KOORDINIERUNGSSTELLE FÜR IT-STANDARDS
KOSIT

Koordinierungsstelle
für IT-Standards

GESICHERTE ÜBERMITTLUNG VON DATEN IM EGOVERNMENT

Vorschlag zum weiteren Vorgehen

Entwurf vom 6. Mai 2015

1 Sachstand

Der IT-Planungsrat hat für die Standardisierungsagenda vom August 2012 den Bedarf an einer verbindlichen Vorgabe für die „gesicherte Übermittlung von Daten im E-Government“ (nachfolgend GÜDE) bestätigt. Der Bedarf besteht in einer einheitlichen Lösung für den elektronischen Datenaustausch, welche die rechtlichen Anforderungen an die Schutzziele Integrität, Authentizität und Vertraulichkeit sowie Nachvollziehbarkeit deckt. Die angestrebte Lösung soll sowohl die Datenübermittlung innerhalb der Verwaltung (G2G), als auch die mit Bürgern (G2C) und der Wirtschaft (G2B) mit einheitlichen Methoden und Technologien ermöglichen (siehe Anhang A dieses Dokuments).

Die Bearbeitung ist gemäß der für die Standardisierungsagenda vereinbarten Prozesse durch die KoSIT zusammen mit einer Fachgruppe erfolgt. Die Bedarfsbeschreibung sollte präzisiert und breit abgestimmt werden, um anschließend eine Lösung auszuwählen. Dabei haben sich jedoch erhebliche Probleme ergeben. Ohne grundlegende Änderungen ist nicht absehbar, dass dieser Prozess erfolgreich zu Ende geführt werden kann.

Der KoSIT-Beirat ist darüber erstmals zu dessen 10. Sitzung am 30.6.2014 unterrichtet worden. Nach Auffassung der KoSIT gibt es erhebliche Überschneidungen mit der vom IT-Planungsrat beauftragten PG „eID Strategie“ in den Bereichen G2C und G2B. Dieser Sachverhalt wurde im KoSIT-Beirat diskutiert. Es bestand Einigkeit, dass es Überschneidungen gibt. Uneinigkeit gab es in der Beurteilung, ob es im Bereich Bürger / Verwaltung durch die Arbeit der PG eID-Strategie für GÜDE *nichts* mehr zu tun gibt. Deshalb wurde im zweiten Fortschrittsbericht, der vom IT-Planungsrat in dessen 15. Sitzung beschlossen worden ist, der Projektstatus als „gefährdet (gelb)“ gewertet. Im weiteren Verlauf des Projekts ergaben sich zusätzliche Schwierigkeiten. Die von der KoSIT eingeleiteten Maßnahmen haben nicht zum gewünschten Erfolg geführt, so dass der Zustand des Projektes Ende 2014 als „kritisch (rot)“ bewertet werden musste. Die Bearbeitung ruht seither.

Die Mitglieder des KoSIT-Beirats haben die KoSIT aufgefordert, einen Vorschlag für das weitere Vorgehen zu erarbeiten. Der mit diesem Dokument vorgelegte Vorschlag wurde mit den Mitgliedern der GÜDE Fachgruppe abgestimmt. Er soll in der 12. Sitzung des KoSIT Beirats diskutiert und ggf. vom IT-Planungsrat entschieden werden. Die Kernaussagen lauten:

1. Für die sichere Datenübermittlung zwischen der Verwaltung und Bürgern / Wirtschaft werden Empfehlungen im Rahmen der vom IT-Planungsrat beschlossenen PG eID-Strategie erarbeitet. Bei planmäßigem Ablauf wird es keinen darüber hinaus gehenden Regelungsbedarf gemäß § 3 IT-Staatsvertrag für die sichere Datenübermittlung zwischen Verwaltung und Bürgern / Wirtschaft geben.
2. Es gibt jedoch weiterhin Regelungsbedarf gemäß § 3 IT-Staatsvertrag für die verwaltungsinterne Datenübermittlung. Entsprechende Regelungen müssen die gegenüber der ursprünglichen Beauftragung veränderten Rahmenbedingungen (IT-NetzG, Entscheidung 2015/03 der 16. Sitzung des IT-Planungsrats) angemessen berücksichtigen.
3. Die Bearbeitung des in Abschnitt 3.7 konkretisierten Standardisierungsbedarfs soll methodisch / strukturell an der von der PG eID Strategie vorgelegten Ergebnissen orientiert erfolgen.

2 Analyse der Ist-Situation

Vor der Erarbeitung eines Verfahrensvorschlags wurde zunächst die bestehende Ist-Situation hinsichtlich bekannter Schwachstellen und veränderter Rahmenbedingungen mit nachfolgendem Ergebnis geprüft.

Das Standardisierungsvorhaben war zu ambitioniert

Die derzeitige Bedarfsbeschreibung sieht vor, dass der Planungsrat für die sichere Datenübermittlung sowohl verwaltungsintern (G2G), als auch an Bürger (G2C) und Wirtschaft (G2B), eine einheitliche Lösung auswählt und verbindlich vorgibt[1]. Dieser Standardisierungsanspruch war zu ambitioniert.

Es gibt sehr unterschiedliche Anforderungen an sichere Datenübermittlungen in verschiedenen Szenarien. Zudem werden derzeit viele verschiedene Lösungen für die sichere Datenübermittlung mit und innerhalb der öffentlichen Verwaltung genutzt. Deren Anzahl muss zweifelsohne reduziert werden, aber es erscheint derzeit unrealistisch, dass sämtliche Szenarien zukünftig durch eine einzige, einheitliche Lösung erfolgreich abgedeckt werden könnten. Selbst wenn es eine solche Lösung gäbe, wäre deren politische Durchsetzbarkeit fraglich.

Die Rahmenbedingungen haben sich verändert

Seit der Entscheidung des Planungsrats über die erste Fassung der Standardisierungsagenda haben sich die Rahmenbedingungen der sicheren Datenübermittlung im E-Government verändert. Insbesondere bei der verwaltungsinternen Datenübermittlung sind der Bund und die Länder intensiv damit beschäftigt, die Sicherheit auf der Netzebene zu verbessern. Diesbezüglich sind insbesondere die IT-Sicherheitsleitlinie und das IT-Netzgesetz zu nennen. Gemäß § 3 IT-NetzG muss die Datenübermittlung zwischen Bund und Ländern seit dem 1.1.2015 über das Verbindungsnetz erfolgen. Die Auswirkungen auf die innerhalb der Verwaltung bestehenden Datenübermittlungen wurden geprüft, und es sind Lösungsvorschläge entwickelt worden, um den Aufbau doppelter Infrastrukturen zu vermeiden.

Diese Entwicklungen erfolgten unabhängig vom Standardisierungsvorhaben GÜDE. Sie haben aber erhebliche Rückwirkungen auf das Vorhaben, weil die Bedarfslage sich ständig verändert hat.

Die Bereiche G2B und G2C werden durch die PG eID Strategie abgedeckt

Im Herbst 2013 hat der IT-Planungsrat die „Strategie für eID und andere Vertrauensdienste im E-Government (eID-Strategie)“ verabschiedet (Beschluss 2013/27). Der Regelungsgegenstand sind Vertrauensdienste der Verwaltung für Bürger und Unternehmen, also G2C und G2B. Bund, Länder und Kommunen sollen auf Ebene der Behörden den elektronischen Zugang mit dem neuen Personalausweis und mit De-Mail eröffnen. Zudem sollen Empfehlungen für weitere Vertrauensdienste erarbeitet werden.

[1] Ob die Lösung für alle Zielgruppen gleich empfohlen wird, sollte im Rahmen der weiteren Bearbeitung geklärt werden.

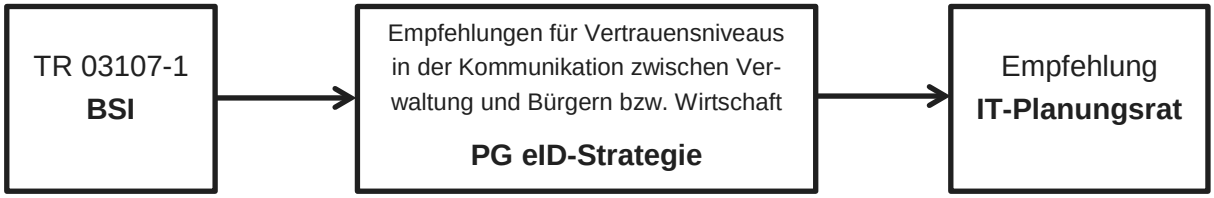
Der IT-Planungsrat hat die Erarbeitung einer eID-Strategie als Teil der Umsetzung der Nationalen E-Government-Strategie (NEGS) beschlossen. Bund, Länder und kommunale Spitzenverbände im IT-Planungsrat haben sich auf eine gemeinsame Strategie für eID und andere Vertrauensdienste im E-Government (eID-Strategie) geeinigt, 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 akzeptiert wird.

Die Grundlage hierfür ist die Technische Richtlinie (TR) 03107 des BSI, in der Vertrauensniveaus und Kriterien für Vertrauensdienste im Bereich G2C und G2B definiert werden. Hierzu gehört insbesondere die „Übermittlung von Dokumenten". Im Sinne der TR ist ein Dokument *„die Repräsentation einer abgeschlossenen Menge zusammengehörender Daten in physischer oder elektronischer Form[2]."* Diese abstrakte Definition umfasst auch die Übermittlung strukturierter Datensätze wie z.B. xjustiz im elektronischen Rechtsverkehr oder XMeld im Meldewesen und ist synonym zur *„Übermittlung von Daten"* im Sinne von GÜDE. Für bestimmte Vertrauensniveaus im Kontext der Übermittlung von Dokumenten / Daten werden Sicherheitsanforderungen gestellt (Vertraulichkeit, Integrität, Identifizierung der Kommunikationspartner) und jeweils geeignete Lösungen empfohlen.

Die Projektgruppe eID-Strategie wird dem IT-Planungsrat auf Grundlage der TR 03107 vorschlagen, welche Vertrauensdienste für welche typischen Verwaltungsleistungen, insbesondere solche mit hoher Fallzahl, zum Einsatz kommen sollen. (Maßnahme M5 der vom Planungsrat beschlossenen eID Strategie).

Zudem werden Handreichungen erarbeitet, mit denen die Anwendung der vom IT-Planungsrat 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 sollen durch den IT-Planungsrat veröffentlicht werden (Maßnahme M4 der vom Planungsrat beschlossenen eID Strategie).

Insofern wird es bei einem planmäßigen Verlauf der PG eID Strategie zeitnah Empfehlungen des IT Planungsrats geben, die für typische Verwaltungsdienstleistungen, die sich an Bürger oder Wirtschaft richten, angemessene Vertrauensniveaus und geeignete Lösungen nennen. Diese Empfehlungen werden insbesondere die sichere Übermittlung von Daten bzw. Dokumenten als Prozess innerhalb eines Vertrauensdienstes umfassen.



[2]TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government, Teil 1: Vertrauensniveaus und Mechanismen, Version 1.0 vom 9. 4. 2014, Abschnitt 2.1

Die Notwendigkeit der Erarbeitung einer darüber hinaus gehenden, verbindlichen Vorgabe des IT-Planungsrats gemäß § 3 IT-Staatsvertrag für einen IT-Interoperabilitätsstandard zur sicheren Übermittlung von Daten im E-Government im Sinne der Bedarfsbeschreibung von GÜDE ist damit für die Bereiche G2B und G2C zunächst nicht mehr gegeben.

3 Betrachtung des bestehenden Standardisierungsbedarfs

Angesichts der in Abschnitt 2 dargestellten Entwicklungen ist zunächst zu klären, ob der Bedarf an Vorgaben des IT-Planungsrats für die sichere Übermittlung von Daten im E-Government noch besteht. Da gemäß der obigen Ausführungen entsprechende Empfehlungen für die Datenübermittlungen zwischen der Verwaltung und den Bürgern bzw. der Wirtschaft als Ergebnis der vom IT-Planungsrat beschlossenen eID-Strategie zu erwarten sind, kann sich ein entsprechender Bedarf nur auf die verwaltungsinterne Datenübermittlung (G2G) beziehen.

Anhand von Beispielen kann belegt werden, dass der Bedarf noch besteht und insofern das Standardisierungsvorhaben GÜDE grundsätzlich fortzuführen ist, wenn auch mit Änderungen in der Vorgehensweise und dem angestrebten Geltungsbereich.

3.1 Beispiel „Übermittlung von Akten, Vorgängen und Dokumenten“

Zu den Standardisierungsvorhaben, die derzeit im Rahmen der Standardisierungsagenda bearbeitet werden, gehört auch die Auswahl eines geeigneten Standards für die Übermittlung von Akten, Vorgängen und Dokumenten. Das federführende Land Rheinland-Pfalz hat im März d.J. die Bedarfsbeschreibung veröffentlicht. Darin heißt es:

> *Regelungsgegenstand des Standards ist der Austausch von sogenannten Nachrichten im Zusammenhang mit der Übermittlung von Schriftgutobjekten. … Mechanismen und technische Infrastruktur für die Übertragung und Verschlüsselung sowie Sicherheitsmaßnahmen sind nicht Regelungsgegenstand des Standards[3].*

Die Trennung zwischen einem Fachstandard zur einheitlichen Darstellung fachlicher Inhalte (in diesem Fall die zu übermittelnden Schriftgutobjekte bzw. deren Metadaten) und fachunabhängigen Mechanismen zu deren sicheren Übermittlung ist ein bewährtes Verfahren. Konsequenterweise wird es zur Herstellung der vollständigen Interoperabilität bei der elektronischen Übermittlung von Schriftgutobjekten nicht ausreichend sein, wenn der IT-Planungsrat zum Abschluss des Standardisierungsvorhabens einen Fachstandard festlegt.

Es wird darüber hinaus der verbindlichen Vorgabe von Standards für die sichere Übertragung der Schriftgutobjekte in der vom IT Planungsrat bereitgestellten Infrastruktur bedürfen, da andernfalls unterschiedliche technische Gegebenheiten zwischen Bund und Ländern dem reibungslosen Datenaustausch entgegenstehen.

3.2 Beispiel „Übermittlung von Sterbefallmitteilungen“

Im Rahmen der Umsetzung des Personenstandsgesetzes ist unter Federführung des Landes NRW ein Fachstandard für die Übermittlung von Personenstandsdaten entwickelt worden.

[3] STANDARD FÜR DEN AUSTAUSCH VON AKTEN, VORGÄNGEN UND DOKUMENTEN / Bedarfsbeschreibung Version 1.0, Abschnitt 2.1

Ein bundesweiter elektronischer Informationsverbund der Standesämter ist erfolgreich in Betrieb. Zur Gewährleistung der Interoperabilität wird in der Personenstandsverordnung neben dem Fachstandard XPersonenstand auch OSCI für die sichere Datenübermittlung unter Nutzung der vom IT-Planungsrat bereitgestellten Infrastruktur vorgegeben.

Im Rahmen einer von mehreren Ländern gemeinsam genutzten Erweiterung sollen Sterbefallmitteilungen von Standesämtern an Gesundheitsämter übermittelt werden. Eine besondere Schwierigkeit bei dieser Erweiterung liegt darin begründet, dass die IT-Verfahren der Gesundheitsämter derzeit noch nicht auf die Nutzung der Infrastruktur des IT-Planungsrats vorbereitet sind. Dies betrifft sowohl die Sicherheit der Datenübermittlung (OSCI), als auch die Nutzung der erforderlichen Verzeichnisdienste (DVDV).

Eine Vorgabe des IT-Planungsrats für die sichere, verwaltungsinterne Datenübermittlung wäre hilfreich. Wenn es entsprechende Vorgaben gäbe, die auch in der Infrastruktur der Gesundheitsämter umgesetzt sind, könnte man sich darauf konzentrieren, die rechtlichen und fachlichen Aspekte der neuen Datenübermittlung abzustimmen.

3.3 Beispiel „Datenaustausch im Waffenwesen“

Die bisherige erfolgreiche föderale Gestaltung des Nationalen Waffenregisters (NWR) belegt bestehende Potenziale zur weiteren Modernisierung der Waffenverwaltung. Mit dem geplanten weiteren Ausbau des NWR können Prozesse im Waffenwesen zielgerichtet mit den Möglichkeiten des E-Government verbunden werden. Bei der Weiterentwicklung könnten zukünftig elektronische Prozessketten eingeführt werden, um manuelle Erfassungsaufwände zu reduzieren und die Auswertungsmöglichkeiten für die Polizeien von Bund und Ländern bedarfsgerecht zu erweitern.

Hierfür bedarf es jedoch zunächst einer Vereinheitlichung und Vereinfachung von Kommunikationswegen und Standards zwischen Fachverfahren im Waffenwesen. Denn aus der Perspektive eines Fachverfahrens, des Herstellers und der betreibenden Stelle erfolgt in der Praxis heute jeweils eine individuelle Anbindung auf unterschiedlicher technologischer Basis und möglicherweise auch über jeweils eigenständige Kommunikationsinfrastrukturen (z. B. OSCI, EGVP, DOI/Netze des Bundes, Internet) mit eigenständigen Betriebskosten[4].

3.4 Beispiel „Internetbasierte Fahrzeugzulassung“

Im Rahmen des Projektes „Internetbasierte Fahrzeugzulassung (i-KFZ)“ können Kommunen dezentrale Portale betreiben. Für die Absicherung der Kommunikationsverbindung dieser Portale mit dem KBA wird zumindest für die erste Stufe des Projektes kein herstellerunabhängiger Standard vorgegeben. Stattdessen wird mitgeteilt, welche Produkte eines bestimmten Herstellers im KBA eingesetzt werden. Diese herstellerspezifische Vorgabe wurde von einigen Ländern mit Überraschung zur Kenntnis genommen. Auf entsprechende Nachfragen hat sich der Bund dahingehend geäußert, dass es keine Möglichkeit gäbe, Einwände zu erheben, weil es bislang keinen Beschluss des IT-Planungsrats für ein verbindliches Übertragungsprotokoll gibt und dieser nicht kurzfristig zu erwarten sei.

[4] Bedarfsdarstellung *„Vereinfachung und Vereinheitlichung der Kommunikation zwischen Fachverfahren in der Waffenverwaltung“*, Projekt NWR, Dokument vom 20. 2. 2015. Der dort beschriebene Bedarf bezieht sich teilweise auf Datenübermittlungen zwischen der Verwaltung und externen Stellen, zum Teil auf verwaltungsinterne Datenübermittlungen zwischen Behörden.

Dies belegt den Standardisierungsbedarf. Gäbe es eine bereits Vorgabe des IT-Planungsrats für die sichere Datenübermittlung im E-Government auf der Basis eines IT-Interoperabilitätsstandards, dann bestünde keine Notwendigkeit zur Vorgabe produktspezifischer Lösungen durch Bundesbehörden.

3.5 Zur Rolle des IT-NetzG und des Verbindungsnetzes

Diese und weitere Beispiele zeigen den grundsätzlichen Bedarf an einer Vereinheitlichung der Infrastruktur für die sichere Datenübermittlung innerhalb der öffentlichen Verwaltung in Deutschland. Der Bund und die Länder haben seit der Feststellung des Standardisierungsbedarfs GÜDE im Jahr 2012 bereits wichtige Schritte zur Konsolidierung und Vereinheitlichung bestimmter Anteile die dieser Infrastruktur unternommen. Hier sind insbesondere das Steuerungsprojekt „Leitlinie Informationssicherheit“ des IT-Planungsrats (Beschluss 2013/01) sowie das Verbindungsnetz zu nennen, für dessen Koordination gemäß § 4 IT-Staatsvertrag der IT-Planungsrat zuständig ist. Insofern ist zu klären, ob die vereinbarten Maßnahmen so weitgehend sind, dass der in GÜDE postulierte Bedarf inzwischen nicht mehr besteht, oder ob es weiterhin einen Vereinheitlichungsbedarf gibt, wenn auch ggf. in modifizierter Form. Insbesondere ist zu klären, ob durch die seit dem 1.1.2015 bestehende Verpflichtung zur Nutzung des Verbindungsnetzes bereits eine hinreichende Vereinheitlichung der sicheren Datenübermittlung im E-Government erreicht worden ist, so dass es keiner darüber hinausgehenden Maßnahmen bedarf.

Der Bund hat das Verbindungsnetz zur Verbindung der informationstechnischen Netze des Bundes und der Länder errichtet. Der Datenaustausch zwischen dem Bund und den Ländern muss seit Beginn des Jahres 2015 über das Verbindungsnetz erfolgen. Mit der Bereitstellung dieser zentralen Infrastrukturkomponente und der rechtlichen Verpflichtung zu deren Nutzung unter bestimmten Umständen ist ein wichtiger Bereich erfolgreich vereinheitlicht worden. Dies ist jedoch aus folgenden Gründen nicht ausreichend, um den in diesem Dokument beschriebenen Bedarf vollumfänglich zu decken:

3.5.1 Sicherheit und Interoperabilität nur auf der Netzebene

Bei der Datenübermittlung werden unterschiedliche Ebenen bzw. Schichten unterschieden, auf denen jeweils unterschiedliche Aufgaben mit unterschiedlichen Mechanismen gelöst werden. Die entsprechenden Ebenen- bzw. Schichtenmodelle sind teilweise sehr differenziert (siehe z.B. das Open Systems Interconnection Model der ISO). Für die Diskussion im Rahmen dieses Dokuments ist eine Betrachtung von drei Schichten ausreichend[5]:

- **Netzebene:** Auf dieser Ebene werden Direktverbindungen zwischen Netzwerkkomponenten betrachtet. Die Aufgabe dieser Schicht ist es, zu einem empfangenen Datenpaket das nächste Zwischenziel zu ermitteln und das Datenpaket dorthin weiterzuleiten.
- **Transportebene:** Aus der Existenz elektronischer Netze folgt noch nicht die Erreichbarkeit der angeschlossenen IT-Verfahren. Es bedarf weitergehender Regelungen zum technischen Transport der Nachrichten. Die Transportschicht ermöglicht eine Ende-zu-Ende-Kommunikation. Dies betrifft Fragenstellungen der Adressierung auf Basis verwaltungsei-

[5] Vereinfachte Darstellung, orientiert am TCP/IP-Referenzmodell, siehe Beitrag „Internetprotokollfamilie“ in Wikipedia (http://de.wikipedia.org/wiki/Internetprotokollfamilie#TCP.2FIP-Referenzmodell)

gener Verzeichnisdienste, der zuverlässigen Zustellung sowie der Behandlung von Fehlern. Dieser Ebene sind auch Mechanismen zuzuordnen, die eine sichere Aufbewahrung von Nachrichten für den Fall realisieren, dass Empfänger nicht jederzeit erreichbar sind.

- **Anwendungsebene:** Die Anwendungsschicht umfasst alle Protokolle, die mit Anwendungsprogrammen zusammenarbeiten und die Netzwerkinfrastruktur für den Austausch anwendungsspezifischer Daten nutzen.

Verwaltungseigene Netze können Sicherheitsmechanismen und Interoperabilität originär nur auf der Netzebene bieten. Für entsprechende Funktionalitäten auf den beiden darüber liegenden Ebenen sind Ergänzungen (in Form von Protokollen oder Diensten) erforderlich.

Das vom IT-Planungsrat koordinierte Verbindungsnetz setzt Sicherheitsmechanismen grundsätzlich nur für *die* OSI-Schichten um, die der Netzebene zuzurechnen sind. Sicherheitsmechanismen höherer OSI-Schichten, die der Transport- und der Anwendungsebene zuzurechnen sind, werden nur für manche Dienste im Verbindungsnetz explizit gefordert. Zu diesen Diensten gehören die zentrale Verteilung interner E-Mails sowie DNS-Dienste.

Darüber hinaus dient das Verbindungsnetz der Verbindung der informationstechnischen Netze des Bundes und der Länder. Bei Datenübermittlungen, in denen das Verbindungsnetz involviert ist, sind insoweit grundsätzlich drei verwaltungseigene Netze zu betrachten:

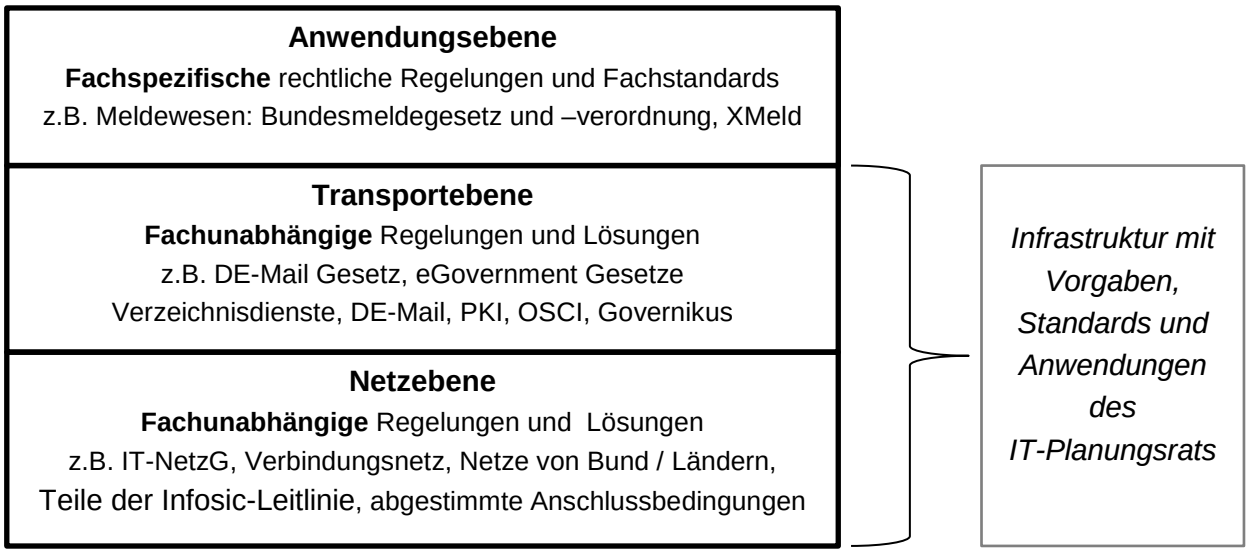
- Das verwaltungseigene Netz desjenigen Bundeslandes (oder des Bundes), in dem sich der erste der beiden Kommunikationspartner befindet;
- Das verwaltungseigene Netz desjenigen Bundeslandes (oder des Bundes), in dem sich der zweite der beiden Kommunikationspartner befindet;
- Das Verbindungsnetz, welches die beiden verwaltungseigenen Netze verbindet.

Sicherheitsanforderungen, die sich auf die gesamte Strecke zwischen den beiden Kommunikationspartnern beziehen, können nicht durch Mechanismen *eines* der beteiligten Netze umgesetzt werden. Hierfür bedarf es ergänzender Protokolle, die oberhalb der Netzebene zu realisieren sind. Dies ist in dem nachfolgenden Bild für eine Datenübermittlung zwischen zwei Kommunikationspartnern A und B dargestellt.

Für die verwaltungsinterne Datenübermittlung im E-Government ist es erforderlich, dass die Sicherheit und die Interoperabilität auf der gesamten Strecke und somit auch auf der Transport- und der Anwendungsebene gewährleistet werden können. Zu den Regelungssachverhalten, die der Transport- bzw. Anwendungsebene zuzurechnen sind und insofern grundsätzlich nicht durch das IT-NetzG bzw. das Verbindungsnetz allein gewährleistet werden können, gehören insbesondere die Authentizität der Kommunikationspartner sowie die Nachvollziehbarkeit der Übermittlung von Nachrichten zwischen dem Sender und dem Empfänger. Die Integrität der Datenübermittlung kann durch verwaltungseigene Netze auf der Netzschicht sichergestellt werden. Dies ist zu unterscheiden von der Integrität auf der Transportebene, die naturgemäß nicht durch die einzelnen Übertragungsnetze gewährleistet wer-

den kann. Auch die Ende-zu-Ende Verschlüsselung, d.h. der Schutz der übermittelten Daten auch vor den an der Übermittlung beteiligten Stellen, muss mit Mechanismen oberhalb der Netzebene sichergestellt werden.

Während die Anwendungsebene regelhaft fachspezifisch ist und entsprechende Vorgaben zur Gewährleistung von Sicherheit und Interoperabilität üblicherweise in Fachstandards bzw. Fachgesetzen zu finden sind, sind technische Maßnahmen für die Sicherheit und Interoperabilität auf der Transportebene fachunabhängig. Insoweit sehen wir eine Zuständigkeit des IT Planungsrats für Maßnahmen, die geeignet sind, die Interoperabilität und Sicherheit von Datenübermittlungen auf der Transportebene herzustellen bzw. zu optimieren. Die Mechanismen und Lösungen der Netz- und der Transportebene müssen aufeinander abgestimmt sein. Sie bilden eine gemeinsame Infrastruktur für sichere und interoperable Datenübermittlungen im E-Government.



3.5.2 Betrifft nicht alle verwaltungsinternen Datenübermittlungen

Angesichts der Verpflichtung, dass der Datenaustausch zwischen den Netzen des Bundes und denen der Länder nach § 3 IT-NetzG über das Verbindungsnetz erfolgt, hat der IT-Planungsrat für den Datenaustausch, an dem die Netze des Bundes nicht beteiligt sind, im Rahmen seiner 16. Sitzung beschlossen[6], dass folgendes gelten soll:

1. Nach Möglichkeit Sicherstellung der Nutzung des Verbindungsnetzes für den Datenaustausch durch Verwendung geeigneter Routingverfahren (ohne Anpassungen von Fachverfahren).
2. Wo dies nicht möglich ist, Feststellung des Schutzbedarfs (Erhebung der betroffenen Fachverfahren). Bei hohem und sehr hohem Schutzbedarf sollte das Verbindungsnetz genutzt werden, falls nicht bereits alternative und ausreichend sichere Sicherheitstechniken eingesetzt werden (z.B. OSCI-Transport, Verwaltungs-PKI).

[6] Entscheidung 2015/03 der 16. Sitzung am 18. März 2015 in Hannover

3. Die für die betroffenen Fachverfahren Verantwortlichen werden gebeten, entsprechende Maßnahmen zeitnah einzuleiten und bis zur Umsetzung dieser Maßnahmen die Verfahren in der jetzigen Form weiterzuführen.

Insofern wird es auch zukünftig Datenübermittlungen zwischen Verwaltungen unterschiedlicher Bundesländer geben, bei denen das Verbindungsnetz nicht genutzt werden wird. In diesen Fällen sind Vorgaben des Planungsrats nicht nur für die Transportebene, sondern auch für die Netzebene erforderlich[7].

Die Sicherheit auf der Netzebene wird in diesen Fällen durch alternative und ausreichend sichere Sicherheitstechniken zu gewährleisten sein. Hierfür bedarf es Lösungen, die zwischen Bund und Ländern abgestimmt worden sind, weil nur so die Interoperabilität sichergestellt werden kann. Das dafür zuständige Gremium ist der IT-Planungsrat.

3.6 Zusammenfassung des Standardisierungsbedarfs

Der ursprünglich vom IT Planungsrats beschlossene Standardisierungsbedarf für die gesicherte Übermittlung von Daten im E-Government (GÜDE) gemäß der Bedarfsbeschreibung vom Juni 2012 besteht heute nicht mehr. Bei einer planmäßigen Bearbeitung der im Rahmen der eID-Strategie beschlossenen Maßnahmen wird es zeitnah Empfehlungen des IT-Planungsrats für die sichere Datenübermittlung zwischen Verwaltung und Bürgern (G2C) und der Wirtschaft (G2B) geben. Diese Empfehlungen werden auf der technischen Richtlinie 03107 basieren. Für diese beiden wichtigen Bereiche der Datenübermittlungen besteht inzwischen kein Bedarf an zusätzlichen Beschlüssen im Sinne des § 3 IT-Staatsvertrag, der über die bereits beschlossenen Maßnahmen der eID-Strategie hinausgeht.

Es besteht jedoch weiterhin ein Standardisierungsbedarf für die sichere und interoperable Datenübermittlung innerhalb der Verwaltung (G2G). Mit der Errichtung des Verbindungsnetzes und den rechtlichen Verpflichtungen zu dessen Nutzung im IT-NetzG sind zwar erhebliche Fortschritte für eine Vereinheitlichung erzielt worden. Gleichwohl bedarf es aus den nachfolgenden Gründen ergänzender Regelungen bzw. Vorgaben des IT-Planungsrats:

- Verwaltungseigene Netze können Sicherheitsmechanismen nur auf der Netzschicht gewährleisten. Für die Authentisierung von Sender und Empfänger der Nachrichten (Kommunikationsendpunkte), für die Nachvollziehbarkeit der Datenübermittlungen (Quittungen), für die Ende-zu-Ende Verschlüsselung und für die Integrität (auf Transportebene) der Nachrichtenübermittlungen bedarf es Mechanismen, die nicht der Netzebene, sondern der Transport- bzw. der Anwendungsebene zuzuordnen sind.
- Gemäß der Beschlusslage des IT-Planungsrats (Entscheidung 2015/03 der 16. Sitzung) wird es auch zukünftig Datenübermittlungen zwischen Behörden unterschiedlicher Bundesländer geben, die nicht das Verbindungsnetz nutzen, sondern stattdessen andere, ausreichend sichere Sicherheitstechniken.

[7] Ggf. mit Ausnahme jener Fälle, in denen Bundesländer gemeinsame Verfahren bei einem gemeinsamen ITK-Dienstleister betreiben (z.B. Dataport für HH, SH und HB). In diesen Fällen werden abgestimmte Sicherheitsmechanismen und die Interoperabilität durch dem Betreiber gewährleistet.

3.7 Konkrete Benennung des Standardisierungsbedarfs

1. Geltungsbereich: Betroffen sind elektronische Übermittlungen von Daten (bzw. Dokumenten im Sinne der TR 03107), bei denen sowohl der Sender als auch der Empfänger zur öffentlichen Verwaltung gehören[8].
2. Unabhängig davon, ob das Verbindungsnetz für den Datenaustausch genutzt wird oder nicht, besteht folgender Regelungsbedarf:
   a. *Welche Sicherheitsanforderungen bestehen, die der Transportebene zuzuordnen sind und daher durch das Verbindungsnetz nicht abgedeckt werden?*
   b. *Welche Mechanismen sollen eingesetzt werden, um diese Anforderungen abzudecken?*
3. Sofern für den Datenaustausch das Verbindungsnetz gemäß Ziffer 2 der Entscheidung 2015/03 nicht genutzt wird, besteht zusätzlich folgender Regelungsbedarf:
   c. *Welche Sicherheitstechniken sollen eingesetzt werden, um die Sicherheitsanforderungen umzusetzen, die der Netzebene zuzuordnen sind?*

Eine Betrachtung der aktuellen Situation für typische Szenarien der sicheren Datenübermittlung zeigt, dass es inzwischen für alle in der Praxis vorkommenden Szenarien im Sinne der obigen Darlegung des Standardisierungsbedarfs eine Vielzahl von Lösungen gibt. Sie reichen von herstellerspezifischen Produkten (z. B. die Vorgabe des KBA zur Anbindung dezentraler Portale in der ersten Stufe des i-KFZ Projektes) über domänenspezifische Regelungen (z.B. EGVP im elektronischen Rechtsverkehr) bis zu konkurrierenden Standards und Lösungen für unterschiedliche Zielgruppen (z. B. eXtra und OSCI).

Der Bedarf an Vorgaben des Planungsrats für die sichere, verwaltungsinterne Datenübermittlung im E-Government bezieht sich insoweit nicht auf die Behebung eines Mangels. Es besteht weder der Bedarf an zusätzlichen technischen Lösungen noch an der Entwicklung eines zusätzlichen Standards. Vielmehr geht es darum, die Vielzahl der Mechanismen, Standards und Anwendungen durch Vorgaben des IT-Planungsrats auf ein überschaubares und wirtschaftlich vertretbares Maß zu reduzieren.

[8] Diese Formulierung wurde bewusst so gewählt, dass sie grundsätzlich auch landesinterne Datenübermittlung umfassen kann. Unabhängig von Fragen der rechtlichen und tatsächlichen Durchsetzbarkeit von Vereinbarungen auf Basis des IT-Staatsvertrags sind wir der Auffassung, dass der hier beschriebene Standardisierungsbedarf auch bei landesinternen Datenübermittlungen besteht.

4 Empfehlung zum weiteren Vorgehen

Nachdem dargelegt worden ist, dass es den Bedarf an Vorgaben des IT Planungsrats für den sicheren Datenaustausch innerhalb der öffentlichen Verwaltung gibt und wie er beschaffen ist, ist der Weg zu entsprechenden Vorgaben des IT-Planungsrats zu klären.

4.1 Erarbeitung einer technischen Richtlinie

Zur Deckung des in Abschnitt 3.6 dargelegten Standardisierungsbedarfes ist die Erarbeitung einer technischen Richtlinie geeignet, die methodisch an die TR 03107-1 angelehnt ist. Die genannte TR deckt ausschließlich die elektronische Kommunikation der Verwaltung mit externen Stellen (Bürger, Wirtschaft) ab. Ihr grundsätzlicher Aufbau kann jedoch auch für Festlegungen der verwaltungsinternen elektronischen Dienste genutzt werden:

- Festlegung von drei unterschiedlichen Vertrauensniveaus (normal, hoch, hoch+) für unterschiedliche Qualitäten und Anforderungen an die Kommunikation;
- Festlegung grundsätzlicher Kriterien z.B. für Authentisierungsmechanismen, Absicherung der Kommunikationsbeziehungen, etc. für die genannten Vertrauensniveaus;
- Festlegung spezifischer Kriterien für die betrachteten Vertrauensdienste (Identifizierung, Abgabe einer Willenserklärung, Dokumentenübermittlung, Übermittlung von Identitätsdaten);
- Bestimmung der Mechanismen (Standards / Technologien / Verfahren), welche die Kriterien erfüllen und insofern für die Vertrauensdienste geeignet sind, wenn ein bestimmtes Vertrauensniveau gefordert wird.

Daher wird die Erarbeitung einer technischen Richtlinie *„TR 03107-x „Verwaltungsinterne Elektronische Identitäten und Vertrauensdienste im E-Government“* (Arbeitstitel) vorgeschlagen. Basierend auf einer solchen TR können im Rahmen von GÜDE Handreichungen für typische verwaltungsinterne Dienste, insbesondere für solche mit einer hohen Fallzahl, erarbeitet werden. (Analog der Erarbeitung von Handreichungen für G2B und G2C durch die PG eID Strategie, basierend auf der TR 03107-1)

Ein wesentlicher Unterschied dieser Vorgehensweise zu dem bisher im Vorhaben GÜDE gewählten Vorgehen besteht darin, dass GÜDE das Ziel hat, einen einzigen IT-Interoperabilitätsstandard für die sichere Datenübermittlung festzulegen. Die TR 03107-1 lässt hingegen für bestimmte Kombinationen von Vertrauensdiensten und gefordertem Vertrauensniveau mehr als einen Mechanismus zu. Beispielsweise sind für den Vertrauensdienst „Abgabe einer Willenserklärung“ drei Mechanismen festgelegt[9], sofern das Vertrauensniveau „Normal“ als ausreichend erachtet wird.

Dies entspricht nicht dem Ideal, die vollständige Interoperabilität der Datenübermittlung dadurch zu erreichen, dass vom IT Planungsrats ein einziger Standard vorgegeben wird, der bei Bund und Ländern umgesetzt werden muss. Diesem Einwand kann entgegengehalten werden, dass es aus heutiger Sicht unrealistisch ist, dass Bund und Länder sich auf eine

[9] Die drei Mechanismen sind: a) Fortgeschrittene elektronische Signatur mit Softwaretoken, b) Nutzerinteraktion und c) TAN-Verfahren. Siehe TR 3107-1 Version 1.0, Tabelle 7 in Abschnitt 5.

einzige Lösung verständigen werden, selbst wenn dafür sehr großzügige Übergangsregelungen gelten sollen. Angesichts der großen Vielfalt von Produkten, bereichsspezifischen Lösungen und konkurrierenden Standards, die derzeit bei Bund, Ländern und Kommunen umgesetzt sind, ist der Zwischenschritt der Reduktion auf ein fachlich und wirtschaftlich vertretbares Portfolio von Lösungen praxistauglicher als das Ziel einer einzigen Lösung.

4.2 Entscheidung des IT-Planungsrats

Nach der Erarbeitung einer entsprechenden technischen Richtlinie kann der IT-Planungsrat diese entscheiden. Der IT-Planungsrat entscheidet durch Beschluss oder Empfehlung.

Für die TR 03107-1 bzw. die darauf basierenden Handlungsempfehlungen der PG eID-Strategie ist eine Entscheidung durch Empfehlung vorgesehen.

Bezüglich der von uns vorgeschlagenen TR 03107-x bzw. darauf basierenden Handlungsempfehlungen für die verwaltungsinterne Kommunikation sollte zu gegebener Zeit diskutiert werden, ob eine Empfehlung oder ein Beschluss angemessen ist. Wenn der Weg des Beschlusses gewählt wird, so entsteht Bindungswirkung bei Bund und Ländern. In diesem Fall ist die Frist zur Umsetzung des Beschlusses von IT-Planungsrat festzulegen.

4.3 Bearbeitung außerhalb der Standardisierungsagenda

Der übliche Weg für eine Beschlussfassung des Planungsrats zur verbindlichen Vorgabe eines IT-Interoperabilitätsstandards ist in den Prozessen der Standardisierungsagenda beschrieben. Das derzeit noch aktuelle Vorhaben GÜDE sollte entsprechend dieser Prozesse bearbeitet werden.

Die Prozesse der Standardisierungsagenda sind jedoch aus den nachfolgend dargestellten Gründen für das vorgeschlagene Vorgehen nicht geeignet:

Die Standardisierungsagenda ist für den Zweck entwickelt worden, dass aus einer Menge von IT-Interoperabilitätsstandards derjenige ausgewählt wird, der am besten geeignet ist, einen zuvor präzise beschriebenen Bedarf zu decken. Die vereinbarten Prozesse bieten Mechanismen, die erforderlich sind, um diesen Auswahlprozess nachvollziehbar und transparent zu gestalten.

Dieses Vorgehensmodell passt jedoch nicht für den hier unterbreiteten Vorschlag zum weiteren Verfahren. Die zu erarbeitende technische Richtlinie TR 03107-x soll nicht als ein möglicher Lösungskandidat betrachtet werden, dessen Eignung im Vergleich zu anderen, konkurrierenden Lösungen zu prüfen wäre. Sie soll vielmehr zielgerichtet so entwickelt werden, dass sie anschließend vom IT Planungsrats entschieden werden kann.

Aus diesem Grund wird vorgeschlagen, das Vorhaben „gesicherte Übermittlung von Daten im e-Government“ bei der nächsten Beschlussfassung des IT-Planungsrats zur Fortschreibung der Standardisierungsagenda von dieser zu entfernen und stattdessen die KoSIT zu beauftragen, die Erarbeitung einer Technischen Richtlinie für verwaltungsinterne Elektronische Identitäten und Vertrauensdienste im E-Government sowie darauf aufbauende Handlungsempfehlungen für typische verwaltungsinterne Dienste zu organisieren.

Die Erfahrungen aus der PG eID-Strategie legen nahe, dass ein Zeitraum von ca. zwei Jahren für die Bearbeitung dieses Themas vorzusehen ist.

A Aktuell geltende Bedarfsbeschreibung (Stand 2012)

Der IT-Planungsrat hat in der 8. Sitzung am 21. Juni 2012 mit der Entscheidung 2012/23 die erste Fassung der Standardisierungsagenda beschlossen. Diese enthält unter anderem den folgenden Standardisierungsbedarf.

Gesicherte Übermittlung von Daten im E-Government (GÜDE)

Zur Realisierung medienbruchfreier Prozesse des E-Government bedarf es einer einheitlichen Lösung für den elektronischen Datenaustausch, der die rechtlichen Anforderungen an die Schutzziele Integrität, Authentizität und Vertraulichkeit sowie Nachvollziehbarkeit deckt.

Daten sollen in unstrukturierter wie auch strukturierter Form übertragen werden können, um auch die Maschine-zu-Maschine-Kommunikation gezielt unterstützen zu können.

Die angestrebte Lösung soll sowohl die Datenübermittlung innerhalb der Verwaltung (G2G), als auch die mit Bürgern (G2C) und der Wirtschaft (G2B) mit einheitlichen Methoden und Technologien ermöglichen. Ob die Lösung für alle Zielgruppen gleich empfohlen wird, ist in der weiteren Bearbeitung zu klären.

Die bestehenden rechtlichen Anforderungen müssen durch die angestrebte Lösung allgemeingültig und auf der Basis existierender Infrastrukturen gedeckt werden. Dies sind insbesondere die Verzeichnisdienste DVDV und SAFE, die Public-Key- Infrastruktur PKI-1-Verwaltung, die bei Bund, Ländern und Kommunen betriebenen Intermediäre sowie die in vielen Ländern eingerichteten Clearingstellen.

Die angestrebte Lösung muss in Kombination mit dem vom IT-Planungsrat koordinierten Verbindungsnetz genutzt werden können und dieses um die erforderlichen Mechanismen zur Authentisierung, Integrität und Nachvollziehbarkeit ergänzen.

Die im Zusammenhang mit dem neuen Personalausweis aufgebaute Infrastruktur sowie die existierenden Infrastrukturen zur Verwendung elektronischer Signaturen müssen genutzt werden können. Dies soll die Einbindung von Bürgern und Unternehmen in die o.g. Kommunikationsszenarien vereinfachen.

Die öffentliche Verwaltung betreibt Anwendungen mit unterschiedlichsten Sicherheitsanforderungen. Deshalb muss die angestrebte Lösung mittels Profilierung unterschiedliche Schutzbedarfsklassen effizient und wirtschaftlich umsetzen können.

Um eine wirtschaftliche Umsetzung zu gewährleisten, muss die angestrebte Lösung so weit wie möglich auf existierenden internationalen und europäischen Standards basieren.