



IT-Planungsrat

Digitale Zukunft gestalten

Sachstandsbericht Projektgruppe eID-Strategie

Stand: August 2016

Inhaltsverzeichnis

1	Ausgangssituation	3
2	Vorlage eines Papiers zu rechtlichen Rahmenbedingungen für interoperable Servicekonten	3
3	Vorlage eines Eckpunktepapiers zum interoperablen Identitätsmanagement von Servicekonten für Bürgerinnen, Bürger und Unternehmen	4
4	Prototyp interoperables Servicekonto	4
5	Anlagen	7

1 Ausgangssituation

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung am 17.06.2015 für eine flächendeckende Verbreitung von Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Die Projektgruppe „eID-Strategie“ wurde bis zu seiner 19. Sitzung im März 2016 in diesem Beschluss um:

- eine Definition der rechtlichen Rahmenbedingungen interoperabler Servicekonten,
- eine Konzeption interoperabler Servicekonten,
- einen beispielhaften Prototypen für die interoperable Kommunikation zwischen Servicekonto-Angeboten und
- die Durchführung einer Wirtschaftlichkeitsbetrachtung für die weitere Umsetzung interoperabler Servicekonten

gebeten. Bereits am Anfang soll berücksichtigt werden, wie das Servicekonto im Endausbau ausgestaltet sein soll.

Die Vorarbeiten fallen umfangreicher als geplant aus, so dass die Projektgruppe „eID-Strategie“ in dem hier vorliegenden Sachstandsbericht Auskunft über den aktuellen Stand der Umsetzung des Beschlusses gibt.

2 Vorlage eines Papiers zu rechtlichen Rahmenbedingungen für interoperable Servicekonten

Zur Definition der rechtlichen Rahmenbedingungen interoperabler Servicekonten wurde ein Papier erstellt. Es wurden Regelungsbedarfe im Schwerpunkt in folgenden Bereichen identifiziert: einheitliche Begriffsbestimmung „Servicekonto“, Einrichtung einer sog. „Verantwortlichen Stelle“, Datenübermittlung und Austausch von Daten. Das Papier ist als Anlage 1 beigefügt.

3 Vorlage eines Eckpunktepapiers zum interoperablen Identitätsmanagement von Servicekonten für Bürgerinnen, Bürger und Unternehmen

Um die wesentlichen Rahmenbedingungen für die Interoperabilität von Servicekonten zu klären, hat die PG eID-Strategie ein Eckpunktepapier erstellt. Dort wird dargestellt,

- was unter einem Servicekonto zu verstehen ist,
- der Umfang der Interoperabilität darstellt und
- unter welchen Voraussetzungen ein Servicekonto für Unternehmen auf Vertrauensniveau hoch geführt werden kann.

Das Papier ist als Anlage Nr. 2 beigelegt.

4 Prototyp interoperables Servicekonto

Der IT-Planungsrat hat die PG eID-Strategie auch mit der Entwicklung eines Prototypen für die interoperable Nutzung der Servicekonten beauftragt. Der Freistaat Bayern hat sich als Federführer bereit erklärt, einen solchen Prototyp zu erstellen. Das Land Nordrhein-Westfalen beteiligt sich als zu pilotierender Partner am Prototyp.

Der Prototyp soll sich nah an einem zukünftigen Produktivsystem orientieren. Ziele des Prototyps sind der Nachweis der Machbarkeit, Erkenntnisse für die spätere technische Umsetzung sowie eine Kostenprognose zur Entwicklung und zum laufenden Betrieb.

Im Rahmen dieses Prototypen hat der Freistaat Bayern eine Schnittstelle bereitgestellt, an die sich neben Nordrhein-Westfalen auch weitere interessierte Länder anschließen können. Interesse haben u.a. die Länder Schleswig-Holstein, Baden-Württemberg und Rheinland-Pfalz signalisiert.

Der Freistaat Bayern hatte für die Ausgestaltung und weitere Umsetzung des Prototyps in einem ersten Schritt eine Projektskizze erstellt und diese mit dem Land Nordrhein-Westfalen Anfang März 2016 final in der Version 1.0 abgestimmt.

Folgende Aktivitäten wurden für den Prototypen durchgeführt:

Aufbau und Bereitstellung der Laborumgebung

Um die technischen Fragen an die Interoperabilität von Servicekonten zu klären, wurde eine virtuelle Umgebung aufgebaut. Der Aufbau erfolgte automatisiert. Die Einrichtung wurde dokumentiert, die Umgebung ist somit reproduzierbar. Ab September 2016 steht die Laborumgebung für die prototypische Anbindung der Servicekonten des Landes Nordrhein-Westfalen und dem Freistaat Bayern bereit. Im weiteren Verlauf werden ausgehend von der prototypischen Anbindung der beiden Länder weitere fachliche Anforderungen an die Laborumgebung definiert und eingepflegt.

Die Laborumgebung beinhaltet vereinfachte Verwaltungsdienste und Servicekonten aus mindestens zwei unterschiedlichen Domänen.

a) Bereitstellung von Verwaltungsdiensten

Um die Anwendungsfälle zwischen einem Servicekonto und einem Verwaltungsdienst exemplarisch durchführen zu können, wurde ein einfacher Test-Verwaltungsdienst realisiert. Dieser Dienst kann die wesentlichen Verbindungsparameter zur Anzeige bringen und Formulareingaben entgegennehmen.

Die Implementierung des Verwaltungsdiensts wird in jeder Domäne installiert und kann unterschiedlich konfiguriert werden. In einer Domäne kann beispielsweise eine Authentifizierung mit Vertrauensniveau „normal“ ausreichend sein, wohingegen in einer anderen Domäne das Vertrauensniveau „substantiell“ zur Nutzung des Diensts gefordert wird.

b) Bereitstellung von Servicekonten

Für den technischen Prototypen wurden vereinfachte Servicekonten implementiert, die auf die Benutzerverwaltung und andere Zusatzdienste verzichten und ausschließlich zur Identitätsfeststellung in der Laborumgebung verwendet werden.

Implementierung der Anwendungsfälle

Die bereitgestellten Verwaltungsdienste und Servicekonten in der Laborumgebung wurden so konfiguriert, dass die beiden folgenden Anwendungsfälle gezeigt werden können:

- **Anmeldung am eigenen Servicekonto**
Ein Nutzer nutzt den Verwaltungsdienst mit dem Servicekonto beim gleichen Anbieter.
- **Anmeldung am fremden Servicekonto**
Ein Nutzer meldet sich zur Nutzung eines Verwaltungsdienstes an einem fremden Servicekonto an.

Bereitstellung eines Informationsportals

Für die Teilnehmer am Prototypen wurde ein Informationsportal bereitgestellt, das die Beteiligten mit den Informationen für die Anbindung von Servicekonten an den technischen Prototypen versorgt. Dieses Portal soll projektbegleitend schrittweise ausgebaut werden und beispielsweise um einen FAQ-Bereich ergänzt werden.

5 Anlagen

- 5.1 Anlage 1: Papier mit ersten Überlegungen zu rechtlichen Rahmenbedingungen für interoperable Servicekonten**

- 5.2 Anlage 2: Eckpunktepapier mit wesentlichen Rahmenbedingungen für die Interoperabilität von Servicekonten**

Referat ITI4

ITI4-17000/26#16

Rechtliche Rahmenbedingungen für interoperable Servicekonten

Erste Überlegungen

Projektgruppe „eID-Strategie“

Stand: 29.06.2016

Inhalt

1	Ausgangssituation und Zielsetzung.....	3
2	Grundsatz der Freiwilligkeit.....	3
3	Einheitliche Begriffsbestimmung „Servicekonto“	4
4	Einrichtung verantwortliche Stelle jeweils in den Ländern bzw. im Bund	4
5	Datenspeicherung.....	6
6	Datenübermittlung bei der interoperablen Nutzung von Servicekonten.....	9
7	Austausch von Nachweisen	9
8	Bekanntgabe von Verwaltungsakten über Postfächer von Servicekonten.....	10
	Anlage 1: Regelungen Verantwortliche Stelle	11

1 Ausgangssituation und Zielsetzung

Der IT-Planungsrat hat sich in seiner 17. Sitzung am 17.06.2015 für eine flächendeckende Verbreitung von Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen.¹ Die Projektgruppe „eID-Strategie“ wurde gebeten folgende Inhalte zu erarbeiten:

- eine Definition der rechtlichen Rahmenbedingungen interoperabler Servicekonten,
- eine Konzeption interoperabler Servicekonten,
- einen beispielhaften Prototypen für die interoperable Kommunikation zwischen Servicekonto-Angeboten und
- die Durchführung einer Wirtschaftlichkeitsbetrachtung für die weitere Umsetzung interoperabler Servicekonten.

Bereits am Anfang soll berücksichtigt werden, wie das Servicekonto im Endausbau ausgestaltet sein soll.

Das hier vorliegende Papier dokumentiert die ersten Überlegungen zu rechtlichen Rahmenbedingungen interoperabler Servicekonten. Es berücksichtigt die EntschlieÙung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 06./07. April 2016. Die Überlegungen können als Empfehlungen für die weitere Umsetzung in Bund und Länder genutzt werden. Änderungsbedarf und Umfang der Änderungen richten sich nach den Rahmenbedingungen in den einzelnen Ländern.

2 Grundsatz der Freiwilligkeit

Die Errichtung und Nutzung der Identifizierungskomponente eines Servicekontos sind freiwillig. Die Nutzung eines Servicekontos bieten Bürgerinnen, Bürgern und Unternehmen einen optionalen Zugang zur Verwaltung, der zusätzlich neben den bisherigen Zugängen wie der schriftlichen Beantragung einer Verwaltungsdienstleistung und/oder durch Antragstellung vor Ort in einer Behörde eröffnet wird.

Für die Erhebung personenbezogener Daten in Servicekonten ist eine gesetzliche Rechtsgrundlage erforderlich. Da die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default“ eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus. Neben der Erhebungs- und Verarbeitungsbefugnis wird insbesondere in folgenden Teilbereichen Regelungsbedarf gesehen:

- Einheitliche Begriffsbestimmung „Servicekonto“

¹ Die Projektgruppe eID-Strategie hat sich auf Bitten des IT-Planungsrates auf den Begriff „Servicekonto für Bürgerinnen, Bürger und Unternehmen“ verständigt, der den Begriff „Bürgerkonten“ ersetzt. Dies trägt der Tatsache Rechnung, dass Servicekonten sowohl für private als auch geschäftliche Zwecke genutzt werden können.

- Einrichtung „Verantwortliche Stelle“
- Datenspeicherung
- Interoperabler Austausch von Daten
- Bekanntgabe von Verwaltungsakten über Postfächer der Servicekonten

3 Einheitliche Begriffsbestimmung „Servicekonto“

Ausgangssituation

Gemäß Eckpunktepapier² wird unter dem Servicekonto eine zentrale Identifizierungskomponente verstanden, die der Identifizierung der Nutzerinnen und Nutzer vor Inanspruchnahme von Verwaltungsdienstleistungen dient. Für den Ausbau interoperabler Servicekonten ist ein einheitliches Verständnis des Begriffs „Servicekonto“ herzustellen.

Um Zweck und Aufgabe von Servicekonten „als Identifizierungskomponente“ bundesweit festzulegen, sollte eine bundesweit einheitliche Begriffsbestimmung an geeigneter Stelle erfolgen. Hierfür bietet sich beispielsweise das E-Government-Gesetz (EGovG) des Bundes oder – sofern vorhanden – in den Ländern an. In den Ländern, in denen kein EGovG existiert, sind geeignete Stellen zu prüfen, z. B. Datenschutzgesetze oder -verordnungen.

Formulierungsvorschlag

„Das Servicekonto ist eine zentrale Identifizierungskomponente, die eine staatliche Stelle anderen Behörden und Ämtern zur Identifizierung von Bürgerinnen, Bürgern und Unternehmen zu Zwecken der Inanspruchnahme öffentlicher Dienstleistungen bereitstellt. Die Nutzung der Servicekonten für Bürgerinnen, Bürger und Unternehmen ist freiwillig.“

Hinweis: BMI wird parallel eine Änderung des § 21 Personalausweisgesetzes in die Wege leiten, um die Vorschrift an das mit Errichtung und Nutzung von Servicekonten verbundene Identitätsmanagement anzupassen.

4 Einrichtung verantwortliche Stelle jeweils in den Ländern bzw. im Bund

Ausgangssituation

Die verantwortliche Stelle ist aufgrund einer funktionalen Betrachtungsweise zu bestimmen. Maßgeblich ist dabei, wer die Entscheidungsverantwortung über Zweck, Art und Umfang der Datenverarbeitung innehat.

Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da

² Vgl. Eckpunktepapier zu „Einheitliche Rahmenbedingungen für interoperable Servicekonten für Bürgerinnen, Bürger und Unternehmen“; Projektgruppe „eID-Strategie“; Stand: 29.06.2016

zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default“ eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.

Einige Länder haben bereits entsprechende Regelungen in ihren E-Government-Gesetzen bzw. ihren Datenschutzgesetzen getroffen. Dies ist in Baden-Württemberg, Bayern, Sachsen und Schleswig-Holstein der Fall. Berlin, Mecklenburg-Vorpommern und Nordrhein-Westfalen haben Gesetzentwürfe vorgelegt. Die Rechtsgrundlagen bzw. die Entwürfe sind in der Anlage 1 aufgeführt.

In den Ländern Brandenburg, Bremen, Hamburg³, Hessen, Rheinland-Pfalz, Saarland und Sachsen-Anhalt sind bisher keine entsprechende Regelungen zur Einrichtung verantwortlicher Stellen bekannt. Auf Bundesebene fehlt es zurzeit an einer entsprechenden Rechtsgrundlage.

Für die Bundesebene prüft der Bund die Möglichkeit, eine für Bundesanwendungen zentral verantwortliche Stelle zu bestimmen.

Option 1:

Bestimmung einer verantwortlichen Stelle über ein „gemeinsames Verfahren“ gem. § 11 EGovG Bund.

Option 2:

Alternativ besteht auch die Möglichkeit, eine Rechtsgrundlage für eine zentral verantwortliche Stelle zu schaffen, z. B. durch eine Erweiterung des § 11 EGovG Bund.

Das ITZBund kann in eigener datenschutzrechtlicher Verantwortlichkeit die elektronische Abwicklung von Verwaltungsdienstleistungen für Identifizierungen zur behördenübergreifenden Nutzung bereitstellen. Mit Einwilligung des Nutzers können seine Stammdaten zur Verwendung in anderen E-Government-Anwendungen verarbeitet werden.

oder:

Das Bundesministerium des Innern wird ermächtigt, durch Rechtsverordnung einen IT-Diensteanbieter/eine Behörde/einen Zweckverband zu benennen, der in eigener datenschutzrechtlicher Verantwortung...

Entsprechende Regelungen müssten auch in denjenigen Ländern geschaffen werden, die insoweit bisher nicht tätig geworden sind.

³ In Anlehnung an § 3 Abs. 7 BDSG bestimmt Hamburg mit § 4 Abs. 3 HmbDSG den Begriff „Daten verarbeitende Stelle“.

5 Datenspeicherung

Ausgangssituation

Beim Umfangs der zu speichernden und zu übermittelnden Daten ist zu unterscheiden, ob es sich um natürliche Personen oder juristische Personen bzw. auch weitere Institutionen, wie z.B. Vereine, Stiftungen oder Behörden handelt.

Darüber hinaus ist zu beachten, ob die Daten für Verwaltungsdienstleistungen auf Vertrauensniveau „normal“, „hoch“ oder „hoch+“ genutzt werden sollen.⁴

Natürliche Person

Registrierung auf Vertrauensniveau „hoch“ bzw. „hoch+“

Für die Speicherung von Daten auf Vertrauensniveau „hoch“ / „hoch+“ werden folgende Datenfelder zugrunde gelegt: Familienname, Vorname(n), Doktorgrad, Geburtsdatum, Anschrift (Dokumentenart, ausstellender Staat und dienste- und kartenspezifisches Kennzeichen soweit eID-Funktion genutzt wird).⁵

Die eIDAS-Verordnung⁶ fordert eine eindeutige Identifikation. Da Deutschland im Gegensatz zu vielen Mitgliedstaaten kein Personenkennzeichen nutzt, kann die Identität nur eindeutig festgestellt werden, wenn zusätzlich der Geburtsname und Geburtsort aufgenommen wird.

Die Nutzung des Servicekontos auf Vertrauensniveau „hoch“ und „hoch+“ setzt eine eindeutige Identifizierung der Bürgerinnen und Bürger voraus. Wird bei späterer Nutzung des Servicekontos die eID-Funktion des Personalausweises verwendet, sollte aus Gründen der Datensparsamkeit nur das dienste- und kartenspezifische Kennzeichen, die Anschrift und ggf. Doktorgrad abgefragt und übermittelt werden. Die regelmäßige Übermittlung der Anschrift ist erforderlich, um die Aktualität der Anschrift sicherzustellen. Das dienste- und kartenspezifische Kennzeichen dient ausschließlich der Authentisierung am Servicekonto und wird nicht an die konkrete Verwaltungsdienstleistung übermittelt.

Bei Verwaltungsdienstleistungen mit dem Vertrauensniveau „normal“ ist die (Erst-) Registrierung und Nutzung von Verwaltungsdienstleistungen mit Benutzername / Passwort möglich. Folgende Mindestdaten sollen für Eröffnung und Nutzung auf „normal“ erhoben und genutzt werden.

- Name, Vorname,
- Geburtsdatum
- Anschrift

⁴ Dabei handelt es sich um die Vertrauensniveaus gem. der Technischen Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government, Teil 1: Vertrauensniveaus und Mechanismen.

⁵ Dabei handelt es sich um die Datenfelder, die im Musterantrag der VITAKO zur Beantragung eines Berechtigungszertifikats für die eID-Funktion mit der Vergabestelle für Berechtigungszertifikate abgestimmt wurden.

⁶ Verordnung (EU) Nr. 910/2014 i.V.m. Durchführungsverordnung (EU) 2015/1501

- Soll: E-Mail
- Soll: De-Mail

Daneben kann auch eine pseudonyme Nutzung des Servicekontos ausreichen.

Unternehmenskonten auf „Vertrauensniveau „hoch“ und „hoch+“

Um Verwaltungsdienstleistungen auf Vertrauensniveau „hoch“ und „hoch+“ nutzen zu können, ist eine vorherige eindeutige Identifizierung von Unternehmen bei (Erst-)Registrierung und Nutzung sicherzustellen.

Die Identifizierung des Unternehmens ist anhand eindeutiger Daten oder besonderer Identifizierungsmerkmale sicherzustellen.

Dabei kann auf die Identifizierungskriterien zu De-Mail zurückgegriffen werden.

Die BSI TR 01201 Teil 2.1 Accountmanagement De-Mail sieht für juristische Personen und weitere Institutionen folgende Datenfelder vor:⁷

Attribut	Bemerkungen
Name / Bezeichnung	Beinhaltet auch die Kurzform der Institution (z.B. GmbH, AG, GbR, AöR), wenn diese vorhanden ist.
Straße und Hausnummer und / oder Postfach	Sitz oder Hauptsitz
Ort	Sitz oder Hauptsitz
Staat	Sitz oder Hauptsitz
Rechtsform	Sitz oder Hauptsitz
Art des Registers	Soweit vorhanden
Registerort	Soweit vorhanden
Registernummer	Soweit vorhanden
Berechtigung zur Nutzung Versandoption „Abholbestätigung“	Bei öffentlichen Stellen, die formell zustellen dürfen.
Namen der Mitglieder des Vertretungsorgans oder der gesetzliche Vertreter	
Firma, Name oder Bezeichnung, Rechtsform, Art des Registers, Registerort, Registernummer (soweit vorhanden) und Anschrift des Sitzes oder Hauptsitzes	Falls ein Mitglied des Vertretungsorgans oder der gesetzlichen Vertreter eine juristische Person ist.

Tabelle 1: Identitätsattribute juristischer Personen⁸ gemäß BSI TR 01201 Teil 2.1, S.9 f.

⁷ Technische Richtlinie zum Accountmanagement Funktionalitätsspezifikation des Bundesamt für Sicherheit in der Informationstechnik (BSI TR 01201 Teil 2.1)

⁸ „Unter dem Begriff „Institution“ werden hier juristische Personen, Personengesellschaften und öffentliche Stellen zusammengefasst.“ (vgl. BSI BSI TR 01201 Teil 2.1, S. 5)

Formulierungsvorschlag

Zur Feststellung der Identität des Nutzers des Servicekontos auf Vertrauensniveau „hoch“ und „hoch+“ dürfen bei Registrierung und Nutzung eines Servicekontos folgende Daten erhoben, gespeichert und weiterverarbeitet werden:

a. bei einer natürlichen Person: Name, Vorname, Anschrift, Geburtsname, Geburtsort, Geburtsdatum, Doktorgrad, bei Nutzung der elektronischen Identitätsfunktion i.S.d. § 18 PAuswG oder § 78 Abs. 5 AufenthG Abkürzung „D“ für Bundesrepublik Deutschland und die Dokumentenart sowie das dienste- und kartenspezifische Kennzeichen. Bei späterer Nutzung des Servicekontos mit der eID-Funktion sind grundsätzlich das dienste- und kartenspezifische Kennzeichen und die Anschrift zu übermitteln. Soweit eine natürliche Person für ein Unternehmen handelt, sind die in der eID gespeicherten personenbezogenen Daten mit Ausnahme der „Anschrift“ zu verwenden.

b. bei einer juristischen Person oder einer Personengesellschaft: Firma, Name oder Bezeichnung, Rechtsform, Registernummer soweit vorhanden, Anschrift des Sitzes oder der Hauptniederlassung und Namen der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter; ist ein Mitglied des Vertretungsorgans oder der gesetzliche Vertreter eine juristische Person, so sind deren Firma, Name oder Bezeichnung, Rechtsform, Registernummer soweit vorhanden und Anschrift des Sitzes oder der Hauptniederlassung zu erheben.

Durch die Nutzung unterschiedlicher Berechtigungszertifikate bei der Nutzung für eine natürliche Person und bei der Nutzung für ein Unternehmen ist sicherzustellen, dass nur die erforderlichen Daten aus der eID ausgelesen werden können.

Option:

Die Identifizierung kann auch auf Grundlage folgender Identifizierungsmerkmale sichergestellt werden.

a)...

b)...

(Die Eröffnung von Servicekonten für Unternehmen auf hohem Vertrauensniveau ist nur durch eine vertretungsberechtigte Person zulässig. Sie kann Mitarbeiter zur Nutzung des Servicekontos berechtigen. Servicekonten können für Verwaltungsdienstleistungen mit hohem Vertrauensniveau genutzt werden, wenn die vertretungsberechtigte Person bei Eröffnung und der Mitarbeiter bei Nutzung sich durch ein Identifizierungsmittel auf dem Vertrauensniveau „hoch“ / „hoch+“ identifiziert haben.

6 Datenübermittlung bei der interoperablen Nutzung von Servicekonten

Ausgangssituation

Die bundesweite Interoperabilität der Identifizierungskomponente von Servicekonten setzt entsprechende Rechtsgrundlagen für die Übermittlung dieser Daten voraus:

Neben § 5 Abs. 3 könnte zusätzlich auch eine Spezialvorschrift zur länderübergreifenden Datenübermittlung bei Servicekonten aufgenommen werden

Die zuständige Behörde kann erforderliche Identifizierungen, mit auf Anforderung Einwilligung des Verfahrensbeteiligten im Einzelfall und mit seiner Einwilligung direkt bei der öffentlichen Stelle elektronisch einholen, bei der der Bürger oder das Unternehmen ein Servicekonto führt. Zu diesem Zweck dürfen die anfordernde Behörde und die abgebende öffentliche Stelle die für die Nutzung der Verwaltungsdienstleistung erforderlichen personenbezogenen Daten erheben, verarbeiten und nutzen.

Diese Regelungen könnte im EGovG Bund (§ 5 Abs. 4) aufgenommen werden. Entsprechende Regelungen wären in allen Ländern, die an der interoperablen Nutzung der Identifizierungskomponente teilnehmen, zu schaffen.

7 Austausch von Nachweisen

Ausgangssituation

Die bundesweite Interoperabilität von Servicekonten setzt entsprechende Rechtsgrundlagen für die Übermittlung dieser Daten voraus:

Die Rechtsgrundlage ist in § 5 Abs. 2 EGovG Bund bzw. - soweit vorhanden - entsprechend auf Länderebene - bereits vorhanden.

Nach diesen Vorschriften kann die zuständige Behörde erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, auf Anforderung des Verfahrensbeteiligten im Einzelfall und mit seiner Einwilligung direkt bei der ausstellenden öffentlichen Stelle elektronisch einholen. Zu diesem Zweck dürfen die anfordernde Behörde und die abgebende öffentliche Stelle die erforderlichen personenbezogenen Daten erheben, verarbeiten und nutzen.

Auf Länderebene ist eine entsprechende Regelung, beispielsweise in Bayern vorhanden. Nach Artikel 6 Abs. 3 Satz 3 des Bayerischen EGovG kann eine Behörde bestimmte, von einer deutschen öffentlichen Stelle ausgestellte Nachweise oder Unterlagen in automatisierter Weise elektronisch abrufen, soll sie diese in elektronisch geführten Verfahren selbst einholen, wenn die datenschutzrechtlichen Voraussetzungen der Erhebung bei Dritten vorliegen oder wenn die Betroffenen in den Abruf einwilligen.

Entsprechende Regelungen wären in allen am interoperablen Datenaustausch teilnehmenden Ländern zu schaffen.

8 Bekanntgabe von Verwaltungsakten über Postfächer von Servicekonten

Die Bekanntgabe von Verwaltungsakten über die Postfächer von Servicekonten richtet sich nach der geltenden Fassung des § 41 VerwVfG des Bundes bzw. entsprechender Regelungen der Länder.

Anlage 1: Regelungen Verantwortliche Stelle

Land	Regelung
Bund	Option über § 11 EGovG Bund möglich
Baden-Württemberg	§ 15 Abs. 4 und 5 Gesetz zur Förderung der elektronischen Verwaltung und zur Änderung weiterer Vorschriften (E-Government-Gesetz Baden-Württemberg – EGovG BW)
Bayern	Bayern Art. 9 Bayerisches E-Government-Gesetz (BayEGovG)
Berlin	Artikel 8 Abs. 2 Berliner E-Government-Gesetz i.V.m. § 15 des Berliner Datenschutzes
Brandenburg	Keine Regelung bekannt
Bremen	Keine Regelung bekannt
Hamburg	Keine Regelung bekannt
Hessen	Keine Regelung bekannt
Mecklenburg-Vorpommern	§ 2 Abs. 3 S. 2 Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (E-Government-Gesetz Mecklenburg-Vorpommern-EGovG M-V)
Niedersachsen	Keine Regelung bekannt
Nordrhein-Westfalen	§ 3 Abs. 3 E-Government-Gesetz NRW (eGovG NRW)
Rheinland-Pfalz	Keine Regelung bekannt
Saarland	Keine Regelung bekannt
Sachsen	§ 10 Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (Sächsisches E-Government-Gesetz – SächsEGovG)
Sachsen-Anhalt	Keine Regelung bekannt
Schleswig-Holstein	§ 8 Abs. 3 Gesetz zur elektronischen Verwaltung für Schleswig-Holstein (E-Government-Gesetz - EGovG)
Thüringen	Keine Regelung bekannt

Referat ITI4

ITI4-17000/26#16

Interoperables Identitätsmanagement von Servicekonten für Bürgerinnen, Bürger und Unternehmen

Eckpunktepapier

Projektgruppe „eID-Strategie“

Stand: 29.06.2016

Inhalt

1	Ausgangssituation	3
2	Mehrwerte und Nutzen	4
3	Was ist ein Servicekonto?	5
3.1	Identifizierungskomponente für Antragstellung	5
3.2	Postfach-Funktionalität	5
3.3	Dokumentensafe	5
3.4	Abgrenzungen und Schnittstellen zu anderen Projekten	6
3.5	Flächendeckende Bereitstellung zentraler Servicekonto-Strukturen	6
3.6	Anwendungsbereich des Servicekontos	6
4	Regelungen zu Servicekonten	6
4.1	Wahlfreiheit	6
4.2	Freiwilligkeit	7
4.3	Einsatz von Identifizierungsmitteln	7
4.4	Nutzung von Servicekonten	7
4.5	Servicekonto für Unternehmen	7
4.5.1	Anwendungsbereich: Wer ist „Unternehmen“ im Sinne des Servicekontos?	7
4.5.2	Rahmenbedingungen Servicekonto für Unternehmen	8
4.5.3	Nutzung eines Servicekontos für Unternehmen	8
4.6	Löschung eines Servicekontos	8
4.7	Nutzung Postfach	8
4.8	Einwilligung, Dokumente und Daten von anderen Behörden einzuholen	9
5	Interoperabilität	9
5.1	Gründe, Mehrwerte, Nutzen der Interoperabilität von Servicekonten	9
5.2	Umfang der Interoperabilität	9
5.2.1	Einsatz von Identifizierungsmitteln	10
5.2.2	Voraussetzungen für Servicekonten für Unternehmen auf Vertrauensniveau „hoch“ / „hoch+“	10

1 Ausgangssituation

In zahlreichen Ländern werden bereits zentrale Servicekonten angeboten. Die Bereitstellung spart Aufwände und Kosten in einzelnen Behörden, da diese die elektronische Identifizierung von Bürgerinnen, Bürgern und Unternehmen über eine zentrale Stelle durchführen können. Auf der Grundlage der Erfahrungen und Strukturen vorhandener Servicekonten soll die flächendeckende Bereitstellung von Servicekonten weiter vorangetrieben werden. Besonderer Wert wird auf die einfache Nutzbarkeit sowie auf Mehrwerte und Nutzen für Bürgerinnen, Bürger, Unternehmen und Behörden gelegt.

Servicekonten sind politisch-strategisch verankert.¹ So verbindet der Koalitionsvertrag auf Bundesebene damit die Zielsetzung, mittels eines einheitlichen Stammdaten-Accounts die Kommunikation mit der Verwaltung zusätzlich zu vereinfachen. Zur elektronischen Identifizierung soll der Personalausweis mit eID-Funktion² genutzt werden. Auch die Digitale Agenda und das Regierungsprogramm Digitale Verwaltung 2020 der Bundesregierung sehen hierüber die Möglichkeit, möglichst viele Verwaltungsdienstleistungen der Kommunen, der Länder und des Bundes einfach und sicher zu nutzen.

Im Rahmen der Strategie des IT-Planungsrates für eID und andere Vertrauensdienste im E-Government (eID-Strategie) wurden ein Erfahrungsbericht zu vorhandenen Servicekonten und eine Studie für ein interoperables Identitätsmanagement erstellt. Diese zeigten, wie Nutzerinnen und Nutzer ihre in einem bestehenden Servicekonto gespeicherten Identitätsdaten verwenden können, um sich an einem elektronischen Verwaltungsverfahren in einer Behörde einer Kommune, eines Landes oder des Bundes anzumelden, unabhängig davon, wo sie dieses initial erstellt haben.

Der IT-Planungsrat hat sich in seiner 17. Sitzung am 17.06.2015 für eine flächendeckende Verbreitung von Servicekonten ausgesprochen. Die Projektgruppe „eID-Strategie“ wurde gebeten,

- eine Definition der rechtlichen Rahmenbedingungen interoperabler Servicekonten und
- eine Konzeption interoperabler Servicekonten vorzulegen,
- einen beispielhaften Prototypen für die interoperable Kommunikation zwischen Servicekonto-Angeboten zu entwickeln und
- die Durchführung einer Wirtschaftlichkeitsbetrachtung für die weitere Umsetzung interoperabler Servicekonto durchzuführen.

Bereits am Anfang soll berücksichtigt werden, wie das Servicekonto im Endausbau ausgestaltet sein soll.

¹ Die Projektgruppe eID-Strategie hat sich auf Bitten des IT-Planungsrates auf den Begriff „Servicekonto für Bürgerinnen, Bürger und Unternehmen“ verständigt, der den Begriff „Bürgerkonten“ ersetzt. Dies trägt der Tatsache Rechnung, dass Servicekonten sowohl für private als auch geschäftliche Zwecke genutzt werden können.

² In den folgenden Ausführungen bezieht sich der Begriff eID-Funktion bzw. Online-Ausweisfunktion auch auf die elektronische Funktion des Aufenthaltstitels.

Die Projektgruppe „eID-Strategie“ hat eine Unterarbeitsgruppe „Interoperables Identitätsmanagement für Servicekonten“ eingerichtet. In der Unterarbeitsgruppe sind das Bundesministerium des Innern, das Bundesamt für Sicherheit in der Informationstechnik, das Bundesverwaltungsamt, die Länder Bayern, Baden-Württemberg, Berlin, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Schleswig-Holstein, der Deutsche Städtetag und die BLK-Arbeitsgruppe „IT-Standards in der Justiz“ (SAFE, Koordinierungsprojekt des IT-Planungsrates) vertreten. Die Inhalte werden mit der Projektgruppe „eID-Strategie“ abgestimmt.

Die Unterarbeitsgruppe hat die folgenden Eckpunkte festgelegt. Anliegen der Länder ist es, nur die wesentlichen Rahmenbedingungen zu klären, die Voraussetzung für die Interoperabilität von Servicekonten sind.

Die Eckpunkte eines interoperablen Identitätsmanagements von Servicekonten für Bürgerinnen, Bürger und Unternehmen sind nicht unabhängig von den rechtlichen Rahmenbedingungen zu betrachten. Zu der vom IT-Planungsrat erbetenen Definition der rechtlichen Rahmenbedingungen interoperabler Servicekonten wurden erste Überlegungen in einem eigenen Papier dokumentiert. Rechtliche Rahmenbedingungen sind daher nicht Bestandteil des hier vorliegenden Eckpunktepapiers.

2 Mehrwerte und Nutzen

Festlegung 1: Die Ausgestaltung des Servicekontos muss sich zwingend am Bedarf und am Nutzen für Bürgerinnen und Bürger, Unternehmen und Behörden orientieren! Nur wenn für alle Nutzerinnen und Nutzer ein Mehrwert mit der Nutzung verbunden ist, wird das Servicekonto ein Erfolg.

Erläuterung: Neben den grundsätzlichen Vorteilen und Mehrwerten, die ein Servicekonto beinhalten sollte, wie einfache und schnelle Bedienbarkeit, Sicherheit und Kostensparsamkeit, sollten spezifische Anforderungen der Zielgruppen Berücksichtigung bei der weiteren Ausgestaltung des Servicekontos finden.

So legen Bürgerinnen, Bürger und Unternehmen Wert auf eine medienbruchfreie Online-Abwicklung von Verwaltungsdienstleistungen, und das sowohl Behörden- als auch Verwaltungsebenen-übergreifend.

Grundsätzlich soll die sichere Übertragung und Speicherung von persönlichen und Unternehmens-Daten und ggf. auch ein digitaler Austausch von Unterlagen und Informationen ermöglicht werden.

Im Mittelpunkt steht die eindeutige Identifizierung der Bürgerinnen und Bürger bzw. von Unternehmen/juristischen Personen³ auf unterschiedlichen Vertrauensniveaus. Die Festlegung

³ Zu juristischen Personen zählen neben Unternehmen auch weitere Institutionen, z. B. Vereine, Stiftungen oder Behörden. Vgl. Kapitel 5.

konkreter Vertrauensniveaus ist nur für die Interoperabilität notwendig. Bürgerinnen, Bürger und für Unternehmen handelnde Personen sollen ihre Verwaltungsdienstleistungen (Bund, Land, Kommune) möglichst unter Nutzung der gleichen Identifizierungskomponente abwickeln können.

3 Was ist ein Servicekonto?

3.1 Identifizierungskomponente für Antragstellung

Festlegung 2: Wesentlicher Bestandteil eines Servicekontos ist eine zentrale Identifizierungskomponente. Sie dient der Identifizierung der Nutzerinnen und Nutzer vor Inanspruchnahme von Verwaltungsdienstleistungen. Die Identifizierungskomponenten sollen für alle Verwaltungsdienstleistungen auf Bundes-, Länder- und kommunaler Ebene genutzt werden und bundesweit interoperabel gestaltet werden. Im Rahmen der Interoperabilität sollen sich die Identifizierungskomponenten gegenseitig vertrauen können.

Festlegung 3: Einzelne Verwaltungsdienstleistungen können auch eigene Identifizierungskomponenten anbieten.

Erläuterung: Neben den in einigen Ländern bereits bestehenden zentralen Identifizierungskomponenten nutzen einzelne Fachanwendungen eigene Identifizierungskomponenten. Diese können auch künftig parallel angeboten werden.

3.2 Postfach-Funktionalität

Festlegung 4: Die Postfach-Funktionalität kann ebenfalls Bestandteil des Servicekontos sein. Das Postfach soll den Versand von Mitteilungen, Bescheiden und Benachrichtigungen zum Bearbeitungsstatus ermöglichen. Der interoperable Ausbau der Postfach-Funktionalität soll zu einem späteren Zeitpunkt geprüft werden.

Erläuterung: Mit der Postfach-Funktionalität können Verwaltungsabläufe grundsätzlich auch in beide Richtungen sicher und vollständig medienbruchfrei über das Servicekonto abgewickelt werden.

Die Postfach-Funktionalität kann individuell gestaltet werden (z. B. auch durch eine Anbindung von De-Mail).

3.3 Dokumentensafe

Festlegung 5: Der Dokumentensafe kann Bestandteil des Servicekontos sein. In Anbetracht der Komplexität der zu prüfenden Fragen werden weitere Überlegungen zum Dokumentensafe zurückgestellt.

Erläuterung: Der Dokumentensafe erlaubt die Speicherung von digitalen Daten und Dokumenten. Bürgerinnen, Bürger und Unternehmen können diese bei Bedarf für Verwaltungsdienstleistungen nutzen.

3.4 Abgrenzungen und Schnittstellen zu anderen Projekten

Festlegung 6: E-Payment ist nicht Bestandteil des Servicekontos. Bezahlplattformen werden i.d.R. als eigene standardisierte Services bereitgestellt. Dabei handelt es sich um eigenständige Komponenten. Diese können in das Servicekonto integriert werden.

3.5 Flächendeckende Bereitstellung zentraler Servicekonto-Strukturen

Festlegung 7: Servicekonten sollen so weit wie möglich zentral sowohl auf Länder- als auch auf Bundesebene bereitgestellt werden, um Kosten und Aufwände in den einzelnen Behörden der jeweiligen Länder bzw. des Bundes zu reduzieren.

Erläuterung: Der IT-Planungsrat hat sich am 17. Juni 2015 für den flächendeckenden Aufbau von Servicekonten ausgesprochen.

Festlegung 8: Die bundesweit zentrale Einrichtung eines Servicekontos ist nicht vorgesehen. Es besteht Konsens, dass auf bestehenden bzw. sich derzeit bereits im Aufbau befindlichen Strukturen in Bund und Ländern aufgesetzt wird. Um in der Öffentlichkeit die Übereinstimmung der unterschiedlich bezeichneten Lösungen zu verdeutlichen, ist es wünschenswert, ein gemeinsames Logo für Servicekonten und ggf. ein weiteres Logo für interoperable Servicekonten einzuführen, das alle Anbieter nutzen können.

3.6 Anwendungsbereich des Servicekontos

Festlegung 9: Bund und Länder streben an, dass Servicekonten sowohl für Behörden im Geltungsbereich der Verwaltungsverfahrensgesetze als auch mittelfristig für Verwaltungsdienstleistungen der Bereiche Justiz, Soziales und Finanzen genutzt werden können.

4 Regelungen zu Servicekonten

4.1 Wahlfreiheit

Festlegung 10: Bürgerinnen, Bürger und Unternehmen haben Wahlfreiheit bei der Auswahl aus dem Servicekontenangebot der Kommunen und Länder.

Erläuterung: Verwaltungsdienstleistungen werden sowohl von Kommunen, Ländern als auch vom Bund bereitgestellt. Je nach behördlicher Zuständigkeit bestehen unterschiedliche Möglichkeiten, ein Servicekonto einzurichten.

Festlegung 11: Bürgerinnen, Bürger und Unternehmen können sich mehrere Servicekonten einrichten und diese parallel führen.

Erläuterung: Eine zwingende Begrenzung auf ein einziges Servicekonto ist in der Praxis schwierig umzusetzen. Dies würde im Fall einer (Erst-)Registrierung eine Prüfung voraussetzen, ob bereits ein Servicekonto an anderer Stelle angelegt wurde. Die mit der Realisierung einer derartigen Abfrage verbundenen Aufwände sollen vermieden werden. Im Rahmen einer geeigneten Kommunikation sollen stattdessen die Vorteile der Nutzung eines einheitlichen Servicekontos

für alle Verwaltungsdienstleistungen vermittelt werden, um Bürgerinnen, Bürger und Unternehmen zur Nutzung eines einzigen Servicekontos zu bewegen.

4.2 Freiwilligkeit

Festlegung 12: Eröffnung und Nutzung eines permanenten Servicekontos sind freiwillig.

Festlegung 13: Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen soll auch ohne dauerhafte Speicherung der Daten möglich sein. Für diesen Zweck sollen sog. temporäre Servicekonten angeboten werden. Die Nutzung eines temporären Servicekontos ist freiwillig.

Festlegung 14: Darüber hinaus sollen insbesondere Verwaltungsdienstleistungen, die keinen Personenbezug erfordern, auch ohne Servicekonto in Anspruch genommen werden können.

4.3 Einsatz von Identifizierungsmitteln

Festlegung 15: Der Einsatz eines Identifizierungsmittels am Servicekonto ist abhängig vom jeweiligen Vertrauensniveau der konkreten Verwaltungsdienstleistung.

Festlegung 16: Im Sinne der Einheitlichkeit und damit der einfachen Nutzbarkeit sollen gleichartige Verwaltungsdienstleistungen bundesweit auf demselben Vertrauensniveau genutzt werden. Grundsätzlich soll das Fachrecht das Vertrauensniveau der Verwaltungsdienstleistung definieren. Sofern eine fachgesetzliche Regelung nicht vorhanden ist, werden für die wichtigsten Verwaltungsdienstleistungen Empfehlungen erarbeitet. Grundlage ist die Handreichung des IT-Planungsrates mit Empfehlungen für die Zuordnung von Vertrauensniveaus in der Kommunikation zwischen Verwaltung und Bürgerinnen und Bürger bzw. der Wirtschaft.

4.4 Nutzung von Servicekonten

Festlegung 17: Für die Nutzung von Verwaltungsdienstleistungen melden sich Bürgerinnen und Bürger am Servicekonto mit einem Identifizierungsmittel an, mit dem sie/er mindestens das geforderte Vertrauensniveau erreichen kann.

Für Verwaltungsdienstleistungen für die kein besonderes Vertrauensniveau notwendig ist, ist eine pseudonyme Nutzung möglich. Außerhalb des Servicekontos ist auch eine anonyme Nutzung von Verwaltungsdienstleistungen möglich.

Festlegung 18: Grundsätzlich sollen Bürgerinnen und Bürger oder für Unternehmen handelnde Personen ihr Servicekonto auf unterschiedlichen Vertrauensniveaus nutzen.

4.5 Servicekonto für Unternehmen

4.5.1 Anwendungsbereich: Wer ist „Unternehmen“ im Sinne des Servicekontos?

Festlegung 19: Neben Servicekonten für Bürgerinnen und Bürger werden auch Servicekonten für Unternehmen bereitgestellt. Unternehmenskonten können nicht nur juristische Personen eröffnen und nutzen, sondern auch weitere Institutionen, wie z.B. Vereine, Stiftungen oder Behörden.

4.5.2 Rahmenbedingungen Servicekonto für Unternehmen

Festlegung 20: Bei Servicekonten für Unternehmen handeln natürliche Personen für ein Unternehmen.

Festlegung 21: Servicekonten für Unternehmen sind von den dazu berechtigten Personen zu eröffnen und zu verwalten.

Festlegung 22: Berechtigte Personen haben die erforderlichen Identitätsdaten zum Unternehmen zu übermitteln, die für spätere Verwaltungsdienstleistungen genutzt werden sollen.

Festlegung 23: Servicekonten für Unternehmen können grundsätzlich von mehreren Beschäftigten genutzt werden. Sollen Beschäftigte über das Servicekonto Verwaltungsdienstleistungen auf Vertrauensniveau „hoch“ / „hoch+“ nutzen, unterliegt das Hinzufügen dieser Personen dem Vertrauensniveau „hoch“ / „hoch+“.

Festlegung 24: Die vom Servicekonto für Unternehmen bereitgestellten Rollen und Berechtigungen sind von den Unternehmen in unternehmerischer Selbstverantwortung eigenverantwortlich zu steuern. Anbieter von Servicekonten können zusätzlich für Verwaltungsdienstleistungen ihres Zuständigkeitsbereichs Funktionalitäten zur Verwaltung von Rollen und Berechtigungen zur Unterstützung bereitstellen.

4.5.3 Nutzung eines Servicekontos für Unternehmen

Festlegung 25: Auch das Servicekonto für Unternehmen kann auf unterschiedlichen Vertrauensniveaus genutzt werden.

4.6 Löschung eines Servicekontos

Festlegung 26: Im Fall von eingerichteten, aber nicht genutzten Servicekonten, kann die Löschung eines Servicekontos innerhalb einer von dem Servicekonto-Anbieter zu definierenden Frist erfolgen.

Erläuterung: Hiermit soll die Anzahl eingerichteter, aber nicht genutzter Servicekonten und damit auch vorzuhaltenden Speicherkapazitäten sinnvoll beschränkt werden. Die Nutzerinnen und Nutzer sollen über diese Frist informiert und auf eine Löschung im Vorfeld hingewiesen werden. Es wird eine Frist von drei Jahren empfohlen.

4.7 Nutzung Postfach

Festlegung 27: Um auf Nachrichten des Postfachs zugreifen zu können, soll eine Identifizierung mit dem von der Dienstleistung bzw. der Nachricht abhängigen Vertrauensniveau erfolgen (vgl. Festlegungen 13 - 15).

Erläuterung: Je nach Gestaltung des Postfachs ist zu berücksichtigen, dass die Regelungen des Telekommunikationsgesetzes und des Telemediengesetzes anzuwenden und die sich daraus ergebenden technischen und organisatorischen Maßnahmen umzusetzen sind.

4.8 Einwilligung, Dokumente und Daten von anderen Behörden einzuholen

Festlegung 28: Es existieren Verwaltungsdienstleistungen, die erforderliche Nachweise aus bereits abgeschlossenen vorherigen Verwaltungsdienstleistungen benötigen. Das Servicekonto soll eine Einwilligungsfunktion enthalten, mit der eine Verwaltungsbehörde berechtigt wird, diese Unterlagen direkt bei einer anderen Verwaltungsstelle anzufordern, bei der diese Nachweise vorliegen, falls es dafür eine Rechtsgrundlage gibt.

Erläuterung: § 5 (2) EGovG Bund oder entsprechende Gesetze der Länder sehen vor: Die zuständige Behörde kann erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, mit der Einwilligung des Verfahrensbeteiligten direkt bei der ausstellenden öffentlichen Stelle elektronisch einholen. Zu diesem Zweck dürfen die anfordernde Behörde und die abgebende öffentliche Stelle die erforderlichen personenbezogenen Daten erheben, verarbeiten und nutzen. Einige Bundesländer haben jedoch eine solche Rechtsgrundlage derzeit nicht.

5 Interoperabilität

5.1 Gründe, Mehrwerte, Nutzen der Interoperabilität von Servicekonten

Neben der flächendeckenden Errichtung der Servicekonten wird mittelfristig die bundesweite Verknüpfung aller Servicekonten (Interoperabilität) angestrebt. Ein interoperabler Ausbau der Komponente Identifizierung ist mit Mehrwerten für viele Beteiligte verbunden:

- Bürgerinnen und Bürger können sich mit ihrem vertrauten Servicekonto identifizieren und dadurch Verwaltungsdienstleistungen in Deutschland und perspektivisch auch in der Europäischen Union in Anspruch nehmen. Der Zugang zu einfachem und sicherem E-Government wird damit erleichtert. Damit wird eine hohe Anwenderfreundlichkeit bei gleichzeitig angemessenen hohen Sicherheitsstandards geschaffen.
- Für Unternehmen wird ebenfalls die Möglichkeit einer zentralen Identifizierung gegenüber der Verwaltung geschaffen.
- Anbieter von Servicekonten steigern die Attraktivität ihres Servicekontos, indem sie Bürgerinnen und Bürgern die Möglichkeit bieten, sich für die Nutzung von Verwaltungsdienstleistungen über die Grenzen der Zuständigkeit ihres Servicekontos hinaus zu identifizieren.
- IT-Verantwortliche investieren in Servicekonten, die einem länderübergreifenden Standard entsprechen. Dies bietet hohe Investitionssicherheit.

5.2 Umfang der Interoperabilität

Festlegung 29: Perspektivisch sollen sich Nutzerinnen und Nutzer gegenüber ihrem Servicekonto identifizieren und damit Verwaltungsdienstleistungen einer Kommune, eines Landes und des Bundes in Anspruch nehmen können. Dies erfolgt unabhängig von der Zuständigkeit der Verwaltungsdienstleistung. Dabei ist insbesondere die datenschutzrechtliche Ausgestaltung zu berücksichtigen.

Erläuterung: Sofern gegenüber einer Verwaltungsdienstleistung eine Identifizierung über ein Servicekonto erforderlich ist, soll es für Nutzerinnen und Nutzer keine Rolle spielen, ob diese von der Kommune oder dem Land angeboten wird. Bei Umzug einer Person ist somit der „Umzug“ eines Servicekontos nicht erforderlich.

Festlegung 30: Servicekonten müssen bundesweit angebotenen Servicekonten vertrauen können. Aus diesem Grund wird bei der interoperablen Nutzung des Servicekontos ein Attribut zum Status des Vertrauensniveaus der Authentifizierung mitgeliefert.

Festlegung 31: Die Herstellung einer Interoperabilität mit anderen EU-Staaten wird mit der Europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS) verfolgt. Die damit verbundenen Anforderungen an Servicekonten werden berücksichtigt. Gleiches gilt für zusätzliche Aspekte der Entwicklung des Einheitlichen Ansprechpartners.

Festlegung 32: Die Übertragung von personenbezogenen Daten zwischen Servicekonten erfolgt ausschließlich über gesicherte Kommunikationswege.

Festlegung 33: Es sollen bevorzugt standardisierte technische Lösungen, bestehende Plattformen sowie bereits definierte Schnittstellen zum Einsatz kommen.

5.2.1 Einsatz von Identifizierungsmitteln

Festlegung 34: Welche Vertrauensniveaus in interoperablen Servicekonten zum Einsatz kommen, ist in der PG eID-Strategie unter Beteiligung des BSI zu entscheiden

Festlegung 35: Welche Identifizierungsmittel in den unterschiedlichen Vertrauensniveaus der interoperablen Servicekonten zum Einsatz kommen, ist in der PG eID-Strategie unter Beteiligung des BSI zu entscheiden.

5.2.2 Voraussetzungen für Servicekonten für Unternehmen auf Vertrauensniveau „hoch“ / „hoch+“

Festlegung 36: Folgende Voraussetzungen sind für die Nutzung von Verwaltungsdienstleistungen auf einem von der Verwaltungsdienstleistung geforderten und interoperabel definierten Vertrauensniveau über das Servicekonto für Unternehmen zu erfüllen:

- Die für das Unternehmen handelnde Person meldet sich zur Nutzung der Verwaltungsdienstleistung mindestens mit dem geforderten Vertrauensniveau an.
- Es liegen Daten und Nachweise zum Unternehmen vor, die den in Festlegung 37 dargestellten Voraussetzungen entsprechen und die eine eindeutige Identifizierung des Unternehmens sicherstellen.

Für die erste Ausbaustufe der Interoperabilität von Servicekonten für Unternehmen wird der Schwerpunkt auf die Vertrauensniveaus „hoch“ / „hoch+“ gesetzt.

Festlegung 37: Daten und Nachweise zum Unternehmen können für Verwaltungsdienstleistungen auf Vertrauensniveau „hoch“ / „hoch+“ unter folgenden Voraussetzungen genutzt werden:

a) Die berechtigte Person, meldet sich zur Übermittlung der Unternehmensdaten mit dem Vertrauensniveau „hoch“ / „hoch+“ am Servicekonto an und

b) sie übermittelt folgende Daten zum Unternehmen: Name oder Bezeichnung, Rechtsform, Registernummer soweit vorhanden, Anschrift des Sitzes oder der Hauptniederlassung und Namen der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter; ist ein Mitglied des Vertretungsorgans oder der gesetzliche Vertreter eine juristische Person, so sind deren Firma, Name oder Bezeichnung, Rechtsform, Registernummer soweit vorhanden und Anschrift des Sitzes oder der Hauptniederlassung zu erheben.

Erläuterung: Für juristische Personen und weitere Institutionen, die nicht in Registern geführt werden, entfällt die Angabe der Nummer aus einem Register.

c) Die berechtigte Person lädt im Servicekonto einen aktuellen Registereuszug des Unternehmens (z. B. Handelsregistereuszug) oder einen vergleichbaren Nachweis hoch.

Erläuterung: Langfristig wird angestrebt, dieses Verfahren durch einen elektronischen Abruf der Register zu ersetzen.

Nicht alle juristischen Personen werden in Registern geführt. Dies ist beispielsweise bei freiberuflich Selbstständigen, Rechtsanwälten oder Architekten der Fall. Als vergleichbare Nachweise gelten die in der Technischen Richtlinie TR 01201 „De-Mail Accountmanagement, Funktionalitätsspezifikation“ aufgeführten Identitätsnachweise für juristische Personen und weitere Institutionen.

d) Die berechtigte Person lädt zusätzlich auch die ihr eingeräumte Vollmacht hoch, wenn das Servicekonto nicht von einer der für das Unternehmen vertretungsberechtigten Person eingerichtet bzw. geführt wird.

Erläuterung: Beschäftigte, die ein Servicekonto einrichten bzw. verwalten, sind oft nicht identisch mit den vertretungsberechtigten Personen, die beispielsweise in einem Register eingetragen sind. Der Nachweis, dass ein Beschäftigter für das Unternehmen handeln darf, ist über eine Vollmacht nachzuweisen.

e) Eine Behörde prüft die Richtigkeit der eingegebenen Daten zum Unternehmen, die Nachweise zum Unternehmen und die Vollmacht und gibt die Unternehmensdaten für das Servicekonto frei.

Die berechtigte Person kann die in a) bis d) genannten Anforderungen auch im Rahmen eines persönlichen Erscheinens in der Behörde nachkommen. Die Behörde hat die berechtigte Person anhand von Ausweisdokumenten zu identifizieren.