Mitteilungen

Qualifizierte elektronische Signatur

Teil A
Mitteilungen der Bundesnetzagentur

Mitteilung Nr. 208/2018

Verfügung gemäß § 11 Absatz 1 VDG

Im Bundesgesetzblatt Nr. 52 wurde am 28.07.2017 das Gesetz zur Durchführung der 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-Durchführungsgesetz) verkündet (BGBl. I, S. 2745). Artikel 1 des eIDAS-Durchführungsgesetzes beinhaltet das Vertrauensdienstegesetz (VDG).

Das VDG ist gemäß Artikel 12 Absatz 1 Satz 1 des eIDAS-Durchführungsgesetzes am 29.07.2017 in Kraft getreten.

In § 11 Absatz 1 VDG wird der Bundesnetzagentur die Aufgabe zugewiesen, im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik eine Festlegung zu treffen, welche sonstigen Identifizierungsmethoden im Sinne des Artikels 24 Absatz 1 Unterabsatz 2 Buchstabe d Satz 1 der Verordnung (EU) Nr. 910/2014 anerkannt sind und welche Mindestanforderungen dafür jeweils gelten.

Dieser Verfügung ist eine Anhörung der betroffenen Kreise vorausgegangen. Sie erfolgt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik.

Anerkannte „sonstige Identifizierungsmethoden“ i. S. d. § 11 Absatz 1 VDG i.V.m. Artikel 24 Absatz 1 Unterabsatz 2 Buchstabe d Satz 1 der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung)

Identifizierung einer natürlichen Person im Rahmen der Beantragung eines qualifizierten Zertifikates unter Nutzung einer Videoübertragung (Videoidentifizierung).

Für Verfahren, die nach dieser Identifizierungsmethode erfolgen, und für welche die zuständige Aufsichtsstelle erstmalig gem. Art. 21 Abs. 2, Art. 24 Abs. 1, UAbs. 2 d) der eIDAS-Verordnung i.V.m. § 11 des Vertrauensdienstegesetzes über die Erteilung oder nach Ablauf der Frist des Art. 20 Abs. 1 Satz 1 der eIDAS-Verordnung über die Verlängerung des Qualifikationsstatus zu entscheiden hat, gelten folgende Vorgaben:

1. **Anforderungen aus Normen des Europäisches Instituts für Telekommunikationsnormen (ETSI)**

   Soweit in der Verfügung keine anderen Vorgaben getroffen werden, müssen Identifizierungsmethoden den Vorgaben für Registrierungsstellen in den einschlägigen ETSI-Normen für Anbieter elektronischer Vertrauensdienste entsprechen. Einschlägig sind diesbezüglich die ETSI EN

   319 401
   319 411-1
   319 411-2

   in der jeweils aktuellen Fassung.

2. **Anforderungen an das Personal**

   Eine Videoidentifizierung darf nur von fachkundigem, qualifiziertem und zuverlässigem Personal durchgeführt werden.

a) Fachkunde

Zum Nachweis der Fachkunde der Mitarbeiter muss der Vertrauensdiensteanbieter Belege für eine Erst- und regelmäßige Folgeschulungen vorhalten. Diese sind ihm im Falle einer Auslagerung der Tätigkeit auf einen beauftragten Dritten von diesem vor einer Tätigkeit der fraglichen Person zu übermitteln.

Die Schulungen müssen mindestens die Kenntnis der mittels Videoidentifizierung prüfbaren Merkmale umfassen, einschließlich der anzuwendenden Prüfverfahren derjenigen Dokumente, die im Rahmen der Videoidentifizierung zulässig sind (s. Abschnitt 5.). Die Mitarbeiter müssen hinsichtlich gängiger Fälschungsmöglichkeiten dieser Dokumente geschult sein. Ferner ist eine Kenntnis der maßgeblichen Rechtsnormen, insbesondere des Datenschutzrechtes und der in dieser Verfügung gestellten Anforderungen, notwendig.

Die vorgenannten Inhalte müssen den Mitarbeitern vor Aufnahme ihrer Identifizierungstätigkeit angemessen vermittelt werden. Nachfolgend ist die Schulung in regelmäßigen Abständen (mindestens einmal jährlich) sowie bei Bedarf zu wiederholen und hierüber beim Vertrauensdiensteanbieter eine Dokumentation der vermittelten Inhalte zu erstellen. Die Notwendigkeit einer Schulung kann sich z.B. aus einer Änderung der gesetzlichen und/oder aufsichtsrechtlichen bzw. datenschutzrechtlichen Anforderungen oder im Falle eines Auftretens einer signifikanten Zahl von Betrugsversuchen, des Bekanntwerdens neuer Betrugsmöglichkeiten oder sonstigen Veränderungen im Verfahrensablauf ergeben.

b) Qualifikation

Die Qualifikation eines Mitarbeiters zum Einsatz als Identifizierungskraft bemisst sich nach seiner Fähigkeit, den Prozess der Identifizierung, also insbesondere des Abgleichs der antragstellenden Person mit einem Ausweisdokument, durchzuführen. Er muss zur Wahrnehmung der maßgeblichen Überprüfungskriterien in der Lage sein. Für die Kommunikation mit dem Antragsteller müssen je nach Angebot des Vertrauensdiensteanbieters i.S. des § 7 Abs. 1 des Vertrauensdienstegesetzes (Barrierefreie Dienste) geeignete Methoden (z.B. Sprache, Fremdsprache, Gebärdensprache) zur Verfügung stehen.

c) Zuverlässigkeit

Zum Nachweis der Zuverlässigkeit der Mitarbeiter muss der Vertrauensdiensteanbieter vor der Aufnahme der Tätigkeit des Mitarbeiters ein aktuelles Führungszeugnis einsehen. Lediglich Mitarbeiter mit einem Führungszeugnis ohne Eintragungen sind als Identifizierungskraft zu beschäftigen. Die Einsichtnahme in ein aktuelles Führungszeugnis durch den Vertrauensdiensteanbieter ist im Abstand von 2 Jahren zu wiederholen. Im Falle einer Auslagerung der Tätigkeit auf einen beauftragten Dritten gelten die Anforderungen an Vertrauensdiensteanbieter für diesen entsprechend.

3. Bauliche Anforderungen

Die Mitarbeiter müssen sich während der Identifizierung in zutrittsgeschützten Räumen aufhalten, zu denen nur autorisierte Mitarbeiter Zutritt haben.

4. Allgemeine Anforderungen an den Identifizierungsprozess

a) Bei der Zuteilung der Identifizierungsvorgänge an die Mitarbeiter müssen Mechanismen eingesetzt werden, die einer vorhersehbaren Zuteilung von Vorgängen und damit der dadurch bestehenden Möglichkeit einer Manipulation entgegenwirken.

b) Die Durchführung der Videoidentifizierung muss in Echtzeit und ohne Unterbrechung erfolgen.

c) Die audiovisuelle Kommunikation zwischen dem Mitarbeiter und der zu identifizierenden Person ist in Bezug auf Integrität und Vertraulichkeit ausreichend abzusichern; aus diesem Grund sind nur Ende-zu-Ende verschlüsselte Videochats zulässig. Es sind hierbei die Empfehlungen der Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) TR-02102 einzuhalten.

d) Die Bild- und Tonqualität der Kommunikation muss in einem ausreichenden Maße gegeben sein, um eine zweifelsfreie Identifizierung anhand aller in dieser Verfügung geforderten Prüfungen uneingeschränkt zu ermöglichen.

e) Ist die vorstehend beschriebene Überprüfung – etwa aufgrund von schlechten Lichtverhältnissen oder einer schlechten Bild- oder Tonqualität/-übertragung – und/oder eine sprachliche Kommunikation mit der zu identifizierenden Person nicht möglich, ist der Identifizierungsprozess abzubrechen.

f) Zur Überprüfung der Aktualität des Vorganges muss der Anbieter geeignete Maßnahmen ergreifen.

5. Anforderungen an geeignete Identitätsdokumente

Nur Identitätsdokumente, die über hinreichend fälschungssichere und im Verfahren prüfbare Sicherheitsmerkmale verfügen, können für die Identitätsüberprüfung herangezogen werden.

6. Anforderungen an die Überprüfung des Identitätsdokumentes und des Antragstellers

Die Echtheit des Identitätsdokuments und die Zugehörigkeit zu der zu identifizierenden Person müssen zuverlässig überprüft werden. Der Anbieter muss geeignete Maßnahmen ergreifen, um eine Manipulation des Videobildes bzw. des Identitätsdokumentes oder der Person zu erkennen. Hierzu können organisatorische Maßnahmen gehören, die durch Interaktion mit dem verwendeten Ausweisdokument gemäß Anweisung des Mitarbeiters oder der zu identifizierende Person eine Manipulation erkennbar machen. Ferner kann der Anbieter technische Maßnahmen treffen, um eine Veränderung des Videostreams zu erkennen.

7. Anforderungen an die Aufzeichnung und Aufbewahrung

a) Einwilligung zur Aufzeichnung

Die zu identifizierende Person hat zu Beginn einer Videoidentifizierung ihre ausdrückliche Einwilligung dazu zu erklären, dass Passagen des Identifizierungsprozesses aufgezeichnet werden.

Dem Nutzer ist detailliert zu beschreiben, wozu er eine Einwilligung erteilt (z.B.: Worauf bezieht sich die Einwilligung im Einzelnen, welche Art der Datenverarbeitung

ist vorgesehen, durch wen und wie lange werden die Daten gespeichert, wie wird mit den Daten bei Abbruch der Identifizierung umgegangen?)

b) Inhalt und Dauer der Aufzeichnung

Hinsichtlich des Inhalts der Aufzeichnung des Prozesses einer Identifizierung mittels Videotechnologie sowie der Aufbewahrung der in diesem Prozess erworbenen Daten sind die Vorgaben des § 16 Absatz 4 Nr. 2 VDG i.V.m. Artikel 24 Absatz 2 Buchstaben f) bis h) der Verordnung (EU) Nr. 910/2014 zu beachten.

§ 16 Abs. 4 Nr. 2 VDG:

„*Qualifizierte Vertrauensdiensteanbieter haben für die gesamte Zeit ihres Betriebs die dazugehörigen Aufzeichnungen nach Artikel 24 Absatz 2 Buchstabe h der Verordnung (EU) Nr. 910/2014 aufzubewahren.“*

Artikel 24 Absatz 2 Buchstaben f) bis h) der Verordnung (EU) Nr. 910/2014:

f) Sie verwenden vertrauenswürdige Systeme für die Speicherung der ihnen übermittelten Daten in einer überprüfbaren Form, so dass

i) diese nur mit Zustimmung der Person, auf die sich die Daten beziehen, öffentlich abrufbar sind,

ii) nur befugte Personen Daten eingeben und gespeicherte Daten ändern können,

iii) die Daten auf ihre Echtheit hin überprüft werden können.

g) Sie ergreifen geeignete Maßnahmen gegen Fälschung und Diebstahl von Daten.

h) Sie zeichnen alle einschlägigen Informationen über die von dem qualifizierten Vertrauensdiensteanbieter ausgegebenen und empfangenen Daten auf und bewahren sie so auf, dass sie über einen angemessenen Zeitraum, auch über den Zeitpunkt der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters hinaus, verfügbar sind, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können.

Insbesondere hinsichtlich der Anforderung nach § 16 Abs. 4 Nr. 2 VDG i.V.m. Art. 24 Abs. 2 Buchstabe h) der Verordnung (EU) Nr. 910/2014 sind die Grundsätze der Erforderlichkeit und der Datensparsamkeit mit dem Zweck der nachhaltigen Unabstreitbarkeit der Identifizierung in Einklang zu bringen. Die wesentlichen Passagen des Identifizierungsvorgangs sind mit Ton sowie Fotos bzw. Screenshots der Person und des verwendeten Identitätsdokuments dauerhaft aufzuzeichnen.

Auf den Fotos/Screenshots sind die zu identifizierende Person sowie Vorder- und Rückseite des von dieser zur Identifizierung verwendeten Identitätsdokumentes und die darauf jeweils enthaltenen Angaben deutlich erkennbar aufzunehmen. Daten, die nicht zur Ausstellung des qualifizierten Zertifikates erforderlich sind, sind unkenntlich

zu machen. Die erforderlichen Daten ergeben sich aus ETSI EN 319 411-2 V2.1.1 (2016-02), Kapitel 6.2.2..

Für eine Eignung der Aufzeichnung zum Zwecke der Beweisführung i.S.d. § 16 Abs. 4 Nr. 2 VDG i.V.m. Art. 24 Abs. 2 Buchstabe h) der Verordnung (EU) Nr. 910/2014 ist es erforderlich, dass die antragstellende Person zweifelsfrei erkennbar und sprachlich oder gebärdensprachlich klar wahrnehmbar ist. Das verwendete Identitätsdokument muss inhaltlich und hinsichtlich der geprüften sicherheitstechnischen Vorkehrungen aufgezeichnet werden. Von dem qualitativ verwertbaren Videomaterial ist mindestens eine Sequenz von 15 Sekunden aufzuzeichnen.

Die Einwilligung zur Aufzeichnung des Identifizierungsvorgangs ist zusätzlich zu der Sequenz von 15 Sekunden Dauer aufzuzeichnen und so lange aufzubewahren wie der zugehörige Datensatz.

Die Auswertung der Anforderungen an die Aufzeichnung und Aufbewahrung muss in einem 4-Augen-Prinzip beurteilt werden. Dabei sind die Korrektheit der erhobenen Daten zu überprüfen sowie der Abgleich von verwendeten Identitätsdokumenten und antragstellender Person zu bestätigen und freizugeben.

8. Meldung von mutmaßlichen Betrugsfällen

Der Vertrauensdiensteanbieter oder der von ihm zur Videoidentifizierung beauftragte Dritte meldet mutmaßliche Betrugsversuche an das Postfach tsp-incidents@bnetza.de.

9. Feststellung der geeigneten Umsetzung

Die geeignete Umsetzung der in der Verfügung festgelegten Anforderungen ist durch eine Konformitätsbewertungsstelle im Rahmen der Bestätigung nach Artikel 24 Absatz 1 Unterabsatz 2 Buchstabe d Satz 1 der Verordnung (EU) Nr. 910/2014 zu beurteilen. Bei der Beurteilung ist der Stand der Technik zu beachten. Hierzu zählen die ergänzenden Kriterien zur Bewertung von sonstigen Identifizierungsmethoden nach Artikel 24 Absatz 1 Unterabsatz 2 Buchstabe d Satz 1 der Verordnung (EU) Nr. 910/2014 in der zum Zeitpunkt der Bewertung aktuellen Fassung. Diese werden bei berechtigtem Interesse von der Bundesnetzagentur zur Verfügung gestellt. Bei der

Erstellung wirken Bundesamt für Sicherheit in der Informationstechnik und Bundesnetzagentur zusammen, die betroffenen Kreise werden angehört.

10. Einschränkungen

a) Die Anerkennung der Methode ist ausgeschlossen für das Ausstellen qualifizierter Zertifikate für die Website-Authentifizierung.

b) Die Anerkennung der Methode ist ferner für das Ausstellen qualifizierter Zertifikate für qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel beschränkt auf die Ausgabe von einmalig nutzbaren Zertifikaten (sog. Ad-Hoc-Zertifikate). Solche Zertifikate sind unmittelbar nach der vom Vertrauensdiensteanbieter mit Zustimmung der Akzeptanzstelle vorgegebenen Nutzung (z.B. Abschluss eines Mietvertrages für ein KFZ), jedenfalls innerhalb von 24 Stunden nach der Ausstellung, von diesem zu widerrufen, sofern sie zu diesem Zeitpunkt noch gültig sind. Die einmalige Nutzung darf insbesondere nicht zur Beantragung eines neuen qualifizierten Zertifikates oder für andere Identifizierungen dienen. Die Anerkennung ist befristet bis zum 31.12.2020.

Rechtsbehelfsbelehrung

Gegen diese Verfügung kann innerhalb eines Monats nach Bekanntgabe Widerspruch bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Referat IS 15, Canisiusstraße 21, 55122 Mainz oder bei einer sonstigen Dienststelle der Bundesnetzagentur erhoben werden.