Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government

Teil 1: Vertrauensniveaus und Mechanismen

Version 1.1
31.10.2016

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung ... 7
1.1 Identitäten ... 7
1.2 Prozesse ... 8
1.3 Vertrauensniveaus ... 8
1.4 Europäischer Rahmen ... 8
1.5 Gesamtsystem ... 9
2 Definitionen ... 10
2.1 Grundbegriffe ... 10
2.2 Prozesse ... 11
2.3 Vertrauensniveaus ... 11
2.4 Bedarfsfeststellung ... 13
2.5 Bewertung von Mechanismen ... 13
3 Grundlegende Kriterien für Vertrauensniveaus ... 15
3.1 Angriffspotential ... 15
3.2 Enrolment ... 15
3.2.1 Identitätsprüfung ... 15
3.2.2 Ausgabe der Authentisierungsmittel ... 17
3.2.3 Informationen für den Inhaber ... 18
3.3 Authentisierungsmittel und -protokoll ... 18
3.3.1 Authentisierungsmittel ... 18
3.3.2 Authentisierungsprotokoll ... 20
3.4 Rückruf/Sperrung ... 20
3.4.1 Sperrung ... 21
3.4.2 Reaktivierung ... 21
3.5 Vertrauenswürdigkeit von Stellen ... 21
3.5.1 Bekannte Stelle ... 22
3.5.2 Vertrauenswürdige Stelle ... 22
3.5.3 Behörde / behördlich anerkannte Stelle ... 22
3.6 Absicherung von Kommunikationsbeziehungen ... 22
3.6.1 ... zwischen Authentisierungsmittelinhaber und vertrauender Entität ... 22
3.6.2 ... zwischen Stellen des Authentisierungssystems ... 23
3.7 Kryptographie ... 23
3.7.1 Schlüsselspeicherung ... 23
3.7.2 Agilität ... 23
3.8 Anforderungen an die Nutzerumgebung ... 24
4 Authentisierungsverfahren ... 25
4.1 Elektronischer Identitätsnachweis ... 25
4.2 Kryptographische Token ... 25
4.3 One Time Passwords ... 26
4.3.1 iTAN ... 27
4.3.2 smsTAN ... 27
4.3.3 pushTAN ... 27
4.3.4 TAN-Generatoren ... 27
4.4 Nutzername/Passwort ... 28

5 Identifizierung einer Person ... 29
5.1 Funktionen ... 29
5.2 Kriterien für Vertrauensniveaus ... 30
5.2.1 Grundlegende Kriterien ... 30
5.2.2 Identifizierung des Dienstanbieters ... 31
5.2.3 Bindung der Identifizierung an den Sitzungskontext ... 31
5.2.4 Vertraulichkeit der Identitätsattribute ... 31
5.3 Mechanismen ... 31
6 Identifizierung eines Dienstanbieters ... 32
6.1 Funktionen ... 32
6.2 Kriterien für Vertrauensniveaus ... 32
6.2.1 Grundlegende Kriterien ... 33
6.2.2 Absicherung der Verbindung ... 33
6.2.3 Bindung der Identifizierung an den Sitzungskontext ... 33
6.3 Mechanismen ... 33
7 Abgabe einer Willenserklärung ... 34
7.1 Funktionen ... 34
7.2 Kriterien für Vertrauensniveaus ... 36
7.2.1 Grundlegende Kriterien ... 36
7.2.2 Vertrauensniveau der Identifizierung des Erklärenden ... 36
7.2.3 Integritätssicherung des Dokumentes ... 36
7.2.4 Bindung der Identität an das Dokument ... 37
7.2.5 Auslösung der Abgabe einer Willenserklärung ... 37
7.3 Mechanismen ... 37
8 Dokumentenübermittlung ... 39
8.1 Funktionen ... 39
8.2 Kriterien für Vertrauensniveaus ... 40
8.2.1 Grundlegende Kriterien ... 40
8.2.2 Sender- und Empfängeridentifizierung ... 40
8.2.3 Verschlüsselung und Integritätssicherung ... 40
8.2.4 Bindung der Identitäten an das übermittelte Dokument ... 41
8.3 Mechanismen ... 41
9 Übermittlung von Identitätsdaten ... 42
9.1 Funktionen ... 42
9.2 Kriterien für Vertrauensniveaus ... 43
10 Mechanismen ... 44
10.1 Elektronischer Identitätsnachweis ... 44
10.1.1 Identifizierung einer Person ... 44
10.1.2 Identifizierung eines Dienstanbieters ... 45
10.1.3 Abgabe einer Willenserklärung ... 45
10.1.4 Dokumentenübermittlung ... 46
10.1.5 Vertrauensniveau ... 46
10.2 Kryptographische Token ... 47
10.2.1 Identifizierung einer Person ... 47
10.2.2 Abgabe einer Willenserklärung ... 48
10.2.3 Vertrauensniveau ... 49

10.3 TAN-Verfahren ... 49
10.3.1 Identifizierung einer Person ... 49
10.3.2 Abgabe einer Willenserklärung ... 49
10.3.3 Vertrauensniveau ... 50
10.4 Nutzername/Passwort ... 50
10.4.1 Identifizierung einer Person ... 50
10.4.2 Abgabe einer Willenserklärung ... 50
10.4.3 Vertrauensniveau ... 51
10.5 De-Mail ... 51
10.5.1 Dokumentenübermittlung ... 51
10.5.2 Abgabe einer Willenserklärung ... 52
10.5.3 Übermittlung von Identitätsdaten ... 52
10.5.4 Vertrauensniveau ... 52
10.6 TLS-Verbindung und -Zertifikate ... 53
10.6.1 Identifizierung eines Dienstanbieters ... 53
10.6.2 Übermittlung eines Dokumentes ... 54
10.6.3 Vertrauensniveau ... 54
10.7 E-Mail mit S/MIME ... 55
10.7.1 Dokumentenübermittlung ... 55
10.7.2 Vertrauensniveau ... 56
10.8 OSCI-Transport ... 56
10.8.1 Dokumentenübermittlung ... 56
10.8.2 Vertrauensniveau ... 57

Anhang A: Vertrauensniveaus nach [eIDAS] ... 58

Literaturverzeichnis ... 59

Tabellenverzeichnis

Tabelle 1: Gefährdungen und Vertrauensniveaus ... 14
Tabelle 2: Grundlegende Kriterien für die Vertrauensniveaus ... 16
Tabelle 3: Eigenschaften von Authentisierungsfaktoren ... 18
Tabelle 4: Kriterien „Identifizierung einer Person“ ... 30
Tabelle 5: Typische Mechanismen für die Identifizierung einer Person ... 31
Tabelle 6: Kriterien „Identifizierung eines Dienstanbieters“ ... 32
Tabelle 7: Typische Mechanismen für die Identifizierung eines Dienstanbieters ... 33
Tabelle 8: Kriterien „Abgabe einer Willenserklärung“ ... 36
Tabelle 9: Typische Mechanismen für die Abgabe einer Willenserklärung ... 37
Tabelle 10: Kriterien „Dokumentenübermittlung“ ... 40
Tabelle 11: Typische Mechanismen für sichere Dokumentenübermittlung ... 41
Tabelle 12: Kriterien „Übermittlung von Identitätsdaten“ ... 43
Tabelle 13: Vertrauensniveaus nach eIDAS, ISO/IEC 29115 und dieser TR ... 58

1 Einleitung

Ziel dieser Technischen Richtlinie ist es, Verfahren zu elektronischen Identitäten und Vertrauensdiensten für verschiedene Prozesse des E-Government zu bewerten und Vertrauensniveaus zuzuordnen. Dafür werden sowohl generische Kriterien, die für alle Prozesse gelten, als auch spezielle Kriterien für die verschiedenen Prozesse vorgegeben.

Der Begriff *Vertrauensdienst* umfasst dabei Dienste, die basierend auf elektronischen Identitäten weitergehende Funktionen anbieten, etwa Abgabe von Willenserklärungen, Übermittlung von Dokumenten, oder föderierte Identitätsverfahren. Vertrauensdienste sollen das Vertrauen von Bürgern, Unternehmen und Behörde in die Kommunikation zwischen diesen erhöhen[1]. Begrifflich hiervon zu unterscheiden ist die *Vertraulichkeit*, die den Schutz von Daten vor unberechtigter Kenntnisnahme meint. Notwendig für Vertrauen in diese Dienste ist neben der technischen Sicherheit der Verfahren auch die Vertrauenswürdigkeit/Glaubwürdigkeit der entsprechenden Hersteller und Dienstleister.

Die Kriterien und Zuordnungen sind weitgehend unabhängig davon, ob die Verfahren für E-Government oder E-Business eingesetzt werden, so dass die Kriterien und Einordnungen grundsätzlich auch für den zweiten Fall anwendbar sind. Bei der Bewertung rechtlicher Vorgaben (etwa Formerfordernisse oder Rechtswirkung) kann es jedoch zu Unterschieden kommen.

Diese Technische Richtlinie umfasst mehrere Teile:

1. Der vorliegende Teil 1 definiert Vertrauensniveaus für die elektronische Identifizierung und für Vertrauensdienste. Darüber hinaus werden ausgewählte Mechanismen in diese Vertrauensniveaus eingeordnet.
2. Teil 2 macht Vorgaben und beschreibt die Prozesse für die Verwendung des elektronischen Identitätsnachweises des Personalausweises/Aufenthaltstitels für den Schriftformersatz nach §3a [VwVfG] (vgl. auch Abschnitt 10.1.3).

1.1 Identitäten

Die *Identität* einer natürlichen oder juristischen Person wird durch verschiedene Eigenschaften beschrieben, wie beispielsweise Name, Anschrift, Geburtsdatum, Email-Adressen oder auch Pseudonyme. Identitäten benennen und charakterisieren aber nicht nur Personen, sondern auch Dinge, Ressourcen, Dienste und andere Objekte. In der virtuellen Welt werden Namen und Eigenschaften durch Attribute einer elektronischen Identität abgebildet.

Um den Zugang zu Systemen, Prozessen und Dienstleistungen zu ermöglichen, muss ein Nutzer erkennbar sein, d. h. bestimmte Identitätsinformationen müssen dem System zur Verfügung gestellt werden. Für die sichere Nutzung ist die *Authentizität* dieser Identitätsdaten von entscheidender Bedeutung. Sind diese gefälscht, veraltet oder nicht nachweisbar, kann auch eine sichere Infrastruktur keine vertrauenswürdige Kommunikation erzeugen.

Hat sich ein Nutzer authentisiert, so muss das System entscheiden, was dieser Nutzer darf. Die *Autorisierung* umfasst die Zuweisung und Überprüfung von Zugriffsrechten auf Daten, Dienste und Ressourcen.

Auf Basis der Authentisierung und festgestellten Autorisierung können nun Geschäftsprozesse initiiert und durchgeführt werden.

1 Der Begriff *Vertrauensdienst* wird ebenfalls in der „Verordnung zu elektronischen Identitäten und Vertrauensdiensten für elektronische Transaktionen im Binnenmarkt“ (eIDAS-Verordnung) genutzt. Dort umfasst er einerseits weitere Prozesse (z.B. Zeitstempel), ist aber technologisch enger gefasst (z.B. werden zur Abgabe von Willenserklärungen nur Signaturen betrachtet).

1.2 Prozesse

Im Laufe der Jahre wurden verschiedene technische Lösungen für unterschiedliche Anwendungsbereiche entwickelt und eingeführt. Diese Lösungen decken unterschiedliche Prozesse des Identitätsmanagements auf unterschiedlichen Sicherheitsniveaus ab.

In dieser Technischen Richtlinie werden Mechanismen für elektronische Verwaltungs- und Geschäftsprozesse zwischen natürlichen/juristischen Personen einerseits und Behörden oder anderen Dienstanbietern andererseits betrachtet und kategorisiert. Unterschieden werden dabei folgende Prozesse:

- Identifizierung von Personen, Organisationseinheiten oder Ressourcen
- Abgabe einer Willenserklärung/Transaktionsauthentisierung, zum Beispiel als Zustimmung zu bestimmten Verwaltungsdienstleistungen/Geschäftsvorgängen oder Dokumenteninhalten
- Elektronische Übermittlung von Dokumenten und Identitätsdaten.

Für jeden dieser Prozesse wird angegeben, welche Funktionen ein Mechanismus erfüllen muss, um für diesen Prozess geeignet zu sein.

1.3 Vertrauensniveaus

Um verschiedene Mechanismen vergleichen zu können, werden zur Kategorisierung der Mechanismen *Vertrauensniveaus* definiert:

- **normal**: Die Schadensauswirkungen bei einer Kompromittierung sind begrenzt und überschaubar;
- **substantiell**: Die Schadensauswirkungen bei einer Kompromittierung sind substantiell;
- **hoch**: Die Schadensauswirkungen bei einer Kompromittierung können beträchtlich sein.

Zusätzliche Anforderungen über Vertrauensniveau *hoch* hinaus können aufgrund rechtlicher **Formvorschriften** bestehen, gekennzeichnet durch „**hoch** +“. Bei Geschäftsprozessen, für die die Schadensauswirkungen bei einer Kompromittierung vernachlässigbar sind, ist das Vertrauensniveau **untergeordnet**, welches in dieser Richtlinie nicht weiter betrachtet wird.

Über die hier betrachteten Mechanismen hinaus können die Kriterien auch zur Bewertung weiterer Mechanismen genutzt werden.

Betrachtet werden ausschließlich elektronische Verfahren für diese Prozesse/Mechanismen. Ebenfalls mögliche nicht-elektronische Verfahren liegen außerhalb des Rahmens dieser Richtlinie und werden daher hier nicht bewertet.

Die Bewertung der Mechanismen berücksichtigt die Gefährdungen für die Kommunikation zwischen Kommunikationspartnern über öffentliche Netze. Erfolgt die Kommunikation über nicht-öffentliche/geschlossene Systeme mit abgegrenzter Nutzergruppe[2], so kann die Bewertung abweichen, insbesondere wenn der geschlossene Kommunikationsraum bereits Gefährdungen durch weitere Maßnahmen abwehrt.

1.4 Europäischer Rahmen

Im Rahmen der Verordnung „über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (kurz: eIDAS-Verordnung, [eIDAS]) werden für den Prozess *Identifizierung von Personen* ebenfalls Vertrauensniveaus[3] definiert. Die Anforderungen an die Vertrauensniveaus ergeben

2 Eine *abgegrenzte Nutzergruppe* ist hier als *a priori* abgegrenzt zu verstehen, z.B. eine Beschränkung eines Systems auf besondere Berufe. Eine abweichende Bewertung kann in diesem Fall etwa durch besondere Sorgfaltsanforderungen an die Nutzer oder besondere Sicherheitsmaßnahmen der Kommunikationssysteme bedingt werden. Ein Mechanismus, der zwar nur für registrierte Nutzer zugänglich ist, die Registrierung aber nicht auf eine bestimmte Gruppe beschränkt ist, ist nicht geschlossen in diesem Sinne.

3 Das in der englischen Version der Verordnung genutzte „assurance level“ wird in der deutschen Version etwas unglücklich mit „Sicherheitsniveau“ statt dem eigentlich passenderen „Vertrauensniveau“ übersetzt.

sich aus der Verordnung bzw. dem zugehörigen Durchführungsrechtsakt [eIDAS LoA]. Für die übrigen in dieser Richtlinie behandelten Prozesse (Identifizierung von Diensten, Abgabe einer Willenserklärung, Übermittlung von Dokumenten/Identitätsdaten) werden in der Verordnung keine Vertrauensniveaus definiert.

Auch im Bereich der Identifizierung von Personen ist [eIDAS LoA] nicht unmittelbar außerhalb des Anwendungsbereiches der Verordnung anwendbar. Zum einen verweist der Durchführungsrechtsakt an einigen Stellen ausdrücklich auf nationale Anforderungen, zum anderen gehen die Vertrauensniveaus nach [eIDAS LoA] von einer Notifizierung des eID-Systems und einer damit verbundenen Haftungsübernahme durch einen Mitgliedstaat aus.

1.5 Gesamtsystem

Diese Technische Richtlinie betrachtet nicht das Gesamtsystem des Verwaltungs- oder Geschäftsprozesses, sondern lediglich den Zugang zu diesen mittels Identitäten, Willenserklärungen und Dokumentenübermittlung. Eine Betrachtung des Gesamtsystems erfordert die Erstellung eines umfassenden Sicherheits- und Datenschutzkonzeptes.

In diesem Konzept müssen auch allgemeine und anwendungsspezifische Anforderungen, die über die reine Kommunikation zwischen Person und Dienstanbieter hinausgehen, berücksichtigt werden. Dies kann z.B. den Schutz erhobener Informationen im Gesamtsystem umfassen, aber auch weitergehende Anforderungen wie die Revisionssicherheit der Prozesse.

Diese Richtlinie kann unterstützend für die Erstellung eines entsprechenden Konzeptes genutzt werden.

2 Definitionen

2.1 Grundbegriffe

Im Folgenden werden einige grundlegende Begriffe des Identitätsmanagements, wie sie in dieser Richtlinie genutzt werden, definiert (angelehnt an [ISO24760-1]):

- Eine **Entität** ist eine Person, eine Organisation, ein Gegenstand, ein Teilsystem oder eine abgrenzbare Gruppe mehrerer davon. Im Rahmen dieser Richtlinie sind Entitäten natürliche Personen, Behörden/Unternehmen und Ressourcen wie Dienstleistungen oder Webseiten.
- Ein **Identitätsattribut** oder ein **Identitätsdatum** ist eine Charakteristik oder eine Eigenschaft einer Entität. Beispiele für Identitätsattribute einer natürlichen Person sind Name, Geburtsdatum oder die Eigenschaft, ein bestimmtes Alter erreicht zu haben. Identitätsattribute von Behörden umfassen etwa Bezeichnung der Behörde oder deren Webadresse.
- Eine **Identität** ist eine Menge von Identitätsattributen, die einer Entität zugeordnet sind. Eine Entität kann mehrere Identitäten haben, ebenso können mehrere Entitäten die gleiche Identität haben. Eine Identität ist daher im Allgemeinen nicht eindeutig, kann dies aber in einem bestimmten Anwendungskontext sein.
- Eine **eindeutige Identität** ist eine Identität, die innerhalb eines bestimmten Anwendungskontextes die zugehörige Entität eindeutig repräsentiert, unterschiedliche Entitäten haben unterschiedliche eindeutige Identitäten. Eine Identität (das heißt eine Menge von Identitätsattributen), die innerhalb eines Anwendungskontextes eindeutig ist, ist dies nicht notwendigerweise auch in einem anderen Kontext.

Es werden verschiedene Typen von Entitäten unterschieden:

- Eine **Person** ist eine natürliche oder eine juristische Person.
- Eine **Dienstanbieter** ist eine Entität, die Personen die Nutzung von elektronischen Geschäftsprozessen anbietet und dafür Prozesse auf Basis elektronischer Identitäten verwendet, z.B. eine Behörde oder ein Unternehmen.
- Eine **vertrauende Entität** ist eine Entität, die sich auf die Echtheit und Gültigkeit einer Identität oder anderer übermittelter Daten verlässt. Anwendungsabhängig können an einem Prozess mehrere vertrauende Entitäten beteiligt sein. Beispiele für vertrauende Entitäten sind Dienstanbieter (Identifizierung einer Person durch einen Dienstanbieter, Abgabe einer Willenserklärung einer natürlichen Person gegenüber einem Dienstanbieter) oder eine Person (Identifizierung eines Dienstanbieters durch eine Person, Dokumentenübermittlung vom Dienstanbieter zur Person).

In Prozessen basierend auf Identitäten (siehe Abschnitt 2.2) werden weiter folgende Begriffe genutzt:

- Ein **Dokument** ist die Repräsentation einer abgeschlossenen Menge zusammengehörender Daten in physischer oder elektronischer Form. Beispiele sind ein Vertrag oder ein ausgefülltes Formular.
- Ein **Vorgang** ist eine abgeschlossene Menge zusammengehörender Daten in Form eines oder mehrerer Dokumente, die einen Geschäftsvorgang eindeutig beschreiben. Beispielsweise kann ein Vorgang eine Identität einer Person, eine Identität eines Dienstanbieters und eine eindeutige Beschreibung eines von der Person gewünschten Dienstes umfassen.
- Eine **Transaktion** im Sinne dieser Richtlinie ist die Abwicklung eines Vorgangs.

Für die Verarbeitung von Identitäten oder anderer Daten sind diese Begriffe relevant:

- Eine **Authentisierung** ist das Versehen einer Identität oder anderer übermittelter Daten mit Metadaten, die es einer vertrauenden Entität ermöglichen, die Herkunft, Echtheit und Gültigkeit der

Identität oder der Daten zu überprüfen. Der Überprüfungsvorgang durch die vertrauende Entität ist die **Authentifizierung** der Identität/der Daten[4].

- **Authentisierungsmittel** sind technische Mittel, die es dem **Inhaber** erlauben, eine Identität (das heißt eine Menge von Identitätsattributen) oder andere übermittelte Daten zu authentisieren. Beispiele für Authentisierungsmittel sind Passwörter, der Personalausweis oder kryptographische Token. Sind mehrere technische Mittel notwendig (etwa Chipkarte und PIN), so besteht das vollständige *Authentisierungsmittel* aus mehreren **Authentisierungsfaktoren**.
- Ein **Authentisierungssystem** ist die Gesamtheit der technischen Infrastruktur einschließlich organisatorischer Prozesse und rechtlicher Rahmenbedingungen, die die Authentisierung und Authentifizierung mittels Authentisierungsmittel ermöglichen.
- Das **Enrolment** ist die Registrierung einer Entität in einem Authentisierungssystem, meist verbunden mit einer Identitätsprüfung, die in der Ausgabe von Authentisierungsmitteln mündet.

2.2 Prozesse

Basierend auf Identitäten können verschiedene Prozesse zur Unterstützung elektronischer Geschäftsprozesse umgesetzt werden:

- Eine **Identifizierung** ist die Übermittlung von anwendungsbezogen geeigneten Identitätsattributen (einer *Identität*), einschließlich authentisierender Metadaten (*Authentisierung*), sowie die Überprüfung (*Authentifizierung*) dieser Identität durch die vertrauende Entität.
- Die **Autorisierung** einer Entität ist die Zuordnung und Überprüfung von Rechten zu einer Entität, zum Beispiel Zugriffsrechte oder das Recht, eine bestimmte Anwendung zu nutzen. Eine Autorisierung erfolgt immer anwendungsbezogen und ist daher nicht Inhalt dieser Richtlinie.
- Eine **Abgabe einer Willenserklärung** ist eine Äußerung eines auf die Herbeiführung einer Rechtswirkung gerichteten Willens: Sie bringt einen Rechtsfolgewillen zum Ausdruck und kann daher nur durch natürliche Personen erfolgen. Im Rahmen dieser Richtlinie kann die Abgabe einer Willenserklärung die Zustimmung zu einem Vorgang oder dem Inhalt eines Dokumentes umfassen. Die Wirksamkeit der Willenserklärung erfolgt erst mit Zugang zum intendierten Empfänger.
- Eine **Dokumentenübermittlung** ist die zweckgerichtete Übermittlung eines Dokumentes an einen definierten Empfänger.

In dieser Richtlinie werden die Prozesse Identifizierung, Abgabe einer Willenserklärung und Dokumentenübermittlung betrachtet.

Grundsätzlich sollten in den Prozessen nach Möglichkeit nur Mechanismen eingesetzt werden, die über die für den Prozess notwendigen Funktionen hinaus keine weiteren Funktionen umfassen. So sollte zum Beispiel eine qualifizierte elektronische Signatur nicht zur Identifizierung eingesetzt werden, da technisch die Nutzung einer qualifizierten elektronischen Signatur für die Abgabe einer Willenserklärung nicht von einer Nutzung für eine Identifizierung unterschieden werden kann. Damit besteht die Gefahr, dass unabsichtlich eine nicht intendierte Rechtsfolge ausgelöst wird. Sofern von dieser Empfehlung z.B. aufgrund rechtlicher Vorgaben abgewichen wird, so muss besondere Sorgfalt darauf verwendet werden, unerwünschte Nebeneffekte zu vermeiden.

2.3 Vertrauensniveaus

Um die Qualität und Vertrauenswürdigkeit von Mechanismen charakterisieren und vergleichen zu können, müssen verschiedene organisatorische und technische Faktoren im Zusammenhang betrachtet werden. Die Zuordnung zu einem Vertrauensniveau berücksichtigt dabei

4 Da beide Begriffe im englischen mit *authentication* übersetzt werden, werden sie auch im deutschen vermehrt gleichwertig genutzt. Diese Richtlinie unterscheidet zwischen beiden Bedeutungen.

- die technische Sicherheit des Verfahrens, zum Beispiel die Sicherheit
  - der genutzten Authentisierungsmittel (Token, Passwörter, ...),
  - der relevanten IT-Infrastruktur und
  - der eingesetzten kryptographischen Verfahren;
- die organisatorische Sicherheit des Verfahrens, zum Beispiel
  - die Qualität des Identifikationsprozesses, das heißt, wie vertrauenswürdig die persönlichen Daten bei der Registrierungsinstanz nachgewiesen werden, sowie den Nachweis der Zugehörigkeit der Daten zur Person,
  - die Qualität des Ausstellungs- und Auslieferungsprozesses der Authentisierungsmittel (zum Beispiel per E-Mail, Briefpost, Download, persönliche Übergabe),
  - die Vertrauenswürdigkeit des Ausstellers (zum Beispiel Staat, Zertifizierungsstelle, private Organisation),
  - die Vertrauenswürdigkeit der Beteiligten in der Nutzungsphase (zum Beispiel Identity Provider, dritte Stellen bei der Datenübermittlung);
- die rechtlichen Rahmenbedingungen, insbesondere Regelungen in den Prozessordnungen (z.B. Beweislastregelungen wie widerlegliche gesetzliche Vermutungen) oder besondere gesetzliche Verpflichtungen beteiligter Stellen.

Darüber hinaus werden gegebenenfalls bekannte konkrete Schwachstellen oder Sicherheitslücken sowie Angriffe gegen Mechanismen berücksichtigt.

Die Kriterien werden in Abschnitt 3 bzw. den darauf folgenden prozessspezifischen Abschnitten detailliert.

In dieser Richtlinie werden drei Vertrauensniveaus verwendet:

- **normal**: Die Schadensauswirkungen bei einer Kompromittierung sind begrenzt und überschaubar. Dieses Vertrauensniveau entspricht in etwa dem Sicherheitsniveau *normal* gemäß IT-Grundschutz [BSI100-2].
- **substantiell**: Die Schadensauswirkungen bei einer Kompromittierung sind substantiell. Dieses Vertrauensniveau liegt zwischen den Sicherheitsniveaus *normal* und *hoch* gemäß IT-Grundschutz [BSI100-2].
- **hoch**: Die Schadensauswirkungen bei einer Kompromittierung können beträchtlich sein. Dieses Vertrauensniveau entspricht in etwa dem Sicherheitsniveau *hoch* gemäß IT-Grundschutz [BSI100-2].

Bestehen rechtliche **Formvorschriften** oder sind die Auswirkungen einer unrichtigen Identifizierung / unrichtigen Zuordnung eines Vorgangs zu einer Identität als schwerwiegend anzusehen, sind ggf. über das Vertrauensniveau *hoch* hinaus besondere Anforderungen an das Enrolment, die beteiligten Stellen oder eine besondere rechtliche Absicherung[5] des Verfahrens auf Basis einer gesetzlichen Grundlage notwendig. Diese besonderen Anforderungen werden auch kurz mit **hoch** + gekennzeichnet.

Das Sicherheitsniveau *sehr hoch* nach IT-Grundschutz findet keine Entsprechung in den hier definierten Vertrauensniveaus. Das Sicherheitsniveau *sehr hoch* im Sinne des Grundschutzes ist mit Mechanismen, die IT-Systeme des Endanwenders nutzen, im Allgemeinen nicht erreichbar.

Die analogen Definitionen nach [eIDAS] finden sich in Anhang A.

In den Kapiteln 5 bis 8 werden verschiedene Mechanismen des Identitätsmanagements Prozessen und Vertrauensniveaus zugeordnet.

5 Eine spezifische rechtliche Absicherung ist oft auch verbunden mit einer rechtlichen Privilegierung eines Mechanismus in Bezug auf Rechtswirksamkeit, Beweiswert oder andere rechtliche Eigenschaften.

2.4 Bedarfsfeststellung

Der Betreiber eines Geschäftsprozesses, im E-Government also die verantwortliche Behörde/im E-Business das verantwortliche Unternehmen, muss unter Berücksichtigung der spezifischen Gefährdungen und rechtlicher Rahmenbedingungen anwendungsbezogen ermitteln und festlegen, welches Vertrauensniveau für die Prozesse notwendig ist.

Angelehnt an [BSI100-2] und [ISO29115] können die Gefährdungen durch den Verantwortlichen für einen Geschäftsprozesses anhand der möglichen Auswirkungen/Beeinträchtigungen gemäß Tabelle 1 den Vertrauensniveaus zugeordnet werden.

Für Geschäftsprozesse, die besondere Formvorschriften erfüllen müssen (z.B. Schriftformersatz) oder die dem hoheitlichen Handeln zuzuordnen sind (z.B. Pass- und Ausweisrecht, Melderecht), gelten ggf. über die hier definierten Vertrauensniveaus *normal*, *substantiell* und *hoch* hinausgehende Anforderungen an die Verfahren.

In komplexen Geschäftsprozessen kann die Bedarfsfeststellung für verschiedene Teilprozesse oder verschiedene Teilmengen der verarbeiteten Daten zu unterschiedlichen Ergebnissen kommen.

Es wird empfohlen, die Feststellung des notwendigen Vertrauensniveaus auf Basis einer Schutzbedarfsfeststellung nach [BSI100-2] unter zusätzlicher Berücksichtigung rechtlicher Vorgaben durchzuführen.

Bei Geschäftsprozessen, bei denen im Falle eines Missbrauchs im Wesentlichen keine Schäden entstehen, kann auf Mechanismen gemäß dieser Richtlinie verzichtet werden.

2.5 Bewertung von Mechanismen

Für die Prozesse

- Identifizierung von Personen (Kapitel 5)
- Identifizierung von Dienstanbietern (Kapitel 6)
- Abgabe einer Willenserklärung (Kapitel 7)
- Dokumentenübermittlung (Kapitel 8)
- Übermittlung von Identitätsdaten (Kapitel 9)

werden in den entsprechenden Kapitel Funktionen definiert, die von den Mechanismen abgebildet werden müssen. Die Zuordnung der Mechanismen, die diese Funktionen erfüllen, zu einem Vertrauensniveau erfolgt anhand von Kriterien, die in Abschnitt 3 allgemein benannt werden und in den prozessspezifischen Kapiteln um spezifische Kriterien ergänzt werden.

<table>
<tr><th rowspan="2">Gefährdung</th><th colspan="3">Potentieller Schaden bedingt Vertrauensniveau</th></tr>
<tr><th>Normal</th><th>Substantiell</th><th>Hoch</th></tr>
<tr><td rowspan="2">Verstoß gegen Gesetze/Vorschriften</td><td rowspan="2">Verstoß mit geringfügigen Konsequenzen</td><td rowspan="2">Verstoß mit substantiellen Konsequenzen</td><td>Verstoß mit erheblichen Konsequenzen</td></tr>
<tr><td>Besondere Formvorschriften (hoch +) bei Gefahr eines Verstoßes mit schwerwiegenden Konsequenzen</td></tr>
<tr><td rowspan="2">Unrichtige Identifizierung oder Zuordnung zu einer Identität</td><td rowspan="2">Geringfügige Konsequenzen</td><td rowspan="2">Substantielle Konsequenzen</td><td>Erhebliche Konsequenzen</td></tr>
<tr><td>Besondere Formvorschriften (hoch +) bei Gefahr von schwerwiegenden Konsequenzen</td></tr>
<tr><td>Beeinträchtigung des informationellen Selbstbestimmungsrechts</td><td>Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen beeinträchtigen können.</td><td>Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen substantiell beeinträchtigen können.</td><td>Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen können.</td></tr>
<tr><td>Beeinträchtigung körperlicher/persönlicher Unversehrtheit</td><td>Beeinträchtigung erscheint nicht möglich</td><td>Beeinträchtigung kann nicht vollständig ausgeschlossen werden</td><td>Beeinträchtigung kann nicht ausgeschlossen werden</td></tr>
<tr><td>Beeinträchtigung der Aufgabenerfüllung</td><td>Beeinträchtigung wird von den Betroffenen als tolerabel eingeschätzt</td><td>Beeinträchtigung wird von einzelnen Betroffenen als tolerabel eingeschätzt</td><td>Beeinträchtigung wird als nicht tolerabel eingeschätzt</td></tr>
<tr><td>Negative Innen- oder Außenwirkung</td><td>Geringe/nur interne Ansehens- oder Vertrauensbeeinträchtigung zu erwarten</td><td>Substantielle Ansehens- oder Vertrauensbeeinträchtigung zu erwarten</td><td>Breite Ansehens- oder Vertrauensbeeinträchtigung zu erwarten</td></tr>
<tr><td>Finanzielle Auswirkungen</td><td>Finanzieller Schaden tolerabel</td><td>Substantieller finanzieller Schaden möglich</td><td>Beachtliche finanzielle Verluste, jedoch nicht existenzbedrohend</td></tr>
<tr><td colspan="4">Zu beachten: Die Aggregation von Gefährdungen kann zur Erhöhung des notwendigen Vertrauensniveaus führen. Zum Beispiel kann die Verarbeitung personenbezogener Daten mit Schutzbedarf substantiell zu einem notwendigen Vertrauensniveau hoch führen, wenn viele Personen von einer Beeinträchtigung betroffen sind.

Sind mehrere Gefährdungen relevant, so ist für die Gesamtbewertung das Maximum der einzeln ermittelten notwendigen Vertrauensniveaus anzunehmen.</td></tr>
</table>

Tabelle 1: Gefährdungen und Vertrauensniveaus

3 Grundlegende Kriterien für Vertrauensniveaus

In diesem Kapitel werden grundlegende Kriterien für die Einordnung von Mechanismen zu Vertrauensniveaus benannt, die in den folgenden Kapiteln durch prozessspezifische Kriterien ergänzt werden. Diese Kriterien können nur als Mindestanforderungen dienen, die Einordnung eines konkreten Mechanismus muss immer anhand einer Bewertung des Gesamtsystems erfolgen. Eine Übersicht der Kriterien findet sich in Tabelle 2.

Die Erfüllung von besonderen Formvorschriften setzt ggf. einen staatlichen Betrieb oder eine staatliche Kontrolle des Verfahrens bzw. Anerkennung der Beteiligten voraus. Die Anforderungen an das Enrolment, das heißt an die initiale Identitätsverifikation, sind gegenüber Vertrauensniveau *hoch* erhöht.

3.1 Angriffspotential

Bei der Bewertung von Verfahren wird die Sicherheit gegen Angreifer mit einem definierten Angriffspotential bewertet:

- Für Vertrauensniveau *normal* muss das Verfahren Angriffe eines Angreifers mit Angriffspotential *enhanced-basic* verhindern;
- Für Vertrauensniveau *substantiell* muss das Verfahren Angriffe eines Angreifers mit Angriffspotential *moderate* verhindern;
- Für Vertrauensniveau *hoch* muss das Verfahren Angriffe eines Angreifers mit Angriffspotential *high* verhindern;

Zur Definition der Angriffspotentiale wird auf [ISO18045][6], Anhang B.4, verwiesen.

3.2 Enrolment

Das Enrolment ist die Registrierung einer Entität in ein Authentisierungssystem. Typischerweise wird als Teil des Enrolments eine Identitätsprüfung der Entität durchgeführt und anschließend ein Authentisierungsmittel (gegebenenfalls bestehend aus mehreren Faktoren) ausgegeben bzw. ein vorhandenes Authentisierungsmittel registriert.

3.2.1 Identitätsprüfung

Die Identitätsprüfung kann anhand physisch vorgelegter Dokumente oder elektronisch mittels eines eID-Systems auf geeignetem Vertrauensniveau erfolgen.

Die im Authentisierungssystem verfügbaren Identitätsattribute können so nachgewiesene (externe) Identitätsattribute sowie (interne) Identitätsattribute, die erst im System erzeugt werden, umfassen. Sowohl für externe als auch interne Attribute muss festgelegt sein, inwiefern deren Gültigkeit erlischt, wenn sich die zugrunde liegende nachgewiesene Identität der Entität ändert (vgl. auch Abschnitt 3.4).

Die Identitätsprüfung muss auf Basis von veröffentlichten Verfahrensvorgaben[7] mindestens auf dem Vertrauensniveau des Authentisierungssystems erfolgen, für das das Enrolment durchgeführt wird. Die Prüfung muss durch Stellen gemäß 3.5 durchgeführt werden.

6 Gleichlautend auch verfügbar als *Common Criteria Evaluation Methodology* (CEM) unter https://www.commoncriteriaportal.org/cc/.

7 Die Veröffentlichung der Verfahrensvorgaben dient der Transparenz und Nachvollziehbarkeit durch alle Beteiligten. Die Vorgaben können z.B. im Rahmen der AGBs der Registrierungsstelle oder durch rechtliche Vorgaben, etwa in Form von Verwaltungsvorschriften, veröffentlicht werden.

		Vertrauensniveau		
		normal	**substantiell**	**hoch**
Enrolment (Abschnitt 3.2)		Bekannte Stelle (vgl. Abschnitt 3.5.1)	Vertrauenswürdige Stelle (vgl. Abschnitt 3.5.2)	Vertrauenswürdige Stelle (vgl. Abschnitt 3.5.2)
				Für Formvorschriften (*hoch +*) ggf. besondere Anforderungen (vgl. Abschnitt 3.5.3)
	Identitätsprüfung (Abschnitt 3.2.1)	Nach [eIDAS LoA]		
	Ausgabe (Abschnitt 3.2.2)	Nur an Berechtigte	Nur an Berechtigte Zwei Wege	Nur an Berechtigte Zwei Wege Explizite Aktivierung
Authentisierung (Abschnitt 3.3)		Sicher gegen Angriffspotential *enhanced-basic*	Sicher gegen Angriffspotential *moderate*	Sicher gegen Angriffspotential *high*
	Faktoren (Abschnitt 3.3.1)	Ein Faktor	Zwei Faktoren	Zwei Faktoren manipulationssicher
	Verfahren (Abschnitt 3.3.2)		Dynamische Authentisierung	Dynamische Authentisierung
Rückruf/Sperrung (Abschnitt 3.4)		≤ 24h	≤ 12h	≤ 1h
Alle relevante Stellen (Abschnitt 3.5)		Bekannte Stelle (vgl. Abschnitt 3.5.1)	Vertrauenswürdige Stelle (vgl. Abschnitt 3.5.2)	Vertrauenswürdige Stelle (vgl. Abschnitt 3.5.2)
				Für Formvorschriften (*hoch +*) ggf. besondere Anforderungen (vgl. Abschnitt 3.5.3)
Absicherung von Kommunikationsbeziehungen (Abschnitt 3.6)		Absicherung auf Transportebene	Ende-zur-Ende-Beziehung bzw. Absicherung durch vertrauenswürdige Stellen (vgl. Abschnitt 3.5.2)	Ende-zur-Ende-Beziehung bzw. Absicherung durch vertrauenswürdige Stellen (vgl. Abschnitt 3.5.2)
				Für Formvorschriften (*hoch +*) ggf. besondere Anforderungen (vgl. Abschnitt 3.5.3)
Beim Einsatz von Kryptographie (Abs. 3.7)	**Algorithmen / Schlüssellängen**	[TR-03116] / [TR-02102]		
	Schlüsselspeicherung	Vor unberechtigtem Zugriff geschützt	Vor unberechtigtem Zugriff geschützt	Nach geeignetem Common Criteria-Schutzprofil zertifizierte Hardware für private Schlüssel

Tabelle 2: Grundlegende Kriterien für die Vertrauensniveaus

Wird ein elektronisches Identifizierungssystem für die Identitätsprüfung genutzt, so muss dieses die Anforderungen gemäß Abschnitt 5 auf dem entsprechenden Vertrauensniveau des Authentisierungssystems erfüllen.

Anderenfalls müssen die Anforderungen der jeweils relevanten Abschnitte 2.1.2 – 2.1.4 in [eIDAS LoA] erfüllt werden[8].

Dabei ist zu beachten:

- Der Begriff „verlässliche Quelle“ kann Dokumente und Datenbanken umfassen. Die Authentizität der Dokumente bzw. aus einer Datenbank abgerufenen Daten muss auf dem Niveau gemäß Abschnitt 3.1 überprüfbar sein. Für physikalische Dokumente bedeutet dies die verlässliche Prüfung physikalischer Sicherheitsmerkmale, die die Authentizität des Dokumentes nachweisen können. Bei Abruf von Daten aus Datenbanken muss sowohl die Authentizität der Datenbank als auch die Unversehrtheit der abgerufenen Daten (z.B. während der Übertragung) sichergestellt werden.

  Die Dokumente bzw. Datenbanken müssen durch Stellen gemäß Abschnitt 3.5 ausgegeben bzw. geführt werden.
- Der Begriff „mit Foto oder biometrischen Merkmalen versehener Identitätsnachweis“ ist als hoheitliches Identitätsdokument (Pass, Personalausweis) oder rechtlich und technisch gleichwertiges Dokument zu verstehen.
- Die Prüfung physikalischer Sicherheitsmerkmale von Dokumenten und die Verifizierung der Identität einer Person durch Lichtbildvergleich oder andere biometrische Verfahren muss durch entsprechend geschultes Personal durchgeführt werden.

Für die Bewertung von Mechanismen zur Identitätsprüfung siehe auch Kapitel 10.1 von [ISO29115] sowie die Guidance zu [eIDAS LoA].

3.2.2 Ausgabe der Authentisierungsmittel

Die Ausgabe der Authentisierungsmittel muss durch Stellen gemäß 3.5 durchgeführt werden.

Es muss sichergestellt werden, dass Authentisierungsmittel nur an den berechtigten Inhaber ausgegeben werden.

Die Ausgabe für Vertrauensniveaus *substantiell/hoch* muss so erfolgen, dass die beiden Sicherungsfaktoren (siehe Abschnitt 3.3) auf verschiedenen Übermittlungswegen ausgegeben werden. Diese Anforderung kann auch dadurch erfüllt werden, in dem die beiden Faktoren zeitlich getrennt auf gleichem Wege übermittelt werden, sofern sichergestellt ist, dass der erste Faktor den Inhaber erreicht hat, bevor der zweite übermittelt wird.

Die Ausgabe eines auf Besitz basierenden Sicherungsmittels muss so erfolgen, dass der berechtigte Inhaber nach Erhalt erkennen kann, ob das Sicherungsmittel unberechtigt benutzt wurde, etwa durch Verwendung einer Transport-PIN zur Sicherung einer Chipkarte.

Die Ausgabe von wissensbasierten Sicherungsmitteln muss so erfolgen, dass der Inhaber unberechtigte Kenntnisnahme erkennen kann („PIN-Brief“).

Für Vertrauensniveau *hoch* ist eine explizite Aktivierung der Authentisierungsmittel durch den Inhaber notwendig. Die Aktivierung muss so gestaltet sein, dass sie nur den berechtigten Inhaber erfolgt bzw. dieser zuverlässig eine unberechtigte Aktivierung erkennen kann.

8 Das BSI erstellt zur Zeit eine Richtlinie zur Bewertung von Identitätsprüfungsverfahren zur Präzisierung und Operationalisierung der entsprechenden Vorgaben nach [eIDAS LoA]. Nach Fertigstellung wird eine entsprechende Referenz eingefügt.

3.2.3 Informationen für den Inhaber

Dem Inhaber der Authentisierungsmittel müssen in geeigneter Weise die Geschäftsbedingungen sowie notwendige Verhaltensregeln zum Umgang mit den Authentisierungsmitteln übermittelt werden.

Wenn sich die Geschäftsbedingungen oder notwendigen Verhaltensregeln ändern, so müssen alle betroffenen Stellen und insbesondere der Authentisierungsmittelinhaber geeignet über die Änderungen informiert werden.

3.3 Authentisierungsmittel und -protokoll

Wichtiges Kriterium bei der Bewertung eines Mechanismus ist die Kontrolle des Inhabers über die ihm zugeordneten Authentisierungsmittel und das verwendete Authentisierungsprotokoll.

Für die Authentisierungsmittel und -verfahren sind die Anforderungen aus Abschnitt 3.7 einzuhalten.

3.3.1 Authentisierungsmittel

Für die Sicherung der Authentisierungsmittel können verschiedene Faktoren eingesetzt werden, die sich in verschiedene Kategorien unterteilen lassen. Wesentliche Eigenschaften verschiedener Faktoren werden in Tabelle 3 zusammengefasst.

Die Authentisierungsmittel müssen so gestaltet werden, dass der berechtigte Inhaber sie gegen Missbrauch durch Dritte mit Angriffspotential gemäß Abschnitt 3.1 schützen kann.

	Besitz	**Wissen**	**Biometrie**
Prävention			
Bindung an Inhaber	Einmaligkeit des Besitzes, Besitz darf nicht kopierbar sein und Inhaber darf Besitz nicht weitergeben	Nur Inhaber kennt das Wissen, Wissen darf nicht weitergegeben werden.	Inhaberspezifische biometrische Merkmale, Lebenderkennung
Kontrolle durch Inhaber setzt voraus:	Besitz unter physischer Kontrolle des Inhabers, Besitz wird nur zur Authentisierung genutzt	Wissen wird nur zur Authentisierung genutzt	Biometrisches Merkmal wird nur zur Authentisierung genutzt
Detektion			
Erkennen des Kontrollverlustes	Verlust des Besitzes; zusätzlich durch Missbrauchserkennung	Nur nachträglich durch Missbrauchserkennung in der Anwendung / heuristisches Profiling durch zentralen Server	
Reaktion			
Sperren der Mittel	Sperre über eindeutiges Merkmal des Besitzes	Sperren des zugehörigen Accounts (bei entfernter Verifikation durch Server) oder Besitzes (bei lokaler Verifikation durch Besitztoken)	
Ersatz für gesperrte Authentisierungsmittel	Ausstellen eines neuen Besitztokens	Setzen eines neuen Passworts / einer neuen PIN	Registrierung und Nutzung eines anderen biometrischen Merkmals

Tabelle 3: Eigenschaften von Authentisierungsfaktoren

3.3.1.1 Besitz

Besitz als Sicherungsfaktor im Sinne dieser Richtlinie ist ein physikalischer Token, den der Inhaber unter alleiniger Kontrolle hat.

Dies setzt voraus, dass der Token durch einen Angreifer mit Angriffspotential entsprechend Abschnitt 3.1 nicht kopiert werden kann. Für Vertrauensniveau *hoch* muss der Token auch gegen Veränderung (Manipulation) durch Angreifer mit hohem Angriffspotential geschützt sein. Darüber hinaus muss der Inhaber sicherstellen können, dass der Besitztoken nur für ein intendierte Authentisierung aktiviert wird.

Dies kann durch die Verwendung geeigneter Hardware und geeigneten kryptographischen Verfahren (siehe Abschnitt 3.7) erreicht werden.

3.3.1.2 Wissen

Wissen im Sinne dieser Richtlinie ist Wissen, das ausschließlich dem berechtigten Inhaber und der verifizierenden Entität (zum Beispiel Server im Falle von Passwörtern, Chipkarte im Falle einer Chipkarten-PIN) bekannt ist.

- Bei Nutzung von Wissen als alleinigem Sicherungsfaktor sind die Anforderungen aus Maßnahme M 2.11 „Regelung des Passwortgebrauchs“ der IT-Grundschutz-Kataloge des BSI (siehe [BSI-GS]) einzuhalten.
- Bei Nutzung von Wissen in Kombination mit Besitz müssen beide Sicherungsfaktoren miteinander verknüpft sein, zum Beispiel die Benutzung einer PIN zur Freischaltung einer Chipkarte. Dadurch wird verhindert, dass ein Angreifer Wissen und Besitz von verschiedenen Inhabern zu einem gültigen Authentisierungsmittel kombinieren kann.

  Bei Verwendung eines Fehlbedienungszählers, der maximal drei Versuche, eine PIN zu raten zulässt, sollte eine PIN mindestens 4 (Vertrauensniveau *normal*), 5 (Vertrauensniveau *substantiell*) bzw. 6 (Vertrauensniveau *hoch*) dezimale Stellen haben (vgl. [AIS 20/31]).

Grundsätzlich sollte Wissen durch den Inhaber festgelegt werden, das heißt der Inhaber wählt Passwörter/PINs selbst (ausgenommen Einmalpasswörter und Passwörter, die nicht zur Authentisierung genutzt werden können).

3.3.1.3 Biometrie

Biometrie im Sinne dieser Richtlinie ist eine physische Eigenschaft einer Person, die als Sicherungsfaktor genutzt wird.

Biometrie ist im Allgemeinen nicht als alleiniger Faktor für die Verwendung in Online-Verfahren geeignet. Problematisch sind in Online-Szenarien u.a. der Schutz gegen Replay (also die Wiederverwendung einer früher gemachten Aufnahmen eines biometrischen Merkmals) und die Lebenderkennung.

Die Nutzung von Biometrie in Kombination mit Besitz als Ersatz für den Sicherungsfaktor Wissen in Kombination mit Besitz ist unter bestimmten Umständen grundsätzlich möglich. Bei der Einordnung eines biometrischen Verfahrens ist neben der Resistenz gegen Replay und der Güte der Lebenderkennung auch die biometrische Erkennungsqualität zu betrachten. Die Erkennungsqualität wird üblicherweise durch die False Acceptance Rate und die False Rejection Rate beschrieben. Die Erfolgswahrscheinlichkeit für eine Überwindung der biometrischen Erkennung, ausgedrückt durch False Acceptance Rate, darf nicht wesentlich schlechter als die entsprechende Vorgaben für den Sicherungsfaktor Wissen sein (siehe voriger Abschnitt).

3.3.1.4 Zwei-Faktor-Authentisierung

Zur Erreichung des Vertrauensniveaus *substantiell* ist grundsätzlich die Nutzung von zwei Faktoren zur Absicherung der Authentisierungsmittel notwendig, die die alleinige Kontrolle des Nutzers über seine Authentisierungsmittel sicherstellen. Dabei müssen die beiden Faktoren unterschiedlichen Kategorien angehören.

Die Authentisierungsmittel und das Authentisierungsprotokoll müssen so gestaltet sein, dass es nicht möglich ist, beide Faktoren unabhängig voneinander anzugreifen, d.h. beide Faktoren müssen miteinander verknüpft sein (z.B. PIN-Eingabe bei einer Smartcard). Insbesondere darf ein Angreifer das Fehlschlagen eines Authentisierungsversuches nicht einem einzelnen Authentisierungsfaktor zuordnen können. Ebenso dürfen nicht beide Faktoren gemeinsam durch einen einzelnen Angriff auf die Nutzerumgebung angreifbar sein.

Für Vertrauensniveau *hoch* müssen die Authentisierungsmittel gegen Duplizierung und Manipulation durch Angreifer mit hohem Angriffspotential (siehe Abschnitt 3.1) geschützt sein.

3.3.2 Authentisierungsprotokoll

Das Authentisierungsprotokoll muss gegen Angreifer mit Angriffspotential gemäß Abschnitt 3.1 sicher sein. Es wird empfohlen, für kryptographische Verfahren einen Sicherheitsbeweis durchzuführen.

Bei der Bewertung eines Authentisierungsprotokolls müssen insbesondere die in Abschnitt 10.3.2 von [ISO29115] genannten Bedrohungen berücksichtigt werden:

- Raten von Authentisierungsdaten (Online und Offline);
- Duplizieren von Authentisierungsdaten;
- Abfangen/Verfälschen von Informationen (Phishing, Eavesdropping, Spoofing, Man-in-the-middle);
- Angriffe gegen die Sitzungsbindung (Replay, Session Hijacking);
- Diebstahl von Authentisierungsmitteln;

Daneben müssen mechanismenspezifische Anforderungen, wie z.B. Integrität/Vertraulichkeit übermittelter Daten, berücksichtigt werden.

Sofern für einen Mechanismus die Vertraulichkeit ein Sicherheitsziel ist, so sollen kryptographische Verfahren eingesetzt werden, die Vorwärtssicherheit (Forward Secrecy) bieten, d.h. die Vertraulichkeit ausgetauschter Identifizierungsdaten bleibt auch nach einer Kompromittierung von Langzeitschlüsseln oder Passwörtern/PINs gewährleistet.

Für Vertrauensniveaus *substantiell* und *hoch* muss das Authentisierungsprotokoll dynamisch sein, d.h. das Verfahren muss dazu geeignet sein nachzuweisen, dass sich die Authentisierungsmittel im Augenblick der Authentisierung unter Kontrolle des Inhabers befinden. Dieser Nachweis muss für jede Authentisierung neu erzeugt werden. Beispiele sind kryptographische Challenge-Response- oder Diffie-Hellman-Verfahren, bei denen die vertrauende Entität die Challenge bzw. einen ephemeralen Diffie-Hellman-Schlüssel erzeugt.

Die Anforderungen aus Abschnitt 3.7 sind einzuhalten.

3.4 Rückruf/Sperrung

Im Falle der Kompromittierung von Authentisierungsmitteln muss es dem Inhaber möglich sein, die Authentisierungsmittel zu sperren. Ein Rückruf von Authentisierungsmitteln ist auch notwendig, wenn die authentisierten Identitätsattribute nicht mehr gültig sind (z.B. Namensänderung) oder der Inhaber nicht mehr zum Besitz berechtigt ist.

3.4.1 Sperrung

Für alle Vertrauensniveaus muss der Rückruf bzw. Sperrung von Authentisierungsmitteln durch den Inhaber möglich sein. Eine Sperrung ist *effektiv* zu dem Zeitpunkt, an dem die Sperrinformation für vertrauende Entitäten zur Verfügung steht. Grundsätzlich sollte eine effektive Sperrung so schnell wie möglich erfolgen (umgehend), die im folgenden genannten Fristen sind als Minimalanforderungen zu verstehen.

- Für das Vertrauensniveau *normal* muss die effektive Sperrung eines Authentisierungsmittels spätestens 24 Stunden nach der Sperrmeldung durch den Inhaber erfolgen. Eine Möglichkeit zur Übermittlung der Sperrmeldung (Hotline o. ä.) muss mindestens während der üblichen Geschäftszeiten zur Verfügung stehen.
- Für das Vertrauensniveau *substantiell* muss die effektive Sperrung eines Authentisierungsmittels spätestens 12 Stunden nach der Sperrmeldung durch den Inhaber erfolgen. Eine Möglichkeit zur Übermittlung der Sperrmeldung (Hotline o. ä.) muss jederzeit zur Verfügung stehen.
- Für das Vertrauensniveau *hoch* muss die effektive Sperrung eines Authentisierungsmittels spätestens 1 Stunde nach der Sperrmeldung durch den Inhaber erfolgen. Eine Möglichkeit zur Übermittlung der Sperrmeldung (Hotline o. ä.) muss jederzeit zur Verfügung stehen und allgemein bekannt sein.

Die Möglichkeit zur Übermittlung der Sperrmeldung muss über öffentliche Kommunikationswege verfügbar sein und den Inhabern von Authentisierungsmittels in geeigneter Weise bekannt gemacht werden.

3.4.2 Reaktivierung

Für eine Rücknahme einer Sperrung – sofern vom System unterstützt – muss eine Identifizierung des Inhabers eines Authentisierungsmittels mindestens auf dem Vertrauensniveau des Authentisierungssystems erfolgen.

Es muss sichergestellt sein, dass die Sicherheit der Authentisierungsmittel nicht kompromittiert wurde.

3.5 Vertrauenswürdigkeit von Stellen

Bei den meisten Mechanismen übernehmen – neben dem Inhaber der Authentisierungsmittel und der vertrauenden Entität – weitere Stellen für die Sicherheit des Mechanismus relevante Aufgaben, zum Beispiel Enrolment, Identitätsprüfung und Ausgabe der Authentisierungsmittel (Abschnitt 3.2), Sicherung von Kommunikationsbeziehungen (Abschnitt 3.6) oder Speicherung von Daten. Auch Identitätsprovider sind Stellen in diesem Sinne.

Alle Stellen müssen

- Behörden oder juristische Personen sein und rechtlich befugt sein, die jeweilige Aufgabe wahrzunehmen;
- für ihre jeweiligen wahrgenommen Aufgaben ein Regelwerk aufstellen und dieses einhalten;
- organisatorisch und technisch in der Lage sein, die Aufgaben auf Basis des Regelwerks wahrzunehmen;
- genügend Ressourcen für die Erfüllung der Aufgaben und ggf. die Übernahme der sich aus den Aufgaben ergebener Haftung haben; und
- ein Informationssicherheitsmanagementsystem auf Basis etablierter Standards (z.B. IT-Grundschutz [BSI100-2] oder [ISO27001]) haben.

Sofern der Inhaber eines Authentisierungsmittels oder die vertrauende Stelle einen Dritten unmittelbar beauftragt (Auftragsdatenverarbeiter), so gelten für diesen die Anforderungen an Inhaber/vertrauende Entität und der Dritte fällt nicht unter die Anforderungen dieses Abschnitts.

3.5.1 Bekannte Stelle

Für alle Vertrauensniveaus dürfen diese Aufgaben nur durch Stellen wahrgenommen werden, die durch den Systembetreiber für die jeweilige Aufgabe identifiziert und im System bekannt sind. Die Zahl der Stellen sollte auf das notwendige Minimum reduziert sein.

Für alle Stellen wird die Erstellung und Fortschreibung eines Sicherheitskonzeptes sowie eine zugehörige regelmäßige Auditierung nach IT-Grundschutz [BSI100-2] oder nach [ISO27001] empfohlen. Dabei muss der Audit alle durch die Stelle wahrgenommen Aufgaben und die Einhaltung der zugeordneten Schutzziele umfassen.

3.5.2 Vertrauenswürdige Stelle

Zur Erreichung des Vertrauensniveaus *substantiell* müssen diese Stellen als vertrauenswürdig anerkannt sein.

Die Erstellung und Pflege eines Sicherheitskonzeptes sowie eine zugehörige regelmäßige Auditierung mit Testat nach IT-Grundschutz [BSI100-2] oder nach [ISO27001] sind verpflichtend. Der Audit muss durch eine neutrale Instanz (zum Beispiel ein anerkannter Auditor) erfolgen.

Das Sicherheitskonzept und der Audit müssen alle durch die Stelle wahrgenommen Aufgaben und die Einhaltung der zugeordneten Schutzziele umfassen. Sofern für die durch die Stelle wahrgenommene Aufgaben Technische Richtlinien des BSI (z.B. [TR-03145] für Certification Authorities), Normen oder anderer Stand der Technik für die Überprüfung zur Verfügung stehen, so sind diese einzuhalten.

Für Vertrauensniveau *hoch* gilt zusätzlich für die Überprüfung der Stelle, dass diese ein Zertifikat nach IT-Grundschutz [BSI100-2] oder nach [ISO27001] auf Sicherheitsniveau *hoch* umfassen muss. Dabei muss der Audit/das Zertifikat alle durch die Stelle wahrgenommen Aufgaben und die Einhaltung der zugeordneten Schutzziele umfassen.

Für qualifizierte Vertrauensdienstanbieter nach [eIDAS] wird die Einhaltung der Anforderungen für die erbrachten qualifizierten Vertrauensdienste angenommen.

3.5.3 Behörde / behördlich anerkannte Stelle

Zur Erfüllung besonderer gesetzlicher Vorgaben bzw. Formvorschriften (*hoch +*) müssen die Stellen Behörden bzw. behördlich anerkannte Stellen sein, da Behörden im öffentlichen Interesse handeln und besonderen Sorgfaltsanforderungen unterliegen.

Soweit die Stelle nicht selbst eine Behörde ist, muss die Anerkennung für die wahrgenommene Aufgabe durch eine Behörde auf Basis gesetzlicher Vorgaben bzw. eines formalisierten Prozesses erfolgen.

3.6 Absicherung von Kommunikationsbeziehungen

Für alle Kommunikationsbeziehungen sind beim Einsatz von Kryptographie zur Absicherung die Anforderungen aus Abschnitt 3.7 zu beachten.

3.6.1 ... zwischen Authentisierungsmittelinhaber und vertrauender Entität

Grundsätzlich sollten Authentisierungssysteme bevorzugt werden, bei denen eine unmittelbare Kommunikations- bzw. Vertrauensbeziehung zwischen den Inhabern von Authentisierungsmitteln und den vertrauenden Entitäten besteht bzw. hergestellt wird. Eine direkte Kommunikation in diesem Sinne findet auch dann statt, wenn Auftragsdatenverarbeitende der vertrauenden Entität involviert sind. Bei einer Beteiligung weisungsunabhängiger Dritter hängt die Sicherheit der Authentisierung wesentlich von der Vertrauenswür-

digkeit dieser dritten Parteien ab, und diese müssen die Anforderungen an beteiligte Stellen nach Abschnitt 3.5 erfüllen.

3.6.2 ... zwischen Stellen des Authentisierungssystems

Für Vertrauensniveau *normal* ist eine Absicherung der Kommunikation zwischen den beteiligten Stellen auf Transportebene ausreichend

Für Vertrauensniveaus *substantiell* und *hoch* ist eine Ende-zu-Ende-Beziehung zwischen den beteiligten Stellen notwendig. Dies kann durch eine unmittelbare sichere Verbindung auf Transportebene oder durch eine Sicherung auf Inhaltsdatenebene erfolgen. Insbesondere für Vertrauensniveau *hoch* ist letzteres zu bevorzugen.

Die sichere Kommunikation setzt die Identifizierung der Kommunikationspartner auf entsprechendem Vertrauensniveau voraus:

- Für die Authentizität der übertragenen Daten ist eine Identifizierung des Senders notwendig;
- Für die Vertraulichkeit der übertragenen Daten ist eine Identifizierung des Empfängers notwendig.

Sofern ein Authentisierungssystem dritte Parteien oder Intermediäre umfasst, so sind diese in die Bewertung des Vertrauensniveaus einzubeziehen. Es gelten die Vorgaben aus Abschnitt 3.5.

3.7 Kryptographie

Kryptographische Verfahren können in diversen Bereichen der Authentisierungssysteme eingesetzt werden, etwa zur Absicherung der Authentisierung selbst, der sicheren Übertragung von Identitätsdaten oder der Authentizitätssicherung von Dokumenten.

Für verschiedene Mechanismen werden konkrete kryptographische Anforderungen in den verschiedenen Teilen der [TR-03116] festgelegt, die jeweils in den Beschreibungen der Mechanismen referenziert werden. Sofern die [TR-03116] für einen Mechanismus keine Vorgaben enthält, so sind die Anforderungen aus [TR-02102] einzuhalten.

3.7.1 Schlüsselspeicherung

Private kryptographische Schlüssel aller Entitäten eines Authentisierungssystems (einschließlich des Inhabers von Authentisierungsmitteln) müssen sicher, das heißt vertraulich, gespeichert werden. Dies setzt voraus, dass der private Schlüssel gegen Kopieren geschützt ist und die Verwendung des Schlüssels durch Unberechtigte verhindert wird.

Ebenso müssen öffentliche Schlüssel, die für die Authentifizierung genutzt werden, sicher, also gegen Manipulation geschützt, gespeichert werden.

Zur Erreichung des Vertrauensniveaus *hoch* ist dazu die Verwendung geeigneter Hardware (zum Beispiel nach Common Criteria auf Assurance Level EAL 4 / *hohes* Angriffspotential nach einem geeigneten Schutzprofil zertifizierte Chipkarten oder HSMs) notwendig. Bei Betrieb der Hardware in einer geschützten Umgebung (entsprechend [ISO27001]) durch eine vertrauenswürdige Stelle (Abschnitt 3.5.2) ist eine Resistenz gegen *moderates* Angriffspotential ausreichend.

3.7.2 Agilität

Die kryptographischen Verfahren müssen so gestaltet werden, dass sie neuen kryptographischen Erkenntnissen angepasst werden können. Dies umfasst insbesondere die Möglichkeit des Austausches von Schlüsseln, den Austausch kryptographischer Primitive und die Erhöhung von Schlüssellängen. Es wird empfohlen, bereits bei der Entwicklung eines Systems ein Migrationskonzept zu erstellen.

3.8 Anforderungen an die Nutzerumgebung

Das BSI gibt für Bürger Empfehlungen zur Absicherung des lokalen Rechners heraus (https://www.bsi-fuer-buerger.de). Diese Empfehlungen umfassen unter anderem:

- Installation von Firewall, Virenscanner und aller Sicherheitsupdates
- Abschalten aktiver Inhalte im Browser soweit möglich
- Abschalten über die Sitzungsdauer hinaus persistenter Cookies im Browser

Diese Auflistung ist nicht umfassend, es gilt der jeweils aktuelle Stand nach https://www.bsi-fuer-buerger.de. Es muss sichergestellt werden, dass die Mechanismen mit entsprechend den Empfehlungen konfigurierten Rechnern verwendbar sind, Mechanismen dürfen keine Anforderungen stellen, die den Empfehlungen des BSI widersprechen.

Bei der Bewertung von Mechanismen muss berücksichtigt werden, dass diese Empfehlungen ggf. nicht flächendeckend umgesetzt werden.

Darüber hinaus sollten Mechanismen bevorzugt werden, die mit möglichst vielen Betriebssystemen und Browsern zusammenarbeiten, um dem Anwender Wahlfreiheit des eingesetzten lokalen Rechners zu geben und im Falle von Sicherheitswarnungen für bestimmte Systeme Alternativen nutzen zu können.

4 Authentisierungsverfahren

In vielen Mechanismen kommt dem **Authentisierungsverfahren** eine besondere Bedeutung zu. So kann etwa ein Identifizierungsmechanismus auf einer Authentisierung einer Person gegenüber einem Identitätsprovider („Identity Provider" – IdP) bestehen, der dann die dem Authentisiserungsmittel zugeordneten Identitätsdaten an die vertrauende Entität weitergibt.

Authentisierungsverfahren müssen den Inhaber der Authentisierungsmittel gegenüber der Gegenstelle eindeutig identifizieren (üblicherweise durch die Registrierung einer eindeutigen Kennung des Authentisierungsmittels bei der Gegenstelle). Das Authentisierungsverfahren muss einerseits diese Kennung der Gegenstelle gegenüber entsprechend der Anforderungen des jeweiligen Vertrauensniveaus nachweisen, Dritten darf die Kennung aus Datenschutzgründen aber nicht bekannt werden.

Die Authentisierung muss an einen sicheren Kanal zwischen Authentisierungsmittelinhaber und vertrauenden Entität gebunden werden, damit auf der Authentisierung aufbauende Geschäftsprozesse sicher abgewickelt werden können (vgl. Abschnitt 6).

Es gelten die Anforderungen für Vertrauensniveaus gemäß

- Abschnitt 3.3 für Authentisierungsmittel und -protokoll;
- Abschnitt 3.4 für Rückruf und Sperrung – sofern das Authentisierungsverfahren keine Rückruf-/Sperrmöglichkeit bietet, muss die entsprechende Funktion durch das Verfahren geleistet werden, das die Authentisierung einsetzt;
- der Abschnitte 3.5, 3.6.1 und 3.7 für die Anforderungen an die Vertrauenswürdigkeit beteiligter Stellen, der Absicherung von Kommunikationsbeziehungen und Kryptographie.

Authentisierungsverfahren lassen sich in zwei Kategorien aufteilen, „symmetrische" und „asymmetrische" Verfahren. Bei symmetrischen Verfahren sind die Authentisierungsdaten, die der Nutzer nutzt, in gleicher oder ähnlicher Form zur Gegenstelle übermittelt bzw. als Verifikationsdaten dort gespeichert, z.B. Passwörter oder Verfahren basierend auf One-Time-Passwörtern. Ein Angreifer kann sich durch Kompromittieren dieser gespeicherten Daten („Passwortdatenbank") für den eigentlichen Authentisierungsmittelinhaber ausgeben. Bei asymmetrischen Verfahren, z.B. kryptographischen Challenge-Response-Verfahren, sind die für die Authentisierung erforderlichen Authentisierungsdaten nicht bei der Gegenstelle gespeichert. Daher sind in diesem Sinne asymmetrische Verfahren als Authentisierungsverfahren zu bevorzugen.

Eine Gesamtbewertung des Vertrauensniveaus eines Mechanismus des Identitätsmanagements, der ein Authentisierungsverfahren entsprechend dieses Abschnitts einsetzt, (vgl Abschnitt 10) muss die Integration des Authentisierungsverfahrens in den Gesamtmechanismus berücksichtigen.

4.1 Elektronischer Identitätsnachweis

Der *elektronische Identitätsnachweis* (siehe Abschnitt 10.1) kann durch den Einsatz des Pseudonyms (dienste- und kartenspezifische Kennung) für die Authentisierung auf hohem Vertrauensniveau eingesetzt werden.

4.2 Kryptographische Token

Ein kryptographisches Token speichert einen privaten kryptographsichen Schlüssel. Bei entsprechender Zuordnung des Tokens zu einer Person (etwas durch die Registrierung des zugehörigen öffentlichen Schlüssels/Zertifikates bei der Gegenstelle), kann das Token zur Authentisierung der Person genutzt werden. Die Authentisierung erfolgt üblicherweise durch ein Challenge-Response-Verfahren, das den Besitz des privaten Schlüssels zu diesem Zertifikat nachweist.

Beispiele für Hardwaretoken sind elektronische Mitarbeiterausweise, spezielle USB-Sticks oder Schlüsselkarten aus der Deutschland-Online-Infrastruktur (DOI). Neben der Speicherung des privaten Schlüssels auf ei-

nem Hardwaretoken ist auch die Speicherung des Schlüssels auf dem Rechner des Inhabers möglich (Softwaretoken oder „Softwarezertifikat“[9]).

Für Vertrauensniveau *substantiell* muss das Authentisierungsmittel aus zwei Faktoren bestehen. Für Softwaretoken hängt es von der konkreten Ausgestaltung und Einsatzumgebung ab, ob diese Anforderung erfüllt ist. Die Anforderungen aus Maßnahme M 2.11 „Regelung des Passwortgebrauchs“ der IT-Grundschutz-Kataloge des BSI (siehe [BSI-GS]) sind für das Passwort, welches den Zugriff auf den privaten Schlüssel schützt, einzuhalten.

Vertrauensniveau *hoch* kann durch die Anforderung der Resistenz gegen Duplizierung und Manipulation gegen hohes Angriffspotential durch Softwaretoken nicht erreicht werden.

Es gelten die Anforderungen aus Abschnitt 3.7. Die privaten kryptographischen Schlüssel dürfen nicht außerhalb des Tokens vorliegen (kein Key-Backup oder Key-Escrow). Sofern Schlüssel außerhalb des Tokens erzeugt werden, so muss dies in einer sicheren Umgebung erfolgen und die außerhalb des Tokens vorliegenden privaten Schlüssel vor Auslieferung des Tokens gelöscht werden.

Das Vertrauensniveau hängt vom Kontext und den gewählten Verfahren für die Registrierung des Tokeninhabers (Enrolment) und der Ausgabe der Token ab. Eine Bewertung muss im Einzelfall erfolgen.

4.3 One Time Passwords

One Time Passwords (OTPs) oder Transaktionsnummern (TANs) sind Authentisierungsverfahren, bei denen Einmalpasswörter zur Authentisierung genutzt werden. Die Einmalpasswörter werden je nach Verfahren vorab in Form von Listen dem Inhaber zur Verfügung gestellt, oder im Augenblick der Authentisierung auf einem getrennten Kanal übermittelt bzw. durch ein separates Gerät erzeugt.

Beispiele für TAN-Verfahren sind:

- Das klassische TAN-Verfahren (TAN-Liste mit Benutzung einer beliebigen TAN von der Liste) sollte aufgrund der vielen bekannten praktischen Angriffe nicht verwendet werden.
- Das iTAN-Verfahren: Es werden indizierte TAN-Listen verwendet, die zu verwendende TAN wird von der vertrauenden Entität vorgegeben. Die TAN-Liste ist nicht kopiergeschützt, und daher nicht als Faktor „Besitz“ zu werten. Vielmehr ist die TAN-Liste „aufgeschriebenes Wissen“, d.h. es gelten die Anforderungen aus Abschnitt 3.3.1.2.
- Das mTAN-Verfahren (mobile TAN, auch smsTAN) nutzt die Verbindung zu einer registrierten Telefonnummer zur Übermittlung einer vorgangsspezifischen TAN per SMS. Im Sinne von Abschnitt 3 ist die mTAN ein Authentisierungsprotokoll zum Nachweis des Besitzes (Abschnitt 3.3.1.1) einer SIM-Karte (bzw. genauer der zugehörigen Telefonnummer).
- Im Unterschied zur Übermittlung der TAN per SMS bei der smsTAN wird bei beim pushTAN-Verfahren die TAN über die Internet-Verbindung des Mobilgerätes an eine vorher registrierte App übermittelt. Dieses Verfahren weist den Zugriff des Nutzers auf die (üblicherweise PIN-/passwortgeschützte) App nach.
- Verfahren basierend auf TAN-Generatoren (auch chipTAN) nutzen eine separate Hardware, den TAN-Generator, zur Erzeugung von vorgangsspezifischen TANs. Analog zur mTAN ist die chipTAN ein Verfahren zum Nachweis des Besitzes des TAN-Generators.

Das Vertrauensniveau *hoch* kann grundsätzlich nur mit TAN-Verfahren erreicht werden, bei der wesentliche Vorgangsdaten in die Erzeugung der TAN eingehen und dem Nutzer unabhängig von der primären Verbindung zwischen Bürger und vertrauenden Entität angezeigt werden. Dies ist notwendig, um die Verwendung einer TAN durch einen unberechtigten Dritten für einen anderen Vorgang/Sitzung zu verhindern (z.B. per Phishing).

9 Diese (übliche) Bezeichnung ist ungenau, da die Speicherung des privaten Schlüssels entscheidend ist, nicht die des (öffentlichen) zugehörigen Zertifikates.

Darüber hinaus muss das Verfahren für Vertrauensniveau *hoch* eine Zwei-Faktor-Authentisierung (vgl. Abschnitt 3.3) unabhängig von der primären Verbindung zwischen Bürger und vertrauenden Entität abbilden.

4.3.1 iTAN

Das iTAN-Verfahren ist zur Zeit noch für Vertrauensniveau *normal* einsetzbar, entspricht aber nicht mehr dem Stand der Technik und sollte so bald wir möglich durch ein anderes Verfahren abgelöst werden. Für neue Verfahren darf das iTAN-Verfahren nicht mehr eingesetzt werden.

4.3.2 smsTAN

Mit dem smsTAN-Verfahren ist Vertrauensniveau *hoch* nicht erreichbar. Der Faktor Besitz, repräsentiert durch die SIM-Karte (genauer: die Telefonnummer), ist nicht gegen Duplizierung/Übernahme durch einen Angreifer mit hohem Angriffspotential geschützt[10]. Daneben ist die Entropie einer (üblicherweise) 6-stelligen TAN sowie die Übertragungssicherheit im Mobilnetz nicht ausreichend, um als Authentisierungsprotokoll den Besitz auf hohem Vertrauensniveau nachzuweisen.

Für neue Verfahren mit Schutzbedarf *hoch* / *substantiell* sollte smsTAN nicht mehr eingeführt werden.

Für bestehende Verfahren ist Vertrauensniveau *substantiell* nur unter folgenden Voraussetzungen erreichbar:

- Die Registrierung der SIM-Karte (bzw. genauer der Telefonnummer) auf das Konto des Bürgers bei der Behörde erfolgt in Verbindung mit einer Identifizierung des Bürgers mindestens auf Vertrauensniveau *substantiell* (vgl. Abschnitt 5).
- Das smsTAN-Verfahren bildet eine Zwei-Faktor-Authentisierung über die Telefonnummer (Faktor Besitz) und den Zugangscode (PIN, Geste – Faktor Wissen) des Mobiltelefons. Daher darf das Verfahren nur mit Mobiltelefonen benutzt werden, die einen eingeschalteten und wirksamen Mechanismus zur Zugangssperre haben. Alternativ kann die smsTAN in Verbindung mit einem anderen wissensbasierten Faktor eingesetzt werden, wobei Abschnitt 3.3.1.4 zu beachten ist.
- Die primäre Verbindung zwischen Bürger und Behörde (d.h. die eigentliche Transaktion) erfolgt nicht über das Mobiltelefon, sondern über ein separates Endgerät und ein anderes Netzwerk.

Die letzte Voraussetzung wird mit der heutigen Durchdringung von mobilen Geräten als Primärgerät im Allgemeinen nicht mehr erfüllbar sein, so dass die smsTAN – abgesehen von Anwendungen, in denen diese Trennung organisatorisch sichergestellt werden kann – ohne weitere Maßnahmen nicht Vertrauensniveau *substantiell* erreicht.

4.3.3 pushTAN

Verfahren dieser Art werden üblicherweise für mobile Anwendungen in Kombination mit einem Passwort eingesetzt, d.h. die Anwendung und die pushTAN-App laufen auf dem gleichen Endgerät und kommunizieren über den gleichen Kommunikationsweg (Internet). Ohne weitere Maßnahmen ist die pushTAN also kein gegenüber der Anwendung und der dortigen passwortbasierten Authentisierung unabhängiger Faktor, insbesondere bei automatischer Übernahme der TAN aus der pushTAN-App in die Anwendung.

4.3.4 TAN-Generatoren

Mit einem TAN-Generator ist Vertrauensniveau *substantiell* / *hoch* unter folgenden Voraussetzungen erreichbar:

10 Auch wenn die Karte selbst ggf. hohem Angriffspotential standhält, so kann bei einigen Mobilfunkprovidern auf recht einfachem Wege eine zweite SIM-Karte für die gleiche Telefonnummer (auch durch einen Angreifer) angefordert werden, und somit der Besitz effektiv kopiert werden.

- Der TAN-Generator muss individuell sein, d. h. Generatoren unterschiedlicher Inhaber sind nicht gegeneinander austauschbar. Diese Bedingung ist auch erfüllt, wenn der eigentliche Generator durch eine Chipkarte individualisiert wird.
- Der Generator/die Chipkarte (Faktor Besitz) ist zur Erzeugung der TAN durch eine PIN oder Ähnliches (Faktor Wissen) geschützt. Es gelten die Kriterien aus Abschnitt 3.3. Alternativ kann die chipTAN in Verbindung mit einem anderen wissensbasierten Faktor eingesetzt werden, wobei Abschnitt 3.3.1.4 zu beachten ist.

Aufgrund der Vielzahl und herstellerspezifisch unterschiedlichen Ausprägung kann eine abschließende Bewertung aller Verfahren hier nicht erfolgen. Diese muss auf Basis der hier definierten Kriterien anhand des konkreten Verfahrens und seiner Umsetzung erfolgen.

4.4 Nutzername/Passwort

Es sind die Anforderungen aus Maßnahme M 2.11 „Regelung des Passwortgebrauchs“ der IT-Grundschutz-Kataloge des BSI (siehe [BSI-GS]) einzuhalten.

Es kann nur das Vertrauensniveau *normal* erreicht werden.

5 Identifizierung einer Person

Die **Erstidentifizierung** oder **Registrierung** einer natürlichen oder einer juristischen Person ist die Grundlage für viele elektronische Geschäftsprozesse. Für ein vertrauenswürdiges Identitätsmanagement ist diese Identifizierung (bzw. die im Rahmen der Registrierung durchgeführte Identifizierung) die Basis für alle weiteren Aktivitäten, wie beispielsweise die Vergabe von Berechtigungen (Autorisierung).

Entsprechend der Definition in Abschnitt 2 ist eine Identität, und damit auch eine Identifizierung, nicht notwendigerweise eindeutig. Die notwendigen Attribute einer Identität werden durch den jeweiligen Anwendungskontext bestimmt, so kann die Identität anwendungsbezogen den Wohnort enthalten, in einem anderen Zusammenhang aber lediglich das Alter umfassen.

Eine **Authentisierung einer Person** ist in diesem Zusammenhang der Spezialfall der Identifizierung einer bereits registrierten Person lediglich mit einem Attribut zur Wiedererkennung der Person. Die eigentlichen Identitätsdaten sind beim Dienstanbieter gespeichert und werden auf Basis eines Authentisierungsverfahrens dem Dienst bereitgestellt.

Identifizierungssysteme, bei denen die Identitätsdaten bei einem Betreiber unabhängig vom Dienstanbieter gespeichert werden („Identity Provider“) müssen als Gesamtsystem betrachtet werden. Aus Sicht des Dienstanbieters stellt das System bestehend aus *Identity Provider* und *Authentisierung des Nutzers beim Identity Provider* (vgl. Abschnitt 4) den Mechanismus „Identifizierung einer Person“ zur Verfügung, d.h. sowohl die Authentisierung als auch der Identity Provider sowie deren Zusammenspiel sind für die Zuordnung zu einem Vertrauensniveau relevant.

Die Identifizierung einer juristischen Person kann auch durch die Identifizierung einer natürlichen Person, die für die juristische Person für den angestrebten Anwendungszweck vertretungsberechtigt ist, erfolgen. Die Vertretungsberechtigung kann etwa

- durch eine Autorisierung auf Seiten des Dienstanbieters (zum Beispiel ein der Identität zugeordneter Datenbankeintrag) erfolgen,
- als Identitätsattribut durch den Identifizierungsmechanismus oder einen Mechanismus zur Übermittlung von Identitätsdaten zur Verfügung gestellt werden, oder
- durch die Verwendung einer abgeleiteten Identität einschließlich der Vertretungsberechtigung erfolgen.

Die Feststellung der Vertretungsberechtigung muss dabei auf dem gleichen (oder höheren) Vertrauensniveau wie die Identifizierung der natürlichen Person erfolgen.

5.1 Funktionen

Bei der Identifizierung einer Person muss unterschieden werden, ob beim zu nutzenden Dienst bereits eine verifizierte Identität vorliegt („Nutzerkonto“) oder ob ein Konto neu angelegt bzw. ein Dienst ohne explizite Erstellung eines Kontos genutzt werden soll. Im ersten Fall ist der Anwendungszweck die *Anmeldung* bzw. das *Login*, im zweiten die *Registrierung* oder *Erstidentifizierung*.

Eine Identifizierung im Sinne dieses Abschnittes ist immer die Registrierung bzw. Anmeldung, üblicherweise mit dem Ziel, im Anschluss Dienste zu nutzen, das heißt ein synchroner Vorgang. Für asynchrone Vorgänge, zum Beispiel Übermittlung eines Dokumentes in Verbindung mit Identitätsdaten, siehe Abschnitte 8 und 9.

Grundsätzlich können Erstidentifizierung und Anmeldung auf unterschiedlichem Vertrauensniveau erfolgen, zum Beispiel kann ein Konto mittels elektronischem Identitätsnachweis angelegt werden, die Nutzung aber über ein Passwort erfolgen. In diesem Fall ist das Vertrauensniveau der Anmeldung das Minimum der Vertrauensniveaus beider Vorgänge.

Die Identifizierung einer Person ist ein flüchtiger Vorgang, sie hat Gültigkeit nur für den Augenblick und ist Dritten gegenüber nicht nachweisbar. Dies entspricht dem Begriff der Identifizierung im nicht-elektroni-

schen Fall, etwa per Vorlage des Personalausweises bei natürlichen Personen. Die reine Identifizierung (Prüfung des Ausweises) ist Dritten gegenüber nicht nachweisbar, also flüchtig. Diese Flüchtigkeit sollte sich aus Datenschutzgründen grundsätzlich auch in der verwendeten Technologie für die Identifizierung widerspiegeln („deniability"), im Gegensatz zur Unabstreitbarkeit („non-repudiation") bei Willenserklärungen.

In einigen Fällen ist eine spätere Nachweisbarkeit jedoch trotzdem erforderlich. In diesen Fällen sind zusätzliche Prozessschritte oder Maßnahmen auf der Seite des Dienstanbieters erforderlich, etwa die sichere Speicherung der Identifizierungsdaten in den Systemen des Anbieters. Dies entspricht im nicht-elektronischen Fall der Erstellung einer Ausweiskopie[11], die gegebenenfalls als zusätzliche Maßnahme notwendig ist. Entsprechende Maßnahmen sind, sofern notwendig, bei der Konzeption der Anwendung zu berücksichtigen.

Die Identifizierung muss an den Sitzungskontext gebunden sein, es findet jedoch keine Bindung an eine Transaktion oder weitere Prozesse statt. Sofern dies in einer Anwendung notwendig ist, muss die Bindung durch den Anwendungskontext erfolgen.

Die Funktionen der Identifizierung einer Person gegenüber einem Dienstanbieter sind:

- Authentizität/Integrität der übermittelten Identitätsattribute
- Bindung der Identifizierung an den Sitzungskontext
- Vertraulichkeit der übermittelten Identitätsattribute; dies setzt eine Identifizierung des Empfängers, d.h. des Dienstanbieters, voraus, siehe Abschnitt 6.
- Bindung der übermittelten Identitätsattribute an die berechtigte Person
- Datensparsame Übermittlung von Identitätsattributen und Flüchtigkeit der Identifizierung.

5.2 Kriterien für Vertrauensniveaus

Für die Einordnung eines Mechanismus zur Identifizierung einer Person zu einem Vertrauensniveau werden die folgenden Kriterien verwendet (vgl. Tabelle 4).

Identifizierung einer Person	**Vertrauensniveau**		
	Normal	**Substantiell**	**Hoch**
Anforderungen nach Abschnitt 3	*Normal*	*Substantiell*	*Hoch*
Identifizierung des Dienstanbieters (siehe Abschnitt 6)	*Normal*	*Substantiell*	*Hoch*
Bindung der Identifizierung an den Sitzungskontext	Organisatorisch	Kryptographisch	Kryptographisch
Vertraulichkeit der Identitätsattribute (siehe Abschnitt 3.6)	Absicherung der Kommunikation auf Vertrauensniveau *normal*	Absicherung der Kommunikation auf Vertrauensniveau *substantiell*	Absicherung der Kommunikation auf Vertrauensniveau *hoch*

Tabelle 4: Kriterien „Identifizierung einer Person"

5.2.1 Grundlegende Kriterien

Die allgemeinen Anforderungen aus Abschnitt 3 müssen entsprechend des angestrebten Vertrauensniveaus erfüllt werden.

11 Dabei sind die Regelungen zur rechtlichen Zulässigkeit von Ausweiskopien zu beachten.

5.2.2 Identifizierung des Dienstanbieters

Eine vorhergehende Identifizierung des Dienstes (und damit verbunden der Aufbau einer sicheren Verbindung) ist Voraussetzung für die nachfolgenden Kriterien und muss daher mindestens mit dem angestrebten Vertrauensniveau der Identifizierung einer Person erfolgen. Kriterien und Mechanismen für die Identifizierung eines Dienstes werden in Abschnitt 6 betrachtet.

5.2.3 Bindung der Identifizierung an den Sitzungskontext

Die übertragene Identität muss an den Sitzungskontext gebunden werden. Dies bedeutet unter anderem, dass die Identität einer Person eindeutig einer bestimmten Session und nicht lediglich einem bestimmten Kommunikationsendpunkt zugeordnet werden muss und auch nur dort gültig sein darf. Für Vertrauensniveaus *substantiell*/*hoch* muss diese Bindung über geeignete technische/kryptographische Mechanismen erfolgen.

5.2.4 Vertraulichkeit der Identitätsattribute

Die Vertraulichkeit der Identitätsattribute einer Person setzt eine Identifizierung des empfangenden Dienstanbieters auf gleichem Vertrauensniveau wie die Identifizierung der Person voraus (s.o.).

Es muss sichergestellt sein, dass Identitätsattribute erst nach erfolgter Freigabe durch die Person übermittelt werden.

Für die eigentliche Übertragung der Identitätsattribute sind die Anforderungen in Abschnitt 3.6 zu beachten.

5.3 Mechanismen

In Abschnitt 10 werden verschiedene Mechanismen zur Identifizierung einer Person vorgestellt und entsprechend der Kriterien in diesem Abschnitt bewertet.

<table>
<tr><th rowspan="2">Vertrauensniveau</th><th colspan="3">Identifizierung einer Person</th></tr>
<tr><th>Registrierung / Erstidentifizierung</th><th colspan="2">Anmeldung / Login</th></tr>
<tr><td rowspan="2">Hoch</td><td colspan="2">Elektronischer Identitätsnachweis (Abschnitt 10.1)</td><td></td></tr>
<tr><td>--</td><td>Kryptographische Hardwaretoken (Abschnitt 10.2)</td><td>--</td></tr>
<tr><td>Substantiell</td><td>--</td><td>Kryptographische Softwaretoken (Abschnitt 10.2)</td><td rowspan="2">TAN-Verfahren (Abschnitt 10.3)</td></tr>
<tr><td>Normal</td><td>--</td><td>Nutzername/Passwort (Abschnitt 10.4)</td></tr>
</table>

Tabelle 5: Typische Mechanismen für die Identifizierung einer Person

Werden für eine Identifizierung einer Person besondere Formvorschriften verlangt, so sind diese i.A. nur durch den elektronischen Identitätsnachweis zu erfüllen.

6 Identifizierung eines Dienstanbieters

Neben der Identifizierung des Nutzers gegenüber einem Dienst ist meist auch eine (eindeutige) Identifizierung des Dienstes gegenüber dem Nutzer notwendig. Meist erfolgt die Identifizierung des Dienstanbieters vor der Identifizierung der Nutzers. Die Identifizierung des Dienstanbieters ist Voraussetzung für die Vertraulichkeit der Identitätsattribute der Person, da nur so sichergestellt werden kann, dass die Attribute nicht an unberechtigte Dritte übermittelt werden.

6.1 Funktionen

Diese Richtlinie betrachtet nur öffentlich zugängliche Dienste, d. h. die Identität des Dienstes muss nicht vertraulich behandelt werden. Es muss lediglich die Authentizität und Integrität sichergestellt werden. Ebenso ist eine datensparsame Identifizierung nicht notwendig, sondern der Dienst identifiziert sich der Person gegenüber eindeutig.

Die Identifizierung eines Dienstes dient meist der Vorbereitung weiterer Interaktionen mit dem Dienst, d. h. die Identifikation muss an eine „Sitzung" bzw. an eine Verbindung zwischen Person und Dienst gebunden werden. Diese Funktion ist nicht notwendig, wenn der Geschäftsprozess mit der Identifizierung abgeschlossen wird, das heißt keine weitere „Sitzung" notwendig ist.

Damit sind die Funktionen einer Dienstanbieter-Identifizierung:

- Authentizität/Integrität der übermittelten Identität des Dienstanbieters
- Aufbau einer an die Identifizierung des Dienstanbieters gebundenen sicheren Verbindung zwischen Person und Dienstanbieter zur Verwendung für die nachfolgenden Prozesse

6.2 Kriterien für Vertrauensniveaus

Für die Einordnung eines Mechanismus zur Identifizierung eines Dienstanbieters zu einem Vertrauensniveau werden die folgenden Kriterien verwendet (vgl. Tabelle 6).

Identifizierung eines Dienstanbieters	**Vertrauensniveau**		
	Normal	**Substantiell**	**Hoch**
Anforderungen nach Abschnitt 3	*Normal*	*Substantiell*	*Hoch*
Absicherung der Verbindung (siehe Abschnitt 3.6)	Absicherung der Kommunikation auf Vertrauensniveau *normal*	Absicherung der Kommunikation auf Vertrauensniveau *substantiell*	Absicherung der Kommunikation auf Vertrauensniveau *hoch*
Bindung der Identifizierung an den Sitzungskontext	Organisatorisch	Kryptographisch	Kryptographisch

Tabelle 6: Kriterien „Identifizierung eines Dienstanbieters"

Das notwendige Vertrauensniveau für die Identifizierung des Dienstanbieters ist abhängig vom notwendigen Vertrauensniveau für die übertragenen Daten selbst und kann daher ggf. vom notwendigen Vertrauensniveau für die anderen Funktionen abweichen. Die Bewertung geht von einem einheitlichen Vertrauensniveau für alle Funktionen aus.

6.2.1 Grundlegende Kriterien

Die allgemeinen Anforderungen aus Abschnitt 3 müssen entsprechend des angestrebten Vertrauensniveaus erfüllt werden.

6.2.2 Absicherung der Verbindung

Wegen der Nutzung der aufgebauten Verbindung für einen nachfolgenden Geschäftsprozess ist die Sicherheit dieser Verbindung über die reine Identifizierung hinaus wichtig. Eine Umverschlüsselung o. ä. durch Dritte (sofern nicht Auftragsdatenverarbeiter) ist für Vertrauensniveau *substantiell*/*hoch* daher nicht statthaft, es ist eine Ende-zu-Ende-Absicherung im Sinne der Authentizität und der Vertraulichkeit zwischen Nutzer und Dienstanbieter (bzw. dessen Auftragsdatenverarbeiter) notwendig.

Die Anforderungen aus Abschnitt 3.6 sind einzuhalten.

6.2.3 Bindung der Identifizierung an den Sitzungskontext

Als Bestandteil des Aufbaus eines Sitzungskontextes muss sichergestellt werden, dass die Identifizierungen des Dienstes an diese Sitzung gebunden werden. Dies umfasst, dass die Identität eindeutig einer bestimmten Session und nicht lediglich einem bestimmten Kommunikationsendpunkt zugeordnet werden muss und auch nur dort gültig sein darf. Für Vertrauensniveau *substantiell*/*hoch* muss diese Bindung über geeignete technische/kryptographische Mechanismen erfolgen, etwa kryptographisch sichere Session-Identifier/-Cookies.

6.3 Mechanismen

In Abschnitt 10 werden verschiedene Mechanismen zur Identifizierung eines Dienstanbieters vorgestellt und entsprechend der Kriterien in diesem Abschnitt bewertet.

Vertrauensniveau	**Identifizierung eines Dienstanbieters**
Hoch	Berechtigungszertifikat als Bestandteil des elektronischen Identitätsnachweises (Abschnitt 10.1)
Substantiell	TLS-Zertifikate (Abschnitt 10.6)
Normal	

Tabelle 7: Typische Mechanismen für die Identifizierung eines Dienstanbieters

7 Abgabe einer Willenserklärung

Eine *Abgabe einer Willenserklärung* (oder technisch eine *Transaktionsauthentisierung*) ist eine Äußerung eines auf die Herbeiführung einer Rechtswirkung gerichteten Willens durch einen Erklärenden.

Im Rahmen dieser Richtlinie umfasst die Abgabe einer Willenserklärung die Zustimmung zu einem Vorgang oder dem Inhalt eines Dokumentes. Da die Zustimmung zu einem Vorgang ersetzt werden kann durch die Zustimmung zu einem Dokument, das die Vorgangsdaten als Inhalt hat, wird im Folgenden nur der Fall der Zustimmung zu einem Dokument betrachtet.

Die Wirksamkeit der Willenserklärung erfolgt erst mit Zugang zum Adressaten, so dass nach der Abgabe der Willenserklärung das Dokument i.A. übermittelt werden muss.

Im Rahmen dieser Richtlinie werden Willenserklärungen einer Person gegenüber einem Dienstanbieter betrachtet.

7.1 Funktionen

Das höchste Vertrauensniveau für die Abgabe einer Willenserklärung wird im Verwaltungsrecht durch die Schriftform erreicht. Diese bildet die Eigenschaften der klassischen Unterschrift ab, von der sich die im Folgenden dargestellten Funktionen ableiten (zitiert aus [BRSchriftform]):

- *Perpetuierungsfunktion: Schriftform setzt auch im Verwaltungsrecht immer die Verkörperung der Erklärung in einer Urkunde voraus. Durch die Verkörperung der Erklärung in einer Urkunde (Urkundeneinheit) wird gewährleistet, dass die Erklärung dauerhaft festgehalten ist. Dies ermöglicht es, ihren Inhalt zu überprüfen.*
- *Warnfunktion: Wenn zur Einhaltung der Schriftform die eigenhändige Unterzeichnung der Erklärung erforderlich ist, wird der Erklärende durch den bewussten Akt des Unterzeichnens auf die erhöhte rechtliche Verbindlichkeit und die persönliche Zurechnung der unterzeichneten Erklärung hingewiesen. Hierdurch soll er vor Übereilung geschützt werden.*
- *Abschlussfunktion: Durch die eigenhändige Unterschrift wird die Erklärung räumlich abgeschlossen; Bestandteil der Erklärung ist grundsätzlich nur, was vor der Unterschrift steht. Die eigenhändige Unterschrift grenzt bei nicht empfangsbedürftigen Erklärungen auch die verbindliche Erklärung vom Entwurf ab.*
- *Identitäts- und Verifikationsfunktion: Durch eigenhändige Namensunterschrift ist der Aussteller der Urkunde erkennbar und identifizierbar, da die unverwechselbare Unterschrift eine unzweideutige Verbindung zur Person des Unterzeichners herstellt. Die Identität kann im Streitfall z. B. durch einen Unterschriftenvergleich verifiziert werden.*
- *Echtheitsfunktion: Die räumliche Verbindung der Unterschrift mit der Urkunde, die die Erklärung enthält, stellt einen Zusammenhang zwischen der Erklärung und Unterschrift her. Hierdurch soll gewährleistet werden, dass die Erklärung inhaltlich vom Unterzeichner herrührt und nicht nachträglich verfälscht werden kann.*
- *Beweisfunktion: Durch die Verkörperung der Erklärung in einer Urkunde, die vom Aussteller eigenhändig unterschrieben ist, wird ein Beweismittel geschaffen. Mit der Urkunde kann bewiesen werden, welchen Inhalt die Erklärung hat und wer sie abgegeben hat. Dieser Beweis kann aufgrund der Verifikationsfunktion der Unterschrift, insbesondere durch einen Unterschriftenvergleich erbracht werden.*

Diese Funktionen müssen durch einen elektronischen Mechanismus, der die Schriftform allgemein in der Kommunikation zwischen Bürger und Behörde – oder allgemeiner zwischen einer natürlichen Person und einem Dienstanbieter – abdecken soll, erfüllt werden.

Grundsätzlich jedoch gilt, dass in vielen Anwendungsfällen die Schriftform nicht zwingend erforderlich ist. Nach § 10 [VwVfG] ist das Verwaltungshandeln grundsätzlich formfrei. Die Schriftform ist aufgrund gesetzli-

cher Formvorschriften nur für einige Verwaltungsdienstleistungen erforderlich. Der Betreiber eines Geschäftsprozesses muss daher bewerten, welche Funktionen für seinen Geschäftsprozess relevant sind oder auf welche Funktionen verzichtet werden kann.

Wenn die Schriftform für einen Verwaltungsprozess gesetzlich vorgeschrieben ist, kann sie, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, nach § 3 a [VwVfG] durch die elektronische Form ersetzt werden:

1. mit einer qualifizierten elektronischen Signatur (siehe Abschnitt 10.2.2);
2. mit der Abgabe der Willenserklärung über ein Formular bei der Behörde in Verbindung mit der elektronischen Identitätsfunktion (siehe Abschnitt 10.1.3), oder
3. mittels Nutzung von De-Mail mit der Versandoption „absenderbestätigt“ (siehe Abschnitt 10.5.2).

Darüber hinaus können „sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten“ (§ 3 a Nr. 4 [VwVfG]) die Schriftform ersetzen. Nach aktuellem Stand ist bisher kein solches Verfahren festgelegt worden.

In den Fällen 2. und 3. müssen die Funktionen der Schriftform, die nicht durch den Mechanismus direkt abgedeckt werden durch entsprechende Maßnahmen auf Seiten der Behörde ersetzt werden (siehe Abschnitte 10.1.3 bzw. 10.5.2).

Bei nicht-signaturbasierten Verfahren können grundsätzlich nicht alle Funktionen der Schriftform durch das Verfahren selbst sichergestellt werden. So kann etwa die Abschlussfunktion im Allgemeinen nicht durch TAN-Verfahren abgebildet werden. Die nicht durch das Verfahren selbst dargestellten Funktionen müssen – sofern für den Geschäftsprozess notwendig – durch technische und organisatorische Prozesse, zum Beispiel des Empfängers einer Willenserklärung oder eines vertrauenswürdigen Dritten, ersetzt werden.

7.2 Kriterien für Vertrauensniveaus

Für die Einordnung eines Mechanismus zur Willenserklärung zu einem Vertrauensniveau werden die folgenden Kriterien verwendet (vgl. Tabelle 8).

Abgabe einer Willenserklärung	**Vertrauensniveau**		
	Normal	**Substantiell**	**Hoch**
Anforderungen nach Abschnitt 3	*Normal*	*Substantiell*	*Hoch*
Vertrauensniveau der Identifizierung des Erklärenden (vgl. Abschnitt 5)	*Normal*	*Substantiell*	*Hoch*
Integritätssicherung des Dokuments	Organisatorisch	Kryptographisch oder organisatorisch durch vertrauenswürdige Stelle (Abschnitt 3.5.2)	Kryptographisch oder organisatorisch durch vertrauenswürdige Stelle (Abschnitt 3.5.2)
			Für Formvorschriften ggf. besondere Anforderungen (Abschnitt 3.5.3)
Bindung der Identität an das Dokument	Organisatorisch	Kryptographisch oder organisatorisch durch vertrauenswürdige Stelle (Abschnitt 3.5.2)	Kryptographisch oder organisatorisch durch vertrauenswürdige Stelle (Abschnitt 3.5.2)
			Für Formvorschriften ggf. besondere Anforderungen (Abschnitt 3.5.3)
Auslösung der Abgabe	Einfache Nutzerinteraktion	Auf Vertrauensniveau *substantiell* dem Nutzer zuzurechnen	Auf Vertrauensniveau *hoch* dem Nutzer zuzurechnen

Tabelle 8: Kriterien „Abgabe einer Willenserklärung“

7.2.1 Grundlegende Kriterien

Die allgemeinen Anforderungen aus Abschnitt 3 müssen entsprechend des angestrebten Vertrauensniveaus erfüllt werden.

7.2.2 Vertrauensniveau der Identifizierung des Erklärenden

Die Identifizierung des Erklärenden muss mindestens auf dem angestrebten Vertrauensniveau des Mechanismus für Abgabe einer Willenserklärung erfolgen, siehe Abschnitt 5.

7.2.3 Integritätssicherung des Dokumentes

Die Integrität des Dokumentes muss dauerhaft sichergestellt werden. Die notwendige Dauer ergibt sich aus den Anforderungen des Fachverfahrens und den gesetzlichen Aufbewahrungsfristen. In Fällen, in denen das Dokument aus mehreren Teilen besteht, müssen alle Teile des Dokumentes gesichert werden (Abschluss-

funktion). Zum Beispiel besteht im Falle der Eingabe über ein Webformular das Dokument aus dem Formular und den eingegebenen Daten.

Die Integritätssicherung kann kryptographisch durch die Person erfolgen (signaturbasierte Verfahren), oder durch technisch / organisatorische Maßnahmen beim Dienstanbieter.

Für eine Integritätssicherung beim Dienstanbieter gilt:

- Für Vertrauensniveau *normal* reicht eine organisatorische Sicherung, zum Beispiel Speicherung des Dokumentes durch den Empfänger in einer Datenbank.
- Soll Vertrauensniveau *substantiell/hoch* auf diesem Wege erreicht werden, so muss die Speicherung durch eine für diesen Vorgang als vertrauenswürdig anerkannte Stelle erfolgen.
- Zur Erfüllung besonderer Formvorschriften muss die Speicherung durch eine Behörde bzw. durch eine behördlich für diesen Anwendungszweck geprüfte Stelle (vgl. Abschnitt 3.5.3) in einer elektronischen Akte erfolgen.

Alternativ kann die Sicherung beim Dienstanbieter auch kryptographisch erfolgen, zum Beispiel durch eine kryptographische Signatur (zu den Anforderungen vgl. Abschnitt 3.7) des Dokumentes oder durch eine dauerhafte Archivierung nach [TR-03125].

7.2.4 Bindung der Identität an das Dokument

Die Identität muss dauerhaft überprüfbar an das die Willenserklärung verkörpernde Dokument gebunden werden. Dies kann auf verschiedenem Wege erfolgen. Die Anforderungen aus dem vorigen Abschnitt gelten entsprechend.

7.2.5 Auslösung der Abgabe einer Willenserklärung

Die Abgabe einer Willenserklärung kann im einfachsten Fall durch eine Nutzerinteraktion (zum Beispiel Klick auf einen Button) erfolgen. Auf Vertrauensniveau *substantiell/hoch* muss die Auslösung der Abgabe auf entsprechendem Niveau dem Nutzer zuordenbar sein. Dies kann zum Beispiel geschehen, indem die Auslösung innerhalb einer sicheren Verbindung nach Abschnitt 5 erfolgt, bei deren Aufbau der Nutzer auf dem gewünschten Vertrauensniveau identifiziert wurde. Bei entsprechender Ausgestaltung der Identifizierung (etwa PIN-Eingabe unmittelbar vor Abgabe der Willenserklärung) kann auch diese selbst zur Auslösung der Abgabe genutzt werden.

7.3 Mechanismen

In Abschnitt 10 werden verschiedene Mechanismen zur Willenserklärung vorgestellt und entsprechend der Kriterien in diesem Abschnitt bewertet.

<table>
<tr><th rowspan="2">Vertrauensniveau</th><th colspan="3">Abgabe einer Willenserklärung</th></tr>
<tr><th>Elektronische Signaturen
(Abschnitt 10.2)</th><th colspan="2">Nicht signaturbasiert</th></tr>
<tr><td>Hoch</td><td>Qualifizierte elektronische Signatur /
Fortgeschrittene elektronische Signatur
mit Hardwaretoken</td><td colspan="2">Formular in Verbindung mit Elektronischem Identitätsnachweis
(Abschnitt 10.1) /
De-Mail mit sicherer Anmeldung
(Abschnitt 10.5)</td></tr>
<tr><td>Substantiell</td><td>Fortgeschrittene elektronische Signatur
mit Softwaretoken</td><td>--</td><td rowspan="2">TAN-Verfahren
(Abschnitt 10.3)</td></tr>
<tr><td>Normal</td><td></td><td>Nutzerinteraktion
(Abschnitt 10.4)</td></tr>
</table>

Tabelle 9: Typische Mechanismen für die Abgabe einer Willenserklärung

Die qualifizierte elektronische Signatur, der elektronische Identitätsnachweis in Verbindung mit einem Formularserver und De-Mail mit sicherer Anmeldung erfüllen die besondere Formvorschrift des Schriftformersatzes nach Verwaltungsverfahrensgesetz.

8 Dokumentenübermittlung

Ein wichtiger Prozess im E-Government ist die Übermittlung von Dokumenten – in beiden Richtungen – zwischen Personen und Behörde, zum Beispiel die Übermittlung eines Antrages oder einer Mitteilung, oder umgekehrt der Abruf von Informationen von einer Behörde durch eine identifizierte Person bzw. der Übermittlung eines Bescheids von der Behörde zur Person.

Unterschieden werden muss hierbei zwischen der reinen Dokumentenübermittlung, die in diesem Abschnitt behandelt wird, und einer gegebenenfalls damit verbundenen Abgabe einer Willenserklärung, zum Beispiel für die Wirksamkeit eines Antrags (siehe Abschnitt 7).

8.1 Funktionen

Ein System zur sicheren Dokumentenübermittlung muss die folgenden Funktionen abdecken:

- Vertraulichkeit des Dokumentes während der Übermittlung. Das notwendige Niveau des Schutzes der Vertraulichkeit des Dokumentes hängt dabei wesentlich vom Inhalt des Dokumentes ab.
- Integrität des Dokumentes während der Übermittlung. Diese Funktion gewährleistet nur die Unveränderheit des Dokumentes während der Übertragung. Die Authentizität des Dokumentes setzt die Identifizierung des Senders und die Gewährleistung der Integrität während der Übermittlung voraus.
- Identifizierung des Empfängers. Diese ist Voraussetzung für die Gewährleistung der Vertraulichkeit des Dokumentes, da nur über die Identifizierung des Empfängers sichergestellt werden kann, dass nur dieser Kenntnis vom Inhalt des Dokumentes erhalten kann.
- (Optional) Identifizierung des Senders. Für die reine Übermittlung des Dokumentes ist die Identifizierung des Senders unerheblich, sie kann aber anwendungsbezogen für die durch die Übermittlung ausgelösten Verwaltungsprozesse relevant sein.

Sofern die Dokumentenübermittlung als Zustellung im Sinne des [VwVfG] genutzt werden soll, so muss dies durch entsprechende rechtliche Vorschriften abgesichert werden. Die Identifizierung des Empfängers eines Dokumentes ist notwendige Voraussetzung für die Zustellfunktion.

Bei signierten Dokumenten ist die Integrität des Dokumentes und die Identifizierung des Verfassers bereits durch die Signatur gegeben, d.h. muss nicht mehr notwendigerweise durch das System zur Dokumentenübermittlung geleistet werden.

Je nach Einsatzszenario bzw. übermittelten Dokumenten kann es notwendig sein, als Empfänger nicht eine Behörde zu identifizieren/zu adressieren, sondern eine Organisationseinheit einer Behörde oder auch direkt einen einzelnen Behördenmitarbeiter.

8.2 Kriterien für Vertrauensniveaus

Für die Einordnung eines Mechanismus zur Dokumentenübermittlung zu einem Vertrauensniveau werden die folgenden Kriterien verwendet (vgl. Tabelle 10).

Dokumentenübermittlung	**Vertrauensniveau**		
	Normal	**Substantiell**	**Hoch**
Anforderungen nach Abschnitt 3	*Normal*	*Substantiell*	*Hoch*
Empfängeridentifizierung nach Abschnitt 5/6	*Normal*	*Substantiell*	*Hoch*
Senderidentifizierung nach Abschnitt 5/6 (opt.)	*Normal*	*Substantiell*	*Hoch*
Verschlüsselung und Integritätssicherung (Abschnitt 3.6)	Absicherung der Kommunikation auf Vertrauensniveau *normal*	Absicherung der Kommunikation auf Vertrauensniveau *substantiell*	Absicherung der Kommunikation auf Vertrauensniveau *hoch*
Bindung der Empfänger- und der Senderidentität an das übermittelte Dokument	Organisatorisch	Kryptographisch oder organisatorisch durch vertrauenswürdige Stelle (Abschnitt 3.5.2)	Kryptographisch oder organisatorisch durch vertrauenswürdige Stelle (Abschnitt 3.5.2) Für Formvorschriften ggf. besondere Anforderungen (Abschnitt 3.5.3)

Tabelle 10: Kriterien „Dokumentenübermittlung“

8.2.1 Grundlegende Kriterien

Die allgemeinen Anforderungen aus Abschnitt 3 müssen entsprechend des angestrebten Vertrauensniveaus erfüllt werden.

8.2.2 Sender- und Empfängeridentifizierung

Für die Identifizierung von Sender und Empfänger können die Mechanismen aus Abschnitt 5 genutzt werden. Ein Vertrauensniveau *substantiell*/*hoch* kann nur erreicht werden, wenn auch die Empfängeridentifizierung und ggf. die Senderidentifizierung dieses Vertrauensniveau erreicht.

8.2.3 Verschlüsselung und Integritätssicherung

Für Vertrauensniveau *normal* ist eine Verschlüsselung/Authentisierung auf Transportebene ausreichend.

Die Nutzung eines sicheren Transportnetzes (zum Beispiel IVBB/IVBV, Deutschland-Online-Infrastruktur) ist für das Vertrauensniveau *normal* ausreichend, sofern an das Transportnetz ausschließlich bekannte Stellen angeschlossen sind. Die Nutzung eines sicheren Transportnetzes ist für Vertrauensniveau *substantiell* / *hoch* für sich nicht ausreichend.

Vertrauensniveau *substantiell* / *hoch* bei der Dokumentenübermittlung kann nur erreicht werden, wenn

- die Übermittlung Ende-zu-Ende-verschlüsselt und authentisiert erfolgt, oder

- die Zwischenstationen der Übermittlung eine besondere, gesetzlich abgesicherte, Vertrauenswürdigkeit besitzen und die Übermittlung zwischen diesen verschlüsselt und authentisiert erfolgt. Für die Zwischenstationen gelten die Anforderungen an die Vertrauenswürdigkeit von Stellen (Abschnitt 3.5) entsprechend des Vertrauensniveaus.

Als Sonderfall der zweiten Variante sind die Virtuelle Poststelle (siehe [VPS]) und darauf aufsetzende fachverfahrensspezifische Mechanismen (zum Beispiel das elektronische Gerichts- und Verwaltungspostfach, siehe [EGVP]) einzuordnen. Bei Nutzung der Virtuellen Poststelle werden in einer von der adressierten Behörde zentral betriebenen Stelle die kryptographischen Funktionen Ver-/Entschlüsselung und Signaturerzeugung/-prüfung im Auftrag des eigentlichen Senders/Empfängers durchgeführt. Die Virtuelle Poststelle stellt also eine Zwischenstation zwischen Sender und endgültigem Empfänger dar. Die Virtuelle Poststelle wird von der empfangenden Behörde selbst betrieben und steht damit einer Einordnung des Verfahrens auf Vertrauensniveau *hoch* nicht entgegen.

8.2.4 Bindung der Identitäten an das übermittelte Dokument

Für Vertrauensniveau *normal* ist es ausreichend, wenn die Identitäten von Empfänger (und ggf. Sender) organisatorisch mit dem übermittelten Dokument verbunden werden. Für die weiteren Vertrauensniveaus muss die Bindung durch kryptographische Mechanismen oder organisatorisch durch vertrauenswürdige Stellen gemäß Abschnitt 3.5 erfolgen.

Wenn an der Dokumentenübermittlung mehrere Stellen beteiligt sind und die Bindung organisatorisch erfolgt, so ist das Vertrauensniveau der Bindung das niedrigste Vertrauensniveau der beteiligten Stellen.

8.3 Mechanismen

In Abschnitt 10 werden verschiedene Mechanismen zur Dokumentenübermittlung vorgestellt und entsprechend der Kriterien in diesem Abschnitt bewertet.

<table>
<tr><th rowspan="3">Vertrauensniveau</th><th colspan="4">Dokumentenübermittlung</th></tr>
<tr><th colspan="3">Versand</th><th rowspan="2">Web Up-/Download</th></tr>
<tr><th>De-Mail
(Abschnitt 10.5)</th><th>OSCI
(Abschnitt 10.8)</th><th>E-Mail
(Abschnitt 10.7)</th></tr>
<tr><td>Hoch</td><td rowspan="2">De-Mail
mit sicherer Anmeldung;
mit Empfangsbestätigung förmliche Zustellung</td><td rowspan="2">OSCI mit Ende-zu-Ende Verschlüsselung/Signatur</td><td>--</td><td>... mit Elektronischem Identitätsnachweis
(Abschnitt 10.1.4)</td></tr>
<tr><td>Substantiell</td><td>E-Mail mit S/MIME mit dedizierter PKI</td><td rowspan="2">... mit TLS-Zertifikat
(Abschnitt 10.6)</td></tr>
<tr><td>Normal</td><td>De-Mail</td><td>OSCI mit Transport-Verschlüsselung/-Signatur</td><td>E-Mail mit S/MIME mit Internet-PKI</td></tr>
</table>

Tabelle 11: Typische Mechanismen für sichere Dokumentenübermittlung

De-Mail mit sicherer Anmeldung erfüllt die Vorgaben der besonderen Formvorschrift der förmlichen Zustellung (Zustellfiktion).

9 Übermittlung von Identitätsdaten

Als Spezialfall der Übermittlung eines Dokumentes ist die Übermittlung von Identitätsdaten (Identitätsattribute und verknüpfte Daten) zu sehen. Gemeint ist hierbei die Übermittlung von personenbezogenen Attributen, die bei einem Identitätsprovider gespeichert sind, an einen identifizierten Empfänger. Eine Übermittlung der Identitätsattribute muss dabei ausdrücklich durch die durch die Daten identifizierte Person veranlasst werden.

9.1 Funktionen

Ein System zur sicheren Übermittlung von Identitätsdaten muss die folgenden Funktionen abdecken, vgl. auch Abschnitt 8.1:

- Vertraulichkeit der Identitätsdaten während der Übermittlung.
- Integrität der Identitätsdaten während der Übermittlung. Diese Funktion gewährleistet nur die Unveränderheit der Identitätsdaten während der Übertragung. Die Authentizität der Daten setzt die Identifizierung des Senders und die Gewährleistung der Integrität während der Übermittlung voraus.
- Identifizierung des Empfängers. Diese ist Voraussetzung für die Gewährleistung der Vertraulichkeit der Identitätsdaten, da nur über die Identifizierung des Empfängers sichergestellt werden kann, dass nur dieser Kenntnis von den Daten erhalten kann.

Über die aus den Funktionen für die Dokumentenübermittlung abgeleiteten Funktionen muss ein Mechanismus für die Übermittlung von Identitätsdaten folgende Funktionen abdecken:

- Sichere Erstidentifizierung. Die beim Identitätsprovider gespeicherten Daten müssen über eine sichere Erstidentifizierung erhoben werden.
- Sichere Speicherung der Identitätsdaten beim Identitätsprovider. Der Identitätsprovider führt ein Konto mit den erhobenen Identitätsdaten. Die Daten müssen sicher (vertraulich, authentisch) gespeichert werden.
- Anmeldung am Konto und Auslösung der Datenübermittlung. Es muss sichergestellt werden, dass lediglich die durch die Identitätsdaten bezeichnete Person die Übermittlung der Identitätsdaten veranlassen kann.

Das notwendige Vertrauensniveau für die Vertraulichkeit der Identitätsdaten/Identifizierung des Empfängers ist abhängig von den Daten selbst und kann daher ggf. vom notwendigen Vertrauensniveau für die anderen Funktionen abweichen. Die Bewertung geht von einem einheitlichen Vertrauensniveau für alle Funktionen aus.

9.2 Kriterien für Vertrauensniveaus

Für die Einordnung eines Mechanismus zur Übermittlung von Identitätsdaten zu einem Vertrauensniveau werden die folgenden Kriterien verwendet (vgl. Tabelle 12).

Übermittlung von Identitätsdaten	**Vertrauensniveau**		
	Normal	**Substantiell**	**Hoch**
Anforderungen nach Abschnitt 3	*Normal*	*Substantiell*	*Hoch*
Empfängeridentifizierung nach Abschnitt 5/6	*Normal*	*Substantiell*	*Hoch*
Verschlüsselung und Integritätssicherung nach Abschnitt 8.2.3	*Normal*	*Substantiell*	*Hoch*
Erstidentifizierung nach Abschnitt 5	*Normal*	*Substantiell*	*Hoch*
Anmeldung am Konto nach Abschnitt 5	*Normal*	*Substantiell*	*Hoch*

Tabelle 12: Kriterien „Übermittlung von Identitätsdaten“

10 Mechanismen

In diesem Abschnitt werden konkrete Mechanismen vorgestellt und anhand der in den vorigen Kapiteln dargestellten Kriterien in die Vertrauensniveaus einsortiert. In einigen Fällen kann keine abschließende Bewertung vorgenommen werden, da diese ggf. von Rahmenbedingungen im konkreten Einsatz des Mechanismus abhängt.

10.1 Elektronischer Identitätsnachweis

Der *elektronische Identitätsnachweis* wird durch das Personalausweisgesetz [PAuswG] für den Personalausweis, und analog durch das Aufenthaltsgesetz [AufenthG] für den Aufenthaltstitel, normiert. Beide sind zusammen als technisch einheitliches System realisiert. Die technische Ausgestaltung wird in [TR-03127] und den dort referenzierten Dokumenten spezifiziert.

Der elektronische Identitätsnachweis dient der sicheren gegenseitigen Authentisierung von Bürgern einerseits und elektronischen Dienstleistungen aus Wirtschaft und Verwaltung andererseits in Geschäftsprozessen im Internet. Der Anbieter eines Dienstes weist im ersten Schritt durch ein Berechtigungszertifikat seine Identität nach und die Tatsache, dass er zum Abfragen bestimmter Daten berechtigt ist. Im zweiten Schritt weist der Bürger elektronisch seine Identität gegenüber dem Dienstanbieter nach.

Im Rahmen des elektronischen Identitätsnachweises stehen die folgenden Identitätsattribute zur Verfügung:

- Vornamen, Familienname, ggf. Ordens- oder Künstlername sowie Doktorgrad; Geburtsname verfügbar in Ausweisen ausgegeben ab Q2/2012[12];
- Geburtstag und Geburtsort, bzw. Altersbestätigung, sofern nur das Überschreiten einer Altersgrenze sichergestellt werden muss;
- Anschrift, bzw. Wohnortbestätigung, sofern nicht die vollständige Adresse benötigt wird;
- Pseudonym (dienste- und kartenspezifische Kennung für den pseudonymen Zugang);
- Dokumententyp und ausgebender Staat;

Im Aufenthaltstitel stehen darüber hinaus die Staatsangehörigkeit und die aufenthaltsrechtlichen Nebenbestimmungen zur Verfügung.

Voraussetzung für die Nutzung des elektronischen Identitätsnachweises zur Identifizierung von natürlichen Personen in Geschäftsprozessen ist eine Berechtigung der Vergabestelle für Berechtigungszertifikate (VfB) im Bundesverwaltungsamt (BVA). Die Vergabestelle prüft die Identität des Dienstanbieters und legt fest, welche personen- und ausweisbezogenen Daten aus dem Personalausweis übermittelt werden dürfen. Welche Stelle konkret als Dienstanbieter i.S.d. §2 (3) [PAuswG] die Berechtigung bei der Vergabestelle beantragt, hängt davon ab, wer die datenschutzrechtliche Verantwortlichkeit für die Datennutzung trägt. Dies kann auch ein Dienstleister oder ein Zweckverband sein, dem die Aufgabe der Identifizierung der Bürger übertragen wurde und der einen gemeinsamen Zugang für mehrere Behörden betreibt.

Der elektronische Identitätsnachweis bietet die Identifizierung des Inhabers und des Dienstanbieters in einem Schritt. Aktuell bietet damit der elektronische Identitätsnachweis als einziges aufgeführtes System die sichere gegenseitige Identifizierung des Inhabers und Dienstanbieters in einem Schritt ohne zusätzliche Maßnahmen.

10.1.1 Identifizierung einer Person

Alle Funktionen der Identifizierung einer (natürlichen) Person werden vom elektronischen Identitätsnachweis umgesetzt.

12 Die Verfügbarkeit des Geburtsnamens für den elektronischen Identitätsnachweis wurde mit dem E-Government-Gesetz eingeführt.

- Authentizität/Integrität der übermittelten Identitätsattribute:

  Die Identitätsattribute werden im Antragsprozess der Ausweisbehörde erfasst und im Rahmen der Ausweisproduktion sicher und gegen Verfälschung gesichert im Chip des Ausweises gespeichert. Der Dienst prüft im Rahmen des elektronischen Identitätsnachweises kryptographisch die Echtheit des Chips und liest die Daten direkt über einen authentisierten, verschlüsselten und integritätsgesicherten Kanal aus dem Ausweis aus.

- Bindung der Identifizierung an den Sitzungskontext:

  Bei Nutzung eines eID-Clienten nach [TR-03124] wird die Identifizierung der Person an die Sitzung zwischen Web-Browser und Dienst geknüpft („Kanalbindung“).

- Vertraulichkeit der übermittelten Identitätsattribute:

  Die Identitätsattribute werden in einem Ende-zu-Ende authentisierten und verschlüsselten Kanal direkt vom Ausweischip zum identifizierten Dienstanbieter übertragen.

- Bindung der übermittelten Identitätsattribute an die berechtigte Person:

  Ein Auslesen der Identitätsattribute setzt die Eingabe der nur dem Ausweisinhaber bekannten geheimen PIN voraus.

- Datensparsame Übermittlung von Identitätsattributen und Flüchtigkeit der Identifizierung:

  Die maximal zu übermittelnden Attribute werden durch die VfB festgelegt und können durch den Ausweisinhaber beliebig weiter eingeschränkt werden. Der elektronische Identitätsnachweis ist so gestaltet, dass die Authentizität der Identitätsattribute im Augenblick der Identifizierung durch den Dienst überprüft werden kann, Dritten gegenüber aber nicht nachgewiesen werden kann.

10.1.2 Identifizierung eines Dienstanbieters

Alle Funktionen der Identifizierung eines Dienstanbieters werden vom elektronischen Identitätsnachweis umgesetzt.

- Authentizität/Integrität der übermittelten Identität des Dienstes:

  Die Identität des Dienstes wird durch die Vergabestelle für Berechtigungszertifikate überprüft und in den Berechtigungszertifikaten kryptographisch gesichert gespeichert. Das Berechtigungszertifikat – und damit die Authentizität/Integrität der Identität des Dienstes – wird durch den Ausweischip überprüft.

- An Identifizierung des Dienstes gebundene sichere Verbindung:

  Bei Nutzung eines eID-Clienten nach [TR-03124] wird die Identifizierung des Dienstes an die Verbindung zwischen Web-Browser und Dienst geknüpft („Kanalbindung“).

10.1.3 Abgabe einer Willenserklärung

Nach § 3 a [VwVfG] kann im Verwaltungshandeln eine schriftformersetzende Abgabe einer Willenserklärung über ein elektronisches Formular, das von der Behörde zur Verfügung gestellt wird, durchgeführt werden, sofern der Erklärende durch den elektronischen Identitätsnachweis identifiziert wird:

§3a Satz 4 VwVfG

Die Schriftform kann auch ersetzt werden

1. durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;

2. - 4. [...]

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.

Die Kombination eines Formulars mit dem elektronischen Identitätsnachweis zur Abgabe einer Erklärung kann mit der klassischen Abgabe einer Willenserklärung zur Niederschrift/durch persönliches Erscheinen verglichen werden, bei der ein Behördenmitarbeiter den Erklärenden identifiziert und die Erklärung aufnimmt. Eine Unterschrift durch den Erklärenden ist hierbei nicht notwendig. Der Einsatz von elektronischen Formularen in Verbindung mit dem elektronischen Identitätsnachweis zum Schriftformersatz ist in Teil 2 dieser Richtlinie beschrieben ([TR-03107-2]).

Die elektronische Identität des Personalausweises/Aufenthaltstitels in Verbindung mit sicherem Verwaltungshandeln erfüllt die angegebenen Funktionen unter folgenden Bedingungen (zitiert aus [BRSchriftform], Details siehe dort):

Der elektronische Identitätsnachweis ermöglicht entsprechend seinem primären Verwendungszweck insbesondere eine Abbildung der Identitätsfunktion der Schriftform. Durch die Eingabe der eID-PIN, ggf. verbunden mit einem Hinweis auf die bevorstehende Transaktion, kann auch die Warnfunktion abgedeckt werden. [...]

Eine Abbildung der verbleibenden Funktionen der Schriftform (Abschluss-, Perpetuierungs-, Echtheits-, Verifikations- und Beweisfunktion der Schriftform) kann – sofern erforderlich – für den Bereich der Kommunikation mit staatlichen Stellen durch technisch-organisatorische Maßnahmen innerhalb der beteiligten staatlichen Stelle unter Wahrung angemessener Sicherheitsanforderungen umgesetzt werden.

Sofern Abschluss-, Perpetuierungs-, Echtheits-, Verifikations- und Beweisfunktion für den Geschäftsprozess notwendig sind, so können sie zum Beispiel durch eine gesicherte Übertragung vom Bürger zur Behörde in Verbindung mit anschließender kryptographischer Signatur der Vorgangsdaten durch die Behörden oder Speicherung in einem vertrauenswürdigen IT-System der Behörde abgebildet werden (zu Details siehe [TR-03107-2].

10.1.4 Dokumentenübermittlung

Der elektronische Identitätsnachweis kann die sichere Dokumentenübermittlung zwischen einer Person und einem Dienstanbieter unterstützen. Basierend auf einer TLS-Verbindung wird mit dem elektronischen Identitätsnachweis eine sichere Identifizierung der Person und des Dienstanbieters durchgeführt. Diese Identifizierungen werden bei Nutzung eines eID-Clienten nach [TR-03124] an die TLS-Verbindung gebunden („Kanalbindung“).

Die so unabhängig von den genutzten TLS-Zertifikaten authentisierte Verbindung kann zur sicheren Übermittlung von Dokumenten genutzt werden, vgl. auch Abschnitt 10.6.

10.1.5 Vertrauensniveau

Die Verwendung des elektronischen Identitätsnachweises stellt die Identifizierung einer Person und eines Dienstanbieters auf Vertrauensniveau *hoch* sicher.

Für das Vertrauensniveau einer Willenserklärung ist neben der (beidseitigen) Identifizierung auch der auf hohem Vertrauensniveau authentisierte Sitzungskontext wesentlich (siehe [TR-03107-2]). Das Vertrauensniveau des Gesamtverfahrens hängt von der Umsetzung der weiteren Funktionen – soweit jeweils notwendig – durch den Dienstanbieter ab.

10.1.5.1 Erfüllung von Formerfordernissen

Der elektronische Identitätsnachweis erfüllt die Anforderung einer behördlichen Identitätsprüfung des Ausweisinhabers und ist damit geeignet, für die Identifizierung besondere Formvorschriften zu erfüllen.

Werden die Anforderungen nach [TR-03107-2] erfüllt, so erfüllt der elektronische Identitätsnachweis in Verbindung mit einem Formularserver die Formvorschrift des Schriftformersatzes nach §3a [VwVfG].

10.2 Kryptographische Token

Kryptographische Token können auf verschiedene Weise für die elektronische Identifizierung oder Vertrauensdienste Verfahren eingesetzt werden. Grundsätzlich unterschieden werden muss einerseits die Verwendung eines Tokens zur Authentisierung gegenüber einem Identity Provider/Vertrauensdienst (siehe Abschnitt 4.2).

Andererseits können Identitätsattribute in einem zu dem im Token gespeicherten Schlüssel gehörigen Zertifikat enthalten sein, und das Token unmittelbar zur Identifizierung/Signaturerzeugung eingesetzt werden. Abhängig davon, ob das Token einer natürlichen oder juristischen Person zugeordnet ist, enthält dabei das Zertifikat die Identität einer natürlichen oder juristischen Person. Darüber hinaus besteht die Möglichkeit, einem Zertifikat einer natürlichen Person weitere Zertifikate zuzuordnen, die zum Beispiel die Rolle einer natürlichen Person als Vertreter einer juristischen Person beschreiben (Attributzertifikate).

10.2.1 Identifizierung einer Person

Kryptographische Token erfüllen die Funktionen der Identifizierung einer Person wie folgt:

- Authentizität/Integrität der übermittelten Identitätsattribute:

  Für im Zertifikat gespeicherte Identitätsattribute ist die Authentizität/Integrität der Attribute durch die Signatur des Zertifikates kryptographisch gesichert. Bei einem Identity Provider gespeicherte Attribute werden nicht vom Tokeninhaber aus übermittelt, sondern vom Identity Provider zum Dienstanbieter. Die Authentizität/Integrität wird durch die Einhaltung von Abschnitt 3.6.2 sichergestellt.

- Bindung der Identifizierung an den Sitzungskontext:

  Abhängig von der konkreten eingesetzten Technik.

- Vertraulichkeit der übermittelten Identitätsattribute:

  Die üblichen auf kryptographischen Token basierenden Systeme übermitteln die Identitätsattribute nicht verschlüsselt. Für die Vertraulichkeit ist der vorherige Aufbau einer gesicherten Verbindung zwischen Dienst und Person einschließlich der Dienstanbieteridentifizierung auf entsprechendem Vertrauensniveau notwendig, zum Beispiel per TLS (siehe Abschnitt 10.6). Daher kann für diese Funktion nur das Vertrauensniveau der TLS-Verbindung erreicht werden.

- Bindung der übermittelten Identitätsattribute an die berechtigte Person:

  Hardware-basierte Token: Die Bindung der übermittelten Identitätsattribute/der Authentisierung an die berechtigte Person erfolgt je nach konkretem System über den Besitz des Tokens bzw. zusätzlich über die Sicherung des Tokens mittels einer geheimen PIN.

  Software-basierte Token: Die Bindung der übermittelten Identitätsattribute/der Authentisierung an die berechtigte Person erfolgt über einen üblicherweise passwortbasierten Zugriffsschutz auf den privaten Schlüssel. Der Zugriffsschutz kann entweder durch das Betriebssystem erzwungen werden („Access Control“), oder das Passwort dient der Entschlüsselung des verschlüsselt gespeicherten privaten Schlüssels.

- Datensparsame Übermittlung von Identitätsattributen und Flüchtigkeit der Identifizierung:

Die meisten verfügbaren zertifikatsbasierten kryptographischen Token bieten keine Mechanismen zur Datensparsamkeit analog der Mechanismen des elektronischen Identitätsnachweises des Personalausweises, sondern bieten lediglich ein Zertifikat, das alle relevanten Identitätsdaten statisch enthält. Diese Token können daher nur für geschlossene Systeme/Systemverbünde eingesetzt werden, in denen immer der gleiche Satz von Identitätsattributen für eine Identifizierung benötigt wird, d.h. die Möglichkeit zur selektiven Übermittlung einzelner Attribute nicht erforderlich ist.

Bei der Nutzung eines Identity Providers sind diesem alle Attribute bekannt. Datensparsame Übermittlung an den Dienstanbieter liegt in der Verantwortung des Identity Providers.

10.2.2 Abgabe einer Willenserklärung

Die Nutzung von kryptographischen Token zur Absicherung der Abgabe einer Willenserklärung (elektronischen Signaturen) ist in der eIDAS-Verordnung [eIDAS] reguliert. Die Verordnung definiert zwei verschiedene Formen der elektronischen Signatur:

- *Fortgeschrittene elektronische Signaturen* sind elektronische Signaturen, die
  1. ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
  2. die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
  3. mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
  4. mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

  Im Allgemeinen werden fortgeschrittene elektronische Signaturen technisch durch asymmetrische kryptographische Signaturen umgesetzt. Dabei muss der private Schlüssel unter alleiniger Kontrolle des Inhabers sein. Zu unterscheiden ist dabei die Speicherung des privaten Schlüssels im Computersystem des Inhabers (Softwaretoken) oder in einem dedizierten, sicheren Hardwaretoken.
- *Qualifizierte elektronische Signaturen* sind fortgeschrittene elektronische Signaturen, die zusätzlich
  1. auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
  2. mit einer sicheren Signaturerstellungseinheit (d.h. mit einem die Anforderungen der eIDAS-Verordnung erfüllendes Hardwaretoken) erzeugt werden.

Fortgeschrittene/qualifizierte elektronische Signaturen sind grundsätzlich geeignet, die Funktionen für die Abgabe einer Willenserklärung zu erfüllen:

- Die Echtheits- und die Abschlussfunktion werden durch die Erzeugung einer kryptographischen Signatur über das gesamte Dokument abgebildet. Das nachträgliche Hinzufügen oder Verändern von Daten ist nicht möglich, ohne dass die Signatur ihre Gültigkeit verliert.
- Die Identifizierungs- und Verifikationsfunktion wird durch das dem Schlüssel zugeordnete Zertifikat abgebildet, welches eine Identität des Schlüsselinhabers enthält. Über die Signatur wird einem signierten Dokument das zugehörige Zertifikat eindeutig zugeordnet.
- Die Warnfunktion wird durch das Auslösen der Signaturerzeugung durch den Schlüsselinhaber abgebildet. Automatisch erzeugte Signaturen erfüllen die Anforderungen der Warnfunktion nicht.
- Die Beweis- und die Perpetuierungsfunktion werden durch die kryptographische Prüfbarkeit der Signatur abgebildet. Sofern eine langfristige Beweiswerterhaltung/Perpetuierung über den Vorhersagezeitraum für geeignete kryptographische Algorithmen und Schlüssellängen hinaus notwendig ist, so ist der Beweiswert durch Mechanismen nach [TR-03125] zu erhalten.

10.2.3 Vertrauensniveau

Für eine Einordnung kryptographischer Token siehe Abschnitt 4.2.

Für eine Bewertung der Nutzung kryptographischer Token in einem Gesamtsystem ist dieses als ganzes zu betrachten. Insbesondere hängt das Vertrauensniveau des Gesamtsystems von der Integration des Tokens in das System ab, etwa die Registrierung der Token bzw. das Enrolment der im Zertifikat enthaltenen Attribute.

10.2.3.1 Erfüllung von Formerfordernissen

Die qualifizierte elektronische Signatur wird durch die eIDAS-Verordnung der Unterschrift und nach [VwVfG] §3a der klassischen Schriftform gleichgestellt und erfüllt damit die Formerfordernis des Schriftformersatzes.

10.3 TAN-Verfahren

TAN-Verfahren (vgl. auch Abschnitt 4.3) sind immer an ein Nutzerkonto gebunden. Um ein bestimmtes Vertrauensniveau zu erreichen, muss auch das Anlegen des Nutzerkontos mindestens auf diesem Niveau erfolgen. Durch die Vielzahl verschiedener TAN-Verfahren kann eine abschließende Einordnung der Verfahren nicht vorgenommen werden.

10.3.1 Identifizierung einer Person

TAN-Verfahren können in Verbindung mit einer Identitätsdatenbank (Identity Provider) zur Identifizierung von Personen eingesetzt werden. Dabei wird das TAN-Verfahren zur Authentisierung des Nutzers gegenüber der Identitätsdatenbank genutzt, welche dann die eigentlichen Identitätsattribute an den Dienstanbieter weiterleitet.

Da das TAN-Verfahren selbst nur die Authentisierung des Nutzers leistet, müssen die speziellen Funktionen der Identifizierung einer Person durch die Identitätsdatenbank bzw. den von dort ausgehenden Prozess der Identitätsdatenübermittlung an den Dienstanbieter geleistet werden.

Da das TAN-Verfahren selbst keine Identitätsdaten umfasst, ist eine Erstregistrierung über TAN-basierte Verfahren nur in Verbindung mit einer Identitätsdatenbank möglich. In diesem Fall sind die weiteren Komponenten, z.B. die Identitätsdatenbank, die dortige Registrierung und die Kommunikationskanäle Teil des Systems und müssen bei der Bewertung mit betrachtet werden.

10.3.2 Abgabe einer Willenserklärung

Die Nutzung von TAN-Verfahren kann die folgenden Funktionen abdecken:

- Die Warnfunktion wird durch die Eingabe der TAN durch den Bürger abgedeckt.
- Die Identifizierungsfunktion wird durch die Zuordnung der TAN-Liste/des Mobiltelefons/des TAN-Generators zu einer bestimmten Person erfüllt. Das Vertrauensniveau *substantiell* kann nur erreicht werden, wenn geeignete Mechanismen gegen brute-force-Angriffe auf die TAN (etwa Fehlbedienungszähler) eingesetzt werden. Die Maßgaben aus Abschnitt 3.3 gelten entsprechend.
- Die Echtheits- und die Abschlussfunktion können für die Daten abgebildet werden, die in die Erzeugung der TAN eingehen. Aufgrund der geringen Entropie der TAN (typischerweise sechs Ziffern) kann für diese Funktion ohne weitere Maßnahmen/typischerweise nur Vertrauensniveau *normal* erreicht werden.

Sofern für den Geschäftsprozess notwendig, müssen die weiteren Funktionen durch zusätzliche Maßnahmen abgedeckt werden.

10.3.3 Vertrauensniveau

Das Vertrauensniveau eines TAN-basierten Mechnanismus hängt wesentlich von der Einbettung der TAN-Verfahrens in das Gesamtsystem ab und muss daher im Einzelfall betrachtet werden. Für eine Betrachtung des TAN-Verfahrens selbst siehe Abschnitt 4.3.

10.4 Nutzername/Passwort

Für die Anmeldung, also die Authentifizierung bereits registrierter Personen ist noch oft ein Nutzername/Passwort-basierter Ansatz üblich. Eine Erstregistrierung ist mit diesem Mechanismus nicht möglich. Grundsätzlich sollte auf Kryptographie beruhenden Verfahren Vorzug vor rein Passwort-basierten Verfahren gegeben werden.

Es sind die Anforderungen aus Maßnahme M 2.11 „Regelung des Passwortgebrauchs“ der IT-Grundschutz-Kataloge des BSI (siehe [BSI-GS]) einzuhalten.

10.4.1 Identifizierung einer Person

Die Funktionen der Identifizierung einer Person werden wie folgt abgedeckt:

- Authentizität/Integrität der übermittelten Identitätsattribute:

  Der Nutzername ist das einzige übermittelte Identitätsattribut. Um die Authentizität/Integrität/Vertraulichkeit des Identitätsattributes während der Übermittlung zu schützen, muss vor Übermittlung eine sichere Verbindung mit einem geeigneten Mechanismus etabliert werden.

- Bindung der Identifizierung an den Sitzungskontext:

  Das Passwort selbst bindet die Identifizierung i.A. nicht an den Sitzungskontext, dies muss durch das Gesamtverfahren gewährleistet werden.

- Vertraulichkeit der übermittelten Identitätsattribute:

  Bei einem Passwort-basierten Verfahren werden üblicherweise keine Identitätsattribute vom Inhaber zur vertrauenden Entität übermittelt, sondern vom Identity Provider zur vertrauenden Entität. Hier gelten die Anforderungen aus Abschnitt 3.6.

- Bindung der übermittelten Identitätsattribute an die berechtigte Person:

  Die Bindung der übermittelten Identitätsattribute an die berechtigte Person erfolgt über das (geheime) Passwort.

- Datensparsame Übermittlung von Identitätsattributen und Flüchtigkeit der Identifizierung:

  Als einziges Identitätsattribut wird der Nutzername übermittelt, der im Sinne des Anwendungszwecks minimal ist. Da keine kryptographischen Mechanismen genutzt werden, ist die Identifizierung flüchtig.

10.4.2 Abgabe einer Willenserklärung

Basierend auf der Identifizierung einer Person per Nutzername/Passwort und einer sicheren Verbindung zwischen Person und Dienstanbieter kann die Abgabe einer Willenserklärung auf Vertrauensniveau *normal* durch eine einfache Nutzerinteraktion, zum Beispiel das Anklicken einer entsprechend beschrifteten Schaltfläche erfolgen. In der Kombination werden dann die Identifizierungsfunktion und die Warnfunktion auf Vertrauensniveau *normal* abgedeckt.

Sofern für den Geschäftsprozess notwendig, müssen die weiteren Funktionen durch zusätzliche Maßnahmen abgedeckt werden.

10.4.3 Vertrauensniveau

Mit diesem Mechanismus kann nur das Vertrauensniveau *normal* erreicht werden.

10.5 De-Mail

Die Konzeption von De-Mail ermöglicht einen authentischen, vertraulichen und verbindlichen Austausch von Nachrichten und Dokumenten über das Internet. Diese Eigenschaften von De-Mail werden u. a. durch folgende gesetzlich in [De-Mail-G] vorgeschriebene Rahmenbedingungen für den Betrieb sichergestellt:

Als ein geschlossenes System darf De-Mail nur von akkreditierten De-Mail-Diensteanbietern (DMDA) betrieben und den potentiellen Nutzern zur Verfügung gestellt werden.

Der Versand und Empfang von De-Mails wiederum ist nur von zuvor seitens des jeweiligen DMDAs eindeutig identifizierten Nutzern möglich.

Die Übertragung erfolgt über verschlüsselte Kanäle. Im Rahmen der InterDMDA-Übertragung kommt zusätzlich eine Inhaltsverschlüsselung zum Einsatz.

Der Accountzugang/Anmeldung ist auf Basis von zwei unterschiedlichen Authentisierungsniveaus möglich.

- Zum einen kann mittels der Kombination Nutzername/Passwort ein Zugang mit dem Authentisierungsniveau *normal* realisiert werden. Der Funktionsumfang ist hier im Vergleich zum Authentisierungsniveau *hoch* eingeschränkt.
- Zum Anderen steht unter zusätzlicher Verwendung eines Tokens (Besitz und Wissen) das Authentisierungsniveau *hoch* in Verbindung mit einem vollen Funktionsumfang zur Verfügung (und damit Vertrauensniveau *hoch*).

10.5.1 Dokumentenübermittlung

Die Funktionen werden wie folgt abgedeckt:

- Vertraulichkeit und Integrität des Dokumentes:

  Die Absicherung erfolgt durch TLS-Verschlüsselung und teilweise (InterDMDA) zusätzlicher S/MIME-Verschlüsselung.

  In einigen Fachgesetzen (zum Beispiel §67 (6) SGB X in Bezug auf Sozialdaten, §87a (1) AO) wird normiert, dass diese Absicherung in Verbindung mit den durch [De-Mail-G] festgelegten Maßnahmen für die Übermittlung entsprechender Fachdaten geeignet ist.

  Im Allgemeinen ist zu beachten, dass beim Versand von Dokumenten mit besonders sensitiven Daten (§3 (9) BDSG) gegebenenfalls zusätzliche eine Ende-zu-Ende-Verschlüsselung notwendig ist. Dies bedingt eine Ver- und Entschlüsselung durch die Kommunikationspartner selbst, d.h. setzt entsprechende Systeme der Kommunikationspartner voraus. Dies wird durch die De-Mail-Infrastruktur unterstützt. Die Verabredung der konkreten Mechanismen zur Verschlüsselung obliegt den Kommunikationspartnern, dabei müssen die Anforderungen aus [TR-03116], Teil 4, eingehalten werden.

- Identifizierung des Senders und des Empfängers

  Erst-Identifizierung des Empfängers gemäß Abschnitt 5 durch den DMDA gemäß der Vorgaben aus [De-Mail-G] und [TR-01201]. Die Erst-Identifizierung erfolgt anhand gültiger Ausweisdokumente (zum Beispiel Personalausweis) oder gleichwertiger Verfahren. Auf elektronischem Wege kann der elektronische Identitätsnachweis genutzt werden, damit wird Vertrauensniveau *hoch* erreicht.

  Die jeweilige Authentisierung vor einem Nutzungsvorgang (Senden und Empfangen von De-Mails) ist möglich auf Basis zwei verschiedener Authentisierungsniveaus:

- Authentisierungsniveau *normal* durch Nutzername/Passwort mit daraus resultierender Einschränkung in der Funktionalität des Accounts hinsichtlich der nachfolgenden Nutzung (zum Beispiel keine Nutzung der Versandoption „persönlich“ und „absenderbestätigt“ beim Versand von De-Mails und keine Lesemöglichkeit von mit der Versandoption „persönlich“ ins Postfach eingegangenen De-Mails)
- Authentisierungsniveau *hoch* durch zusätzliche Nutzung eines Tokens (zum Beispiel elektronischer Identitätsnachweis) mit daraus resultierender vollständiger Funktionalität des Accounts.

10.5.2 Abgabe einer Willenserklärung

Nach § 3 a [VwVfG] kann eine schriftformersetzende Abgabe einer Willenserklärung durch eine De-Mail durchgeführt werden, sofern der Erklärende durch die Nutzung der Option „absenderbestätigt“ nach §5 (5) [De-Mail-G] identifiziert wird:

§3a Satz 4 VwVfG

Die Schriftform kann auch ersetzt werden

1. [...]

2. bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;

3. bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;

4.[...]

De-Mail erfüllt die angegebenen Funktionen und den im Verwaltungsverfahrensgesetz (s.o.) angegebenen Bedingungen.

Die Option „absenderbestätigt“ nach §5 (5) [De-Mail-G] steht nur zur Verfügung, wenn sich der Kontoinhaber mit „sicherer Anmeldung“ nach §4 (1) Satz 2 an seinem De-Mail-Konto angemeldet hat.

10.5.3 Übermittlung von Identitätsdaten

Der Identitätsbestätigungsdienst nach [De-Mail-G] §6 nutzt die De-Mail-Infrastruktur zur Übermittlung von Identitätsdaten. Als Identitätsprovider fungiert hierbei der De-Mail-Diensteanbieter, der das Konto des Dateninhabers führt.

Die Funktionen werden durch die entsprechenden Funktionen der De-Mail-Infrastruktur abgedeckt, siehe Abschnitt 10.5.1. Die zu erfüllenden Anforderungen zur Erreichung eines Vertrauensniveaus gelten entsprechend.

10.5.4 Vertrauensniveau

Für per [De-Mail-G] und [TR-01201] konformen De-Mail-Diensten übermittelte Nachrichten/Dokumente gilt, in Abhängigkeit vom Authentisierungsniveau des Senders zum Zeitpunkt des Versands, das Vertrauensniveau *normal* bzw. *hoch*.

Der Identitätsbestätigungsdienst steht nur bei „sicherer Anmeldung“ zur Verfügung. Daher gilt für per [De-Mail-G] und [TR-01201] konformen De-Mail-Diensten übermittelte Identitätsdaten das Vertrauensniveau

hoch für die Funktionen Integritätssicherung, Identifizierung des Dateninhabers, Speicherung und Anmeldung am Konto. Das Vertrauensniveau der weiteren Funktionen ist abhängig vom Vertrauensniveau der Empfängeridentifizierung.

10.5.4.1 Erfüllung von Formerfordernissen

Bei Nutzung der Option „Abholbestätigung“ nach §5 (9) [De-Mail-G] kann über De-Mail eine förmliche Zustellung von Dokumenten durchgeführt werden. Diese Option steht nur bei Nutzung der „sicheren Anmeldung“ zur Verfügung. Ebenso erfüllen bei Nutzung der „sicheren Anmeldung“ übermittelte Dokumente die Formanforderung des Schriftformersatzes nach §3a [VwVfG].

10.6 TLS-Verbindung und -Zertifikate

Der übliche Mechanismus im Internet, um eine sichere Verbindung zu einem Dienst aufzubauen, und damit verbunden eine Identifizierung des Dienstes durchzuführen, ist der Aufbau einer TLS-Verbindung (*Transport Layer Security*) mit zertifikatsbasierter Identifizierung des Dienstes bzw. der Domäne (Hostname), unter der der Dienst angeboten wird.

Diese Richtlinie geht bei der Bewertung vom Einsatz von TLS gemäß den Anforderungen in [TR-03116], Teil 4, aus, d.h. insbesondere vom Einsatz geeigneter Versionen des Protokolls und geeigneter Cipher Suites.

Um TLS zu verwenden, ist auf Dienstseite ein entsprechendes Zertifikat notwendig, mit welchem sich der Dienst bzw. die Domäne gegenüber dem Bürger identifiziert. Im World Wide Web, d.h. außerhalb geschlossener Systeme, beruhen die Zertifikate auf der „Internet-PKI“ nach [RFC5280]. Damit der Bürger diesem Zertifikat trauen kann, muss es von einer Zertifizierungsstelle ausgestellt werden, die in den gängigen Browsern als vertrauenswürdig eingestuft ist. Das Protokoll etabliert dann eine Ende-zu-Ende-Verbindung zwischen dem identifizierten Dienst und dem Browser, d.h. dem Bürger.

Grundsätzlich werden bei TLS-Zertifikaten verschiedene Typen unterschieden, die sich hauptsächlich durch die Tiefe der Verifizierung der Authentizität und der Autorisierung eines Antragstellers für ein Zertifikat für eine spezifische Domäne unterscheiden:

- *Domain Validation* (DV): Es wird lediglich überprüft, ob der Antragsteller für ein Zertifikat in der Lage ist, E-Mails, die an die Domäne gesendet werden, zu empfangen. Es finden keine weiteren Überprüfungen bzgl. des Dienstes oder der Autorisierung des Antragstellers statt. Das Verfahren bietet keine Sicherheit gegen Man-in-the-middle-Angriffe. DV-Zertifikate sollten für E-Government-Anwendungen nicht eingesetzt werden.
- *Organisation Validation* (OV): Es wird geprüft, dass der Antragsteller berechtigt ist, die Domäne zu nutzen. Darüber hinaus wird eine eingeschränkte Überprüfung der Existenz des Dienstanbieters durchgeführt.
- *Extended Validation* (EV): Hier wird zusätzlich explizit eine Identitätsprüfung des Dienstanbieters anhand von amtlichen Registern durchgeführt. Darüber hinaus wird die Autorisierung des Antragstellers für den Antragsprozess geprüft. Die Domäne muss unter alleiniger Kontrolle des Dienstanbieters stehen.
- Die eIDAS-Verordnung führt darüber hinaus die *Qualifizierten Webseitenzertifikate* als Spezialfall der Extended Validation-Zertifikate ein.

Die genauen Prozesse sind abhängig von der Zertifizierungsstelle.

10.6.1 Identifizierung eines Dienstanbieters

Alle Funktionen der Identifizierung eines Dienstanbieters werden umgesetzt:

- Authentizität/Integrität der übermittelten Identität des Dienstes:

Die Identität des Dienstes wird als Bestandteil des TLS-Zertifikates kryptographisch gesichert. Der Nachweis der Zugehörigkeit des Zertifikates zum Dienst erfolgt über den Nachweis des zugehörigen privaten Schlüssels im Zuge des Aufbaus der TLS-Verbindung.

- An Identifizierung des Dienstes gebundene sichere Verbindung:

  Durch eine kryptographische Schlüsseleinigung (TLS-Handshake) wird eine sichere Verbindung aufgebaut. Die Identität des Dienstes geht in Form des Zertifikates bzw. des zugehörigen Schlüssels in den Verbindungsaufbau ein.

10.6.2 Übermittlung eines Dokumentes

Bei der Übertragung eines Dokumentes per browserbasierten Web-Up- und Download wird zunächst eine sichere Verbindung (TLS-Verbindung) zwischen Person und Dienst aufgebaut. Sofern für den Geschäftsprozess notwendig, kann zusätzlich die Person über ein entsprechendes Verfahren nach Abschnitt 5 identifiziert werden. Wird der elektronische Identitätsnachweis zur Identifizierung (Abschnitt 10.1) genutzt, erfolgen beide Identifizierungsschritte als Teil eines Prozesses.

Das Dokument wird nun innerhalb der aufgebauten Verbindung übertragen, als Upload von der Person zum Dienstanbieter oder umgekehrt als Download vom Dienstanbieter zur Person.

Innerhalb des Dienstes wird das übertragene Dokument entweder zur Abholung durch ein Fachverfahren bzw. eine berechtigte Person innerhalb einer Behörde bereitgehalten oder an diese übermittelt. Hierfür gelten die Abschnitte 8.1 und 8.2 entsprechend, wobei Kriterien auch durch organisatorische Maßnahmen der Behörde bzw. im Rahmen des behördlichen Sicherheitskonzeptes abgedeckt werden können.

Die Funktionen werden wie folgt abgedeckt:

- Vertraulichkeit und Integrität des Dokumentes:

  Absicherung durch die TLS-Verbindung.

- Identifizierung des Senders und des Empfängers:

  Die Identifizierung des Dienstanbieters erfolgt durch das TLS-Zertifikat, d.h. das Vertrauensniveau der Dienstanbieteridentifizierung hängt von der Art des TLS-Zertifikat ab. Sofern der elektronische Identitätsnachweis genutzt wird, wird der Dienstanbieter über diesen identifiziert, d. h. die Identifizierung erfolgt auf dem Vertrauensniveau *hoch*, unabhängig von der Art des verwendeten TLS-Zertifikates.

  Die Identifizierung der Person muss – sofern anwendungsbezogen notwendig – durch eine zusätzliche Identifizierung nach Abschnitt 5 erfolgen.

Im Fall der Übermittlung von Dokumenten mit besonders sensiblen personenbezogenen Daten zu einem Dienstanbieter sind ggf. weitere Maßnahmen zur Sicherstellung der Identität des endgültigen Empfängers (Organisationseinheit beim Dienstanbieter, Mitarbeiter) zu treffen.

10.6.3 Vertrauensniveau

Um eine für Vertrauensniveau *substantiell* hinreichend sichere Identitätsprüfung der Dienstanbieters sicherzustellen, müssen Extended Validation-Zertifikate vertrauenswürdiger Zertifizierungsstellen eingesetzt werden; empfohlen wird der Einsatz von qualifizierten Webseitenzertifikaten, ausgestellt von nach [TR-03145] zertifizierten TLS-Zertifizierungsstellen. Dabei muss sichergestellt werden, dass der Bürger tatsächlich überprüft, dass ihm für den Verbindungsaufbau ein Extended Validation-Zertifikat/qualifiziertes Webseitenzertifikat angeboten wird. Dies kann zum Beispiel durch Überprüfung der Adressleiste des Browsers geschehen.

Weltweit gibt es zahlreiche Zertifizierungsstellen für TLS-Zertifikate, die jeweils für alle Webseiten TLS-Zertifikate ausstellen können. Wird eine Zertifizierungsstelle kompromittiert, sind damit grundsätzlich alle Webseiten gefährdet, nicht nur die Webseiten, die ein legitimes Zertifikat dieser Zertifizierungsstelle nutzen. Ef-

fektiv kann eine kompromittierte Zertifizierungsstelle Identifizierungsmittel einer anderen Stelle duplizieren. In der Vergangenheit wurden TLS-Zertifizierungsstellen wiederholt kompromittiert. Daher kann das Vertrauensniveau *hoch* für die Dienstidentifizierung mittels TLS-Zertifikat – unabhängig vom Vertrauensniveau des Zertifikates, das durch den Dienst selbst genutzt wird – nicht erreicht werden.

Wird eine TLS-Verbindung mittels der Kanalbindung des elektronischen Identitätsnachweises authentisiert (siehe Abschnitt 10.1), so ist das Vertrauensniveau der Verbindung unabhängig vom TLS-Zertifikat, da die Identifizierung des Dienstes über den Enrolment-Prozess der Vergabestelle für Berechtigungszertifikate erfolgt.

Voraussetzung für die Nutzung von TLS-Verbindungen als sichere Verbindung und TLS-Zertifikaten für die Identifizierung von Diensten ist die Einhaltung der Anforderungen in [TR-03116], Teil 4.

Im Rahmen der Nutzung zur Dokumentenübermittlung sind für die Identifizierung der Person die Kriterien des Abschnittes 5 maßgeblich.

10.7 E-Mail mit S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) ist ein IETF-Standard (siehe [RFC5750], [RFC5751]) zur kryptographischen Absicherung von E-Mails und Dateien. Mit S/MIME können Nachrichten kryptographisch signiert bzw. verschlüsselt werden. Technisch werden die Verschlüsselung durch hybride und die Signatur durch asymmetrische Kryptographie umgesetzt. Hierzu stellt S/MIME entsprechende kryptographische Verfahren und Nachrichtenformate (basierend auf dem CMS-Standard [RFC5652]) zur Verfügung.

Die Authentifizierung der Kommunikationspartner erfolgt bei S/MIME über X.509-Zertifikate. Diese müssen von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt werden, um Vertrauen der Kommunikationspartner in die Zertifikate sicherzustellen. Meist werden die gleichen PKI-Strukturen genutzt wie für die Ausstellung von TLS-Zertifikaten (vgl. Abschnitt 10.6).

10.7.1 Dokumentenübermittlung

Bei der Nutzung von E-Mails mit S/MIME werden die notwendigen Funktionen der sicheren Dokumentenübermittlung wie folgt abgedeckt.

- Vertraulichkeit und Integrität des Dokumentes:

  Die Vertraulichkeit wird durch die S/MIME-Verschlüsselung des übermittelten Dokumentes abgebildet. Nur der Schlüsselinhaber kann das übermittelte verschlüsselte Dokument wieder entschlüsseln.

  Die Sicherung der Integrität des Dokumentes erfolgt via Signatur über das gesamte übermittelte Dokument. Eine nachträgliche Veränderung des jeweiligen Dokumentes ist daher nicht möglich, ohne dass die Signatur ihre Gültigkeit verliert.

- Identifizierung des Empfängers:

  Für die Identifizierung des Empfängers wird das einem (Verschlüsselungs-)Schlüssel zugeordnete Zertifikat genutzt, welches die Identität des jeweiligen Schlüsselinhabers bescheinigt. Das Vertrauensniveau der Identifizierung ist abhängig vom X.509-Zertifikat des Empfängers, d. h. von der Vertrauenswürdigkeit der Zertifizierungsstelle und der Qualität des Enrolments.

- Identifizierung des Senders:

  Die Identifizierung des Senders erfolgt über das einem (Signatur-)Schlüssel zugeordnete Zertifikat, welches die Identität des jeweiligen Schlüsselinhabers bescheinigt. Das Vertrauensniveau der Identifizierung ist abhängig vom X.509-Zertifikat des Senders (siehe oben). Da die Integritätssicherung bei der Dokumentenübermittlung via S/MIME per Signatur erfolgt, ist eine Identifizierung des Senders verpflichtend.

10.7.2 Vertrauensniveau

Mit einer Dokumentenübermittlung per E-Mail mit S/MIME kann bei der Verwendung der Internet-PKI (vgl. Abschnitt 10.6) für die Sender-/Empfängeridentifizierung nur das Vertrauensniveau *normal* erreicht werden, da i.A. keine hinreichende Prüfung der Identität des Inhabers für ein höheres Vertrauensniveau erfolgt. Bei Verwendung einer dedizierten PKI und Ausschluss der Internet-PKI kann ggf. auch ein höheres Vertrauensniveau erreicht werden.

Die in [TR-03116], Teil 4 spezifizierten kryptographischen Anforderungen für die Verwendung von S/MIME müssen eingehalten werden. Für die Identifizierung von Empfänger und Sender sind die Vorgaben aus den Abschnitt 5 bzw. 6 sowie [TR-03116], Teil 4 maßgeblich.

10.8 OSCI-Transport

Der Standard OSCI-Transport ist ein Protokoll, welches von vielen XML-Standards der öffentlichen Verwaltung (zumeist XÖV-Vorhaben) genutzt wird. Das Protokoll bietet hierzu ein Rahmenwerk, aus welchem sich die jeweiligen Standards bedienen.

Die Spezifikation wird von der KoSIT (Koordinierungsstelle für IT-Standards) in dem Dokument [OSCI] gepflegt und herausgegeben.

OSCI-Transport bietet eine Vielzahl von Konfigurationsmöglichkeiten. Diese betreffen insbesondere die verschiedenen Ausprägungen des grundsätzlichen Nachrichtenablaufs (synchron/asynchron, etc.) sowie die Möglichkeiten zur Absicherung der Kommunikation. Ausgangspunkt für das Kommunikationsszenario ist dabei eine Umsetzung des Prinzips des doppelten Umschlags. Es wird daher zwischen Autor und Sender sowie Empfänger und Leser unterschieden.

Die Spezifikation liegt in zwei relevanten Versionen vor:

- Version 1.2 ist ein etablierter Standard mit dem Fokus auf Behördenkommunikation, die Kommunikation basiert auf der Nachrichtenübermittlung mittels einer dritten Stelle (Intermediär);
- Version 2.0 hat als Web-Service-Profilierung die Interoperabilität mit Standard-Implementierungen im Fokus, ergänzt diese um Quittierungsmechanismen/Postfachfunkionalität und erlaubt zusätzlich im synchronen Fall eine direkte Kommunikation. Bei der Verwendung öffentlicher Netze/asynchroner Kommunikation ist die Verwendung von Ende-zu-Ende-Verschlüsselung obligatorisch.

OSCI-Transport wird sowohl für die Kommunikation zwischen Behörden als auch für die Kommunikation zwischen Personen und öffentliche Stellen eingesetzt (z.B. Notar/Gericht). In dieser Richtlinie ist nur der zweite Fall relevant.

10.8.1 Dokumentenübermittlung

Bei der Nutzung von OSCI werden die notwendigen Funktionen der sicheren Dokumentenübermittlung wie folgt abgedeckt.

- Vertraulichkeit und Integrität des Dokumentes:

  Die konkreten Maßnahmen zur Sicherung von Vertraulichkeit und Integrität von übermittelten Dokumenten müssen durch die jeweilige Anwendung, die OSCI einsetzt, festgelegt werden, da OSCI selbst keine verpflichtenden Sicherheitsmaßnahmen vorschreibt.

- Identifizierung von Sender und Empfänger:

  Zur Identifizierung und Adressierung der Postfächer und ggf. Intermediäre werden externe Dienste eingesetzt, die bei der Bewertung des Vertrauensniveaus miteinbezogen werden müssen.

  Beispielsweise wird für die Identifizierung und Adressierung von Behörden meist das DVDV (Deutsches Verwaltungsdiensteverzeichnis, [DVDV]) genutzt. Im DVDV können Behörden und von Behör-

den beauftragte Stellen Dienste verzeichnen, die dann wiederum für andere unter den dort verzeichneten Parametern zur Verfügung stehen. Auf diese Weise wird eine sichere Kommunikation der Behörden untereinander ermöglicht.

In bestimmten Anwendungen wird auch die SAFE-Infrastruktur für die Identifizierung und Adressierung genutzt.

10.8.2 Vertrauensniveau

Das mit OSCI-Transport erreichte Vertrauensniveau ist ausschließlich abhängig von den Vorgaben des jeweiligen OSCI-nutzenden Standards. Für die Umsetzung von spezifischen Sicherheitsmaßnahmen ist im Kontext von OSCI-Transport die Verwendung von XML-Signatur und XML-Verschlüsselung für die Inhaltsdaten vorgesehen. Hier gelten dementsprechend die Überlegungen aus Kapitel 3.7.

Abschließend bleibt festzustellen, dass mit der Verwendung von OSCI-Transport eine große Bandbreite an Vertrauensniveaus abgedeckt werden kann, die vom Vertrauensniveau *hoch* bis zu einem vollständigen Verzicht auf Sicherheitsmaßnahmen und somit keinem Vertrauensniveau reicht.

Anhang A: Vertrauensniveaus nach [eIDAS]

Artikel 8 (2) [eIDAS] definiert Vertrauensniveaus wie folgt:

> *Die Sicherheitsniveaus[13] „niedrig", „substanziell" bzw. „hoch" erfüllen folgende Kriterien:*
>
> *a) Das Sicherheitsniveau „niedrig" bezieht sich auf ein elektronisches Identifizierungmittel im Rahmen eines elektronischen Identifizierungssystems, das ein begrenztes Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen – deren Zweck in der Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht – gekennzeichnet ist.*
>
> *b) Das Sicherheitsniveau „substanziell" bezieht sich auf ein elektronisches Identifizierungsmittel im Rahmen eines elektronischen Identifizierungssystems, das ein substanzielles Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich entsprechender technischer Überprüfungen – deren Zweck in der substanziellen Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht – gekennzeichnet ist.*
>
> *c) Das Sicherheitsniveau „hoch" bezieht sich auf ein elektronisches Identifizierungsmittel im Rahmen eines elektronischen Identifizierungssystems, das ein höheres Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person als ein Identifizierungsmittel mit dem Sicherheitsniveau „substanziell" vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen – deren Zweck in der Verhinderung des Identitätsmissbrauchs oder der Identitätsveränderung besteht – gekennzeichnet ist.*

In [eIDAS LoA] werden die Anforderungen an die Identifizierungssysteme näher ausgeführt. Dabei entsprechen sich die Vertrauensniveaus im Wesentlichen wie folgt:

[eIDAS LoA]	**[ISO29115]**	**Diese Richtlinie**
niedrig	2	*normal*
substantiell	3	*substantiell*
hoch	4	*hoch*

Tabelle 13: Vertrauensniveaus nach eIDAS, ISO/IEC 29115 und dieser TR

Diese Gegenüberstellung ist keine direkte Entsprechung, so werden etwa für die Bewertung der Identitätsprüfung unterschiedliche Konzepte genutzt.

Besondere Anforderungen für Formvorschriften (*hoch +*) finden keine Entsprechung in [eIDAS LoA], da Formvorschriften nicht im Anwendungsbereich von [eIDAS] liegen.

13 Das in der englischen Version der Verordnung genutzte „assurance level" wird in der deutschen Version etwas unglücklich mit „Sicherheitsniveau" statt dem eigentlich passenderen „Vertrauensniveau" übersetzt.

Literaturverzeichnis

[AIS 20/31] BSI: AIS 20/31 -- A proposal for: Functionality classes for random number generators

[AufenthG] Aufenthaltsgesetz in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S.162), das durch Artikel 4 Absatz 2 des Gesetzes vom 11. Oktober 2016 (BGBl. I S. 2226) geändert worden ist

[BRSchriftform] Bundesregierung: Bericht der Bundesregierung nach Artikel 5 des Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften (http://dipbt.bundestag.de/dip21/btd/17/107/1710720.pdf)

[BSI-GS] BSI: IT-Grundschutz-Kataloge, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[BSI100-2] BSI: BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

[De-Mail-G] De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), das durch Artikel 3 Absatz 7 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666) geändert worden ist

[DVDV] BIT: Deutsches Verwaltungsdiensteverzeichnis - Verfahrensbeschreibung

[EGVP] Webseite Elektronisches Gerichts- und Verwaltungspostfach, http://www.egvp.de

[eIDAS] VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

[eIDAS LoA] DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

[ISO18045] ISO/IEC: ISO/IEC 18045: Information technology — Security techniques — Methodology for IT security evaluation

[ISO24760-1] ISO/IEC: ISO/IEC 24760-1: Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts

[ISO27001] ISO/IEC: ISO/IEC 27001: Information technology -- Security techniques -- Information security management systems -- Requirements

[ISO29115] ISO/IEC: ISO/IEC 29115: Information technology -- Security techniques -- Entity authentication assurance framework

[OSCI] KoSIT: OSCI-Transport 1.2/2.01, Spezifikation, www.xoev.de/de/download

[PAuswG] Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG) vom 18. Juni 2009 (BGBl. I S. 1346), das durch Artikel 4 Absatz 1 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666) geändert worden ist

[RFC5280] IETF: D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk: RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC5652] IETF: R. Housley, Cryptographic Message Syntax (CMS), 2009

[RFC5750] IETF: B. Ramsdell, S. Turner: RFC 5750, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling

[RFC5751] IETF: B. Ramsdell, S.Turner, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, 2010

[TR-01201] BSI: Technische Richtlinie TR-01201, De-Mail

[TR-02102] BSI: Technische Richtlinie TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen

[TR-03107-2] BSI: Technische Richtlinie TR-03107-2, Elektronische Identitäten und Vertrauensdienste im E-Government -- Teil 2: Schriftformersatz mit elektronischem Identitätsnachweis

[TR-03116] BSI: Technische Richtlinie TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung

[TR-03124] BSI: Technische Richtlinie TR-03124, eID-Client

[TR-03125] BSI: Technische Richtlinie TR-03125, Beweiswerterhaltung kryptographisch signierter Dokumente

[TR-03127] BSI: Technische Richtlinie TR-03127, eID-Karten mit eID- und eSign-Funktion basierend auf Extended Access Control

[TR-03145] BSI: Technische Richtlinie TR-03145, Secure CA Operation

[VPS] Webseite Virtuelle Poststelle, https://www.bsi.bund.de/VPS

[VwVfG] Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), das zuletzt durch Artikel 20 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1679) geändert worden ist