

**AUF DEM WEG ZU EINEM
PERSONALISIERTEN UND
PROAKTIVEN E-GOVERNMENT
EMPFEHLUNGEN FÜR DIE UMSETZUNG
DIGITALER VERWALTUNGSLEISTUNGEN**

VORWORT

Das vorliegende Whitepaper ist im Rahmen des Projektes „Trusted Service Platform“ in Kooperation zwischen der Bundesdruckerei GmbH und dem Forschungsinstitut Fraunhofer FOKUS entstanden. Mit der Trusted Service Platform wird eine umfassende Lösung zur Nutzung digitaler Identitäten im Kontakt zwischen Bürger, Verwaltung und Unternehmen geschaffen. Mit dieser kann der Bürger seine persönlichen Daten und Dokumente (wie z. B. Urkunden und Bescheide) in elektronischer Form verwalten, für die Nutzung in Verwaltungs- und Geschäftsprozessen übertragen und selbständig steuern, welcher Online-Dienst auf welche Identitätsinformationen zugreifen darf. Die Umsetzung des Konzepts „Trusted Service Platform“ macht somit den Kontakt zwischen Bürger, Verwaltung und Unternehmen erheblich einfacher, effizienter und zeitsparender.

Gleichzeitig soll die Trusted Service Platform auch eine sichere Lösung für die Nutzung elektronischer Identitäten bieten. Da die Inanspruchnahme von Verwaltungsleistungen die Einhaltung spezifischer Gesetze und Bestimmungen in unterschiedlichen Komplexitätsgraden erfordert, stellt die Trusted Service Platform in einem Stufenkonzept verschiedene Sicherheitslevel der Authentifizierung bereit, um eine adäquate Abbildung im digitalen Raum zu gewährleisten. Im Rahmen dieses Whitepapers werden diese Sicherheitsstufen zunächst identifiziert und erläutert. Zudem werden die 25 am häufigsten nachgefragten Verwaltungsleistungen den entsprechenden Sicherheitsstufen zur Veranschaulichung zugeordnet. Abschließend werden dem Leser die in diesem Kontext notwendig erscheinenden Handlungsempfehlungen vermittelt

VERWALTUNGSLEISTUNGEN SCHNELL UND EINFACH NUTZEN DURCH NEUE DIGITALE WEGE

Was würde wohl ein Mensch denken, der vor 50 Jahren in eine Zeitmaschine gestiegen wäre, um in unsere Zeit zu reisen? Während man damals noch dachte, dass unsere Gegenwart durch Städte auf dem Meeresboden, fliegende Autos und die Kolonisierung fremder Planeten gekennzeichnet wäre, hat eine andere Erfindung die Welt in einer Weise verändert, die sich die visionärsten Science-Fiction-Autoren in der Form nicht hätten vorstellen können: das Internet. Doch während dieses in den vergangenen 20 Jahren revolutionäre Schübe in Produktion, Handel, Wissenschaft und Unterhaltung gebracht hat, liegt die Verwaltung hier noch hinter ihren Möglichkeiten – dabei verspricht die Digitalisierung von Verwaltungsleistungen konkrete Vorteile für Bürger, Behörden und Unternehmen.

Die Politik hat diesen Handlungsbedarf erkannt. Der Koalitionsvertrag der aktuellen Bundesregierung kündigt die Schaffung von Bürgerkonten an, die zu digitalen Dokumentenpostfächern erweitert werden können. Die Identifizierung soll mittels des elektronischen Personalausweises erfolgen. Die Digitale Agenda der Bundesregierung benennt „die digitale Transformation der öffentlichen Verwaltung“ als eines ihrer expliziten Ziele.

Die Erwartungen der Bürger an Effektivität und Nutzerfreundlichkeit digitaler Verwaltungsleistungen, die durch die bereits erreichten Standards privater Dienstleister geprägt sind, sollen erfüllt werden bei gleichzeitiger Einhaltung der hohen Anforderungen an Vertrauen und Sicherheit. Dies soll u. a. durch Einrichtung persönlicher Nutzeraccounts (sogenannte „Bürgerkonten“), die Schaffung effizienter Schnittstellen zwischen Verwaltung, Bürgern und Unternehmen sowie die möglichst weitgehende Durchsetzung der elektronischen Signatur erfolgen.

EINE VISION FÜR DIE ELEKTRONISCHE VERWALTUNG

Ambitionierte Ziele sind geschaffen – doch diese können nur erste Schritte auf dem Weg der Verwaltung sein. Der Stand der technischen Entwicklung kann noch viel mehr ermöglichen. Dieses Potenzial wollen Fraunhofer FOKUS und die Bundesdruckerei im Projekt „Trusted Service Platform“ umsetzen. Dabei wurden folgende Schwerpunktthemen der Verwaltungsdigitalisierung identifiziert:

- Ein gebündelter Zugang zu den Leistungen verschiedener Verwaltungen, um eine hohe Nutzerfreundlichkeit zu gewährleisten
- Wiederverwendbarkeit von Daten und Dokumenten, um valide Daten und schnelle Durchlaufzeiten zu gewähren
- Ausreichende Sicherheitsmaßnahmen bezogen auf Datenschutz und Informationssicherheit, um dem Sicherheitsbedürfnis der Nutzer und den rechtlichen Anforderungen gerecht zu werden.

Darauf aufbauend wurde folgende Vision für die Zukunft der Verwaltung erarbeitet: Der Kontakt zwischen Bürger und Verwaltung kann fast vollständig über digitale Kanäle abgewickelt und die benötigten Unterlagen wie Formulare, Bescheide, Urkunden usw. durch elektronisch signierte digitale Dokumente ersetzt werden. Der Zugang zu allen online verfügbaren Leistungen wird in einem zentralen Portal gebündelt, das die kommunalen Bürgerservice-Portale integriert und ergänzt – so können beispielsweise im Falle eines Umzugs die Abmeldung am alten und die Anmeldung am neuen Wohnort über den gleichen Kanal erledigt werden. Ein entscheidender Faktor ist dabei die Nutzerfreundlichkeit, denn digitale Verwaltungsprozesse sind heutzutage noch komplex – diese Komplexität sollte aber im Hintergrund ablaufen, während im Vordergrund für Bürger und Unternehmen eine einfach und möglichst intuitiv zu bedienende Oberfläche gestaltet werden sollte, um digitale

Verwaltungsleistungen in Anspruch zu nehmen. Auf Grundlage der aktuellen Lebenslage eines Bürgers (z. B. Umzug, Heirat, Geburt eines Kindes) und der Historie seiner zuletzt genutzten Leistungen kann die Verwaltung dem Bürger automatisch weitere passende Leistungen anbieten (beispielsweise die Beantragung von Kindergeld im Anschluss an die Ausstellung einer Geburtsurkunde). Damit wird der Schritt von der heutigen, größtenteils reaktiven Verwaltung hin zu einer proaktiven Verwaltung mit größerer Serviceorientierung unternommen.

Selbstverständlich kann der Bürger selbst in seinen persönlichen Einstellungen entscheiden, wie stark dieser proaktive Faktor ausgeprägt sein soll. Das heißt, er kann selbst bestimmen, welche Behörden in welcher Form auf seine Daten zugreifen können – ob diese beispielsweise Prozesse automatisch anbieten oder gar anstoßen dürfen, ob dazu seine Bestätigung nötig ist oder ob Prozesse nur durch ihn selbst in Gang gesetzt werden können. Passend dazu können in einem gesonderten Bereich des zentralen Verwaltungsportals auch privatwirtschaftliche Dienstleistungen angeboten werden, die die Verwaltungsleistungen ergänzen – so z. B. Möbelträger und Maler für die Lebenslage „Umzug“ oder passende Kleinkind-Ausstattung und Kita-Angebote für die Lebenslage „Geburt“.

E-VERWALTUNG SPART ZEIT UND AUFWAND

Für die Bürger bringt dies eine massive Zeitersparnis, während die Verwaltungsmitarbeiter sich auf die Bearbeitung anspruchsvollerer Fälle und die Beratung der Bürger konzentrieren können. Dies ist umso wünschenswerter, da der öffentliche Dienst auf Grund von Überalterung, fehlendem Nachwuchs und klammen Kassen mit zunehmendem Personal-mangel zu kämpfen hat. Das Potenzial einer solch weitgehenden Digitalisierung soll im Folgenden anhand eines oft



Foto: MEV Verlag/Thomas Karl

Bürger*	Aktuelle Situation	Zukünftig möglich	Einsparung bis zu
Informationsbeschaffung	an 4 verschiedenen Stellen	an einer zentralen Stelle	75 %
Materialbeschaffung (Download)	an 4 verschiedenen Stellen	an einer zentralen Stelle	75 %
Formularbearbeitung	manuell (bis 85 % gleiche Eingaben)	automatisch	85 %
Dokumentenzusammenstellung	manuell	halb-automatisch	50 %
Einreichung	Persönlich, postalisch, elektronisch	elektronisch	80 %

*Bei der Betrachtung weiterer Verwaltungsleistungen können diese Angaben ebenfalls auf die Zielgruppe Unternehmen angewandt werden.

Abbildung 1: Vergleich aktuelle und zukünftige Situation der Leistungsbeschaffung in der Lebenslage „Geburt“ aus Bürgerperspektive

nachgefragten Beispiels der Lebenslage „Geburt“ verdeutlicht werden: Für die Beantragung von Elterngeld ist es heutzutage erforderlich, einen schriftlichen Antrag beim zuständigen Jugendamt zu stellen. Darin werden u. a. die gleichen persönlichen Angaben von Kind und Eltern abgefragt, die in hundert anderen Verwaltungsleistungen erfasst werden – Name, Vorname, Geburtsdatum und Anschrift. Zusätzlich werden Informationen zum Einkommen und zum Mutterschaftsgeld sowie Krankenversicherungs- und Kontodaten der Eltern erfasst.

All diese Angaben müssen nicht nur in Formulare eingetragen und durch beide Elternteile unterschrieben werden, sondern auch durch Dokumente wie die Geburtsurkunde sowie die Personalausweise, Einkommensnachweise, Bescheinigung der Krankenkasse über das Mutterschaftsgeld usw. belegt werden. Die digitale Umsetzung dieses aufwändigen Prozesses ist bislang nicht über das Anbieten downloadbarer Formulare im Internet hinausgekommen.

Wie könnte diese Leistung nun nutzerfreundlicher und mit reduziertem Aufwand im digitalen Zeitalter erbracht werden?

Das Vorlegen von Original- oder fotokopierten Dokumenten wird unnötig, wenn diese als elektronische Dokumente vorliegen. Durch eine digitale Signierung kann die Vertrauenswürdigkeit der Dokumente im Vergleich zu eventuell manipulierten Fotokopien stark erhöht werden. Auch das Ausfüllen der Formulare selbst kann auf diesem Wege erleichtert werden: Liegen die entsprechenden Unterlagen in elektronischer Form vor, dann können die benötigten Attribute wie Adresse, Versicherungsstand, monatliches Einkommen usw. automatisch in das Formular überführt werden. Für den Bürger entfällt die Aufgabe, stets von neuem die gleichen Daten in Formulare einzutragen. Auf Verwaltungsseite entfällt das händische Übertragen der Informationen aus dem Antrag in die Kartei sowie das Abgleichen mit den Originaldokumenten. Und wenn nach erfolgter Prüfung der Bescheid wiederum in

elektronischer Form ausgestellt wird, kann er als Grundlage für weitere Verwaltungsprozesse dienen – z. B. als Nachweis, wenn die Eltern weitere finanzielle Leistungen wie Kindergeld beantragen.

Eine Leistung wie die des Elterngeldes wird jedoch in der Regel nicht allein beantragt. Je nach Lebenslage des Bürgers fallen weitere Verwaltungsprozesse an – in der Lebenslage „Geburt“ gehören dazu auch die Anmeldung der Geburt beim Standesamt sowie die Beantragung von Kindergeld sowie ggf. Elterngeld und eines Kita-Gutscheins. Die Eltern müssen dafür mit bis zu vier verschiedenen Verwaltungsorganen in Kontakt treten: dem Standesamt, dem Bürgeramt, der Familienkasse und dem Jugendamt. Betrachtet man die gesamte Lebenslage „Geburt“, so wird sichtbar, in welchem großem Ausmaß die Digitalisierung der Verwaltung den Aufwand für den Bürger für diese vier typischen Verwaltungsleistungen senken kann (vgl. Abbildung 1).

VORAUSSETZUNGEN EINER MODERNEN VERWALTUNG

Um dieses Effizienzpotenzial umzusetzen und gleichzeitig die gesetzlichen Standards von Datenschutz und Informationssicherheit zu gewährleisten, muss sichergestellt werden, dass der Bürger auch ohne händische Unterschrift, das Vorlegen physischer Dokumente oder persönliche Vorsprache identifiziert werden kann. Voraussetzung dafür ist die Schaffung einer zentralen Onlineplattform, auf der der Bürger seine Identitätsdokumente sicher speichern und verwalten kann. Diese dient als Authentifizierungsdienst gegenüber der Verwaltung und anderen Diensteanbietern. Darüber hinaus dient sie als Provider von Identitätsattributen, die zur Nutzung von Leistungen nötig sind, und zur Bestätigung von Identitäten und Attributen – z. B. als Ersatz zum heute gängigen PostIdent-Verfahren, bei dem noch immer eine persönliche Vorsprache in der Postfiliale erfolgen muss.

Eine solche Plattform stellt die „Trusted Service Platform“ dar, die aktuell von Fraunhofer FOKUS und der Bundesdruckerei entwickelt wird. Sie ermöglicht es dem Nutzer, sich gegenüber Behörden und Unternehmen zweifelsfrei elektronisch auszuweisen sowie seine Dokumente, Daten und persönlichen Attribute (von Name und Geburtsdatum bis hin zu Adresse, Arbeitsverhältnis, Monatseinkommen usw.) sicher in digitaler Form aufzubewahren, zu verwalten und zu übermitteln.

Das Eintreten der Verwaltung in den digitalen Raum setzt weiterhin voraus, dass die Verwaltungsleistungen in geeigneter Weise digital abgebildet werden. Dabei sollen Mechanismen nicht eins zu eins aus der analogen in die digitale Welt übertragen werden, sondern wo möglich und nötig auch an die neuen Anforderungen angepasst und somit verbessert werden. Die Regelung der Zugangsberechtigung von Nutzern ist eine wesentliche Voraussetzung für Online-Verwaltungsleistungen, bei der es zum jetzigen Zeitpunkt noch keine klaren Vorgaben gibt, sondern oft Interpretationen bestehender Vorschriften notwendig sind. Dies erfordert eine Analyse der Vorgaben zur Authentifizierung des Bürgers. Denn für viele Leistungen gibt es nur eine „gefühlte Schriftformerfordernis“, die nicht gesetzlich vorgeschrieben ist, sondern sich lediglich aus dem bisherigen Alltag der Verwaltungspraxis ergibt.

In unseren Forschungsarbeiten wurden exemplarisch 25 besonders häufig nachgefragte Verwaltungsleistungen für Bürger („Top-25-Leistungen“) auf ihre Übertragbarkeit in den digitalen Raum untersucht. Dabei konnten anhand der tatsächlich gesetzlich gegebenen Authentifizierungsanforderungen drei verschiedene Authentifizierungsstufen identifiziert werden, für die jeweils unterschiedliche Maßnahmen zur Überführung in digitale Angebote nötig sind.

Im Folgenden werden das erarbeitete Konzept der Sicherheitsstufen vorgestellt und Empfehlungen für die Umsetzung digitaler Verwaltungsleistungen gegeben.

DIGITALE ABBILDUNG DURCH PASSGENAUE SICHERHEITSTUFEN

Wie sollte der Zugang zu digitalen Verwaltungsleistungen geregelt sein?

In der heutigen „Papierverwaltung“ gibt der Bürger für jeden Prozess seine Daten erneut ein. Die Ausgabe von Formularen, bei denen zumindest einige Felder bereits vorbefüllt sind, ist die Ausnahme.

Die Untersuchung der Top-25-Leistungen ergibt jedoch, dass für viele Verwaltungsprozesse immer wieder die gleichen Daten der Bürger benötigt werden (vgl. Abbildung 2). Ganz vorn liegt hier die Namensangabe, die in fast allen Prozessen abgefragt wird, gefolgt von den Geburts- und Adressdaten.

Ähnlich verhält es sich bei Dokumenten: Nachweise wie Personalausweis, Geburtsurkunde, Meldebescheinigung, Führungszeugnis etc. müssen häufig bei Verwaltungsleistungen eingereicht werden – ob im Original oder als (beglaubigte) Kopie. Der so entstehende Aufwand für den Bürger lässt sich bei der digitalen Abbildung von Verwaltungsleistungen erheblich senken, wenn der Zugang zu den Leistungen über einen Nutzeraccount geregelt wird, für den der Bürger sich registriert und auf den er exklusiv zugreifen kann. Die entsprechenden personenbezogenen Daten müssen so nur einmal eingegeben (oder automatisch aus bestehenden digitalen Dokumenten übernommen) werden und können danach für alle digitalen Verwaltungsleistungen, die der Bürger in Anspruch nimmt, genutzt werden. Der Bürger kann all seine Daten und Dokumente an einem Ort speichern, schnell und unkompliziert auf sie zugreifen und sie auch selbst bearbeiten, z. B. Adressänderungen im Falle eines Umzugs oder eines Stellenwechsels.

Zudem wird so die Korrektheit der Daten für die Prozesse erhöht, da Fehler aufgrund versehentlicher „Zahlendreher“ oder unleserlich ausgefüllter Formulare entfallen.

Welche Anforderungen muss die Nutzerauthentifizierung erfüllen?

Die zahlreichen Leistungen, die die Verwaltung ausführt, unterscheiden sich nach der Schutzbedürftigkeit der verwendeten Daten. So benötigen Basisinformationen wie der Geburtsort ein weit niedrigeres Schutzniveau als sensible vertrauliche Dokumente wie ärztliche Atteste oder polizeiliche Führungszeugnisse. Zudem sind Verwaltungsleistungen mit unterschiedlichen Berechtigungen verbunden – von reinen Auskünften bis hin zu weitreichenden Vollmachten wie der Vormundschaft. Außerdem beinhalten viele Verwaltungsprozesse die Ausgabe von Geld- oder geldwerten Leistungen, wobei gewährleistet werden muss, dass diese bei der richtigen, als empfangsberechtigt bestätigten Person ankommen.

Daraus begründet sich, dass für den Zugang zu verschiedenen Verwaltungsleistungen auch unterschiedliche Voraussetzungen erbracht werden müssen. Denn einerseits muss sichergestellt werden, dass der Antragsteller zur Nutzung der Leistung berechtigt ist, und andererseits muss der Schutzbedarf erfüllt werden.

Gleichzeitig ist die Verwaltung verpflichtet, mit den ihr von der Gesellschaft zur Verfügung gestellten Steuermitteln sparsam umzugehen. Hochsichere elektronische Authentifizierungsmethoden sollten daher nur bei den Prozessen angewandt werden, bei denen sie tatsächlich nötig sind – so wie es auch in der heutigen Verwaltung nicht zweckmäßig wäre, für jede Auskunft das persönliche Erscheinen des Bürgers im Amt zu verlangen. Ausgehend von diesen Erkenntnissen konnte im Rahmen der Forschungsarbeiten die folgende Abstufung abgeleitet werden:

Stufe 1

Ein Großteil der von der Verwaltung zur Verfügung gestellten Web-Inhalte dient der reinen Information der Bürger. Auch Online-Formulare können anonym ausgefüllt werden und dann ausgedruckt an die Verwaltung versandt werden.

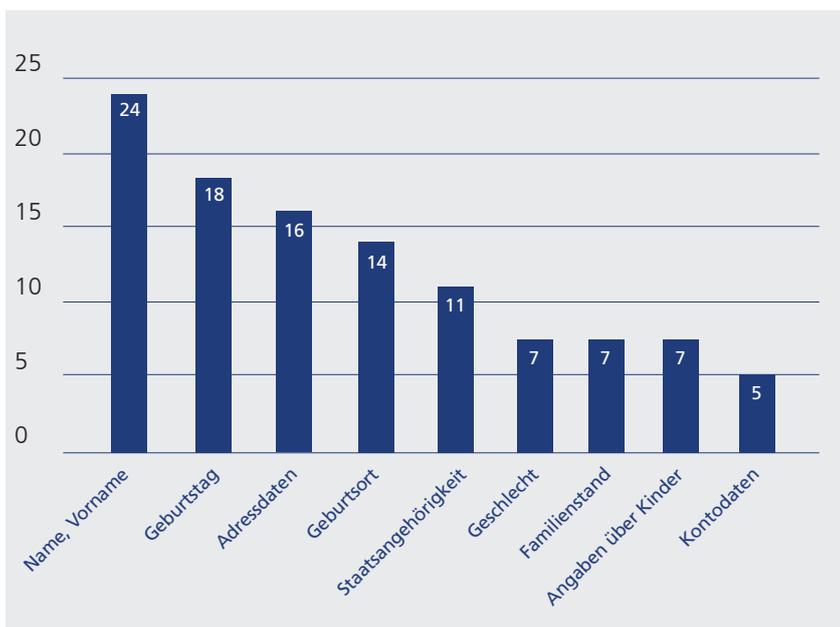


Abbildung 2: Vorkommen personenbezogener Daten in den Top-25-Verwaltungsleistungen für Bürger

Außerdem gibt es komplette Verwaltungsleistungen, die keine Authentifizierung erfordern.

Beispiel: Bei einer einfachen Melderegisterauskunft ist es unerheblich, wer die beantragende Person ist, da laut Gesetz jede Person dazu berechtigt ist. Vertrauensdienste sind hier also nicht gefordert.

Stufe 2

Die Person muss sich der Verwaltung gegenüber zu erkennen geben, bevor sie den Prozess auslösen kann. Höhere Anforderungen per Gesetz wie Schriftformerfordernis oder persönliches Erscheinen sind nicht gefordert.

Beispiel: Bei einem Wohngeldantrag ist es wichtig, dass die beantragende Person gegenüber der Verwaltung authentifiziert wurde (z. B. hier als Kontrollfunktion, damit das Geld nur der Person zukommt, die Anspruch darauf hat). Bei vielen dieser Prozesse besteht heute noch eine „gefühlte Schriftformerfordernis“, die sich lediglich aus langjähriger

Verwaltungspraxis ableitet, ohne dass eine tatsächliche rechtliche Notwendigkeit besteht.

Die Authentifizierung dient hier verschiedenen Funktionen (Kontrollfunktion, Warnfunktion etc. – vgl. unten, Abb. 4). Dementsprechend ist bei einer Digitalisierung eine Reihe an geringeren Formen der Authentifizierung denkbar (z. B. Nutzernamen/Passwort, Einmal-TAN, etc.).

Stufe 3

Per Gesetz muss der Antragssteller beim Amt persönlich erscheinen oder die eingereichten Formulare/Anträge schriftlich unterschrieben im Amt einreichen (Schriftformerfordernis). Die Identitätsprüfung kann hier der Identitätsfunktion, Echtheitsfunktion oder Anschlussfunktion dienen.

Beispiel: Bei der Beantragung eines Führungszeugnisses muss die Person entweder persönlich erscheinen oder einen schriftlichen Antrag stellen.

Stufe	Vorkommen (basierend auf den TOP-25-Verwaltungsleistungen)	Digitale Abbildung
1. ohne Authentifizierung	<ul style="list-style-type: none"> – Einfache Melderegisterauskunft – Anmeldung Gewerbe – Kfz-Kennzeichen (nur Reservierung) – Anmeldung Hundehaltung – Beglaubigung (Abschrift) – Straßenverkehrsbehördliche Erlaubnisse/Ausnahmegenehmigungen – Parkausweis/Bewohnervignette – Gewerberegisterauskunft 	<ul style="list-style-type: none"> – Eingabemasken oder intelligente Formulare, die zum Download angeboten werden – Ausgabe von Unterlagen wie z. B. Bescheiden usw. als elektronische Dokumente
2. Authentifizierung ohne gesetzlich erforderliche Identitätsprüfung	<ul style="list-style-type: none"> – Erweiterte Melderegisterauskunft – Anmeldung Kraftfahrzeug – Beantragung Wohngeld – Beantragung Kfz-Kennzeichen – Beantragung Baugenehmigung – Beantragung Befreiung oder Ermäßigung GEZ – Beantragung Hilfe zur Pflege – Grundsicherung im Alter – Anmeldung der Geburt (Standesamt) – Beantragung Kita-Gutschein 	<ul style="list-style-type: none"> – Nutzernamen/Passwörter – Einmal-TAN (z. B. per SMS) – Einfache digitale Signatur – biometrische Merkmale (z. B. Fingerabdruck) – Abgeleitete Identität (Bei der Identitätsableitung wird eine Identität aus einer vertrauenswürdigen aber evtl. schwer auslesbaren Quelle extrahiert und in ein weniger sicheres aber dafür leichter benutzbareres Format überführt. Abgeleitete Identitäten sind in der Regel temporär beschränkt und in Software realisiert.)
3. Authentifizierung mit Identitätsprüfung	<ul style="list-style-type: none"> – Ausstellung Personalausweis – Ausstellung Reisepass/Kinderpass – Meldung Wohnsitz – Ausstellung Führungszeugnis – Ausstellung Führerschein – Hundehaltung: Aufgabe der Haltung u.a. – Beantragung Ausbildungsförderung – Beglaubigte Willenserklärung – Ausstellung Lohnsteuerkarte – Beantragung Kindergeld – Beantragung Elterngeld 	<ul style="list-style-type: none"> – Authentifizierung durch eID-Funktion des neuen Personalausweises

Abbildung 3: Verteilung und digitale Umsetzung der Sicherheitsstufen



Dementsprechend erfordert der elektronische Prozess eine höhere Sicherheit, die durch die eID-Funktion des neuen Personalausweises oder durch die qualifizierte elektronische Signatur abgebildet werden kann. In seltenen Fällen, in denen ein weiterer Nachweis erfolgen muss, werden zusätzliche elektronische Zertifikate verwendet. Als Beispiel dient das Ausstellen von Gutachten durch Ärzte, die sich durch den elektronischen Arztausweis digital ausweisen können. Abbildung 3 zeigt, wie sich die betrachteten Top-25-Leistungen auf die Sicherheitsstufen verteilen und präsentiert Möglichkeiten ihrer Abbildung im digitalen Raum. Bei der Entwicklung der Sicherheitsstufen wurden auch bereits bestehende Konzepte mit ähnlicher Schwerpunktsetzung vergleichend ausgewertet:

Im Rahmen des EU Projekts STORK (Secure Identity Across Borders Linked) wurde das „Quality of Authentication Assurance Model“ entwickelt. Auch im deutschen Kontext wurden Empfehlungen erarbeitet: Der IT-Planungsrat hat im Rahmen seiner eID-Strategie das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Ausarbeitung der technischen Richtlinie „Elektronische Identitäten und Vertrauensdienste im E-Government“ beauftragt. Während das STORK-Konzept die unterschiedlichen Authentifizierungsanforderungen in vier Vertrauensleveln zusammenfasst, definiert das BSI drei Vertrauensniveaus. Dabei findet das Level 1 von STORK (no or minimal assurance) keine Entsprechung im BSI-Modell. Dafür bestehen große Gemeinsamkeiten zwischen dem STORK-Level 2 (low assurance) und dem BSI-Niveau 1 (normal). Die STORK-Level 3 und 4 (substantial assurance bzw. high assurance) sind hingegen nicht völlig mit den BSI-Niveaus 2 und 3 (hoch bzw. hoch +) gleichzusetzen. Das Niveau 4 des BSI stellt tendenziell höhere Anforderungen an eine Authentifizierung als Level 3 von STORK.

Aus unserer Analyse der Anforderungen der Verwaltungsleistungen folgte eine Einteilung in drei Stufen, die ausreichen, um die Gesamtheit der Verwaltungsleistungen erfassen zu können (also auch jene, für die keine Authentifizierung notwendig ist).

Wie können die gesetzlichen Authentifizierungsvorschriften in digitalen Verwaltungsleistungen abgebildet werden?

Für die Sicherheitsstufen 1 und 3 ergibt sich die digitale Umsetzung unmittelbar aus den rechtlichen Bestimmungen: Während für Prozesse der Stufe 1 keine Authentifizierung erforderlich ist, müssen die Schriftformerfordernis oder die Pflicht zum persönlichen Erscheinen aus Stufe 3 durch entsprechend sichere digitale Lösungen abgebildet werden, wie die qualifizierte elektronische Signatur oder die Anmeldung mit der eID-Funktion des neuen Personalausweises. Schwieriger ist es bei Verwaltungsprozessen der Stufe 2, welche mehr als ein Drittel der TOP-25-Leistungen umfassen.

Gesetzliche Vorschriften, Verwaltungspraxis und objektive Notwendigkeiten liegen hier oft auseinander. Das E-Government-Gesetz sieht vor, dass sämtliche verwaltungsrechtliche Vorschriften des Bundes einem „Normenscreening“ unterzogen werden, bei dem überprüft wird, wo die Anordnung der Schriftform verzichtbar ist. Es ist also davon auszugehen, dass die Anzahl der Verwaltungsleistungen in Stufe 2 in den nächsten Jahren weiter anwachsen wird, indem die gefühlte Schriftform abgebaut werden kann.

Für die digitale Umsetzung dieser Leistungen bleibt viel Spielraum, und es fehlt an klaren allgemeinverbindlichen Richtlinien. Dabei müssen die Attribute, Unterlagen und Daten, die der Bürger in einen Prozess einbringt, auf ihren Verwendungszweck (Funktion) geprüft werden, d. h. auf ihre Funktion für die konkrete Verwaltungsleistung.

Im Rahmen der Fachdiskussion um die Einführung elektronischer Signaturen wird in der Regel eine Reihe von Funktionen unterschieden, wobei wir uns auf sechs Kernfunktionen konzentrieren: Prozessdaten, Identitätsfunktion, Perpetuierungsfunktion, Kontrollfunktion, Warnfunktion und Abschlussfunktion. Diese ließen sich jeweils den unterschiedlichen Sicherheitsstufen zuordnen. Konkret werden diese in Abbildung 4 gezeigt.

Verwendungszweck/ Funktion	Beschreibung	Stufe
Prozessdaten	Notwendige Voraussetzung zur Initiierung und Durchführung des Verwaltungsprozesses	1,2,3
Identitätsfunktion	Notwendige Voraussetzung zur Ermittlung der Identität des Antragstellers oder eines Beteiligten. Alle Voraussetzungen, aus denen sich eine Identität ableiten lässt. Dies können Attribute (Name, Geburtsdatum, Adresse), Ausweisdokumente oder persönliches Kennen sein.	3
Perpetuierungsfunktion	Notwendige Voraussetzung für die dauerhafte Lesbarkeit und Wahrnehmbarkeit der Unterlagen und Attribute. Schriftstücke, Urkunden oder dauerhaft speicherbare elektronische Dokumente ermöglichen es, Voraussetzungen zeitlich versetzt nach ihrer Entstehung/ Erzeugung Dritten zur Wahrnehmung (Lesen, Ansehen, Anhören, ...) zu bringen.	1,2,3
Kontrollfunktion	Notwendige Voraussetzung für die Prüfung der Herkunft und Authentizität der Angaben sowie den Nachweis von Eigenschaften gegenüber Dritten. Mit Hilfe von Ausweispapieren, signierten Dokumenten oder Urkunden als (beglaubigte) Kopien/Originale können die Herkunft von Dokumenten und die Authentizität von Angaben nachgewiesen werden.	2,3
Warnfunktion	Notwendige Voraussetzung zum Schutz vor übereilten, unbedachten Erklärungen. Eine Unterschrift führt z. B. in der Regel zu einer besonderen Aufmerksamkeit und einer Überprüfung des Inhalts einer Erklärung.	1,2,3
Abschlussfunktion	Notwendige Voraussetzung für die räumliche und zeitliche Abgrenzung rechtserheblicher Erklärungen von bloßen Entwürfen, Vorschlägen, etc.	1,2,3

Abbildung 4: Funktionen von Attributen in Verwaltungsprozessen und ihre digitale Umsetzung

HANDLUNGSEMPFEHLUNGEN

Bei der Überführung von Verwaltungsleistungen in den digitalen Raum muss ein besonderes Augenmerk auf die Funktionen gelegt werden, die die dabei verwendeten Attribute des Antragstellers erfüllen sollen. Nötig ist die Schaffung eines für die gesamte deutsche Verwaltung einheitlichen Katalogs, der den jeweiligen Funktionen geeignete technische Maßnahmen zuordnet. Einen solchen Katalog erarbeitet der IT-Planungsrat derzeit in dem Projekt „Föderales Informationsmanagement (FIM)“. Ziel ist die Schaffung einheitlicher, aber erweiterbarer Standards zur Darstellung und Umsetzung von Leistungsbeschreibungen, Formularen und Prozessen.

Auf der Grundlage eines solchen Katalogs können die konkreten Verwaltungsleistungen nach ihrem jeweiligen Sicherheitsniveau klassifiziert und ihre digitale Umsetzung vorgenommen werden. Für elektronische Verwaltungsleistungen muss jeweils die maximal erforderliche Sicherheitsstufe ermittelt und im Prozess angewandt werden – nur bei einem begrenzten Anteil der Prozesse ist tatsächlich die hochsichere Authentifizierung mit der eID-Funktion des neuen Personalausweises notwendig. Dazu muss das im E-Government-Gesetz des Bundes geforderte Normenscreening – also die Überprüfung bestehender Gesetze auf die Möglichkeit, Schriftformerfordernisse zu streichen – durchgängig auch in den entsprechenden Landesgesetzgebungen umgesetzt und harmonisiert werden.

Um bei den verschiedenen Formen der elektronischen Authentifizierung nicht von unterschiedlichsten Systemen und Anbietern abhängig zu sein, sollte ein einheitlicher Identitätsprovider geschaffen werden, der eine Vielzahl an Vertrauensdiensten und weiteren Funktionen abbilden kann: von einfacher Authentifizierung mittels Nutzernamen/Passwort über Zertifikate bis hin zur eID-Funktion des neuen Personalausweises. Dies dient der Vereinheitlichung der Authentifizierung und somit der Kommunikation und Interoperabilität über die kommunalen, Landes- und Ressortgrenzen der Verwaltung. Ein solcher Dienst wird mit der Trusted Service

Plattform entwickelt. Die Auslagerung von diesem Dienst (sofern gewünscht) kann außerdem die Wartungs- und Betriebskosten erheblich senken. In der hier beschriebenen Lösung der Trusted Service Plattform entsteht ein weiterer Vorteil: Alle gängigen Möglichkeiten der technischen Umsetzung zur Identifikation und Authentifizierung werden von vornherein angebunden. Auf diesem Wege kann eine maximale Flexibilität und Nutzerfreundlichkeit bei minimalem Risiko für die Verwaltung erreicht werden.

Weiterhin ist die Trusted Service Plattform um zusätzliche Authentifizierungsmethoden erweiterbar (z. B. elektronische Gesundheitskarte). Damit können Kommunen in Zukunft auch den Vorgaben der Europäischen Kommission gerecht werden, die plant, dass die EU-Mitgliedsstaaten untereinander ihre elektronischen Identifikationslösungen anerkennen sollen. Um das Potenzial der digitalen Verwaltung voll nutzbar zu machen, muss ein solcher Dienst auch über einen „elektronischen Safe“ verfügen, d. h. über die Möglichkeit zur Speicherung elektronischer Dokumente wie Bescheide, Urkunden usw., sodass diese medienbruchfrei in die Verwaltungsprozesse eingehen können. Selbstverständlich müssen dabei der Datenschutz und die Sicherheit der gespeicherten Daten an erster Stelle stehen.

Momentan gibt es bereits in vielen Kommunen und auf Landesebene vorbildliche Projekte für Bürgerkonten, die den Online-Zugang zu diversen Leistungen der jeweiligen Verwaltung bündeln. Diese bauen jedoch auf jeweils eigenen Software-Strukturen auf, sodass die Übertragung von Daten zwischen den einzelnen Systemen – bspw. wenn ein Bürger in eine andere Stadt umzieht – nicht ohne weiteres möglich ist. Bei der Umsetzung des Projekts „Trusted Service Plattform“ ist deshalb auf die Interoperabilität mit bestehenden Bürgerkonten-Lösungen zu achten. So können vorhandene Datensätze weiter genutzt werden, und bewährte Infrastrukturen in den Verwaltungen müssen nicht komplett ersetzt, sondern können ergänzt werden.

FAZIT

Wie eingangs beschrieben bestimmen die zunehmende Digitalisierung und Vernetzung immer mehr Bereiche unseres privaten, gesellschaftlichen, wirtschaftlichen und politischen Handelns. Der Stand der Technik war und ist dabei nie eine Konstante. Vielmehr geben kurze Innovationszyklen den Takt vor und beleben die genannten Bereiche immer wieder neu. Damit die Verwaltung nicht hinter den Erwartungen zukünftiger Zeitreisender bleibt, soll das Projekt „Trusted Service Platform“ technische Potenziale in Hinblick auf eine proaktive, nutzerfreundliche Verwaltung umsetzen.

Die „Trusted Service Platform“ dient dem Bürger dabei als Authentifizierungsdienst gegenüber der Verwaltung und anderen Dienstleistern. Die für die Inanspruchnahme von Verwaltungsleistungen erforderlichen Gesetze und Bestimmungen wie etwa das persönliche Vorsprechen oder die Schriftform erfordern eine geeignete Abbildung im digitalen Raum. Mit Hilfe von adäquaten Sicherheitsstufen der Authentifizierung ist eine entsprechende Umsetzung denkbar.

Hierzu konnten in dem vorliegenden Whitepaper drei Sicherheitsstufen identifiziert werden, die elektronisch abzubilden sind und in einem kurzen Abriss wiederholt werden:

Stufe 1

- Hierunter fallen Verwaltungsleistungen, die von jedem beantragt werden können, ohne eine Authentifizierung zu erfordern. (bspw. einfache Melderegisterauskunft)

Stufe 2

- In Stufe 2 wird für die Erbringung der jeweiligen Verwaltungsleistung meist eine höhere Anzahl persönlicher Daten erfordert. Zudem muss die Nachverfolgbarkeit sichergestellt werden können. Die Missbrauchsgefahr ist hier vergleichsweise gering. (bspw. Beantragung eines Kita-Gutscheines)

Stufe 3

- Verwaltungsleistungen, die mit einer hohen Missbrauchsgefahr einhergehen, und gesetzliche Vorgaben wie etwa das Schriftformerfordernis beanspruchen, sind in Stufe 3 einzuordnen. (bspw. Beantragung eines Reisepasses)

Zudem erfolgte eine Zuordnung der Top-25-Leistungen zu den genannten Sicherheitsstufen. Vor dem Hintergrund des im E-Government-Gesetz des Bundes geforderten Normenscreenings ist ein Zuwachs an Verwaltungsleistungen für Stufe 2 zu erwarten, da es ein erklärtes Ziel ist, die Schriftformerfordernis bei möglichst vielen Leistungen abzubauen.

Um den bestehenden Umsetzungsspielraum aufgrund fehlender allgemeinverbindlicher Richtlinien einzuengen wurden in einem zweiten Schritt ausgewählten Kernfunktionen von Attributen im Verwaltungsprozess die passenden Sicherheitsstufen zugeordnet. Diese Schemata können die Verwaltung bei der Einordnung ihrer Verwaltungsleistungen und der elektronischen Bereitstellungen unterstützen.

Damit wird der Grundstein gelegt für einen einheitlichen Identitätsprovider, der die sichere elektronische Kommunikation persönlicher Daten und Dokumente über Kommunal-, Landes- und Ressortgrenzen hinweg ermöglicht. Damit kann der weiteren Ausbreitung heterogener Lösungslandschaften in der Verwaltung entgegengewirkt und die Interoperabilität entscheidend verbessert werden. Die Trusted Service Platform soll dies ermöglichen und darüber hinaus noch zusätzliche Authentifizierungsmethoden anbieten, die vor dem Hintergrund EU-politischer Bestrebung zukünftig notwendig werden.



**Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS**

Kompetenzzentrum ELAN
Kaiserin-Augusta-Allee 31
10589 Berlin

Ansprechpartner

Marina Grigorian
Tel. +49 30 3463-7388
marina.grigorian@fokus.fraunhofer.de

Jan Ziesing

Tel. +49 30 3463-7312

jan.ziesing@fokus.fraunhofer.de

www.fokus.fraunhofer.de

www.ng-identity.de

Institutsleitung

Prof. Dr. Manfred Hauswirth

Prof. Dr. Ina Schieferdecker

Autoren

Stefanie Hecht

Ulrike Hinz

Markus Wollina

Wolfgang Wunderlich

Jan Ziesing

Bundesdruckerei GmbH

Oranienstrasse 91

10969 Berlin

Ansprechpartnerin

Dr. Ivonne Scherfenberg

ivonne.scherfenberg@bdr.de

www.bundesdruckerei.de



Foto: WTV Verlag/Host Herzig