Governikus KG

# Leitfaden für die öffentliche Verwaltung

Möglichkeiten und Verpflichtungen der eIDAS-Verordnung für die Anerkennung elektronischer Identitäten aus anderen EU-Mitgliedstaaten

# Inhaltsverzeichnis

# 1 Einleitung

Seit November 2010 steht in Deutschland mit dem deutschen Personalausweis und dem elektronischen Aufenthaltstitel die Online-Ausweisfunktion für die elektronische Identifizierung zur Verfügung. Diese ermöglicht es, Dienste, die das Vertrauensniveau „hoch“ nach der europäischen „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (eIDAS Verordnung[1]) erfordern, zu nutzen. Mittlerweile existieren hierzulande zahlreiche Anwendungen der öffentlichen Verwaltung, die diese Funktion für ihr eGovernment-Angebot anbieten.

Mit dem „Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen“ (Onlinezugangsgesetz - OZG[2]) wurde darüber hinaus die Verpflichtung geschaffen, innerhalb der kommenden fünf Jahre alle Verwaltungsleistungen (soweit digitalisierbar) auch elektronisch über Verwaltungsportale anzubieten. Für die Umsetzung kann dabei auf ein „Nutzerkonto“ (auch „Servicekonto“) als eine zentrale Identifizierungskomponente zurückgegriffen werden. Es besteht die Möglichkeit, über ein Nutzerkonto mithilfe der Online-Ausweisfunktion Verwaltungsdienstleistungen auf Vertrauensniveau „hoch“ und den weiteren Vertrauensniveaus zu verwenden. Die jeweilige Anwendung gibt dabei vor, *welches* Vertrauensniveau zu ihrer Nutzung benötigt wird.

Die Anzahl der Online-Angebote der öffentlichen Verwaltung wird aus den oben genannten Gründen in den nächsten Jahren erheblich zunehmen und die Verpflichtungen der eIDAS-Verordnung müssen bei bestehenden und zukünftigen Angeboten berücksichtigt werden.

Die eIDAS-Verordnung schafft nun einen Rahmen zur elektronischen Interaktion zwischen Bürgern, Unternehmen und öffentlichen Stellen auch über die Landesgrenzen der Mitgliedstaaten hinweg. Die eIDAS-Verordnung stellt damit unter anderem ein verbindliches Regelwerk für die Bereiche elektronische Identitäten, Signaturen und Webseiten-Zertifikate auf. Da es sich bei einer Verordnung um einen verbindlichen Rechtsakt handelt, müssen alle Länder der europäischen Gemeinschaft diese in vollem Umfang umsetzen.

Dieser Leitfaden widmet sich ausschließlich dem Teilbereich „elektronische Identitäten“ der eIDAS-Verordnung mit dem Ziel, Informationen zu den sich aus der Verordnung ergebenden Verpflichtungen für die öffentliche Verwaltung in Deutschland zu vermitteln. Im Vordergrund stehen dabei die Anbindung an die zugehörige eIDAS-Infrastruktur, d.h. der durch die EU spezifizierten Interoperabilitätsinfrastruktur[3], sowie eIDAS-relevante Anpassungen für Anwendungen beim Einsatz elektronischer Identitäten. Die eIDAS-Verordnung selbst soll und kann an dieser Stelle nicht im Detail erläutert werden; nützliche Links zu diesem Thema finden Sie im Abschnitt „“ und auf dem Personalausweisportal des Bundesministerium des Innern, für Bau und Heimat (BMI)[4].

Das vorliegende Dokument richtet sich insbesondere an Fach- und IT-Entscheider in den Landes- und Kommunalverwaltungen, dem Bund und der Wirtschaft, um ihre aktuellen

1 Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=DE

2 https://www.gesetze-im-internet.de/ozg/BJNR313800017.html

3 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/Elektronische_Identifizierung/Interoperabilitaet/Interoperabilitaet_node.html

4 https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eIDAS_Verordnung_EU_node.html

Angebote, Projekte und zukünftigen Vorhaben mit den kommenden Verpflichtungen und Möglichkeiten abgleichen zu können, die sich aus der eIDAS-Verordnung ergeben.

# 2 Grundlegende Festlegungen der eIDAS-Verordnung

Im Folgenden werden grundlegende Festlegungen und Begriffe zum Verständnis kurz erläutert. Für tiefergehende Informationen zu den einzelnen Abschnitten beachten Sie bitte die Fußnoten und den Abschnitt „“.

### LEVEL OF ASSURANCE/VERTRAUENSNIVEAU

Die Durchführungsverordnung (EU) 2015/1502 regelt die technischen Mindestanforderungen an die Vertrauensniveaus (in den Texten der Verordnung auch „Sicherheitsniveau“). Es existieren die Vertrauensniveaus: **niedrig, substanziell** und **hoch** (low, substantial, high). Die BSI TR-03107-1 überträgt und detailliert die Anforderungen der eIDAS-Verordnung.

### ANERKENNUNGSVERPFLICHTUNG

Die Anerkennung von eID-Systemen in der Europäischen Union und dem Europäischen Wirtschaftsraum ist nach der eIDAS-Verordnung dann verpflichtend, wenn diese gegenüber der EU-Kommission notifiziert wurden. Gegenstand des Notifizierungsverfahrens ist unter anderem die Festlegung des bereitgestellten „Vertrauensniveaus“ und der „Mindestdatensatz“ des Mitgliedstaates.

Eine erfolgreiche Notifizierung eines eID-Systems wird im Amtsblatt der Europäischen Union veröffentlicht und mündet in einer Anerkennungspflicht durch die Anwendungen der öffentlichen Verwaltung mit einer Übergangsfrist von 12 Monaten.

**Die grundlegende Anerkennungsverpflichtung startet gemäß eIDAS Verordnung am 29.09.2018.** Als erstes eID-System wurde am 26.09.2017 der deutsche Personalausweis mit der Online-Ausweisfunktion auf Vertrauensniveau „hoch“ notifiziert.

Zahlreiche weitere Mitgliedstaaten planen im Laufe des Jahres 2018 und in 2019 die Notifizierung ihrer eID-Systeme.

Die Anerkennungsverpflichtung von weiteren notifizierten eID-Systemen durch die deutsche Verwaltung greift daher noch im Jahr 2019.

Eine Anerkennungsverpflichtung besteht für solche eID-Systeme, die mindestens auf dem Niveau „substantiell“ notifiziert wurden (vgl. auch Abbildung 1: Kurzüberblick Anerkennungspflicht).

In der folgenden Grafik können Sie prüfen, ob die eIDAS-Verordnung für Sie einen Handlungsbedarf nach sich zieht.

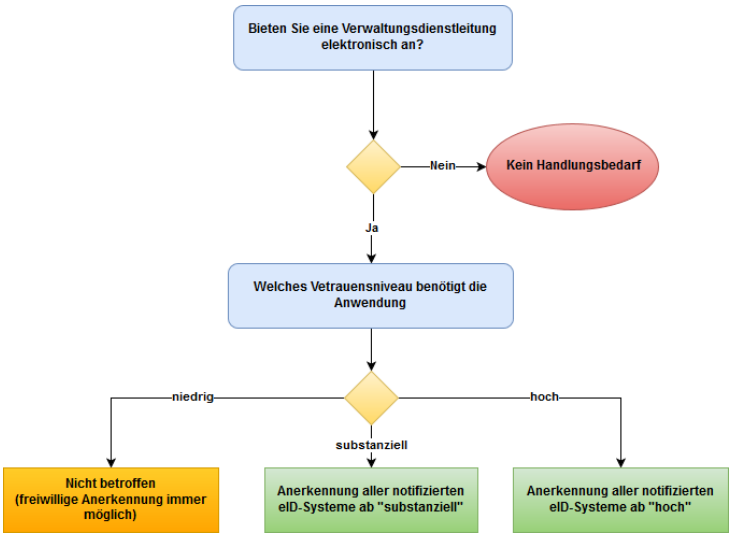


*Abbildung 1:Kurzüberblick Anerkennungspflicht*

| | |
|---|---|
|  | Falls Sie eine Verwaltungsdienstleistung elektronisch anbieten, sollten Sie unabhängig vom Vertrauensniveau weiterlesen. |

### ARCHITEKTURENTSCHEIDUNG

Eine grundlegende Architekturentscheidung für die grenzüberschreitende Authentisierung besteht in der Festlegung, dass der eigentliche Authentisierungsvorgang immer auf dem System des *sendenden* Landes durchgeführt wird. Das kann dabei über einen sog. Proxy oder eine Middleware erfolgen. Der wesentliche Unterschied zwischen diesen beiden Ansätzen ist, dass ein Proxy durch den sendenden EU-Mitgliedsstaat betrieben wird, während die eine Middleware als Software durch den sendenden EU-Mitgliedsstaat bereitgestellt wird. Vertreter aller EU-Mitgliedsstaaten legen technische Spezifikationen fest, in denen festgeschrieben ist, wie die Anfrage übermittelt und das Ergebnis der Authentisierung sowie die entsprechenden Daten an die aufrufende Anwendung im empfangenden Mitgliedstaat zurückgegeben werden.

| | |
|---|---|
|  | **Die Perspektive im eIDAS-Netzwerk ist wichtig.**<br>Das eIDAS-Netzwerk unterscheidet zwischen dem sendenden und dem empfangenden EU-Mitgliedstaat. Der sendende Mitgliedstaat ist das Land des Bürgers, der empfangende Mitgliedstaat ist das Land der Anwendung. Im Fall der eIDAS-Umsetzung in Deutschland ist Deutschland immer der empfangende Mitgliedstaat. |

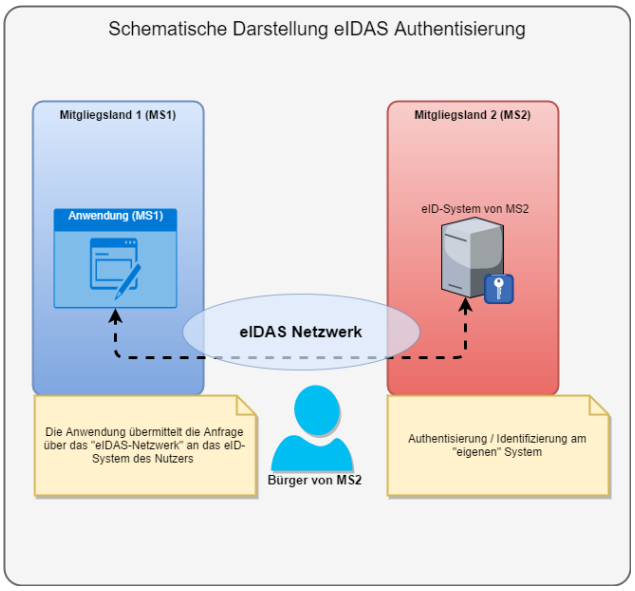


*Abbildung 2: schematische Darstellung Authentisierung*

Das eIDAS-Netzwerk übermittelt die Anfrage der Anwendung mittels verschiedener Komponenten an das eID-System des sendenden Landes. Der Zusammenschluss dieser Komponenten wird als eIDAS-Netzwerk bezeichnet[5].

### MINDESTDATENSATZ

Eine wesentliche Festlegung in der Verordnung (EU) 2015/1501 ist die Definition des **Mindestdatensatzes (MDS)** für natürliche Personen. Dieser legt die Menge der Merkmale fest, mit denen ein Mitgliedsstaat gegenüber einem anderen die eineindeutige Identifizierung einer natürlichen Person garantiert. In der Verordnung wird auch der MDS für juristische Personen festgelegt, der in diesem Leitfaden jedoch nicht weiter betrachtet wird, da es nur um Anwendungsfälle für natürliche Personen geht.

Für natürliche Personen schreibt die Verordnung den folgenden Mindestdatensatz vor:

- **Verpflichtend:** derzeitige(r) Familienname(n), derzeitige(r) Vorname(n), Geburtsdatum, eine eindeutige Kennung
- **Optional:** Vorname(n) und Familienname(n) bei der Geburt, Geburtsort, derzeitige Anschrift, Geschlecht

Im Rahmen des Notifizierungsverfahrens legt ein Land den Umfang des „eigenen“ Mindestdatensatzes fest. Dessen Umfang orientiert sich an den Anforderungen, die zur Realisierung des angestrebten Vertrauensniveaus zu erfüllen sind. Dabei ist der verpflichtende Teil des MDS immer zu verwenden, die optionalen Teile können bedarfsweise hinzugenommen werden. Die folgende Grafik illustriert die Festlegung anhand der Notifizierung der Online-Ausweisfunktion.

5 https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

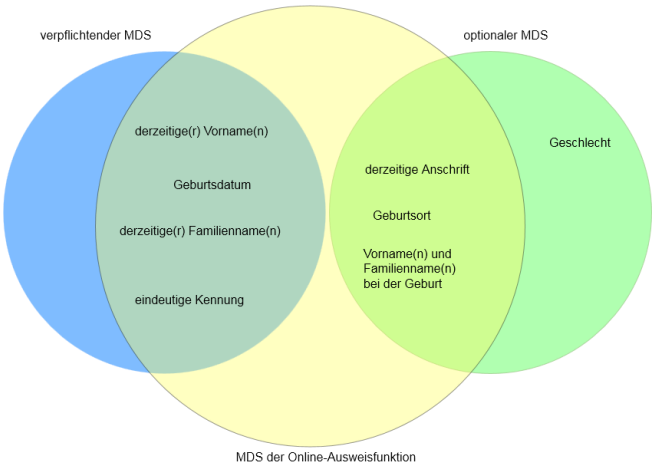


*Abbildung 3: MDS Beispiel Online-Ausweisfunktion*

# 3 Wesentliche Herausforderungen durch die eIDAS-Verordnung

Mit der Umsetzung der eIDAS-Verordnung gehen wesentliche Herausforderungen einher:

## Technische Umsetzung zur Anerkennung von europäischen Identitäten

Im Dezember 2016 startete unter der Konsortialführung der Governikus KG das durch die europäische Kommission geförderte Projekt TREATS (TRans-European AuThentication Services). Es verfolgte das Ziel, die technischen Implikationen der eIDAS-Verordnung zu erproben und die eID-Landschaft in Deutschland in Hinblick auf die Anerkennungsverpflichtung von Identitäten aus dem EU-Ausland eIDAS-fähig zu machen.

Alle bekannten deutschen Hersteller von eID-Servern, die bisher die Online-Ausweisfunktion unterstützen, haben im Rahmen des Projekts TREATS ihre eID-Server so erweitert, dass über diese eIDAS-Authentisierungen ausgelöst werden können.

### Die eID-Landschaft wird eIDAS-fähig

Ausgehend von der Beobachtung, dass in der Regel alle Anwendungen und Nutzerkonten zur Durchführung der Online-Ausweisfunktion entsprechende eID-Server nutzen, lag der Ansatz nahe, diese eID-Server auch eIDAS-fähig zu machen. Die so entstandenen eID(AS)-Server – die Erweiterung der eID-Service um „eIDAS-Konnektoren“ zur Anbindung an die eIDAS-Interoperabilitätsinfrastruktur – ermöglichen mit geringem Aufwand die Nutzung eIDAS-konformer eID-Systeme, sofern die Online-Ausweisfunktion bereits genutzt wird oder genutzt

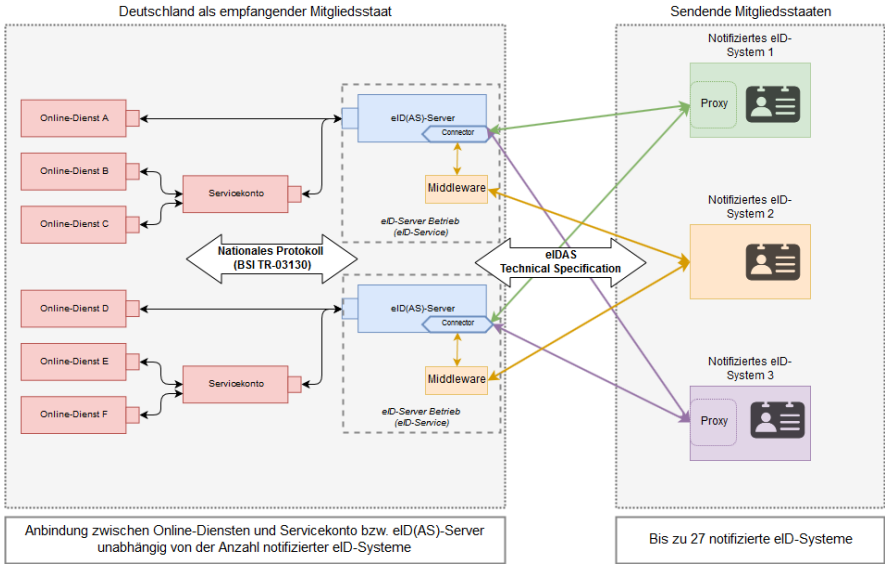


*Abbildung 4: eIDAS Überblick*

werden soll.

Das für die Online-Ausweisfunktion verwendete Protokoll wurde dabei erweitert. Die technische Erweiterung steht über die ergänzten eID(AS)-Server bereit und wurde mit dem eID-Test-System aus Österreich erprobt. Neben der Erweiterung der Infrastruktur war die Erprobung durch ausgewählte Anwendungen zentraler Bestandteil des Projekts.

# 4 Fragestellungen im eIDAS-Kontext

Die Fragestellungen und Antworten, die für Ihre Projekte Relevanz haben könnten, werden im Folgenden beschrieben.

Wie bereits erläutert, wurden sämtliche deutschen eID-Server im Rahmen des TREATS-Projektes befähigt, eIDAS-Authentisierungen durchführen zu können.

Sprechen Sie mit Ihrem eID-Server bzw. eID-Service-Anbieter, ab wann und zu welchen Konditionen diese Erweiterungen zur Verfügung stehen.

### WAS MUSS BEI DER ANBINDUNG VON NUTZERKONTEN BEACHTET WERDEN?

Die Anbindung von Nutzerkonten vereinfacht die Umsetzung des Identitätsmanagements. Hierbei müssen Sie beachten, dass für diese Anbindung ein erweiterter eID-Service genutzt werde muss. Wie Sie die eIDAS-Anbindung an Portalverbund bzw. Nutzerkonten vornehmen, wird in einem Leitfaden, der durch das BMI erstellt wird (Stand Ende Mai 2018 noch nicht veröffentlicht), beschrieben. Sprechen Sie mit dem Hersteller/Anbieter des Nutzerkontos, ab wann diese Erweiterung zur Verfügung steht.

### INTERNATIONALISIERUNG - IN WELCHER SPRACHE STEHT DIE ANWENDUNG ZUR VERFÜGUNG?

Nicht alle Angebote der Verwaltung sind bereits auch in weiteren Sprachen verfügbar. Eine englische Fassung des entsprechenden Angebots sollte in jedem Fall zur Verfügung gestellt werden.

### WAS MUSS ICH TUN, WENN ICH ÜBER DEN DURCH DEN EU-MS FESTGELEGTEN MDS NICHT ALLE DATEN ERHALTE, DIE MEIN ANGEBOT BENÖTIGT?

Die verfahrensverantwortliche Behörde muss entscheiden, in welcher Form eine manuelle Nacherfassung fehlender Daten (z.B. Geburtsname) zulässig ist, ohne das geforderte Vertrauensniveau der Anwendung zu verlassen. Eine Nacherfassung durch manuelle Formulareingabe wird in jedem Fall dazu führen, dass die Identifizierung nicht mehr den Vorgaben an die Vertrauensniveaus substantiell und hoch erfüllt.

### WAS MUSS ICH TUN, WENN DATEN ÜBERMITTELT WERDEN, DIE MEIN ANGEBOT NICHT BENÖTIGT?

Da der sendende Mitgliedstaat festlegt, anhand welcher Attribute die eindeutige Identifizierung der Bürger erfolgt, können auch zusätzliche Daten geliefert werden, die normalerweise in einer deutschen Anwendung nicht erhoben werden (z.B. das Geschlecht). Sollten diese zusätzlichen Daten nicht erhoben oder verarbeitet werden, gilt das zugesicherte Vertrauensniveau des entsprechenden EU-Mitgliedsstaates für die erhobenen Attribute, aber nicht mehr für die Eindeutigkeit der Identifizierung.

### WOHER WEIß ICH, WELCHE LÄNDER IHRE EID–SYSTEME NOTIFIZIERT HABEN?

Notifizierungen werden im europäischen Amtsblatt veröffentlicht. Fragen Sie Ihren eID-Service Anbieter nach dem aktuellen Stand der Anbindung.

### WIE SETZE ICH DIE LÄNDERAUSWAHL UM?

Die erweiterte Technische Richtlinie für eID-Server (BSI TR-03130) sieht zwei Möglichkeiten für die Länderauswahl vor. Entweder erfolgt die Auswahl durch die Online-Anwendung und gibt diese Auswahl im Aufruf des eID-Severs diesem mit; wenn das Land nicht mitgegeben wird, zeigt der eID-Server eine entsprechende Landesauswahl an. Das bedeutet, dass eine Online-Anwendung nicht zwangsläufig eine eigene Länderauswahl umsetzen muss. Die

Möglichkeit eine Länderauswahl in das eigene Angebot zu integrieren besteht und es liegt in der Entscheidungsfreiheit des Verfahrensverantwortlichens die Umsetzung zu gestalten.

### WER LEISTET SUPPORT BEI FEHLERN IM AUSLAND?

Wie im Abschnitt „ARCHITEKTURENTSCHEIDUNG

“ dargestellt, liegen die jeweiligen eID-Systeme in der Verantwortung des entsprechenden Mitgliedsstaates. Sollte ein Nutzer Unterstützung bei der Verwendung der nationalen eID benötigen, wird das entsprechende Land die Unterstützung übernehmen. Bei sonstigen Fehlern, die bei der Nutzung der grenzüberschreitenden Authentisierung auftreten können, kontaktieren Sie Ihren eID-Service Betreiber.

### GIBT ES TESTSYSTEME UM DIE EIDAS-AUTHENTISIERUNG ZU TESTEN?

Testsysteme sind bei den eID-Server Betreibern und Herstellern verfügbar. Eine Liste der verfügbaren Hersteller und Betreiber finden Sie auf der folgenden Seite:

https://www.personalausweisportal.de/DE/Home/home_node.html

### TRANSLITERATION – WAS PASSIERT MIT GRIECHISCHEN ODER KYRILLISCHEN SCHRIFTARTEN?

Personenidentifizierungsdaten werden als Original-Schriftzeichen vom jeweiligen Mitgliedstaat übermittelt. Der für eIDAS erweiterte eID-Server transliteriert den jeweiligen Datensatz zur lateinischen Schriftart, je nach Hersteller können aber auch die originalen Schreibweisen zusätzlich übermittelt werden

| **neugriechisch** | **transliteriert** | **übersetzt** |
|---|---|---|
| νόμος | nómos | Gesetz |

*Tabelle 1: Beispiel für Transliteration*

### IN WELCHEM ZEICHENSATZ WERDEN DIE DATEN ÜBERMITTELT?

Die Übermittelung erfolgt in den UTF-8 Formaten.

# 5 Checkliste

Die folgende Checkliste kann Ihnen dabei helfen, die wesentlichen Aspekte für die eIDAS-Fähigkeit Ihrer Anwendung zu überprüfen.

| Checkliste zur Überprüfung einer Anwendung | |
|---|---|
| | Klärung: Ab wann steht der eID-Server/-Service mit erweitertem eIDAS-Funktionsumfang zur Verfügung. |
| ☐ | Anwendung mehrsprachig zur Verfügung stellen (empfohlen mindestens Deutsch und Englisch). |
| ☐ | Festlegung Vertrauensniveau. |
| ☐ | Klärung: Umgang mit fehlenden Daten. |
| ☐ | Klärung: Umgang mit zusätzlichen Daten. |
| ☐ | Klärung: Länderauswahl (serverseitig oder in der Anwendung). |
| ☐ | Test und Wirksystem beschaffen/beauftragen. |
| ☐ | Zeichensatz für Übermittlung der Daten klären (UTF-8) |

# 6 Weiterführende Informationen

Auf den Seiten des Bundesministerium des Innern (BMI) finden sich neben allgemeinen Informationen zur eIDAS-Verordnung und ihrer Bedeutung unter

https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eIDAS_Verordnung_EU_node.html

auch eine Publikation zum Umsetzungsbedarf und den Auswirkungen der eIDAS-Verordnung für elektronische Verfahren der deutschen Verwaltung unter

https://www.personalausweisportal.de/SharedDocs/Downloads/DE/Weitere-Informationen/eIDAS_Verordnung.pdf?__blob=publicationFile&v=8

und Details zur Vorbereitung der deutschen eID-Funktion für die EU-weite Nutzung

https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eID_Funktion_EU/eID_funktion_eu_node.html

Auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) finden sich neben allgemeinen Informationen zur eIDAS-Verordnung unter

https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/eIDAS_node.html

auch Details zur rechtlichen Basis und der technischen Umsetzung

https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/Elektronische_Identifizierung/Elektronische_Identifizierung_node.html

https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/Elektronische_Identifizierung/Interoperabilitaet/Interoperabilitaet_node.html

https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/Online-Ausweisfunktion/eIDAS-Notifizierung/eIDAS-Notifikation_node.html

Zur Pressemitteilung zum TREATS Projekt gelangen Sie hier

https://www.governikus.de/newsroom-presse/details/?tx_ttnews%5Btt_news%5D=429&cHash=ca9c2bd603cd175b06c8a051975e0018

Informationen zu Governikus als Anwendung des IT Planungsrates finden Sie unter

https://www.it-planungsrat.de/DE/Projekte/Anwendungen/Governikus/governikus_node.html