Bundesministerium des Innern

IT-Planungsrat

Strategie für eID und andere Vertrauensdienste im E-Government (eID-Strategie)

(Steuerungsprojekt Nr. 2 des NEGS-Schwerpunkteprogramms)

(Version 1.0 - Beschlussfassung 12. Sitzung IT-Planungsrat am 02.10.2013)

1. Hintergrund und Leitbild

Die öffentliche Verwaltung in Deutschland stellt zahlreiche Online-Dienste mit dem Ziel bereit, Vorgänge elektronisch abzuwickeln. Diese Dienste beschränken sich allerdings vielfach auf Informations- oder Download-Angebote. Rechtsverbindliche Transaktionsangebote, z.B. für Antragstellungen und Bewilligungen, sind dagegen noch zu selten.

Mit der eID-Funktion des neuen Personalausweises und des elektronischen Aufenthaltstitels (im Folgenden wird der Einfachheit halber nur noch von der eID-Funktion des neuen Personalausweises gesprochen), De-Mail, der qualifizierten elektronischen Signatur und anderen Standards und Technologien gibt es in Deutschland eine gute und solide Basis von Verfahren zu Gewährleistung von Identität, Authentizität, Integrität, Vertraulichkeit und Nachweisbarkeit (im Folgenden Vertrauensdienste). Damit ist die Grundlage vorhanden, um Verwaltungsvorgänge weitgehend medienbruchfrei abzuwickeln. Mit dem E-Government-Gesetz und dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten hat der Gesetzgeber den Einsatz der eID-Funktion des neuen Personalausweises in Verbindung mit elektronischen Formularen und von De-Mail zur Ersetzung der Schriftform für verschiedene Bereiche des E-Government sowie von eJustice ermöglicht und eine Öffnungsklausel für Technologien mit gleichwertiger Sicherheit vorgesehen.

Allerdings werden die vorhandenen Vertrauensdienste aus unterschiedlichen Gründen heute von Verwaltungen häufig noch nicht angeboten oder von Unternehmen, Bürgerinnen und Bürgern zu wenig genutzt.

Um dies zu ändern, muss insbesondere die Akzeptanz für den Einsatz von Vertrauensdiensten bei Verwaltungen sowie bei den nutzenden Unternehmen, Bürgerinnen und Bürgern weiter verbessert werden.

Für die Akzeptanz spielt die einfache Handhabbarkeit der Vertrauensdienste eine zentrale Rolle. Die Nutzer sollen mit möglichst wenigen dieser Verfahren möglichst viele für sie relevante Verwaltungsprozesse abwickeln können. Dies kann zum einen durch Reduzierung der Vielfalt der bestehenden Vertrauensdienste (z.B. unterschiedlicher Identifikationsverfahren) und zum anderen – dort wo es technisch möglich ist - durch gegenseitige Anerkennung und Interoperabilität von Vertrauensdiensten im föderalen System unterstützt werden. Darüber hinaus muss auf Grundlage der gesetzlichen Rahmenbedingen Klarheit darüber bestehen, welche dieser Verfahren für welche Verwaltungsprozesse eingesetzt werden können.

Neben der Akzeptanz spielen auch Datenschutz, Sicherheit und Wirtschaftlichkeit der Verfahren eine wesentliche Rolle. Elektronische Verwaltungsprozesse sollen auf einem Datenschutz- und Sicherheitsniveau abgewickelt werden, das sich aus ihrem Schutzbedarf ergibt. Dabei soll der Einsatz der Verfahren für alle Kommunikationspartner wirtschaftlich sein.

Der IT-Planungsrat hat deshalb als Teil der Umsetzung der Nationalen E-Government-Strategie (NEGS) die Erarbeitung einer eID-Strategie beschlossen. Mit dem vorliegenden Dokument einigen sich Bund, Länder und kommunale Spitzenverbände im IT-Planungsrat auf die folgende gemeinsame **Strategie für eID und andere Vertrauensdienste im E-Government (eID-Strategie)**, durch die ein flächendeckendes Angebot von sicheren elektronischen Verfahren zur Gewährleistung von Identität, Authentizität, Integrität, Vertraulichkeit und Nachweisbarkeit (Vertrauensdienste) in elektronischen Transaktionen erreicht werden soll, das von Bürgerinnen, Bürgern, Unternehmen und der Verwaltung selbst umfassend akzep-

tiert wird. Da der Verbreitung und Nutzung elektronischer Identitäten durch Bürgerinnen, Bürger und Organisationen (z.B. Freiberufler, juristische Personen durch deren Vertretungsberechtigte, Behörden) eine Schlüsselrolle zukommt, steht dieser Bereich im Vordergrund der vorliegenden Strategie und ist ihr Namensgeber. Ausgehend hiervon wird die Strategie im Rahmen der rechtlichen und organisatorischen Weiterentwicklung sowie des technischen Fortschritts sukzessive fortgeschrieben.

Die durch die Strategie getroffenen Festlegungen sollen die Interoperabilität mit entsprechenden Vertrauensdiensten anderer europäischer Staaten sowie auch auf internationaler Ebene berücksichtigen. Festlegungen dieser Strategie werden von deutscher Seite in EU-Rechtssetzungsvorhaben eingebracht.

2. Maßnahmen der eID-Strategie

Im Folgenden werden den Zielen der Strategie (Akzeptanz, Sicherheit und Wirtschaftlichkeit) Maßnahmen zugeordnet. Die Zuordnung richtet sich danach, zu welchem Ziel die jeweilige Maßnahme am meisten beiträgt. Darüber hinaus kann eine Maßnahme auch zur Erfüllung anderer Ziele beitragen.

1. Akzeptanz

Die Verbesserung der Akzeptanz von Vertrauensdiensten bei Bürgerinnen und Bürgern, Unternehmen und Verwaltung ist ein wesentliches Ziel der eID-Strategie, um so eine stärkere Nutzung von E-Government-Diensten bei Bund, Ländern und Kommunen zu erreichen.

Erweiterung der Möglichkeiten zur elektronischen Ersetzung der Schriftform

Die qualifizierte elektronische Signatur hat sich als elektronischer Ersatz zur Schriftform nicht in der breiten Anwendung durchsetzen können. Da bislang viele Verwaltungsdienstleistungen die Schriftform erfordern, sollten gesetzliche Schriftformerfordernisse reduziert werden und weitere sichere Verfahren für die Ersetzung der Schriftform gesetzlich durch Bund, Länder und Kommunen ermöglicht und praktisch angeboten werden.

Maßnahme M1: Anpassung von Rechtsvorschriften	
bis Ende 2016	Mit dem E-Government-Gesetz werden der Einsatz der eID-Funktion des neuen Personalausweises in Zusammenhang mit elektronischen Formularen von Behörden und De-Mails mit der Versandoption „absenderbestätigt“ zur Ersetzung der Schriftform neben der qualifizierten elektronischen Signatur für verschiedene Bereiche des E-Government ermöglicht. Der IT-Planungsrat setzt sich dafür ein, dass Bund, Länder und Kommunen in den Rechtsvorschriften der jeweiligen Verantwortungsbereiche analog zu den Regelungen des E-Government-Gesetzes weitere Möglichkeiten für den Einsatz des neuen Personalausweises und/oder von De-Mail zur Ersetzung der Schriftform sowie für diejenigen Fälle schaffen, bei denen in Rechtsvorschriften bisher explizit nur die qualifizierte elektronische Signatur vorgeschrieben ist.
Maßnahme M2: Zugangseröffnung für den neuen Personalausweis und De-Mail	
bis Ende 2016	Im Bereich des Bundes wird die Zugangseröffnung wie im E-Government-Gesetz vorgesehen ab Anfang 2015 erfolgen. Der IT-Planungsrat setzt sich dafür ein, dass auch die Länder mit ihren Kommunen auf Ebene der Behörden den elektronischen Zugang zu Verwaltungsdienstleistungen mit der eID-Funktion des neuen Personalausweises und mit De-Mail eröffnen – die einzelnen Behörden also grundsätzlich in der Lage sind, Verwaltungsvorgänge mit der eID-Funktion des neuen Personalausweise und/oder mit De-Mail abzuwickeln.

Einfache Handhabbarkeit

Für die Akzeptanz spielt die einfache Handhabbarkeit von Vertrauensdiensten eine herausragende Rolle. Auf Seiten der Verwaltung müssen die Vertrauensdienste möglichst einfach und mit vertretbarem Aufwand in die bestehende Landschaft integriert werden können. Für Bürgerinnen, Bürger und Unternehmen müssen die Vertrauensdienste möglichst einfach zu bedienen sein.

Maßnahme M3: Handreichungen des Bundes	
bis Ende 2013	Der Bund erarbeitet als Ergebnis der gegenwärtig durchgeführten E-Government-Initiative und weiterer bereits vorliegender Informationsunterlagen einen Katalog wesentlicher Handreichungen, mit denen die Anwendung der eID-Funktion des neuen Personalausweises und von De-Mail für Verwaltungen, Bürgerinnen, Bürger und Unternehmen vereinfacht wird. Der Katalog der Handreichungen wird auf der Webseite des IT-Planungsrats veröffentlicht.
Maßnahme M4: Handreichungen des IT-Planungsrats	
bis Ende 2014	Der IT-Planungsrat erarbeitet Handreichungen, mit denen die Anwendung der vom IT-Planungsrat mit Maßnahme M5 empfohlenen weiteren Vertrauensdienste für Verwaltungen, Bürgerinnen, Bürger und Unternehmen vereinfacht wird. Dies beinhaltet auch Empfehlungen zur Integration der Vertrauensdienste in die IT-Verfahren der einsetzenden Behörden sowie die Beschreibung langfristiger Modelle für den Betrieb der benötigten Infrastrukturkomponenten. Diese Handreichungen werden durch den IT-Planungsrat veröffentlicht.

Die einfache Handhabbarkeit soll aber auch dadurch unterstützt werden, dass die Nutzer mit möglichst wenigen dieser Verfahren möglichst viele für sie relevante fachliche Verwaltungsprozesse abwickeln können. Diese Zielsetzung soll auch dadurch erreicht werden, dass grundsätzlich die Vielfalt der durch die Verwaltung angebotenen unterschiedlichen Vertrauensdienste (z.B. im Bereich Identifizierung) reduziert wird.

Maßnahme M5: Empfehlung für den Einsatz von Vertrauensdiensten	
bis Ende 2014	Die Projektgruppe eID-Strategie wird dem IT-Planungsrat auf Grundlage der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen einer Technischen Richtlinie erarbeiteten Kriterien (siehe Maßnahme M10) vorschlagen, welche Vertrauensdienste für welche typischen Verwaltungsleistungen, insbesondere solche mit hoher Fallzahl zum Einsatz kommen sollen. Hierbei werden u.a. auch die Identifizierung über Bürgerkonten, über mobile Endgeräte sowie die Identifizierung von Unternehmen/Institutionen berücksichtigt. Als weitere Kriterien werden die einfache Handhabbarkeit, Nutzerfreundlichkeit, IT-Sicherheit, wirtschaftlicher Einsatz für die beteiligten Kommunikationspartner, Verbreitung, flexible Integration in Fachprozesse, Barrierefreiheit und datenschutzgerechter Einsatz zu Grunde gelegt. Betrachtet werden sollen dabei insbesondere auch bestehende und im Einsatz befindliche Infrastrukturen und die Möglichkeiten zur Nutzung von Lösungen anderer Mitgliedsstaaten der Europäischen Union vor dem Hintergrund der in der vorgeschlagenen EU-Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgesehenen Pflicht zur gegenseitigen Anerkennung. Die Vorschläge berücksichtigen Arbeiten des Normenkontrollrates (NKR), Ergebnisse relevanter IT-Planungsrat-Projekte (insbesondere Föderales Informationsmanagement (FIM), Nationale Prozessbibliothek, Prozessdatenbeschleunigerund LEIKA) sowie bestehende Infrastrukturen (wie z.B. nPA, De-Mail, SAFE, EGVP, Identifizierungsmittel anderer EU-Mitgliedsstaaten).

Maßnahme M6: Berücksichtigung der empfohlenen Vertrauensdienste in der Standardisierungsagenda	
bis Ende 2014	Der IT-Planungsrat entscheidet, wie die Vorschläge aus Maßnahme M5 in der Standardisierungsagenda berücksichtigt werden und macht Vorschläge, wie diese in künftigen Rechtsvorschriften berücksichtigt werden können. Die Ergebnisse sollen in den Evaluierungsbericht nach Artikel 30 Absatz 2 des Entwurfes eines Gesetzes zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) einfließen.

Um die Akzeptanz der Online-Verfahren zu verbessern bieten einzelne Länder und Verwaltungen bereits heute Bürgerkonten an oder planen diese. Hierbei lassen sich zwei Modelle unterscheiden.

Modell A: Temporäres Bürgerkonto

Bei Modell A wird auf Basis eines für alle einschlägigen Dienste geltenden Berechtigungszertifikats (z.B. in einem Portal) die Authentisierung mit der Online-Ausweisfunktion des neuen Personalausweises angeboten. Die an das Portal angeschlossenen Behörden müssen die Authentisierungsfunktion also nicht selbst anbieten; den verschiedenen fachlichen Verwaltungsdiensten dieser Behörden werden die beim Nutzer des neuen Personalausweis angefragten Identitätsdaten zum Zweck der Identifizierung des Nutzers über eine technische Schnittstelle übermittelt. Die Identitätsdaten sind bei Modell A langfristig nur auf dem Personalausweis gespeichert, eine langfristige Speicherung der Identitätsdaten an anderer (zentraler) Stelle ist nicht erforderlich.

Modell B: Permanentes Bürgerkonto

Bei Modell B werden die Identitätsdaten des Nutzers im Bürgerkonto langfristig gespeichert. Der Nutzer kann sich später erneut anmelden und die im Bürgerkonto gespeicherten Identitätsdaten zur Identifizierung an einem angeschlossenen einschlägigen Verwaltungsverfahren freigeben. Da die Identitätsdaten in Modell B im Bürgerkonto gespeichert sind, können hier unter Umständen neben dem neuen Personalausweis auch weitere Authentisierungsverfahren (z.B. Softwarezertifikate) angeboten werden. Modell B bietet die Möglichkeit zusätzlich persönliche Daten, wie z.B. die Bankverbindung, im Bürgerkonto zu speichern, die nach Freigabe durch den Nutzer an das vom Nutzer angeforderte / aufgerufene Verwaltungsverfahren weiter gegeben werden. Hierdurch können beispielsweise Antragsverfahren mittels automatischer Befüllung von Formularen vereinfacht werden.

Beide Modelle erleichtern die Anwendung des neuen Personalausweises und vereinfachen Identifizierungsprozesse für Verwaltungen, Bürgerinnen und Bürger.

Maßnahme M7: Ausbau der Bürgerkonten	
bis Oktober 2014	Der IT-Planungsrat befürwortet den datenschutzgerechten Einsatz temporärer und permanenter Bürgerkonten. Auf Basis der bestehenden und geplanten Lösungen für Bürgerkonten erarbeitet er eine Handreichung, in der Empfehlungen für mögliche Nachnutzungen im Sinne eines Wissenstransfers zusammengefasst werden und ggf. weiterer Handlungsbedarf des IT-Planungsrates aufgezeigt wird.

Modell B kann später dahingehend erweitert werden, dass eine Interoperabilität der in den Bürgerkonten gespeicherten Identitäten auf Basis von Standards ermöglicht wird. Ein Nutzer (Bürger, Unternehmen) kann so beispielsweise seine in einem bestehenden Bürgerkonto gespeicherten Identitätsdaten nutzen, um sich an einem elektronischen Verwaltungsverfahren in einem anderen Bundesland oder bei einer Bundesbehörde anzumelden. Konkrete Anwendungsfälle und technische und datenschutzrechtliche Machbarkeit werden im Rahmen einer Studie des IT-Planungsrates bewertet.

Maßnahme M8: Studie für ein interoperables Identitätsmanagement	
bis Oktober 2014	Der IT-Planungsrat erarbeitet eine Studie zu Anwendungsfällen und technischer Machbarkeit der beschriebenen Erweiterung von Modell B hin zu einem „interoperablen Identitätsmanagements“. Die Erfahrungen aus den Koordinierungsprojekten des IT-Planungsrates werden hierbei berücksichtigt (z.B. S.A.F.E.).

Kommunikation

Der Aufbruch der Verwaltung in das Online-Zeitalter bedarf der Begleitung durch gezielte Informationen zu den Inhalten und Methoden des eGovernment im Allgemeinen und der eID-Strategie im Besonderen. Die bisher laufenden Maßnahmen wie Auftritte im Internet, auf Messen und Konferenzen, Handreichungen und zielgruppenspezifische Veranstaltungen sollten aufeinander abgestimmt und damit aufgewertet werden. Gleichzeitig muss die Rückkopplung mit Verwaltungen, Unternehmen, Bürgerinnen und Bürgern dazu führen, dass der IT-Planungsrat auf sich ändernde Gegebenheiten aktiv und vorausschauend eingehen kann.

Maßnahme M9: Kommunikationskonzept	
bis Oktober 2014	Der IT-Planungsrat erarbeitet ein Kommunikationskonzept, mit dem die in dieser Strategie getroffenen Festlegungen und deren sukzessive Umsetzung in geeigneter Weise in die Verwaltung hinein und gegenüber den Bürgerinnen, Bürgern und Unternehmen kommuniziert werden. Eine erste Version des Kommunikationskonzepts wird nach Beschluss dieser Strategie veröffentlicht.

2. Sicherheit

Die Gewährleistung der Sicherheit der künftig im E-Government eingesetzten Vertrauensdienste ist ein wichtiges Ziel. Abhängig vom Schutzbedarf der jeweiligen Verwaltungsdienstleistung werden die Vertrauensdienste Sicherheit insbesondere im Hinblick auf Identität, Authentizität, Integrität, Vertraulichkeit und Nachweisbarkeit gewährleisten.

Hierbei wird insbesondere vor dem Hintergrund des Schutzbedarfes der jeweiligen Verwaltungsdienstleistungen wie folgt zu unterscheiden sein:

1. Verwaltungsdienstleistungen, bei denen ein gesetzliches Schriftformerfordernis besteht:

   Hierfür können ausschließlich die in § 3a VwVfG des Bundes bzw. den entsprechenden Landesvorschriften genannten Vertrauensdienste eingesetzt werden (nach § 3a VwVfG des Bundes neuer Personalausweis, De-Mail, qualifizierte elektronische Signatur sowie Vertrauensdienste, die zukünftig im Rahmen der dort vorgesehenen Öffnungsklausel durch Rechtsverordnung zugelassen werden).

2. Verwaltungsdienstleistungen, bei denen eine sichere Identifizierung (d.h. die Feststellung der Identität eines Bürgers/einer Bürgerin um nachfolgend Verwaltungsdienste in Anspruch zu nehmen) gesetzlich gefordert oder geboten ist:

Hier können neben der eID-Funktion des neuen Personalausweises und De-Mail weitere Vertrauensdienste zugelassen werden, die über eine gleichhohe Sicherheit zur Identifizierung verfügen.

3. Verwaltungsdienstleistungen, die nicht unter 1. und 2. fallen:

   Hier kann abhängig vom Schutzbedarf der jeweiligen Verwaltungsdienstleistung ein geeigneter und angemessener Vertrauensdienst eingesetzt werden.

Maßnahme M10: Technische Richtlinie für Vertrauensdienste	
bis Ende 2013	Das BSI wird unter Berücksichtigung der unter „2. Sicherheit“ dargestellten Vorgaben den Entwurf einer Technischen Richtlinie (TR) vorlegen, in der Vertrauensniveaus und entsprechende Kriterien für Vertrauensdienste definiert werden.

3. Wirtschaftlichkeit

Bürgerinnen, Bürger und Unternehmen sollen Vertrauensdienste der Verwaltung mit möglichst geringem Aufwand nutzen können. Auf Seiten der Verwaltung sollen die ausgewählten Vertrauensdienste ebenfalls mit vertretbarem Aufwand umgesetzt werden können.

Die Wirtschaftlichkeit des Einsatzes der Vertrauensdienste für die beteiligten Partner ist Grundlage der Empfehlung des IT-Planungsrates (Maßnahme M5). Im Sinne der Vorgaben zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung (Wibe) werden hierbei auch qualitativ-strategische Kriterien, externe Effekte und die Dringlichkeit der Maßnahmen zu Grunde gelegt. Die Reduktion von Kosten aufgrund von Schäden, die durch den abgestimmten Einsatz von Vertrauensdiensten vermieden werden können und die Vermeidung von Doppelentwicklungen bei Bund, Ländern und Kommunen durch verbesserte Koordination bei Entwicklung und Einsatz von Vertrauensdiensten sind hierbei Einflussfaktoren, die sich auf die Gesamtbewertung der Wirtschaftlichkeit auswirken können.

Zusätzlich unterstützen die mit Maßnahmen M3 und M4 erarbeiteten Handreichungen den wirtschaftlichen Einsatz der empfohlenen Vertrauensdienste durch die Verwaltung.