Sicherheitsniveau	Erforderliche Elemente
Substanziell	Zusätzlich zu Nummer 3 des Niveaus „Niedrig“: 1. Der Identitätsnachweis der natürlichen Person, die im Namen der juristischen Person handelt, wird so überprüft, als erfolge er auf dem Niveau „Substanziell“ oder „Hoch“. 2. Die Verknüpfung ist nach auf nationaler Ebene anerkannten Verfahren hergestellt worden, was zu einer Eintragung der Verknüpfung in einer verlässlichen Quelle geführt hat. 3. Die Verknüpfung ist aufgrund von Informationen einer verlässlichen Quelle überprüft worden.
Hoch	Zusätzlich zu Nummer 3 des Niveaus „Niedrig“ und zu Nummer 2 des Niveaus „Substanziell“: 1. Der Identitätsnachweis der natürlichen Person, die im Namen der juristischen Person handelt, wird so überprüft, als erfolge er auf dem Niveau „Hoch“. 2. Die Verknüpfung ist anhand einer im nationalen Umfeld verwendeten eindeutigen Kennung, die die juristische Person repräsentiert, sowie anhand von Informationen einer verlässlichen Quelle, die die natürliche Person eindeutig repräsentieren, überprüft worden.

2.2. *Verwaltung elektronischer Identifizierungsmittel*

2.2.1. Merkmale und Gestaltung elektronischer Identifizierungsmittel

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Das elektronische Identifizierungsmittel benutzt mindestens einen Authentifizierungsfaktor. 2. Das elektronische Identifizierungsmittel ist so gestaltet, dass der Aussteller zumutbare Vorkehrungen trifft, um zu prüfen, dass es nur unter der Kontrolle oder im Besitz der Person, der es gehört, verwendet wird.
Substanziell	1. Das elektronische Identifizierungsmittel benutzt mindestens zwei Authentifizierungsfaktoren unterschiedlicher Kategorien. 2. Das elektronische Identifizierungsmittel ist so gestaltet, dass davon ausgegangen werden kann, dass es nur unter der Kontrolle oder im Besitz der Person, der es gehört, verwendet wird.
Hoch	Zusätzlich zum Niveau „Substanziell“: 1. Das elektronische Identifizierungsmittel bietet Schutz vor Duplizierung und Fälschung wie auch vor Angreifern mit hohem Angriffspotential. 2. Das elektronische Identifizierungsmittel ist so gestaltet, dass es von der Person, der es gehört, zuverlässig vor einer Benutzung durch andere geschützt werden kann.

2.2.2. Ausstellung, Auslieferung und Aktivierung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Nach der Ausstellung wird das elektronische Identifizierungsmittel auf eine Weise ausgeliefert, bei der davon ausgegangen werden kann, dass es nur die beabsichtigte Person erreicht.
Substanziell	Nach der Ausstellung wird das elektronische Identifizierungsmittel auf eine Weise ausgeliefert, bei der davon ausgegangen werden kann, dass es nur in den Besitz der Person gelangt, der es gehört.

Sicherheitsniveau	Erforderliche Elemente
Hoch	Im Aktivierungsprozess wird geprüft, dass das elektronische Identifizierungsmittel nur in den Besitz der Person gelangt ist, der es gehört.

2.2.3. Aussetzung, Widerruf und Reaktivierung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es ist möglich, ein elektronisches Identifizierungsmittel rasch und wirksam auszusetzen und/oder zu widerrufen. 2. Es bestehen Vorkehrungen, um eine unbefugte Aussetzung, einen unbefugten Widerruf oder eine unbefugte Reaktivierung zu verhindern. 3. Eine Reaktivierung darf nur erfolgen, wenn dieselben Sicherheitsanforderungen wie vor der Aussetzung oder vor dem Widerruf weiterhin erfüllt sind.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.2.4. Verlängerung und Ersetzung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Unter Berücksichtigung des Risikos einer Änderung der Personenidentifizierungsdaten müssen für die Verlängerung oder Ersetzung dieselben Sicherheitsanforderungen wie beim ursprünglichen Identitätsnachweis- und -überprüfungsprozess erfüllt sein bzw. muss ein gültiges elektronisches Identifizierungsmittel desselben oder eines höheren Sicherheitsniveaus zugrunde gelegt werden.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Zusätzlich zum Niveau „Niedrig“: Erfolgt die Verlängerung oder Ersetzung aufgrund eines gültigen elektronischen Identifizierungsmittels, so werden die Identitätsdaten anhand einer verlässlichen Quelle überprüft.

2.3. *Authentifizierung*

Dieser Abschnitt betrifft die Bedrohungen im Zusammenhang mit der Verwendung der Authentifizierungsmechanismen und enthält Anforderungen an jedes Sicherheitsniveau. In diesem Abschnitt wird davon ausgegangen, dass die Kontrollmaßnahmen den Risiken des jeweiligen Sicherheitsniveaus angemessen sein müssen.

2.3.1. Authentifizierungsmechanismus

Die folgende Tabelle enthält für jedes Sicherheitsniveau die jeweiligen Anforderungen an den Authentifizierungsmechanismus, mit dem die natürliche oder juristische Person das elektronische Identifizierungsmittel verwendet, um einem vertrauenden Beteiligten ihre Identität zu bestätigen.

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Vor einer Herausgabe von Personenidentifizierungsdaten erfolgt eine zuverlässige Überprüfung des elektronischen Identifizierungsmittels und seiner Gültigkeit. 2. Werden Personenidentifizierungsdaten als Teil des Authentifizierungsmechanismus gespeichert, müssen sie gesichert sein, um sie vor Verlust und vor Beeinträchtigung, einschließlich Offline-Analyse, zu schützen. 3. Im Authentifizierungsmechanismus sind Sicherheitskontrollen zur Überprüfung des elektronischen Identifizierungsmittels implementiert, so dass es höchst unwahrscheinlich ist, dass ein Angreifer mit erhöhtem grundlegenden

Sicherheitsniveau	Erforderliche Elemente
	Angriffspotenzial durch Handlungen wie Erraten, Abhören, Replay oder Manipulation der Kommunikation den Authentifizierungsmechanismus aushebeln kann.
Substanziell	Zusätzlich zum Niveau „Niedrig“: 1. Vor einer Herausgabe von Personenidentifizierungsdaten erfolgt eine zuverlässige Überprüfung des elektronischen Identifizierungsmittels und seiner Gültigkeit durch dynamische Authentifizierung. 2. Im Authentifizierungsmechanismus sind Sicherheitskontrollen zur Überprüfung des elektronischen Identifizierungsmittels implementiert, so dass es höchst unwahrscheinlich ist, dass ein Angreifer mit mäßigem Angriffspotenzial durch Handlungen wie Erraten, Abhören, Replay oder Manipulation der Kommunikation den Authentifizierungsmechanismus aushebeln kann.
Hoch	Zusätzlich zum Niveau „Substanziell“: Im Authentifizierungsmechanismus sind Sicherheitskontrollen zur Überprüfung des elektronischen Identifizierungsmittels implementiert, so dass es höchst unwahrscheinlich ist, dass ein Angreifer mit hohem Angriffspotenzial durch Handlungen wie Erraten, Abhören, Replay oder Manipulation der Kommunikation den Authentifizierungsmechanismus aushebeln kann.

2.4. *Management und Organisation*

Alle Beteiligten, die im Zusammenhang mit der elektronischen Identifizierung im grenzüberschreitenden Umfeld einen Dienst betreiben („Betreiber“) müssen dokumentierte Verfahrensweisen und Vorgaben für das Informationssicherheitsmanagement, Risikomanagementkonzepte und andere anerkannte Kontrollmaßnahmen haben, damit sich die geeigneten Leitungsgremien der elektronischen Identifizierungssysteme in den jeweiligen Mitgliedstaaten vergewissern können, dass wirksame Verfahren bestehen. Im gesamten Abschnitt 2.4 wird davon ausgegangen, dass alle Anforderungen bzw. Elemente den Risiken des jeweiligen Sicherheitsniveaus angemessen sein müssen.

2.4.1. Allgemeine Bestimmungen

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Betreiber, die eine unter diese Verordnung fallende betriebliche Dienstleistung erbringen, sind eine Behörde oder eine juristische Person, die als solche nach den nationalen Rechtsvorschriften eines Mitgliedstaats anerkannt ist, verfügen über eine eingerichtete Organisationsstruktur und sind in allen Teilen, die für die Bereitstellung der Dienste von Bedeutung sind, voll betriebsfähig. 2. Die Betreiber erfüllen alle rechtlichen Anforderungen, die ihnen im Zusammenhang mit dem Betrieb und der Bereitstellung des Dienstes obliegen, unter anderem auch in Bezug darauf, welche Arten von Informationen abgefragt werden können, wie der Identitätsnachweis durchgeführt wird und welche Informationen wie lange aufbewahrt werden dürfen. 3. Die Betreiber können ihre Fähigkeit zur Übernahme des Haftungsrisikos für Schäden nachweisen und verfügen über ausreichende finanzielle Mittel für einen fortlaufenden Betrieb und eine fortlaufende Bereitstellung der Dienste. 4. Die Betreiber sind sowohl für die Erfüllung aller Verpflichtungen, die sie an andere Stellen untervergeben, als auch für die Einhaltung der Systemvorgaben verantwortlich, als würden sie alle Aufgaben selbst wahrnehmen. 5. Elektronische Identifizierungssysteme, die nicht durch nationale Rechtsvorschriften eingerichtet werden, müssen über einen wirksamen Beendigungsplan verfügen. In einem solchen Plan müssen auch eine geordnete Einstellung des Dienstes bzw. die Fortsetzung durch einen anderen Betreiber, die