IT-PLANUNGSRAT

Empfehlungen für die Zuordnung von Vertrauensniveaus in der Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern

Handreichung

Stand: 18.12.2023, Version 5.00

Inhaltsverzeichnis

Vorbemerkung

Die Empfehlungen dieser Handreichung lassen die Zuständigkeiten des Bundes und der Länder sowie des Fachgesetzgebers zur Regelung von Vertrauensniveaus unberührt.

1. Begriffsdefinitionen

§ 2 Abs. 5 Onlinezugangsgesetz (OZG) unterscheidet zwischen zwei Arten von „Nutzerkonten“ für den elektronischen Zugang zu Verwaltungsleistungen: „Bürgerkonten“ für natürliche Personen und „Organisationskonten“[1] insbesondere für juristische Personen und Vereinigungen. Diese Handreichung befasst sich ausschließlich mit Bürgerkonten.

Gemäß § 2 Abs. 5 Satz 3 OZG steht das Bürgerkonto natürlichen Personen zur Verfügung. Für die Abwicklung von Online-Leistungen werden die Bürgerkonten den Antragstellenden (Bürgerinnen und Bürger) für die Identifizierung und Authentifizierung angeboten. Die Bürgerkonten bieten darüber hinaus auch Servicefunktionen (z. B. ein Postfach für die Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern) und werden daher auch als Servicekonten oder Service-Konten bezeichnet. In manchen Fällen wird auch der Oberbegriff Nutzerkonten im Bereich der Bürgerkonten verwendet, ohne hierbei einen Bezug zu den Organisationskonten zu beabsichtigen.

2. Anwendungsbereich und Zielsetzungen der Handreichung

2.1 Ausgangslage

Die Identität eines Nutzers kann auf unterschiedlichen Vertrauensniveaus[2] festgestellt werden. Um die Identität eines Nutzers mit angemessener Sicherheit festzustellen, muss für eine Online-Verwaltungsleistung das notwendige Vertrauensniveau festgelegt werden. Gemäß § 8 Abs. 1 Satz 1 OZG muss ein Nutzerkonto die Verwendung des für das jeweilige Verwaltungsverfahren erforderlichen Vertrauensniveaus ermöglichen. Im Rahmen der Projekt-

[1] Das „Organisationskonto“ wird teilweise auch als „(zentrales/einheitliches) Unternehmenskonto“ bezeichnet.
[2] Siehe Definitionen in Kapitel 3.

gruppe (PG) eID-Strategie des IT-Planungsrates wurde sich auf die Verwendung der Vertrauensniveaus „hoch“ und „substantiell“ der eIDAS-Verordnung[3] und zusätzlich der „Basisregistrierung“ verständigt.[4] Die Fachverantwortlichen für die Verwaltungsleistung ermitteln das jeweils erforderliche Vertrauensniveau der Verwaltungsleistungen in ihrem Zuständigkeitsbereich. Insgesamt betrifft dies mehrere tausend Verwaltungsverfahren auf allen Verwaltungsebenen.

2.2 Anwendungsbereich

Die vorliegende unverbindliche Handreichung will die zuständigen Behörden bei der Ermittlung von Vertrauensniveaus von Verwaltungsleistungen unterstützen. Die Handreichung lässt die Kompetenzen von Bund, Ländern und Kommunen zur Regelung des Verwaltungsverfahrens und der Verwaltungsorganisation gem. Art. 83 ff. Grundgesetz unberührt. Insbesondere steht die Handreichung der Befugnis von Bund, Ländern und Kommunen nicht entgegen, für ihren jeweiligen Zuständigkeitsbereich eigene Regelungen für die Ermittlung von Vertrauensniveaus für Verwaltungsverfahren festzulegen. Gleiches gilt für die Zuständigkeit des Fachgesetzgebers bzw. der zuständigen Fachbehörden, eigene Regelungen für die Ermittlung von Vertrauensniveaus im Rahmen der jeweiligen Fachverfahren, wie z. B. dem Steuerrecht, dem Sozialrecht, dem Beamten- und Haushaltsrecht, dem Sicherheits- und Ordnungsrecht und dem Leistungsverwaltungsrecht, festzulegen.

Die vorliegende Handreichung soll als übergreifende Orientierungshilfe dienen. Aus der Handreichung folgt aber nicht, dass Verwaltungsverfahren der gleichen Sachmaterie (z. B. Kita-Anmeldung), die nach Landesrecht in den Bundesländern unterschiedlich geregelt sind, auch demselben Vertrauensniveau zugeordnet werden müssen. Wenn z. B. in einem Bundesland A für ein bestimmtes Landesverfahren die Angabe von zusätzlichen personenbezogenen Daten erforderlich ist, die das Bundesland B nicht vorsieht, kann dies auch zu abweichenden Vertrauensniveaus führen. Ähnlich kann die Situation sein, wenn ein Bundesland A an ein

[3] Die eIDAS-Verordnung (Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments) befasst sich u. a. mit den Themen elektronische Identifizierung und Vertrauensniveaus bei elektronischen Transaktionen (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014R0910).

[4] Hinzu kommt das Vertrauensniveau „niedrig“, welches gemäß Beschluss der PG eID-Strategie vom 28.06.2021 in Bund und Ländern bei den Bürgerkonten bis auf weiteres nicht eingesetzt wird.

bestimmtes Landesverfahren (teilweise) andere Rechtsfolgen als ein Bundesland B knüpft, etwa in Form von Leistungsansprüchen.

2.3 Informationssicherheit, Verhältnismäßigkeitsgrundsatz und Nutzerorientierung

Die Empfehlungen sollen die Ziele der Informationssicherheit mit dem Ziel der Nutzerfreundlichkeit und dem Grundsatz der Verhältnismäßigkeit in Einklang bringen.[5] Die vorliegenden Empfehlungen sollen und können daher nicht schematisch angewandt werden. Vielmehr ist bei der Anwendung und Auslegung sämtlicher Kriterien der Handreichung immer neben dem Ziel der Gewährleistung eines hinreichend sicheren Verfahrens, auch das Ziel der Gewährleistung eines möglichst nutzerfreundlichen Verfahrens mit in den Blick zu nehmen.
Zudem ist in jedem Einzelfall zu prüfen, ob die jeweilige Verwaltungsleistung tatsächlich im Hinblick auf Missbrauchsrisiken und den damit einhergehenden möglichen Schadensauswirkungen besonders kritisch ist.

2.4 Erfordernis einer Gesamtbetrachtung

Bei der Ermittlung von Vertrauensniveaus von Verwaltungsleistungen ist eine Gesamtbetrachtung unter Berücksichtigung der analogen Welt anzuraten. Stellt man z. B. fest, dass ein Antrag bislang mit Selbstauskünften und ohne persönliches Erscheinen gestellt werden kann, so ist dies ein Indiz, dass die „Basisregistrierung“ für die elektronische Antragstellung ausreichend sein kann.

Auch der Gesamtprozess kann wertvolle Erkenntnisse liefern: So könnte z. B. der digitale Antrag auf Ausstellung eines „Gesundheitszeugnisses“ (d. h. Belehrungen des Lebensmittelpersonals gem. §§ 42, 43 Infektionsschutzgesetz) auf den ersten Blick auf Grund des Gesundheitsdatenschutzes besonders kritisch und damit auf dem Vertrauensniveau „hoch“ einzustufen sein. Bei näherer Betrachtung stellt sich jedoch heraus, dass vor Erstellung des Gesundheitszeugnisses ein Termin beim Gesundheitsamt, zum Zweck der Belehrung, zwingend

[5] Siehe außerdem § 2 Abs. 2 IT-Sicherheitsverordnung Portalverbund zur Einhaltung des Standes der Technik. Ferner sind die datenschutzrechtlichen Einordnungen von Portallösungen und Fachanwendungen in der OZG-Umsetzung zu berücksichtigen.

erforderlich ist. Der konkrete digitale Antrag hat also nur eine Terminvereinbarung beim Gesundheitsamt zur unmittelbaren Folge. Da sich die Antragstellerin oder der Antragsteller beim Termin dann persönlich ausweisen muss, erscheint ein Missbrauch hier praktisch nicht oder kaum möglich. Von daher kann hier sogar eine „Basisregistrierung“ ausreichend sein.

Auch in anderen Fällen wird sich zeigen, dass einfache digitale Anträge der Bürgerinnen und Bürger (also der Kerngehalt des OZG) unter Gesichtspunkten der Sicherheit oft eher unproblematisch sind und daher kein erhöhtes Vertrauensniveau erfordern.

3. Ausgangssituation und Begriffsdefinitionen

Um Online-Verwaltungsleistungen zu nutzen, müssen sich Antragsteller angemessen identifizieren. In der analogen Welt erfolgt die sichere Identifikation des Antragsstellers etwa dadurch, dass der Personalausweis vorgezeigt oder etwa eine Ausweiskopie beigefügt werden muss.

Im digitalen Raum erfolgt die Identifizierung dagegen in der Regel über ein Nutzerkonto (z. B. über ein Bürgerkonto). Die Anmeldung und Identifizierung am Bürgerkonto ist auf verschiedenen Vertrauensniveaus möglich. Das Vertrauensniveau, welches für jede Online-Verwaltungsleistung ermittelt werden muss, gibt dabei an, wie sicher bzw. wie vertrauenswürdig die Herkunft der Daten der Nutzerinnen und Nutzer ist, die an die Online-Verwaltungsleistung übermittelt werden. Je nach Vertrauensniveau stehen verschiedene Anmeldemöglichkeiten für die Identifizierung zur Verfügung. Die unterschiedlichen Anmeldemöglichkeiten werden zentral durch die Nutzerkonto-Anbieter festgelegt und müssen nicht durch die für das Verwaltungsverfahren zuständige Behörde selbst ausgewählt werden. Beispiele hierzu finden sich in den nachfolgenden Abschnitten. Welche Anmeldung bzw. Identifizierung an einem Bürgerkonto erforderlich ist, ist dabei abhängig vom Vertrauensniveau der betreffenden Verwaltungsleistung.

Aufgabe der zuständigen Behörde ist es, das Vertrauensniveau der einzelnen Verwaltungsleistungen in ihrem Zuständigkeitsbereich zu ermitteln. Nach der eIDAS-Verordnung kann ein Vertrauensniveau[6] eine von drei Stufen annehmen:

- „niedrig“: umfasst begrenzte und überschaubare Schadensauswirkungen bei einem Sicherheitsvorfall bzw. einer Kompromittierung
- „substantiell“: umfasst substantielle Schadensauswirkungen bei einem Sicherheitsvorfall bzw. einer Kompromittierung
- „hoch“: umfasst beträchtliche Schadensauswirkungen bei einem Sicherheitsvorfall bzw. einer Kompromittierung.

Neben den drei Vertrauensniveaus der eIDAS-Verordnung wurde durch die PG eID-Strategie zudem eine sogenannte „Basisregistrierung“ eingeführt.[7] Hierbei handelt es sich um ein Angebot zur niederschwelligen Kontonutzung ohne Überprüfung der Identität.

Vor dem Hintergrund, dass sich die Abgrenzungen und Bezeichnungen der Vertrauensniveaus in Deutschland im Zeitverlauf verändert haben, finden sich in anderen Dokumenten teilweise abweichende Bezeichnungen von Vertrauensniveaus.[8] Sind diese Vertrauensniveaus einer Online-Leistung zugeordnet, ist ggf. eine erneute Ermittlung des Vertrauensniveaus unter Berücksichtigung der vorliegenden Handreichung erforderlich.[9]

Zwischen Vertrauensniveau und Schutzbedarf (nach IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[10]) besteht ein teilweiser Zusammenhang. Der Schutzbedarf nach IT-Grundschutz betrachtet die Schutzwürdigkeit der Daten als Ganzes

[6] In der deutschen Übersetzung der eIDAS-Verordnung werden die Vertrauensniveaus als Sicherheitsniveaus bezeichnet. Im Fachkontext geläufiger ist jedoch die Bezeichnung Vertrauensniveau. Daher wird diese auch in diesem Dokument bevorzugt verwendet.
[7] Vgl. auch Fußnote 8 zu weiteren, abweichenden Bezeichnungen von Vertrauensniveaus.
[8] Hierzu zählen „untergeordnet“ (entspricht im Wesentlichen der „Basisregistrierung“), „normal“ (entspricht im Wesentlichen dem Vertrauensniveau „niedrig“) und „hoch +“ (bezieht sich auf besondere Formvorschriften, welche über das Vertrauensniveau „hoch“ hinausgehen).
[9] Darüber hinaus ist auch eine regelmäßige Überprüfung der Vertrauensniveaus der Online-Leistungen zu empfehlen.
[10] Informationen zum Thema IT-Grundschutz sind der Webseite des BSI zu entnehmen (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html).

während der Datenverarbeitung. Das Vertrauensniveau betrachtet dagegen lediglich, wie sicher bzw. wie zuverlässig die Identität eines Nutzers festgestellt wurde.

Erfordert ein Verwaltungsverfahren das Vertrauensniveau „hoch“, so ist in der Regel ebenfalls von mindestens einem hohen Schutzbedarf nach IT-Grundschutz auszugehen, um sicherzustellen, dass die erhobenen und geprüften Identitätsdaten nicht manipuliert werden können.

Eine Ableitung in die entgegengesetzte Richtung ist jedoch nicht zulässig. So kann für ein Verwaltungsverfahren eine „Basisregistrierung“ des Nutzers ausreichend sein, die Datenverarbeitung als Ganzes jedoch mit einem hohen Schutzbedarf bewertet werden. Je nach genutzten Definitionen zur Bewertung des Schutzbedarfes ist häufig etwa bereits von einem hohen Schutzbedarf nach IT-Grundschutz auszugehen, wenn personenbezogene Daten verarbeitet werden.

Je nach Vertrauensniveau kommen unterschiedliche Vertrauensmechanismen zum Einsatz. Das heißt, je höher das Vertrauensniveau ermittelt wird, desto zuverlässiger müssen die genutzten Methoden zur Anmeldung und Identifizierung der Antragstellerin oder des Antragstellers sein. Die Wahl des konkreten Identifizierungsmittels ist dabei abhängig vom Stand der Technik und dem Angebot auf dem Markt. Hier können sich Veränderungen ergeben. Daher ist es wichtig, dass für die Verwaltungsleistung nur das Vertrauensniveau, nicht jedoch das konkrete Identifizierungsmittel festgelegt wird.
I. d. R. werden in Bürgerkonten zur Authentisierung folgende Technologien angeboten:[11]

- „Basisregistrierung“: Benutzername und Passwort
- Vertrauensniveau „niedrig“: *Bis auf weiteres durch Bund und Länder bei den Bürgerkonten nicht eingesetzt; bei Online-Leistungen, für welche bisher das Vertrauensniveau „niedrig“ ermittelt wurde, ist der Einsatz von Authentifizierungsmitteln auf dem Vertrauensniveau „substantiell“ zu prüfen.*

[11] Bund und Länder haben sich verständigt, dass das Vertrauensniveau „niedrig“ in Bund und Ländern bei den Bürgerkonten bis auf weiteres nicht eingesetzt wird.

- Vertrauensniveau „substantiell“: ELSTER-Zertifikate[12] als Identifizierungsmittel.
- Vertrauensniveau „hoch“: Elektronischer Identitätsnachweis mittels Online-Ausweisfunktion des Personalausweises, eID-Karte bzw. elektronischen Aufenthaltstitels (eAT)[13].

Daneben gibt es verschiedene auf den Vertrauensniveaus „substantiell“ und „hoch“ gemäß eIDAS-Verordnung notifizierte Identifizierungsmittel aus anderen EU-Ländern, für die teilweise eine Anerkennungspflicht besteht.

Die PG eID-Strategie des IT-Planungsrates legt unter Beteiligung des BSI fest, welche Identifizierungs- und Authentisierungslösungen in Bürgerkonten zum Einsatz kommen (s. Anhang: Ermittlung der möglichen Vertrauensmechanismen).

Bei Aktualisierung von Fachgesetzen und Fachnormen müssen die für das jeweilige Verwaltungsverfahren zuständigen Behörden daher, sofern eine spezifische Vorgabe angedacht ist, nur das mindestens zu erfüllende Vertrauensniveau der Verwaltungsleistung, welches durch die Bürgerinnen und Bürger zu erreichen ist, angeben (z. B. Vertrauensniveau „hoch“) und nicht den Vertrauensmechanismus (z. B. Einsatz des elektronischen Personalausweises, der eID-Karte bzw. des elektronischen Aufenthaltstitels). Andernfalls besteht die Gefahr, dass die Vorgabe nicht durch alle Anbieter von Bürgerkonten umgesetzt werden kann bzw. dass die Vorgabe nicht mehr dem Stand der Technik entspricht.

Die Ermittlung des Vertrauensniveaus liegt derzeit in der Zuständigkeit der für das jeweilige Verwaltungsverfahren zuständigen Behörde als Fachverantwortliche, welche die Vollzugskompetenz innehat. Somit ist es möglich, dass für gleichartige Verwaltungsleistungen unterschiedliche Vertrauensniveaus ermittelt werden. Empfohlen wird eine Abstimmung zwischen den Fachkolleginnen und -kollegen in den Ländern.

[12] Ein Einsatz von ELSTER-Zertifikaten in weiteren EU-Mitgliedsstaaten ist nicht möglich, da das Verfahren nicht notifiziert wurde.
[13] Das Vertrauensniveau des elektronischen Identitätsnachweises mit einem mobilen Endgerät („Smart-eID“) ist noch zu bestimmen.

4. Zielgruppen der Handreichung

Die Handreichung richtet sich an Fachverantwortliche für Online-Leistungen. Zielsetzung ist es, mit dieser Handreichung bei der Ermittlung von Vertrauensniveaus zu unterstützen. Hierfür werden Empfehlungen für die Einstufung von Vertrauensniveaus gegeben.

Wurde eine Einschätzung zum Vertrauensniveau vorgenommen, sollte diese mit den IT-Sicherheits- und Datenschutzbeauftragten der Behörde abgestimmt werden.

Abbildung 1 gibt einen Überblick über die jeweiligen Akteure, welche im Prozess der Ermittlung des Vertrauensniveaus involviert sind. Die einzelnen Rollen werden im Nachgang noch genauer erläutert:

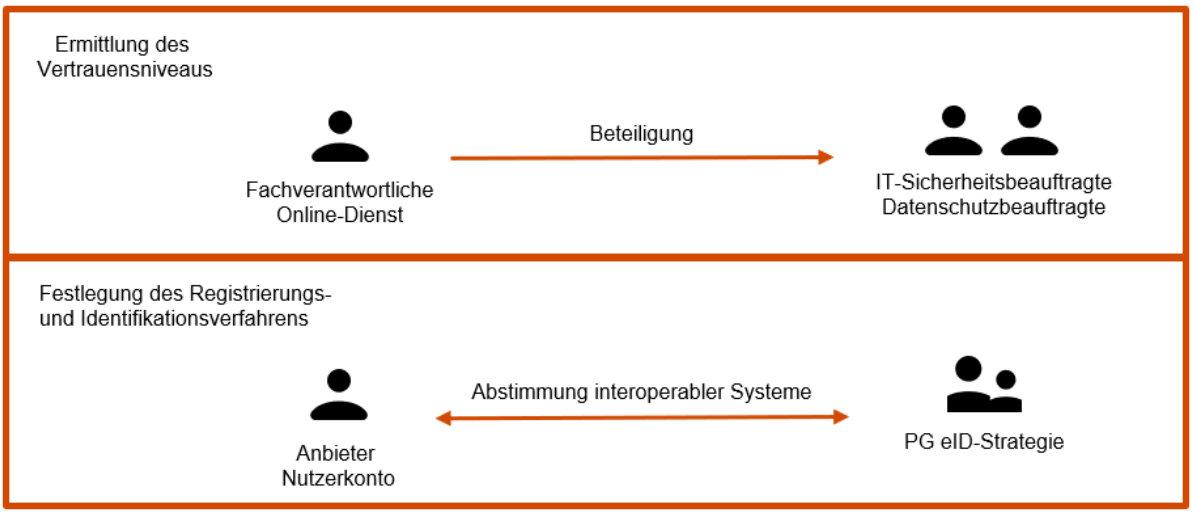

Abbildung 1: Übersicht der Rollen und Aufgaben bei der Ermittlung des Vertrauensniveaus und der Festlegung des Registrierungs- und Identifikationsverfahrens

Die Rollen und Aufgaben sind wie folgt verteilt:

- Fachverantwortliche Online-Dienst: ermittelt Vertrauensniveau.
- IT-Sicherheitsbeauftragte: werden bei Ermittlung des Vertrauensniveaus beteiligt.
- Datenschutzbeauftragte: werden bei Ermittlung des Vertrauensniveaus beteiligt.
- PG eID-Strategie des IT-Planungsrates unter Beteiligung des BSI: entscheidet, welche Registrierungs- und Identifikationsverfahren im Zusammenhang von interoperablen Bürgerkonten bei den jeweiligen Vertrauensniveaus zum Einsatz kommen.

- Anbieter Nutzerkonto: bieten Nutzerkonten als zentrale Identifizierungs- und Authentifizierungskomponenten an.

Hinzu kommt das Digitalisierungsprogramm des IT-Planungsrates, welches Empfehlungen zur Ermittlung des Vertrauensniveaus für ausgewählte Verwaltungsleistungen gibt.

5. Gesetzliches Schriftformerfordernis

Die Anforderung einer Schriftform ist unabhängig von der Einstufung eines Vertrauensniveaus umzusetzen. In Fällen, in denen ein gesetzliches Schriftformerfordernis geregelt ist, sind die Vorgaben zum elektronischen Schriftformersatz (§ 3 a VwVfG bzw. vergleichbare Landesvorschriften und Fachgesetze) zu berücksichtigen.

6. Empfehlungen für die Zuordnung von Vertrauensniveaus

Anforderungen an das Vertrauensniveau können sich z. B. in Bezug auf die Vertraulichkeit oder auf die Übermittlung von Dokumenten (Bescheid, Rückkanal) ergeben. In der Dokumentation zur Ermittlung des Vertrauensniveaus sollte zusätzlich vermerkt werden, dass eine Schriftform besteht und aus welcher Vorgabe diese abgeleitet wird.

Im Folgenden werden zwei Beispiele benannt, bei denen ein elektronischer Schriftformersatz realisiert wurde:

- Beantragung polizeiliches Führungszeugnis beim Bundesamt für Justiz unter https://www.fuehrungszeugnis.bund.de
- Online-Registerauskunft beim Kraftfahrt-Bundesamt unter https://www.kba-online.de/registerauskunft/app/#/

Unabhängig vom Schriftformerfordernis muss die betrachtete Verwaltungsleistung jedoch nicht automatisch das Vertrauensniveau „hoch“ erfordern.

1 Für die Verwaltungsleistung sollte das erforderliche Vertrauensniveau jeweils auf folgende Prozesse bezogen ermittelt werden:

i. **Identifizierung**: Im Rahmen einer Registrierung wird die Identität einer natürlichen Person erfasst und elektronisch gespeichert.
ii. **Willenserklärung**: Die Äußerung eines auf die Herbeiführung einer Rechtswirkung gerichteten Willens durch eine erklärende Person, wie die Zustimmung zu einem Vorgang oder dem Inhalt eines Dokumentes.
iii. **Dokumentenübermittlung**: Die beidseitige Übermittlung von Dokumenten zwischen Personen und Behörde oder der Abruf von Informationen von einer Behörde durch eine identifizierte bzw. authentifizierte Person.

Die getroffenen Ermittlungen und Maßnahmen sind hilfreich für die Ausgestaltung weiterführender oder nachgeordneter Prozesse, wie z. B. die sichere Aufbewahrung und Nachweisführung im Zusammenhang mit der Willenserklärung.

2 Behörden können nach § 5 Abs. 2 EGovG Bund erforderliche Nachweise, die einer anderen öffentlichen Stelle vorliegen, mit Einwilligung der Verfahrensbeteiligten auch bei der entsprechenden Stelle einholen. Somit kann in diesen Fällen auf die Übermittlung der Dokumente durch die Bürgerinnen und Bürger verzichtet werden. Zusätzlich kann bei einer direkten Übermittlung durch die ausstellende Behörde davon ausgegangen werden, dass die übermittelten Dokumente unverfälscht sind.

3 Sind mit einer Online-Leistung Geld- oder Sachleistungen verbunden, hat dies Auswirkungen auf das Vertrauensniveau. Es liegt im Ermessen der für das jeweilige Verwaltungsverfahren zuständigen Behörde, das Vertrauensniveau oberhalb der „Basisregistrierung“ einzustufen.

4 Ist eine Verwaltungsleistung erst nach Entrichtung einer Gebühr zugänglich, kann das Vertrauensniveau ggf. abgesenkt werden, da durch die Gebühr eine zusätzliche Hürde für Betrugsversuche besteht.

5 Damit eine Fehleinschätzung des Vertrauensniveaus vermieden wird, sollte das Vertrauensniveau angemessen und verhältnismäßig bestimmt werden. Eine zu niedrige Einstufung kann zur Folge haben, dass Schäden aufgrund von Missbrauch entstehen. Auf der anderen Seite kann eine zu hohe Einstufung dagegen zur Folge haben, dass ein Online-

Antragsverfahren aufgrund der hohen Sicherheitsanforderungen nicht oder nur vereinzelt verwendet wird und somit die Potenziale der Digitalisierung nicht im vollen Ausmaß genutzt werden.

6 Die Zuordnung der Vertrauensniveaus zu den einzelnen Prozessen (i.) Identifizierung, (ii.) Willenserklärung und (iii.) Dokumentenübermittlung sollte möglichst unabhängig voneinander vorgenommen werden. Falls Prozesse gemeinsam oder kombiniert betrachtet werden, ist für die Gesamtbewertung das Maximum der einzeln ermittelten Vertrauensniveaus anzunehmen.[14] Im Rahmen der Ermittlung des Vertrauensniveaus können folgende Fragestellungen eine Hilfe sein:

- **Identifizierung**: Welche Schäden können entstehen, wenn es gelingt, sich mit falscher Identität zu identifizieren bzw. anzumelden? Besteht für Dritte ein konkreter Täuschungsanreiz (z. B. zur Erlangung geldwerter Vorteile) und damit eine relevante Täuschungswahrscheinlichkeit?

- **Willenserklärung**: Welche Schäden können entstehen, wenn jemand bestreitet, eine Erklärung mit einem bestimmten Inhalt abgegeben zu haben (z. B. im Falle einer falschen oder unvollständigen Steuererklärung)?

- **Dokumentenübermittlung**: Welche Schäden können entstehen, wenn Vertraulichkeit und Integrität der übertragenen Daten verletzt werden (z. B. wenn das Steuer- oder das Sozialgeheimnis verletzt oder Gesundheitsdaten fehlerhaft übermittelt werden)?

- Werden besonders **sensible Daten** (s. Definition in Art. 9 Abs. 1 Datenschutz-Grundverordnung, z. B. Gesundheitsdaten) erfasst bzw. verarbeitet? Besonders sensible Daten sollten bei allen drei Prozessen ((i.) Identifizierung, (ii.) Willenserklärung und (iii.) Dokumentenübermittlung) zur Einstufung auf dem Vertrauensniveau „hoch“ führen.

[14] Zum Beispiel: Die Prozesse (iii.) Dokumentenübermittlung und (ii.) Willenserklärung werden kombiniert. Wird für die Dokumentenübermittlung das Vertrauensniveau „hoch“ ermittelt und ihr als Vertrauensmechanismus eine absenderbestätigte De-Mail zugeordnet, so wird damit bei der Willenserklärung automatisch ebenfalls das Vertrauensniveau „hoch“ umgesetzt, obwohl ggf. nur „substantiell“ gefordert ist.

7. Vorgehensweise für die Zuordnung von Vertrauensniveaus

In einem ersten Schritt wird das jeweilige Vertrauensniveau auf Basis der einzelnen Gefährdungen und potenziellen Schäden unter Berücksichtigung der nachfolgenden Tabelle sowie der abstrakten Eintrittswahrscheinlichkeit ermittelt.

Sind mehrere Gefährdungen relevant, so ist für die Gesamtbewertung das Maximum der einzeln ermittelten Vertrauensniveaus anzunehmen. Die Bewertung sollte den Prozess strukturiert dokumentieren. Zuerst werden die Teilprozesse in (i.) Identifizierung, (ii.) Willenserklärung und (iii.) Dokumentenübermittlung unterteilt, um ein vorläufiges Vertrauensniveau zu ermitteln. Danach können die potenziellen Schäden und deren Eintrittswahrscheinlichkeiten für jeden Prozess ermittelt und die Bewertung diesbezüglich dokumentiert werden.

Die nachfolgende Tabelle 1 wurde der TR-03107-1[15] des BSI entlehnt und gibt einen Überblick über die potenziellen Schäden und die vor diesem Hintergrund empfohlenen Vertrauensniveaus. Je nach Verwaltungsleistung sind aus fachlicher Sicht weitere Gefährdungen denkbar und zu berücksichtigen, die sich aus einer unrichtigen Identifizierung oder Zuordnung zu einer Identität ergeben können.

[15] Es sei darauf hingewiesen, dass die TR-03107-1 teilweise abweichende Bezeichnungen der Vertrauensniveaus verwendet.

Gefährdung	Potenzieller Schaden bedingt Vertrauensniveau		
	Niedrig[16]	Substantiell	Hoch
Verstoß gegen Gesetze/Vorschriften	Verstoß mit geringfügigen Konsequenzen	Verstoß mit substantiellen Konsequenzen	Verstoß mit erheblichen Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen beeinträchtigen können.	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen substantiell beeinträchtigen können.	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen können.
Beeinträchtigung körperlicher/persönlicher Unversehrtheit	Beeinträchtigung erscheint nicht möglich	Beeinträchtigung kann nicht vollständig ausgeschlossen werden	Beeinträchtigung kann nicht ausgeschlossen werden
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung wird von den Betroffenen als tolerabel eingeschätzt	Beeinträchtigung wird von einzelnen Betroffenen als tolerabel eingeschätzt	Beeinträchtigung wird als nicht tolerabel eingeschätzt
Negative Innen- oder Außenwirkung	Geringe/nur interne Ansehens- oder Vertrauensbeeinträchtigung zu erwarten	Substantielle Ansehens- oder Vertrauensbeeinträchtigung zu erwarten	Breite Ansehens- oder Vertrauensbeeinträchtigung zu erwarten
Finanzielle Auswirkungen	Finanzieller Schaden tolerabel	Substantieller finanzieller Schaden möglich	Beachtliche finanzielle Verluste, jedoch nicht existenzbedrohend
Zu beachten: Die Aggregation von Gefährdungen kann zur Erhöhung des notwendigen Vertrauensniveaus führen. Zum Beispiel kann die Verarbeitung personenbezogener Daten mit Schutzbedarf *substantiell* zu einem notwendigen Vertrauensniveau *hoch* führen, wenn viele Personen von einer Beeinträchtigung betroffen sind. Sind mehrere Gefährdungen relevant, so ist für die Gesamtbewertung das Maximum der einzeln ermittelten notwendigen Vertrauensniveaus anzunehmen.			

Tabelle 1: Gefährdungen und Vertrauensniveaus, in Anlehnung an BSI TR-03107-1, Tabelle 1, S. 14

In einem zweiten Schritt können konkrete Erfahrungen der Verwaltungspraxis der jeweiligen Behörde berücksichtigt werden. Weichen die Erfahrungen der Behörde (insbesondere bezogen auf die Eintrittswahrscheinlichkeit) im zu beurteilenden Verfahren erheblich vom abstrakt ermittelten Vertrauensniveau ab, kann das Vertrauensniveau entsprechend erhöht oder reduziert werden. Dabei sollte die Absenkung oder Erhöhung nicht um mehr als eine Stufe erfolgen (siehe Tabelle 2).

[16] Siehe Kapitel 3 bezüglich der Unterscheidung zwischen Vertrauensniveau „niedrig“ und der „Basisregistrierung“.

		Mögliche Auf- und Abwertungen[17]		
Eintrittswahrscheinlichkeit	**unwahrscheinlicher[18]**	Basisregistrierung	substantiell	substantiell
	normal	**Basisregistrierung**	**substantiell**	**hoch**
	wahrscheinlicher[19]	substantiell	hoch	hoch

Tabelle 2: Möglichkeiten der Auf- und Abwertungen

Beispiele für die Verwendung der Tabelle 2:

- Zum Beispiel könnte ohne Berücksichtigung der konkreten Eintrittswahrscheinlichkeit aufgrund der potenziellen Schäden das erforderliche Vertrauensniveau einer Online-Leistung als „hoch“ bewertet werden. Wird der Eintritt des Schadensereignisses aber als unwahrscheinlich eingestuft, könnte das Vertrauensniveau auf „substantiell“ gesenkt werden.
- Bei einem Verfahren mit wahrscheinlichem Schadensereignis (z. B. da ein großer Täuschungsanreiz aufgrund finanzieller Vorteile besteht), das zunächst mit „substantiell“ bewertet wurde, könnte aufgrund der höheren Eintrittswahrscheinlichkeit das Vertrauensniveau auf „hoch“ angehoben werden.

Orientierung für die Bewertung von Eintrittswahrscheinlichkeiten bietet auch:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Hilfsmittel-und-Anwenderbeitraege/Recplast/recplast_node.html

[17] Zur besseren Nachvollziehbarkeit der möglichen Auf- und Abwertungen sei darauf hingewiesen, dass das Vertrauensniveau „niedrig“ zwar zwischen der „Basisregistrierung“ und dem Vertrauensniveau „substantiell“ eingeordnet ist, aber in Bund und Ländern bei den Bürgerkonten bis auf weiteres nicht eingesetzt wird und somit auch keine Auf- oder Abwertung zu diesem Vertrauensniveau möglich ist.
[18] Unwahrscheinlicher im Vergleich zu einer als normal angenommen Eintrittswahrscheinlichkeit.
[19] Wahrscheinlicher im Vergleich zu einer als normal angenommen Eintrittswahrscheinlichkeit.

Dort sind vergleichbare Beispiele einer Risikoanalyse der RECPLAST GmbH aufgeführt, die Auskunft über Änderungen in der Klassifikation, aufgrund von Eintrittswahrscheinlichkeiten, geben.

8. Weiterführende Informationen

1 Informationen zur Zulassung privater Anbieter von Identifizierungs- und Authentisierungslösungen für interoperable Bürgerkonten/Verwaltungsdienstleistungen: https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/zulassungsverfahren-fuer-nutzerkonten/zulassungsverfahren-fuer-nutzerkonten-node.html

2 Online-Kurs: Informationssicherheit mit IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutz-schulung/it-grundschutzschulung_node.html

Anhang: Ermittlung der möglichen Vertrauensmechanismen

Der folgende Abschnitt richtet sich vor allem an die Betreiber der Bürgerkonten. Für Verantwortliche für die Ermittlung des Vertrauensniveaus von Online-Leistungen ist dieser Abschnitt lediglich informativ.

Welche Vertrauensmechanismen konkret zum Einsatz kommen, wird im Bereich der Identifizierung und Authentifizierung durch die Verantwortlichen für die Bürgerkonten festgelegt. Die PG eID-Strategie des IT-Planungsrates entscheidet dabei unter Beteiligung des BSI, welche Mittel für die unterschiedlichen Vertrauensniveaus der interoperablen Bürgerkonten zum Einsatz kommen.

Die Ausgestaltung der Vertrauensmechanismen für die Identifizierung, Willenserklärung und Dokumentenübermittlung liegt im Ermessen der Verantwortlichen für die Bereitstellung der Bürgerkonten.

Die Prozesse der einzusetzenden Vertrauensmechanismen können der folgenden Tabelle 3 entnommen werden. Eine Beschreibung der Vertrauensdienste/Mechanismen ist in der TR-03107-1 des BSI enthalten. In Tabelle 3 wurde berücksichtigt, dass innerhalb der einzelnen Vertrauensniveaus nicht nur die Vertrauensmechanismen zum Einsatz kommen können, die diesem Vertrauensniveau entsprechen, sondern auch solche, die höherer Sicherheit entsprechen.

			Vertrauensniveau		
		Basisregistrierung	niedrig	substantiell	hoch
Identifizierung	Personen: Registrierung / Erstidentifizierung[20, 21]		Das Vertrauensniveau „niedrig“ wird in Bund und Ländern derzeit nicht eingesetzt.	Elektronischer Identitätsnachweis[22]	
	Personen: Anmeldung / Login[16]			Elektronischer Identitätsnachweis	
				Kryptografische Hardwaretoken	
				Kryptografische Softwaretoken	
				TAN-Verfahren[23]	
		Nutzername / Passwort			
	Dienste			TLS Zertifikate	
				Berechtigungszertifikat als Bestandteil des elektronischen Identitätsnachweises	
Willenserklärung	Elektronische Signaturen			Qualifizierte elektronische Signatur[24]	
				Fortgeschrittene elektronische Signatur mit Hardwaretoken	
				Fortgeschrittene elektronische Signatur mit Softwaretoken	
	Nicht signaturbasierend			De-Mail mit sicherer Anmeldung[24]	
				TAN-Verfahren	
		Nutzerinteraktion			
				Formular mit elektronischem Identitätsnachweis	
Dokumentenübermittlung	Versand – De-Mail			De-Mail mit sicherer Anmeldung[24]; mit Abholbestätigung förmliche Zustellung	
		De-Mail			
	Versand – OSCI			OSCI mit Ende-zu–Ende-Verschlüsselung / Signatur[25]	
				OSCI mit Transportverschlüsselung / Signatur mit dedizierter PKI	
		OSCI mit Transportverschlüsselung / Signatur			
	Versand – E-Mail			E-Mail mit S/MIME mit dezidierter PKI	
		E-Mail mit S/MIME mit Internet PKI			
	Web Up-/ Download			TLS-Zertifikat	
				mit elektronischem Identitätsnachweis	

Tabelle 3: Zuordnung verschiedener technischer Lösungen zu Vertrauensniveaus

[20] Innerhalb eines Geschäftsvorgangs können für verschiedene Schritte unterschiedliche Vertrauensniveaus ausreichend bzw. notwendig sein. Siehe auch entsprechende Erläuterungen unterhalb dieser Tabelle.
[21] Neben der Registrierung / Erstidentifizierung auf elektronischem Weg kann die Identität auch direkt in der Behörde festgestellt werden.
[22] Für den elektronischen Identitätsnachweis mittels Online-Ausweis, eAT oder eID-Karte liegt eine eIDAS-Notifizierung auf Vertrauensniveau „hoch“ vor. Als Alternativen zum elektronischen Identitätsnachweis sind alle nach der eIDAS-Verordnung notifizierten ausländischen eID-Systeme auf dem jeweiligen Vertrauensniveau zuzulassen.
[23] Die Einstufung ist abhängig vom konkreten TAN-Verfahren.
[24] Erreicht je nach technischer Umsetzung nicht in allen Fällen das Vertrauensniveau „hoch“ gemäß eIDAS-Verordnung.
[25] Die Qualität der Zertifikate für Verschlüsselung / Signatur muss dem festgestellten Vertrauensniveau und ggf. besonderen gesetzlichen Formvorschriften entsprechen.

Grundlage für die Einschätzung des Vertrauensniveaus ist die TR-03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government – Teil 1: Vertrauensniveaus und Mechanismen“ des BSI in der jeweils gültigen Fassung veröffentlicht auf den Webseiten des BSI.[26] Diese Technische Richtlinie definiert Vertrauensniveaus für die elektronische Identifizierung und für Vertrauensdienste. Für die Vertrauensniveaubewertung der Identitätsprüfung im Rahmen der Registrierung, dient hierbei als Grundlage die auf den Webseiten des BSI veröffentlichte TR-03147 „Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen“ in der jeweils gültigen Fassung.[27] Das BSI hat zudem einen detaillierten Leitfaden für die einheitliche Prüfung von Authentisierungslösungen gemäß TR-03107 für die Vertrauensniveaus „niedrig“, „substantiell“ und „hoch“ („Bewertung von Authentisierungslösungen gemäß TR-03107 in Version 1.1.1“)[28], nebst Vorlage für einen Prüfbericht („Ergebnisse der Prüfung gemäß TR-03107-1 in Version 1.1.1“)[29] , veröffentlicht.

[26] Siehe: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=1
[27] Siehe: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Identitaetspruefung/identitaetspruefung_node.html
[28] Siehe: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1_Anforderungen.pdf?__blob=publicationFile&v=2
[29] Siehe: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1_Pruefberichtsvorlage.pdf?__blob=publicationFile&v=2