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

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die 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 ([1]), insbesondere auf Artikel 8 Absatz 3,

in Erwägung nachstehender Gründe:

(1) Laut Artikel 8 der Verordnung (EU) Nr. 910/2014 muss ein gemäß Artikel 9 Absatz 1 notifiziertes elektronisches Identifizierungssystem die Sicherheitsniveaus „niedrig", „substanziell" und/oder „hoch" angeben, die den nach diesem System ausgestellten elektronischen Identifizierungsmitteln zuerkannt wurden.

(2) Die Festlegung von Mindestanforderungen an die technischen Spezifikationen, Normen und Verfahren ist entscheidend, wenn es darum geht, ein gemeinsames Verständnis der Einzelheiten der Sicherheitsniveaus herzustellen und, wie in Artikel 12 Absatz 4 Buchstabe b der Verordnung (EU) Nr. 910/2014 vorgesehen, die Interoperabilität bei der Zuordnung der Entsprechungen zwischen nationalen Sicherheitsniveaus notifizierter elektronischer Identifizierungsmittel und den Sicherheitsniveaus des Artikels 8 zu gewährleisten.

(3) Bei der Ausarbeitung der in dieser Durchführungsverordnung festgelegten Spezifikationen und Verfahren wurde die internationale Norm ISO/IEC 29115 als die wichtigste internationale Norm auf dem Gebiet der Sicherheitsniveaus für elektronische Identifizierungsmittel berücksichtigt. Die Verordnung (EU) Nr. 910/2014 weist jedoch inhaltliche Unterschiede zu dieser internationalen Norm auf, insbesondere im Hinblick auf Anforderungen an Identitätsnachweis und -überprüfung, aber auch in Bezug darauf, wie die Unterschiede zwischen Identitätsvorschriften der Mitgliedstaaten und die diesbezüglich bestehenden EU-Instrumente berücksichtigt werden. Deshalb sollte der Anhang zwar auf dieser internationalen Norm beruhen, aber keine Verweise auf bestimmte Inhalte der Norm ISO/IEC 29115 enthalten.

(4) Diese Verordnung wurde nach einem ergebnisorientierten Ansatz ausgearbeitet, da dieser sich am besten eignete; dies spiegelt sich auch in den in den Begriffsbestimmungen verwendeten Bezeichnungen und Begriffen wider. Diese tragen dem Ziel der Verordnung (EU) Nr. 910/2014 in Bezug auf die Sicherheitsniveaus elektronischer Identifizierungsmittel Rechnung. Daher sollten das Großpilotprojekt STORK und die dort entwickelten Spezifikationen wie auch die Begriffsbestimmungen und Konzepte der Norm ISO/IEC 29115 bei der Festlegung der in dieser Durchführungsverordnung vorgesehenen Spezifikationen und Verfahren weitestgehend berücksichtigt werden.

(5) Je nach dem Zusammenhang, in dem ein bestimmter Aspekt eines Beweismittels für die Identität überprüft werden muss, können verlässliche Quellen viele verschiedene Formen haben, z. B. Register, Urkunden, Stellen usw. Selbst in einem ähnlichen Zusammenhang können solche verlässlichen Quellen in den verschiedenen Mitgliedstaaten sehr unterschiedlich sein.

(6) Anforderungen an Identitätsnachweis und -überprüfung sollten unterschiedliche Systeme und Verfahrensweisen berücksichtigen, gleichzeitig aber eine hinreichend hohe Sicherheit bieten, um das erforderliche Vertrauen zu schaffen. Daher sollte die Anerkennung von Verfahren, die zuvor für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, vom Nachweis abhängig gemacht werden, dass diese Verfahren die für das betreffende Sicherheitsniveau vorgesehenen Anforderungen erfüllen.

([1]) ABl. L 257 vom 28.8.2014, S. 73.

(7) Üblicherweise werden gewisse Authentifizierungsfaktoren wie Geheimnisse, die allen Beteiligten bekannt sind, physische Mittel oder körperliche Merkmale verwendet. Um die Sicherheit des Authentifizierungsprozesses zu erhöhen, sollte jedoch die Verwendung einer größeren Zahl von Authentifizierungsfaktoren, insbesondere auch aus verschiedenen Kategorien, gefördert werden.

(8) Diese Verordnung sollte Vertretungsbefugnisse juristischer Personen unberührt lassen. Der Anhang sollte aber Anforderungen an die Verknüpfung von elektronischen Identifizierungsmitteln natürlicher und juristischer Personen enthalten.

(9) Die Bedeutung von Informationssicherheits- und Dienstemanagementsystemen sollte genauso anerkannt werden wie die Bedeutung der Verwendung bewährter Methoden und der Anwendung der in Normenreihen wie ISO/IEC 27000 und ISO/IEC 20000 verankerten Grundsätze.

(10) In den Mitgliedstaaten angewandte bewährte Verfahren in Bezug auf Sicherheitsniveaus sollten ebenfalls berücksichtigt werden.

(11) Die IT-Sicherheitszertifizierung auf der Grundlage internationaler Normen ist ein wichtiges Instrument, mit dem überprüft werden kann, ob die Sicherheitsmerkmale der Produkte den Anforderungen dieser Durchführungsverordnung entsprechen.

(12) Der in Artikel 48 der Verordnung (EU) Nr. 910/2014 genannte Ausschuss hat innerhalb der von seinem Vorsitz festgelegten Frist keine Stellungnahme abgegeben —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

(1) Die Sicherheitsniveaus „niedrig", „substanziell" und „hoch" für elektronische Identifizierungsmittel, die nach einem notifizierten elektronischen Identifizierungssystem ausgestellt werden, werden unter Bezugnahme auf die Spezifikationen und Verfahren im Anhang bestimmt.

(2) Die im Anhang festgelegten Spezifikationen und Verfahren werden angewandt, um das Sicherheitsniveau der nach einem notifizierten elektronischen Identifizierungssystem ausgestellten elektronischen Identifizierungsmittel anhand der Zuverlässigkeit und Qualität folgender Elemente zu bestimmen:

a) Anmeldung nach Abschnitt 2.1 des Anhangs dieser Verordnung gemäß Artikel 8 Absatz 3 Buchstabe a der Verordnung (EU) Nr. 910/2014;

b) Verwaltung der elektronischen Identifizierungsmittel nach Abschnitt 2.2 des Anhangs dieser Verordnung gemäß Artikel 8 Absatz 3 Buchstaben b und f der Verordnung (EU) Nr. 910/2014;

c) Authentifizierung nach Abschnitt 2.3 des Anhangs dieser Verordnung gemäß Artikel 8 Absatz 3 Buchstabe c der Verordnung (EU) Nr. 910/2014;

d) Management und Organisation nach Abschnitt 2.4 des Anhangs dieser Verordnung gemäß Artikel 8 Absatz 3 Buchstaben d und e der Verordnung (EU) Nr. 910/2014.

(3) Erfüllt ein elektronisches Identifizierungsmittel, das nach einem notifizierten elektronischen Identifizierungssystem ausgestellt wird, eine Anforderung eines höheren Sicherheitsniveaus, so wird davon ausgegangen, dass es die entsprechende Anforderung eines niedrigeren Sicherheitsniveaus ebenfalls erfüllt.

(4) Soweit im betreffenden Teil des Anhangs nichts anderes festgelegt ist, müssen alle Elemente, die im Anhang zu einem bestimmten Sicherheitsniveau der nach einem notifizierten elektronischen Identifizierungssystem ausgestellten elektronischen Identifizierungsmittel aufgeführt sind, erfüllt sein, damit sie dem beanspruchten Sicherheitsniveau entsprechen.

Artikel 2

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 8. September 2015

Für die Kommission

Der Präsident

Jean-Claude JUNCKER

ANHANG

Technische Spezifikationen und Verfahren für die Sicherheitsniveaus „niedrig", „substanziell" und „hoch" für elektronische Identifizierungsmittel, die nach einem notifizierten elektronischen Identifizierungssystem ausgestellt werden

1. **Begriffsbestimmungen**

Für die Zwecke dieses Anhangs gelten folgende Begriffsbestimmungen:

1. „Verlässliche Quelle" ist eine beliebige Informationsquelle, die auf verlässliche Weise präzise Daten, Informationen und/oder Beweismittel bereitstellt, die zum Identitätsnachweis verwendet werden können;

2. „Authentifizierungsfaktor" ist ein Element, das nachweislich mit einer Person verknüpft ist und (mindestens) einer der folgenden Kategorien angehört:

   a) „besitzabhängiger Authentifizierungsfaktor" ist ein Authentifizierungsfaktor, dessen Besitz der Nutzer bzw. das Subjekt nachweisen muss;

   b) „kenntnisabhängiger Authentifizierungsfaktor" ist ein Authentifizierungsfaktor, dessen Kenntnis der Nutzer bzw. das Subjekt nachweisen muss;

   c) „inhärenter Authentifizierungsfaktor" ist ein Authentifizierungsfaktor, der auf ein körperliches Merkmal einer natürlichen Person abstellt und bei dem der Nutzer nachweisen muss, dass er dieses körperliche Merkmal hat;

3. „dynamische Authentifizierung" ist ein elektronischer Prozess, der unter Einsatz kryptografischer oder anderer Methoden auf Abruf einen elektronischen Nachweis dafür erzeugt, dass der Benutzer bzw. das Subjekt die Identifizierungsdaten unter seiner Kontrolle hat oder besitzt; der Nachweis ändert sich dabei mit jedem Authentifizierungsvorgang zwischen dem Benutzer/Subjekt und dem System, das die Identität des Subjekts überprüft;

4. „Informationssicherheitsmanagementsystem" ist eine Reihe von Prozessen und Verfahren für das Management annehmbarer Risikostufen in Bezug auf die Informationssicherheit.

2. **Technische Spezifikationen und Verfahren**

Die Elemente technischer Spezifikationen und Verfahren in diesem Anhang werden verwendet um festzulegen, wie die Anforderungen und Kriterien des Artikels 8 der Verordnung (EU) Nr. 910/2014 auf elektronische Identifizierungsmittel, die nach einem notifizierten elektronischen Identifizierungssystem ausgestellt werden, anzuwenden sind.

2.1. *Anmeldung*

2.1.1. Beantragung und Eintragung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es ist gewährleistet, dass der Antragsteller die Geschäftsbedingungen für die Benutzung des elektronischen Identifizierungsmittels kennt. 2. Es ist gewährleistet, dass der Antragsteller die empfohlenen Sicherheitsvorkehrungen im Zusammenhang mit dem elektronischen Identifizierungsmittel kennt. 3. Die einschlägigen Identitätsdaten für den Nachweis und die Überprüfung der Identität werden erfasst.
Substanziell	Wie für das Niveau „Niedrig".
Hoch	Wie für das Niveau „Niedrig".

2.1.2. Identitätsnachweis und -überprüfung (natürliche Person)

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es kann davon ausgegangen werden, dass die Person im Besitz eines Beweismittels ist, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und die beanspruchte Identität repräsentiert. 2. Es kann davon ausgegangen werden, dass das Beweismittel echt ist oder laut einer verlässlichen Quelle existiert und dass das Beweismittel dem Anschein nach gültig ist. 3. Eine verlässliche Quelle hat Kenntnis davon, dass die beanspruchte Identität existiert und es kann davon ausgegangen werden, dass die Person, die diese Identität beansprucht, damit identisch ist.
Substanziell	Zusätzlich zum Niveau „Niedrig“ muss eine der Alternativen der Nummern 1 bis 4 erfüllt sein: 1. Es ist überprüft worden, dass die Person im Besitz eines Beweismittels ist, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und die beanspruchte Identität repräsentiert, und das Beweismittel ist geprüft worden, um seine Echtheit festzustellen, oder einer verlässlichen Quelle ist bekannt, dass es existiert und sich auf eine reale Person bezieht, und es wurden Vorkehrungen getroffen, um das Risiko zu mindern, dass die Identität der Person nicht mit der beanspruchten Identität übereinstimmt, z. B. im Hinblick auf verlorene, gestohlene, ausgesetzte, widerrufene oder abgelaufene Beweismittel. ODER 2. Ein Identitätsdokument wird im Rahmen eines Registrierungsverfahrens in dem Mitgliedstaat, in dem es ausgestellt wurde, vorgelegt und bezieht sich dem Anschein nach auf die Person, die es vorlegt, und es wurden Vorkehrungen getroffen, um das Risiko zu mindern, dass die Identität der Person nicht mit der beanspruchten Identität übereinstimmt, z. B. im Hinblick auf verlorene, gestohlene, ausgesetzte, widerrufene oder abgelaufene Dokumente. ODER 3. Bieten Verfahren, die zuvor von einer öffentlichen oder privaten Stelle in demselben Mitgliedstaat für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, eine gleichwertige Sicherheit, die der des Niveaus „Substanziell“ in Abschnitt 2.1.2 entspricht, so braucht die für die Registrierung zuständige Stelle solche früheren Verfahren nicht zu wiederholen, sofern die gleichwertige Sicherheit von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates ([1]) oder von einer gleichwertigen Stelle bestätigt wird. ODER 4. Werden elektronische Identifizierungsmittel aufgrund eines gültigen notifizierten elektronischen Identifizierungsmittels des Sicherheitsniveaus „Substanziell“ oder „Hoch“ und unter Berücksichtigung des Risikos einer Änderung der Personenidentifizierungsdaten ausgestellt, so brauchen die Prozesse für den Nachweis und die Überprüfung der Identität nicht wiederholt zu werden. Wurde das zugrunde gelegte elektronische Identifizierungsmittel nicht notifiziert, so muss das Sicherheitsniveau „Substanziell“ oder „Hoch“ von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt werden.

Sicherheitsniveau	Erforderliche Elemente
Hoch	Es müssen entweder die Anforderungen der Nummer 1 oder der Nummer 2 erfüllt sein: 1. Zusätzlich zum Niveau „Substanziell“ muss eine der Alternativen der Buchstaben a bis c erfüllt sein: a) Ist überprüft worden, dass die Person im Besitz eines mit Foto oder biometrischen Merkmalen versehenen Identitätsnachweises ist, der von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird, und dass der Identitätsnachweis die beanspruchte Identität repräsentiert, so wird das Beweismittel geprüft, um festzustellen, ob es laut einer verlässlichen Quelle gültig ist, und anhand des Vergleichs eines oder mehrerer körperlicher Merkmale der Person mit Angaben aus einer verlässlichen Quelle wird festgestellt, dass der Antragsteller mit der beanspruchten Identität übereinstimmt. ODER b) Bieten Verfahren, die zuvor von einer öffentlichen oder privaten Stelle in demselben Mitgliedstaat für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, eine gleichwertige Sicherheit, die der des Niveaus „Hoch“ in Abschnitt 2.1.2 entspricht, so braucht die für die Registrierung zuständige Stelle solche früheren Verfahren nicht zu wiederholen, sofern die gleichwertige Sicherheit von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt wird, und es werden Schritte unternommen, um zu belegen, dass die Ergebnisse der früheren Verfahren noch gültig sind. ODER c) Werden elektronische Identifizierungsmittel aufgrund eines gültigen notifizierten elektronischen Identifizierungsmittels des Sicherheitsniveaus „Hoch“ und unter Berücksichtigung des Risikos einer Änderung der Personenidentifizierungsdaten ausgestellt, so brauchen die Prozesse für den Nachweis und die Überprüfung der Identität nicht wiederholt zu werden. Wurde das zugrunde gelegte elektronische Identifizierungsmittel nicht notifiziert, so muss das Sicherheitsniveau „Hoch“ von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt werden, und es werden Schritte unternommen, um zu belegen, dass die Ergebnisse des früheren Verfahrens zur Ausstellung eines notifizierten elektronischen Identifizierungsmittels noch gültig sind. ODER 2. Legt der Antragsteller keinen anerkannten, mit Foto oder biometrischen Merkmalen versehenen Identitätsnachweis vor, so werden exakt dieselben Verfahren angewandt, die auf nationaler Ebene in dem Mitgliedstaat, zu dem die für die Registrierung zuständige Stelle gehört, erforderlich sind, um einen solchen anerkannten, mit Foto oder biometrischen Merkmalen versehenen Identitätsnachweis zu erlangen.

(1) Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

2.1.3. Identitätsnachweis und -überprüfung (juristische Person)

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Die beanspruchte Identität der juristischen Person wird anhand eines Beweismittels nachgewiesen, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird.

Sicherheitsniveau	Erforderliche Elemente
	2. Das Beweismittel ist dem Anschein nach gültig und es kann davon ausgegangen werden, dass es echt ist oder laut einer verlässlichen Quelle existiert, sofern die Aufnahme einer juristischen Person in die verlässliche Quelle freiwillig und durch eine Vereinbarung zwischen der juristischen Person und der verlässlichen Quelle geregelt ist. 3. Die verlässliche Quelle hat keine Kenntnis davon, dass sich die juristische Person in einer Lage befindet, in der sie daran gehindert wäre, als diese juristische Person zu handeln.
Substanziell	Zusätzlich zum Niveau „Niedrig" muss eine der Alternativen der Nummern 1 bis 3 erfüllt sein: 1. Die beanspruchte Identität der juristischen Person wird anhand eines Beweismittels nachgewiesen, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und aus dem der Name, die Rechtsform und gegebenenfalls die Registriernummer der juristischen Person hervorgehen, und das Beweismittel ist geprüft worden, um festzustellen, ob es echt ist oder laut einer verlässlichen Quelle existiert, sofern die Aufnahme der juristischen Person in die verlässliche Quelle für die Tätigkeit in ihrem Sektor erforderlich ist, und es wurden Vorkehrungen getroffen, um das Risiko zu mindern, dass die Identität der juristischen Person nicht mit der beanspruchten Identität übereinstimmt, z. B. im Hinblick auf verlorene, gestohlene, ausgesetzte, widerrufene oder abgelaufene Dokumente. ODER 2. Bieten die Verfahren, die zuvor von einer öffentlichen oder privaten Stelle in demselben Mitgliedstaat für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, eine gleichwertige Sicherheit, die der des Niveaus „Substanziell" in Abschnitt 2.1.3 entspricht, so braucht die für die Registrierung zuständige Stelle solche früheren Verfahren nicht zu wiederholen, sofern die gleichwertige Sicherheit von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt wird. ODER 3. Werden elektronische Identifizierungsmittel aufgrund eines gültigen notifizierten elektronischen Identifizierungsmittels des Sicherheitsniveaus „Substanziell" oder „Hoch" ausgestellt, so brauchen die Prozesse für den Nachweis und die Überprüfung der Identität nicht wiederholt zu werden. Wurde das zugrunde gelegte elektronische Identifizierungsmittel nicht notifiziert, so muss das Sicherheitsniveau „Substanziell" oder „Hoch" von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt werden.
Hoch	Zusätzlich zum Niveau „Substanziell" muss eine der Alternativen in den Nummern 1 bis 3 erfüllt sein: 1. Die beanspruchte Identität der juristischen Person wird anhand eines Beweismittels nachgewiesen, das von dem Mitgliedstaat, in dem das elektronische Identifizierungsmittel beantragt wird, anerkannt wird und aus dem der Name und die Rechtsform der juristischen Person sowie zumindest eine eindeutige Kennung, die die juristische im nationalen Umfeld repräsentiert, hervorgeht, und das Beweismittel ist geprüft worden, um festzustellen, ob es laut einer verlässlichen Quelle gültig ist. ODER

Sicherheitsniveau	Erforderliche Elemente
	2. Bieten die Verfahren, die zuvor von einer öffentlichen oder privaten Stelle in demselben Mitgliedstaat für andere Zwecke als die Ausstellung elektronischer Identifizierungsmittel verwendet wurden, eine gleichwertige Sicherheit, die der des Niveaus „Hoch" in Abschnitt 2.1.3 entspricht, so braucht die für die Registrierung zuständige Stelle solche früheren Verfahren nicht zu wiederholen, sofern die gleichwertige Sicherheit von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt wird, und es werden Schritte unternommen, um zu belegen, dass die Ergebnisse dieses früheren Verfahrens noch gültig sind. ODER 3. Werden elektronische Identifizierungsmittel aufgrund eines gültigen notifizierten elektronischen Identifizierungsmittels des Sicherheitsniveaus „Hoch" ausgestellt, so brauchen die Prozesse für den Nachweis und die Überprüfung der Identität nicht wiederholt zu werden. Wurde das zugrunde gelegte elektronische Identifizierungsmittel nicht notifiziert, so muss das Sicherheitsniveau „Hoch" von einer Konformitätsbewertungsstelle im Sinne des Artikels 2 Absatz 13 der Verordnung (EG) Nr. 765/2008 oder von einer gleichwertigen Stelle bestätigt werden, und es werden Schritte unternommen, um zu belegen, dass die Ergebnisse des früheren Verfahrens zur Ausstellung eines notifizierten elektronischen Identifizierungsmittels noch gültig sind.

2.1.4. Verknüpfung von elektronischen Identifizierungsmitteln natürlicher und juristischer Personen

Für die Verknüpfung von elektronischen Identifizierungsmitteln natürlicher Personen und elektronischen Identifizierungsmitteln juristischer Personen („Verknüpfung") gelten, soweit zutreffend, folgende Bedingungen:

1. Es ist möglich, eine Verknüpfung auszusetzen und/oder zu widerrufen. Der Lebenszyklus einer Verknüpfung (z. B. Aktivierung, Aussetzung, Erneuerung, Widerruf) wird nach auf nationaler Ebene anerkannten Verfahren verwaltet.

2. Die natürliche Person, deren elektronisches Identifizierungsmittel mit dem elektronischen Identifizierungsmittel der juristischen Person verknüpft ist, kann die Ausübung der Verknüpfung nach auf nationaler Ebene anerkannten Verfahren an eine andere natürliche Person delegieren. Die delegierende natürliche Person bleibt jedoch verantwortlich.

3. Die Verknüpfung erfolgt auf folgende Weise:

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Der Identitätsnachweis der natürlichen Person, die im Namen der juristischen Person handelt, wird so überprüft, als erfolge er auf dem Niveau „Niedrig" oder höher. 2. Die Verknüpfung ist nach auf nationaler Ebene anerkannten Verfahren hergestellt worden. 3. Die verlässliche Quelle hat keine Kenntnis davon, dass sich die natürliche Person in einer Lage befindet, in der sie daran gehindert wäre, im Namen der juristischen Person zu handeln.
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".

Sicherheitsniveau	Erforderliche Elemente
	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.
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 Angriffspotenzial durch Handlungen wie Erraten, Abhören, Replay oder Manipulation der Kommunikation den Authentifizierungsmechanismus aushebeln kann.

Sicherheitsniveau	Erforderliche Elemente
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 Art und Weise, wie einschlägige Behörden und Endnutzer informiert werden, sowie Einzelheiten dazu geregelt sein, wie Daten in Übereinstimmung mit den Systemvorgaben zu schützen, aufzubewahren bzw. zu zerstören sind.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.2. Veröffentlichte Bekanntmachungen und Benutzerinformationen

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es gibt eine veröffentlichte Definition des Dienstes mit allen geltenden Geschäftsbedingungen und Entgelten sowie möglichen Nutzungsbeschränkungen. Die Definition des Dienstes enthält auch eine Datenschutzerklärung. 2. Es sind geeignete Vorgaben und Verfahren zu schaffen, damit die Benutzer des Dienstes in rascher und verlässlicher Weise informiert werden, wenn sich die Definition des Dienstes selbst, die geltenden Geschäftsbedingungen oder die Datenschutzerklärung in Bezug auf den betreffenden Dienst ändern. 3. Es sind geeignete Vorgaben und Verfahren zu schaffen, damit Auskunftsersuchen vollständig und richtig beantwortet werden.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.3. Informationssicherheitsmanagement

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Es besteht ein wirksames Informationssicherheitsmanagementsystem für das Management und die Beherrschung von Informationssicherheitsrisiken.
Substanziell	Zusätzlich zum Niveau „Niedrig“: Das Informationssicherheitsmanagementsystem folgt bewährten Normen oder Grundsätzen für das Management und die Beherrschung von Informationssicherheitsrisiken.
Hoch	Wie für das Niveau „Substanziell“.

2.4.4. Aufbewahrungspflichten

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Die Aufzeichnung und Aufbewahrung einschlägiger Informationen erfolgt mit einem effektiven Aufzeichnungsverwaltungssystem unter Beachtung geltender Vorschriften und bewährter Verfahren auf dem Gebiet des Datenschutzes und der Datenspeicherung. 2. Aufzeichnungen werden, soweit nach nationalem Recht oder anderen nationalen Verwaltungsregelungen zulässig, aufbewahrt und geschützt, solange dies für Prüfungszwecke und für die Untersuchung von Sicherheitsverletzungen sowie für die Zwecke der Datenspeicherung erforderlich ist; danach werden die Aufzeichnungen auf sichere Weise vernichtet.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.5. Einrichtungen und Personal

Die folgende Tabelle enthält die Anforderungen an Einrichtungen und Personal sowie an etwaige Unterauftragnehmer, die Aufgaben wahrnehmen, die unter diese Verordnung fallen. Die Einhaltung jeder dieser Anforderungen soll im Hinblick auf die Risiken des jeweiligen Sicherheitsniveaus verhältnismäßig sein.

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es gibt Verfahren, die sicherstellen, dass alle Mitarbeiter und Unterauftragnehmer eine ausreichende Ausbildung, Qualifikation und Erfahrung bezüglich der ihnen übertragenen Aufgaben haben. 2. Es gibt eine ausreichende Anzahl von Mitarbeitern und Unterauftragnehmern für einen angemessenen Betrieb und eine angemessene Ausstattung des Dienstes entsprechend den Vorgaben und Verfahren. 3. Die zur Bereitstellung des Dienstes genutzten Einrichtungen werden ständig überwacht und vor Schäden durch Umgebungseinflüsse, unbefugten Zugriff oder andere Faktoren geschützt, die die Sicherheit des Dienstes beeinträchtigen können. 4. Die zur Bereitstellung des Dienstes genutzten Einrichtungen gewährleisten, dass nur befugte Mitarbeiter und Unterauftragnehmer Zugang zu Bereichen haben, in denen personenbezogene Daten, kryptografische oder andere sensible Informationen verarbeitet werden.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.6. Technische Kontrollen

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es gibt angemessene technische Kontrollen für das Risikomanagement in Bezug auf die Sicherheit der Dienste sowie zum Schutz der Vertraulichkeit, Unversehrtheit und Verfügbarkeit der verarbeiteten Informationen. 2. Elektronische Kommunikationswege, die zur Übermittlung personenbezogener oder sensibler Informationen verwendet werden, müssen gegen Abhören, Manipulation und Replay geschützt sein. 3. Der Zugang zu sensiblem kryptografischen Material, das für die Ausstellung elektronischer Identifizierungsmittel und für die Authentifizierung verwendet wird, ist streng auf die Rollen und Anwendungen beschränkt, die diesen Zugang unbedingt benötigen. Es ist sichergestellt, dass solches Material niemals dauerhaft im Klartext gespeichert wird. 4. Es gibt Verfahren, die gewährleisten, dass die Sicherheit dauerhaft aufrechterhalten wird und dass auf geänderte Risikostufen, Vorfälle und Sicherheitsverletzungen reagiert werden kann. 5. Alle Speichermedien, die personenbezogene, kryptografische oder andere sensible Informationen enthalten, werden in sicherer und geschützter Weise aufbewahrt, transportiert und entsorgt.
Substanziell	Zusätzlich zum Niveau „Niedrig“: Sensibles kryptografisches Material, das für die Ausstellung elektronischer Identifizierungsmittel und für die Authentifizierung verwendet wird, ist vor Fälschung geschützt.
Hoch	Wie für das Niveau „Substanziell“.

2.4.7. Einhaltung und Prüfung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Es gibt regelmäßige interne Prüfungen (Audits) aller Bestandteile, die für die Bereitstellung der Dienste von Bedeutung sind, um die Einhaltung der betreffenden Vorgaben zu gewährleisten.

Sicherheitsniveau	Erforderliche Elemente
Substanziell	Es gibt regelmäßige unabhängige interne oder externe Prüfungen (Audits) aller Bestandteile, die für die Bereitstellung der Dienste von Bedeutung sind, um die Einhaltung der betreffenden Vorgaben zu gewährleisten.
Hoch	1. Es gibt regelmäßige unabhängige externe Prüfungen (Audits) aller Bestandteile, die für die Bereitstellung der Dienste von Bedeutung sind, um die Einhaltung der betreffenden Vorgaben zu gewährleisten. 2. Wird das System direkt von einer staatlichen Stelle verwaltet, so erfolgen die Prüfungen nach den nationalen Rechtsvorschriften.