienst. Für die Anbindung eines eID-Service gibt es mehrere Optionen: (1) Implementierung eines eigenen eID-Servers, (2) Lizenzierung und (in-house) Betrieb eines eID-Server-Produktes oder (3) Nutzung eines (außer Haus betriebenen) eID-Services.

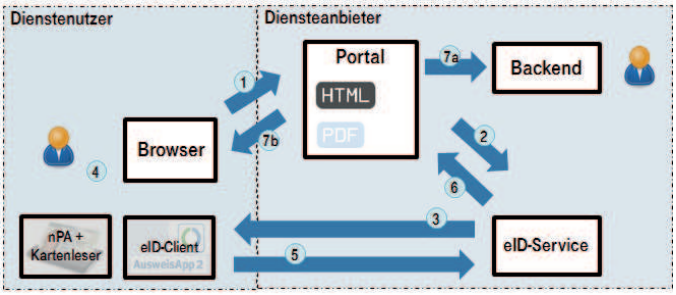

Abb. 3: schematischer Ablauf, eID

Die einzelnen Schritte gestalten sich wie folgt (vgl. Abb. 3): Der Dienstenutzer fordert ein Webformular vom Portal an, befüllt und versendet es (1). Die Daten werden im Portal temporär gespeichert und eine Anfrage an den eID-Service erstellt (2), der eine Verbindung zum eID-Client herstellt, sich authentifiziert und Identitätsdaten anfordert (3). Der Dienstenutzer wird zur Eingabe seiner PIN und zur Freigabe der Identitätsdaten aufgefordert (4), die dann an der eID-Service (5) und zum Portal (6) übermittelt werden. Ist die Authentifizierung erfolgreich, werden Formular- und Identitätsdaten gemeinsam im Backend abgelegt (7a) und dem Nutzer eine Bestätigung angezeigt (7b) [Bu16d].

Formularbefüllung und Identitätsnachweis müssen in der gleichen Websession stattfinden. Neben der eben beschriebenen Variante “Identitätsnachweis **nach** Formularbefüllung” ist auch ein Identitätsnachweis **vor** der Formularbefüllung möglich [Bu14]. Ob

ergänzend zu Webformularen auch lokal ausgefüllte Dokumente (z.B. PDFs) als Anhänge gestattet sind, ist aktuell unklar. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verneint das [Bu14] unter Berufung auf eine Begründung [De12] zur Änderung des VwVfG (in der eine derartige Klarstellung aber nicht auffindbar war). Andere Veröffentlichungen gehen davon aus, dass auch Anhänge erlaubt sind [Mi14].

Elektronische Signaturfunktion des nPA mit sign-me

Die Signaturfunktion des nPA ermöglicht das Unterschreiben von Dokumenten mit einer qualifizierten elektronischen Signatur (QES, vgl. Abschnitt 2.1). QES gab es bereits vor dem nPA - sie war vor der Aufnahme von Online-Ausweisfunktion und De-Mail in das VwVfG der einzig mögliche Schriftformersatz. Aufgrund vergleichsweise hoher Anschaffungsaufwände hat sich QES jedoch bisher kaum durchgesetzt. Mit der Möglichkeit, den nPA als Signaturkarte zu nutzen und qualifizierte elektronische Zertifikate in den Ausweis zu laden, soll die Akzeptanz der QES erhöht werden. Weiteres Vereinfachungspotential sollen Applikationen zur Online-Unterschrift (wie z.B. sign-me von der Bundesdruckerei) bieten [Bu16a]. Damit der Dienstenutzer die Funktion nutzen kann, benötigt er ein Signaturzertifikat auf seinem Personalausweis. Dafür muss er das Zertifikat bei einem Vertriebspartner von „sign-me“ erwerben und sich mit der Online-Ausweisfunktion bei sign-me registrieren. Mit dem nach der Registrierung postalisch versandten Berechtigungscode kann er das Zertifikat auf seinen Ausweis laden und eine Signatur-PIN vergeben. Da QES eine sichere Signaturerstellungseinheit erfordert, muss der Dienstenutzer zudem ein Komfort-Kartenlesegerät besitzen. Laut Bundesdruckerei muss der Diensteanbieter lediglich die Signaturapplikation von sign-me in sein Portal integrieren. Es ist davon auszugehen, dass der Diensteanbieter zusätzlich eine Komponente zur Verifizierung der vom Dienstenutzer angebrachten Signaturen integrieren muss.

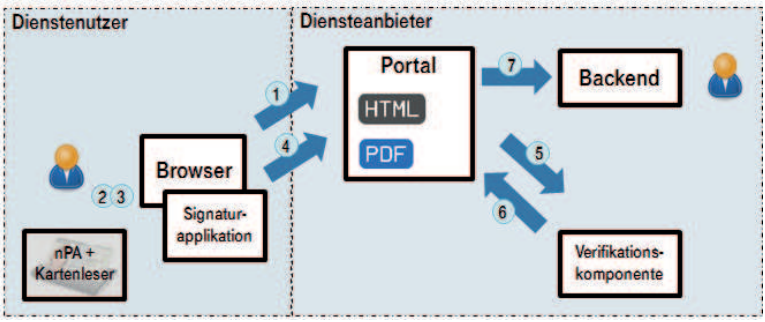

Abb. 4: schematischer Ablauf, sign-me

Abb. 4 zeigt die Komponenten bei Verwendung der Signaturfunktion sowie den Ablauf, der aus folgenden Schritten besteht: (1) Dienstenutzer füllt Formular im Portal aus (HTML) und erhält ein PDF-Dokument zum Signieren. (2) Dokument wird im Trusted Viewer der Signaturapplikation (ein Java-Applet) angezeigt und vom Dienstenutzer unter Eingabe der Signatur-PIN am Kartenleser signiert (2, 3). Signiertes Dokument

wird an Portal übermittelt (4). Signatur wird von der Verifikationskomponente beim Diensteanbieter geprüft (5, 6) und Dokument im Backend abgelegt (7)[6].

3.2 Vergleichende Bewertung

Tabelle 1 zeigt die vergleichende Bewertung der drei Signaturlösungen im Überblick, Bewertungskriterien sind nach Relevanz für Dienstenutzer und Diensteanbieter gruppiert. Es folgen detaillierte Ausführungen zu Bewertungen je Technologie.

Kriterium	De-Mail	Online-Ausweis-Fkt.	Elektronische Signatur-Fkt.
Dienstenutzer			
Kosten Anschaffung	Gering	Mittel (nPA, Basisleser, ca. 60)	Hoch (nPA, Komfortleser, Zertifikat, ca. 200)
Kosten Nutzung	Gering	Gering	Mittel
Aufwand Registrierung	Mittel	Mittel	Hoch
Diensteanbieter			
Verbreitung	Gering (1 Mio.)	Mittel (30% von 40 Mio.)	Sehr gering
Integration Portal	Nur manuell	Direkt	Direkt (wenn wie von sign-me beschrieben)
Integration Backend	Nur mit zusätzlichen Komponenten und manueller Kontrolle	Direkt	Direkt
Webformular	Indirekt (via PDF)	Direkt	Indirekt (via PDF)
PDF (eigenständige Dokumente)	Ja	Unklar	Ja
Aufwand Migration / Parallelbetrieb	Gering	Wenn PDF erlaubt: gering, sonst: hoch	Gering
Bidirektional	Ja	Nein	Nein

Tabelle 1 - Tabellarischer Vergleich der Lösungen

[6] Für die von der Bundesdruckerei nicht dokumentierten Bestandteile von Ablauf und Integration wurden Annahmen getroffen.

Postfach- und Versanddienst von De-Mail

Die Verbreitung von De-Mail ist aktuell gering (Anfang 2015 ca. eine Million registrierte Nutzer) [De15]. Kosten und Aufwand für den Dienstenutzer sind vergleichsweise niedrig, die Registrierung ist meist kostenfrei und für den Versand einer De-Mail fallen geringe Kosten an. Im einfachsten Fall ist keine zusätzliche Software auf Nutzerseite notwendig (webbasierter De-Mail-Client), bei Einsatz von Ende-zu-Ende-Verschlüsselung erhöht sich der Aufwand durch Installation und Nutzung eines Browser-Plugins. Aktuell ist De-Mail nur schlecht in ein Webportal integrierbar, der Nutzer muss Dokumente manuell in eine De-Mail übertragen und diese manuell adressieren (fehleranfällig) [Mi13]. Abhilfe könnten von De-Mail-Anbietern bereitgestellte Schnittstellen schaffen, die im einfachsten Fall analog zu "mailto:"-Links den De-Mail-Client mit einer bereits adressierten De-Mail öffnen. Idealerweise können so auch Verweise auf die im Portal befüllten Dokumente übergeben und die Dokumente automatisiert an eine De-Mail angehängt werden (das erfordert die Umsetzung von Zugriffsberechtigungen des De-Mail-Clients auf Portal-Dokumente). Aufwände auf Seiten des Diensteanbieters können gering sein, wenn auf Integration mit Backend-Systemen weitgehend verzichtet und der De-Mail-Gateway bereits von einem Dienstleister des Landes bzw. Bundes gestellt wird. Migration und Parallelbetrieb gestaltet sich mit De-Mail vergleichsweise einfach: Grundlage von Papierformularen sind meist PDFs, die nun als Anhänge an De-Mails angebracht werden. Die Integration von De-Mail in Backend-Systeme ist - wie bei klassischer E-Mail-Technologie - nur mit zusätzlichem Aufwand möglich: im Portal können zwar möglichst spezifische, die Organisationsstruktur abbildende De-Mail-Adressen hinterlegt werden, die Zuordnung der Daten bzw. Dokumente zu Vorhaben bzw. Vorgängen obliegt jedoch immer einem Sachbearbeiter. Abhilfe könnten zusätzliche Header-Attribute an einer De-Mail schaffen, die mittels Link an den De-Mail-Client übergeben und auf Empfänger-Seite automatisiert ausgewertet werden. Solange es diese De-Mail-Funktionalität nicht gibt, müssen identifizierende Eigenschaften aus den Anhängen der De-Mail extrahiert werden. Automatisiert ist das nur für auf Vorlagen des Diensteanbieters beruhenden Dokumenten möglich. De-Mail eignet sich für die bidirektionale Kommunikation zwischen Dienstenutzer und Diensteanbieter.

Online-Ausweisfunktion des nPA

Die Online-Ausweisfunktion des Personalausweises hat eine vergleichsweise hohe Verbreitung (sie ist bei 30% der 40 Millionen Besitzer eines nPA aktiviert [Bu16b], über die tatsächliche Nutzung gibt es allerdings keine Zahlen). Einer weiteren Verbreitung sind sicher die bereits existierenden Anwendungen zuträglich [Bu16c]. Nach moderaten initialen Kosten für Ausweis und Basislesegerät fallen beim Dienstenutzer keine laufenden Kosten an. Für die Herstellung der Voraussetzungen gibt es moderaten Aufwand, die Nutzung gestaltet sich schließlich vergleichsweise einfach und ist bürgernah dokumentiert. Für den zu installierenden eID-Client gibt es mehrere Alternativen (z.B. *AusweisApp2, Open eCard App, Persoapp*) [7] mit Unterstützung der verbreiteten Be-

[7] https://www.ausweisapp.bund.de/startseite, https://www.openecard.org/startseite, https://www.persoapp.de

triebssysteme. Die Online-Ausweisfunktion kann direkt in ein Portal integriert werden, fehleranfällige manuelle Schritte des Dienstenutzers (wie bei De-Mail) entfallen. Für Beschaffung und Integration eines eID-Service fallen beim Diensteanbieter Aufwände an, die durch Bereitstellung einer zentralen Infrastruktur durch Bund bzw. Land verringert werden können. Die direkte Integration der Online-Ausweisfunktion in das Portal ermöglicht auch eine automatisierte Zuordnung der eingegebenen Daten / Dokumente zu Vorhaben / Vorgängen, manuelle Schritte auf Seiten des Diensteanbieters entfallen. Die Aufwände für Migration bzw. Parallelbetrieb hängen stark davon ab, ob ausschließlich Webformulare oder auch Anhänge erlaubt sind (siehe Abschnitt 3.1). Während im zweiten Fall analog zu De-Mail existierende PDF-Formulare wiederverwendet werden können, ist im ersten Fall mit höheren Aufwänden zu rechnen: existierende PDF- müssen auf Web-Formulare umgestellt und parallel gepflegt bzw. Mechanismen zur möglichst redundanzfreien Pflege beider Technologien eingeführt werden. Durch die Bindung an eine Person eignet sich die Online-Ausweisfunktion nur für die Kommunikation vom Dienstenutzer zum Diensteanbieter, für die umgekehrte Richtung müssen alternative Technologien genutzt werden.

Elektronische Signaturfunktion des nPA

Zur Verbreitung der elektronischen Signaturfunktion liegen keine Daten vor, man kann jedoch davon ausgehen, dass allein aufgrund der zusätzlichen Voraussetzungen nur ein Bruchteil der Nutzer der Online-Ausweisfunktion auch die elektronische Signaturfunktion nutzt[8]. Für den Dienstenutzer sind Aufwand und Kosten zur Nutzung von QES immer noch sehr hoch: neben dem Komfort-Kartenleser[9] wird ein jährlich zu erneuerndes Zertifikat benötigt, hinzukommen mehrere Registrierungs- und Einrichtungsschritte mit zwischenzeitlichen Wartezeiten. Offenbar entfällt jedoch die Installation zusätzlicher Signatursoftware, die Signaturapplikation[10] kann direkt in das Portal des Diensteanbieters integriert und darüber ausgeliefert werden. Die mangelhafte Dokumentation und die geringe Auswahl von Anbietern[11] sind vielleicht dem erst kürzlich beendeten Pilotbetrieb geschuldet, tragen aber sicher nicht zu höherer Akzeptanz bei. Beim Diensteanbieter fallen Aufwände für die Beschaffung und Integration von Signaturapplikation und Verifikationskomponente an. Die direkte Integration ins Portal ermöglicht wie bei der Online-Ausweisfunktion eine automatisierte Zuordnung der eingegebenen Daten / Dokumente zu Vorhaben / Vorgängen. Migration und Parallelbetrieb gestalten sich wie bei De-Mail vergleichsweise einfach: die den Papierformularen zugrundeliegenden PDFs können als elektronisch signierte Dokumente weiterverwendet werden. Eine weitergehende Bewertung der elektronischen Signaturfunktion ist schwierig: insbesondere im Vergleich zur Online-Ausweisfunktion sind Funktionsweise, Kontrollfluss und Integrationsmöglichkeiten für Diensteanbieter nur wenig dokumentiert.

[8] Laut Bund waren vor Einführung des nPA nur etwa 300.000 Personen in der Lage, QES zu nutzen [De12]
[9] Kostet ca. 120 , es gibt zudem aktuell nur ein Modell.
[10] Aktuell ein Java-Applet, zukünftig eine Kombination aus mittels Web Start verteilter Java Applikation und Javascript (http://www.intarsys.de/produkte/sign-live/cloud-bridge)
[11] Jeweils nur ein Anbieter für Signaturapplikation, Zertifikat und Lesegerät.

4 Handlungsempfehlung für die Einführung

Bei der technischen Einführung können drei Szenarien für die Förderfallbeantragung unterschieden werden. Im ersten Fall baut die technische Lösung auf der Integration von De-Mail auf. Das zweite und dritte Szenario konzentriert sich auf die Integration der Ausweis oder Signaturfunktion des nPA. Die Szenarien sind auf vergleichbare Prozesse übertragbar. Jedoch entstehen Synergieeffekte aufgrund von Verbindlichkeiten gemäß §2 (1), (2) EGovG und dem daraus resultierenden Einsatz für andere Verfahren.

4.1 Lösung auf der Basis von De-Mail

In Abschnitt 3.1 wurde der technische Aufbau einer Lösung basierend auf De-Mail beschrieben. Sowohl Dienstenutzer als auch Diensteanbieter müssen demnach über eine Anbindung an ein De-Mail Gateway verfügen. Für den Diensteanbieter kann diese Anbindung einen hohen Aufwand erzeugen, wenn er noch nicht an De-Mail teilnimmt. Es ist ein Ausbau und die Integration der vorhandenen Email Infrastruktur mit der De-Mail Infrastruktur notwendig, um dauerhafte Mehraufwände zu vermeiden. Jedoch entstehen Synergieeffekte, wenn sich De-Mail daneben auch für andere Verfahren einsetzen lässt. Für den Dienstenutzer ist der Ausbau in der Regel mit der Einbindung eines De-Mailkontos abgeschlossen. Der Diensteanbieter hat bis dahin lediglich die Übermittlung von Nutzerdaten auf dem Postweg abgelöst. Um strukturierte Daten automatisch in die Backend-Systeme zu übertragen und somit dauerhaft einen Vorteil zu erlangen, muss er seine erweiterte Email-Infrastruktur mit den Backend-Systemen integrieren. Die Integration beinhaltet dabei die automatische Verifikation und Zuordnung zum Sachbearbeiter, die Weiterleitung der De-Mail an das Backend-System sowie die automatische Übertragung der Nutzerdaten aus der De-Mail in das Backend-System.

4.2 Lösung auf der Basis des nPA

Die Integration des nPA erfordert auf Nutzerseite die Aktivierung der Online-Ausweis- bzw. der Signaturfunktion (vgl. Abschnitt 3.1). Im ungünstigsten Fall sind daher Behördengänge mit entsprechenden Aufwänden erforderlich. Der Ausbau der technischen Infrastruktur beschränkt sich auf den Einsatz benötigter Lesegeräte. Der Diensteanbieter ist auf den eID-Service angewiesen. Seine Vorteile entfaltet dieses Szenario bei der Integration in die Backend-Systeme. Im Unterschied zu De-Mail muss nicht auf ein per Mailprotokoll übertragenes Dokument zugegriffen werden. Ebenso bleibt die eigene Mail-Infrastruktur unberührt - eine automatische Zuordnung von Emails an Sachbearbeiter entfällt. Vielmehr kann das Portal über eine Schnittstelle direkt an die erforderlichen Backend-Systeme angebunden und somit die technische Infrastruktur erweitert werden. Die Verifikation kann noch im Portal erfolgen, die Nutzerdaten werden über die Schnittstelle ins Backend-System und somit direkt in das Verwaltungsverfahren übertragen.

4.3 Fazit

Zusammen genommen bedeuten die beiden genannten Einstiegsszenarien insbesondere einen Ausbau der technischen Infrastruktur auf Nutzer- und Anbieterseite. Der Aufwand des Dienstenutzers beschränkt sich in der Regel auf den Einsatz einer elektronischen Alternative zur Authentifizierung, wie De-Mail oder die Ausweis- und Signaturfunktion des nPA. Auf Anbieterseite ergeben sich nachhaltige Verbesserungen erst dann, wenn die genannten Technologien bis zum Backend-System des Verfahrens integriert werden. Die Lösung auf Basis des nPA kann von einer direkten Schnittstelle zwischen Portal und Backend-System profitieren. Zu berücksichtigen sind bereits vorhandene Lösungen, die in jedem Fall migriert werden müssen (z.B. PDF-Formulare).

Literaturverzeichnis

[Bu01] Gesetz über Rahmenbedingungen für elektronische Signaturen. SigG, 2001.

[Bu03] Verwaltungsverfahrensgesetz. VwVfG, 2003.

[Bu11] De-Mail-Gesetz. De-Mail-G, 2011.

[Bu13] Gesetz zur Förderung der elektronischen Verwaltung. EGovG, 2013.

[Bu14] Technische Richtlinie TR-03107-2 Elektronische Identitäten und Vertrauensdienste im E-Government. Teil 2: Schriftformersatz mit elektronischem Identitätsnachweis, 2014.

[Bu16a] Bundesdruckerei: sign-me. https://www.bundesdruckerei.de/de/199-sign-me, 2016.

[Bu16b] Bundesministerium des Innern: Personalausweisportal - Fragen & Antworten. http://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/FAQ/faq_node.html, 19.03.2016.

[Bu16c] Bundesministerium des Innern: Personalausweisportal - Anwendungen. http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Anwendungen_node.html, 19.03.2016.

[Bu16d] Bundesministerium des Innern: Personalausweisportal - Online-Ausweisen. http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Online-Ausweisen_node.html, 12.03.2016.

[De12] Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften. Bundestagsdrucksache 17/11473, 2012.

[De15] Zwischenbericht der Bundesregierung nach Artikel 4 des Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften weiterer Vorschriften. Drucksache 18/4042, 2015.

[Gr07] Gruhn, V. et al.: Elektronische Signaturen in modernen Geschäftsprozessen. Schlanke und effiziente Prozesse mit der eigenhändigen elektronischen Unterschrift realisieren. Vieweg, Wiesbaden, 2007.

[Mi13] Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg: DV-Konzept De-Mail / Online-Ausweisfunktion im BAföG-Verfahren, 2013.

[Mi14] Ministerium für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern: Fachkonzept zur Abwicklung von Fördermitteln mit der eID-Funktion, 2014.

[MS11] Mehrfeld, J.; Schumacher, A.: Das De-Mail-Konzept: Gesetzlicher Rahmen & Akkreditierungsverfahren, 2011.

[Ni01] Nissel, R.: Neue Formvorschriften bei Rechtsgeschäften. Elektronische Form und Textform im Privatrechtsverkehr ; Erläuterungen, Texte, Materialien. Bundesanzeiger-Verl.-Ges, Köln, 2001