



ZERTIFIKAT

SRC Security Research & Consulting GmbH

bescheinigt hiermit dem Unternehmen

identity Trust Management GmbH
Auenstraße 100
80469 München
Deutschland

für das Modul zur Identitätsfeststellung

identity Management

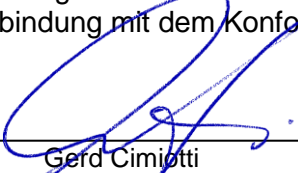
die Erfüllung aller relevanten Anforderungen der Verordnung (EU) Nr. 910/2014¹ (eIDAS)
für die Identitätsfeststellung natürlicher Personen für VDA

Zertifikat gültig bis

26.08.2024

SRC Zertifikatsregistrierungsnummer **SRC.00054.TSP.08.2022**
Dieses Zertifikat gilt nur in Verbindung mit dem Konformitätsbewertungsbericht.

Bonn, den 27. August 2022



Gerd Cimigatti

Die SRC Security Research & Consulting GmbH ist eine akkreditierte Zertifizierungsstelle für Produkte, Prozesse und Dienstleistungen nach DIN EN ISO/IEC 17065 und bietet akkreditierte Dienstleistungen (Konformitätsbewertungsstelle) im Bereich der Verordnung (EU) Nr. 910/2014 an.



¹ 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.

Beschreibung des Moduls zur Identitätsfeststellung

1. Zertifizierungsprogramm

Die Zertifizierungsstelle der SRC Security Research & Consulting GmbH ist bei der „DAkKS Deutsche Akkreditierungsstelle GmbH“¹ als Konformitätsbewertungsstelle vom Typ Zertifizierungsstelle für Produkte, Prozesse und Dienstleistungen nach DIN EN ISO/IEC 17065 akkreditiert. Zertifizierungen werden durchgeführt auf der Grundlage des „Zertifizierungsprogramm eIDAS der Zertifizierungsstelle (KBS) (akkreditierter Bereich) der SRC Security Research & Consulting GmbH“, Version 1.1 vom 28.07.2021. Das akkreditierte Zertifizierungsprogramm wird auf Anfrage zur Verfügung gestellt.

Stellen, die durch die DAkKS akkreditiert wurden, werden geführt in der Datenbank: <https://www.dakks.de/content/akkreditierte-stellen-dakks>

Das Zertifizierungsprogramm wird ergänzt durch die Einhaltung der Anforderungen gemäß [ETSI EN 319 403] an Konformitätsbewertungsstellen, die Vertrauensdiensteanbieter bewerten.

2. Gegenstand der Konformitätsbewertung

2.1 Vertrauensdiensteanbieter

identity Trust Management GmbH

Auenstraße 100

80469 München

www.identity.tm

2.2 Vertrauensdienste / Prüfgegenstand

Der Prüfgegenstand ist das Modul zur Identitätsfeststellung

- **identity Management mit den Identifizierungsverfahren identity Shop, identity Video, identity PoS, identity eID und identity autoid**

Das Modul wird wie folgt identifiziert:

Identifizierung des Moduls zur Identitätsfeststellung	
ServiceTypenidentifizierer	http://uri.etsi.org/TrstSvc/Svctype/IdV/nothavingPKId
ServiceName	identity Management

Hieraus ergibt sich kein Anpassungsbedarf an die durch die Bundesnetzagentur ausgegebene Trust-service Status List (TSL).

¹ Deutsche Akkreditierungsstelle GmbH, Spittelmarkt 10, 10117 Berlin, www.dakks.de

3. Funktionsbeschreibung

identity Trust Management GmbH bietet einen Identitätsfeststellungsdienst an, der die Anforderungen von Art. 24 Abs. 1 der Verordnung (EU) Nr. 910/2014 erfüllt und der von einem Vertrauensdiensteanbieter als Modul zu seinem Vertrauensdienst für die Ausstellung von qualifizierten Zertifikaten genutzt werden kann. Dabei wird identity Trust Management GmbH als beauftragter Dritter vertraglich eingebunden. identity Trust Management GmbH hat zur Erlangung der Konformität seines Identitätsfeststellungsdienstes als Modul für Vertrauensdiensteanbieter eine Konformitätsbewertung vornehmen lassen.

In dem vorliegenden Bericht werden die folgenden von identity Trust Management GmbH angebotenen Identifizierungsverfahren bewertet:

- identity Shop: Identifizierung anhand eines Ausweisdokuments, bei der sich die zu identifizierende Person persönlich in einen Shop begibt.
- identity Video: Identifizierung anhand eines Ausweisdokuments, bei der der Identifizierer die zu identifizierende Person in einer Video-Konferenz identifiziert.
- identity PoS: Identifizierung anhand eines Ausweisdokuments, bei der sich die zu identifizierende Person persönlich in eine Partner-Filiale (Point-of-Sale) begibt und dort identifiziert und registriert wird. Auf Basis der Identifizierung und Registrierung erfolgt im Zusammenhang eine per Fern-Signatur durchgeführte Vertragsunterzeichnung.
- identity eID: Identifizierung mittels Nutzung des elektronischen Identitätsnachweises gemäß §18 PAuswG und § 78 AufenthG.
- identity autoID: Identifizierung durch sonstige Identifizierungsmethoden, die auf nationaler Ebene anerkannt sind und gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten, in diesem Fall die persönliche Identifizierung natürlicher Personen durch ein halbautomatisches Verfahren unter Verwendung amtlicher Ausweisdokumente mit automatisierten Mitteln (App oder webbasierte Selfie-Aufnahme auf einem Mobilgerät) zur Beweiserhebung, auf die immer eine manuelle Überprüfung durch eine natürliche Person folgt. Das Verfahren nutzt das Modul „Autoident Qualified Electronic Signature“ der IDnow GmbH, welches bereits einer erfolgreichen Konformitätsbewertung unterzogen wurde (Registrierungsnummer TUVIT.97174.TSP.06.2021).

Alle Identifizierungsverfahren können für die Identitätsfeststellung einer natürlichen Person verwendet werden, die die Ausstellung eines qualifizierten Zertifikats bei einem Vertrauensdiensteanbieter beantragt. Dabei kann es sich um folgende Arten von Zertifikaten handeln:

1) Qualifizierte Zertifikate, bei denen sich die elektronischen Signaturerstellungsdaten, die den elektronischen Signaturvalidierungsdaten entsprechen, in einer qualifizierten Signaturerstellungseinheit (QSCD) befinden. Diese Zertifikate enthalten das QC-Statement für die Policy QSCP-n-qscd wie von ETSI EN 319 412-5 verlangt.

2) Qualifizierte Zertifikate, bei denen sich die elektronischen Signaturerstellungsdaten, die den elektronischen Signaturvalidierungsdaten entsprechen, nicht in einer

qualifizierten Signaturerstellungseinheit (QSCD) befinden. Diese Zertifikate enthalten das QC-Statement für die Policy QSCP-n wie von ETSI EN 319 412-5 verlangt.

4. Erfüllung der Anforderungen der eIDAS-Verordnung, des Vertrauensdienstegesetzes und der Vertrauensdiensteverordnung

Der vorliegende Konformitätsbewertungsbericht gibt die Erfüllung der Anforderungen der eIDAS-Verordnung, des Vertrauensdienstegesetzes und der Vertrauensdiensteverordnung für die Anforderungen wieder, die für die Identitätsfeststellung natürlicher Personen bei der Ausstellung von qualifizierten Zertifikaten durch einen Vertrauensdiensteanbieter relevant sind. Für den Nachweis wird auf die Erfüllung der Anforderungen relevanter ETSI Standards referenziert. Die Evaluation Reports [ER EN 319 401], [ER EN 319 411-1] und [ER EN 319 411-2] enthalten die detaillierten Prüfergebnisse, die die Erfüllung der Anforderungen gemäß den entsprechenden ETSI Standards [ETSI EN 319 401] (Anforderungen an alle Vertrauensdiensteanbieter), [ETSI EN 319 411-1] (Allgemeine Anforderungen an Vertrauensdiensteanbieter, die Zertifikate ausgeben) und [ETSI EN 319 411-2] (Anforderungen an Vertrauensdiensteanbieter, die EU-qualifizierte Zertifikate ausgeben) angeben.

Für das Identifizierungsverfahren identity Video wurden zusätzlich die Anforderungen des Amtsblatts der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Mitteilungen, Qualifizierte elektronische Signatur, Teil A, Mitteilungen der Bundesnetzagentur, Mitteilung Nr. 208/2018, Verfügung gemäß § 11 Absatz 1 VDG [Nr. 208/2018] geprüft und die Ergebnisse im zugehörigen Prüfbericht [ER VFG] dokumentiert.

Für das Identifizierungsverfahren identity autoID wurden zusätzlich die Anforderungen der vorläufigen Anerkennung einer innovativen Identifizierungsmethode gemäß § 11 Absatz 3 VDG [Verfügung AutoID] berücksichtigt. Die Erfüllung dieser Anforderungen wurde im Rahmen der Konformitätsbewertung von „Autoident Qualified Electronic Signature“ durch TÜViT geprüft. Zu diesen Anforderungen wurden daher keine separaten Berichte durch SRC angefertigt.

4.1 Erfüllung der Anforderungen der eIDAS-Verordnung

Der Identitätsfeststellungsdienst erfüllt die folgenden allgemeinen Anforderungen gemäß der Verordnung (EU) Nr. 910/2014 (eIDAS).

Referenz	Erfüllung durch den Vertrauensdienst
Artikel 15	Zugänglichkeit für Personen mit Behinderungen
	<p>identity Trust Management GmbH bietet seinen Identitätsfeststellungsdienst soweit möglich auch Personen mit Behinderung an. Die Bereitstellung von Endnutzerprodukten zur Nutzung des Vertrauensdienstes ist generell nicht erforderlich und wird durch identity Trust Management GmbH nicht angeboten.</p> <p>Durch die Vielfalt der Identifizierungsverfahren (sowohl online als auch offline) wird soweit möglich ein barrierefreier Service angeboten. In den Prozessen gibt es Möglichkeiten, den Dienst für Menschen mit Behinderungen zugänglich zu machen. Weiterhin hat der Endnutzer die Möglichkeit, das</p>

Referenz	Erfüllung durch den Vertrauensdienst
----------	--------------------------------------

Identifizierungsverfahren zu wechseln, wenn das gewählte Verfahren nicht geeignet ist.

Evaluation Report zu ETSI EN 319 401, Abs. 7.13

Artikel 19	Sicherheitsanforderungen an Vertrauensdiensteanbieter
------------	---

Abs. 1 identity Trust Management GmbH ergreift geeignete technische und organisatorische Maßnahmen zur Beherrschung der Sicherheitsrisiken im Zusammenhang mit dem erbrachten Identitätsfeststellungsdienst. Die Maßnahmen berücksichtigen den Stand der Technik und das Sicherheitsniveau ist der Höhe des Risikos angemessen. Hierzu gehören sowohl technische Maßnahmen zum Betrieb des Vertrauensdienstes sowie organisatorische Maßnahmen, um insbesondere Zuverlässigkeit und Fachkunde des eingesetzten Personals sicherzustellen.

Es wurden Maßnahmen getroffen, um Auswirkungen zu vermeiden und Beteiligte im Falle einer Sicherheitsverletzung zu informieren.

Evaluation Reports zu ETSI EN 319 401, Kap. 7; ETSI EN 319 411-1, Abs. 6.4, 6.5, 6.8; ETSI EN 319 411-2, Abs. 6.4, 6.5, 6.8

Abs. 2 identity Trust Management GmbH informiert alle relevanten Stellen über Sicherheitsverletzungen oder jeden Integritätsverlust innerhalb von 24 Stunden nach Kenntnisnahme des betreffenden Vorfalls, der sich auf den erbrachten Identitätsfeststellungsdienst oder die darin vorhandenen personenbezogenen Daten bezieht.

Evaluation Reports zu ETSI EN 319 401, Abs. 7.9

Artikel 20	Beaufsichtigung qualifizierter Vertrauensdiensteanbieter
------------	--

Abs. 1 Das Modul zur Identitätsfeststellung für einen Vertrauensdiensteanbieter zur Ausstellung von qualifizierten Zertifikaten wird alle 24 Monate durch eine Konformitätsbewertungsstelle geprüft.

Evaluation Reports zu ETSI EN 319 401, Abs. 7.13; ETSI EN 319 411-1, Abs. 6.7; ETSI EN 319 411-2, Abs. 6.7

Artikel 24	Anforderungen an qualifizierte Vertrauensdiensteanbieter
------------	--

Abs. 1 a-d) identity Trust Management GmbH überprüft die Identität der antragstellenden natürlichen Person anhand eines zugelassenen Ausweisdokuments.

Die Informationen werden von identity Trust Management GmbH im Einklang mit dem nationalen Recht entweder

Referenz

Erfüllung durch den Vertrauensdienst

unmittelbar oder unter Rückgriff auf einen Dritten wie folgt überprüft:

a) durch persönliche Anwesenheit der natürlichen Person (identity Shop, identity PoS) oder

b) aus der Ferne mittels elektronischer Identifizierungsmittel, für die vor der Ausstellung des qualifizierten Zertifikats eine persönliche Anwesenheit der natürlichen Person gewährleistet war und die Anforderungen gemäß Artikel 8 hinsichtlich der Sicherheitsniveaus „substanziell“ oder „hoch“ erfüllen (identity eID) oder

d) durch sonstige Identifizierungsmethoden, die auf nationaler Ebene anerkannt sind und gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten (identity Video und identity autoID) .

Die Konformitätsbewertungsstelle bestätigt für das Identifizierungsverfahren identity Video die gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit. Die Konformität des Verfahrens zum Amtsblatt der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Mitteilung Nr. 208/2018, Verfügung gemäß §11 Absatz 1 VDG wurde festgestellt.

Im Identifizierungsverfahren identity autoID erfolgt die Identifizierung mit dem Modul „Autoident Qualified Electronic Signature“ der IDnow GmbH. Dieses Modul wurde bereits einer erfolgreichen Konformitätsbewertung unterzogen (Registrierungsnummer TUVIT.97174.TSP.06.2021). Die Konformitätsbewertungsstelle bestätigt für das Identifizierungsverfahren identity autoID die gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit. Die Konformität des Verfahrens zur vorläufigen Anerkennung einer innovativen Identifizierungsmethode gemäß § 11 Absatz 3 VDG wurde festgestellt.

Evaluation Reports zu ETSI EN 319 411-1, Abs. 6.2.2, 6.2.3; ETSI EN 319 411-2, Abs. 6.2.2, 6.2.3

Prüfbericht zur Erfüllung der Anforderungen gemäß der Verfügung gemäß § 11 Absatz 1 VDG

Abs. 2 a)

identity Trust Management GmbH wird die Aufsichtsstelle über alle Änderungen bei der Erbringung der Identitätsfeststellungsdienste sowie bei einer beabsichtigten Einstellung der Tätigkeit unterrichten.

Evaluation Reports zu ETSI EN 319 401, Abs. 6.1, 7.12; ETSI EN 319 411-1, Abs. 6.4.9; ETSI EN 319 411-2, Abs. 6.4.9

Abs. 2 b)

identity Trust Management GmbH beschäftigt nur Personal und Unterauftragnehmer, die über die erforderliche

Referenz	Erfüllung durch den Vertrauensdienst
	<p>Zuverlässigkeit und Fachkunde verfügen. Das Personal und die Unterauftragnehmer verfügen über die notwendigen Qualifikationen und werden regelmäßig geschult.</p> <p>Evaluation Reports zu ETSI EN 319 401, Abs. 7.2; ETSI EN 319 411-1, Abs. 6.4.4; ETSI EN 319 411-2, Abs. 6.4.4</p>
Abs. 2 c)	<p>identity Trust Management GmbH verfügt über eine angemessene Haftpflichtversicherung.</p> <p>Evaluation Reports zu ETSI EN 319 401, REQ-7.1.1-04; ETSI EN 319 411-1, Abs. 6.8.2; ETSI EN 319 411-2, Abs. 6.8.2</p>
Abs. 2 d)	<p>Nicht relevant, da keine direkte Vertragsbeziehung zwischen identity Trust Management GmbH und der antragstellenden natürlichen Person besteht. Die Unterrichtspflicht obliegt dem Vertrauensdiensteanbieter.</p> <p>Evaluation Reports zu ETSI EN 319 401, Abs. 6.2; ETSI EN 319 411-1, Abs. 6.1, 6.3.4, 6.3.6, 6.8.13, 6.9.4; ETSI EN 319 411-2, Abs. 6.1, 6.3.4, 6.3.6, 6.8.13, 6.9.4</p>
Abs. 2 e)	<p>identity Trust Management GmbH verwendet vertrauenswürdige Systeme und Produkte, die vor Veränderungen geschützt sind und die die technische Sicherheit und Zuverlässigkeit der von ihnen unterstützten Prozesse sicherstellen.</p> <p>Evaluation Reports zu ETSI EN 319 401, Abs. 7.3 bis 7.10; ETSI EN 319 411-1, Abs. 6.4, 6.5; ETSI EN 319 411-2, Abs. 6.4, 6.5</p>
Abs. 2 f)	<p>identity Trust Management GmbH verwendet vertrauenswürdige Systeme für die Speicherung der ihnen übermittelten personenbezogenen Daten in einer überprüfbar Form, so dass diese nur mit Zustimmung der Person, auf die sich die Daten beziehen, öffentlich abrufbar sind, nur befugte Personen Daten eingeben und gespeicherte Daten ändern können und die Daten auf ihre Echtheit hin überprüft werden können. Die Daten verbleiben nur temporär bei identity Trust Management GmbH und werden an den jeweiligen Vertrauensdiensteanbieter übergeben.</p> <p>Evaluation Reports zu ETSI EN 319 401, Abs. 7.4 bis 7.10, 7.13; ETSI EN 319 411-1, Abs. 6.4, 6.5, 6.8.4; ETSI EN 319 411-2, Abs. 6.4, 6.5, 6.8.4</p>
Abs. 2 g)	<p>identity Trust Management GmbH hat geeignete Maßnahmen getroffen, um Daten vor Fälschung und Diebstahl zu schützen.</p> <p>Evaluation Reports zu ETSI EN 319 401, Kap. 7; ETSI EN 319 411-1, Abs. 6.4, 6.5; ETSI EN 319 411-2, Abs. 6.4, 6.5</p>

Referenz	Erfüllung durch den Vertrauensdienst
Abs. 2 h)	<p>identity Trust Management GmbH übermittelt die personenbezogenen Identifikationsdaten nach Beendigung eines Auftrags an den jeweiligen Vertrauensdiensteanbieter und löscht diese Daten spätestens 7 Werktage danach. Die Historie zu den Daten (Auftragsdaten), ohne personenbezogene Identifizierungsdaten, wird durch identity Trust Management GmbH für zwölf Monate verwahrt. Die Aufbewahrung der Daten bis zur Einstellung des Betriebs und darüber hinaus obliegt dem Vertrauensdiensteanbieter.</p> <p>Evaluation Reports zu ETSI EN 319 401, Kap. 7.10; ETSI EN 319 411-1, Abs. 6.4.5, 6.8.4; ETSI EN 319 411-2, Abs. 6.4.5, 6.8.4</p>
Abs. 2 i)	<p>identity Trust Management GmbH verfügt über einen Beendigungsplan, der im Falle der Beendigung der Tätigkeit befolgt wird.</p> <p>Evaluation Reports zu ETSI EN 319 401, Kap. 7.12; ETSI EN 319 411-1, Abs. 6.4.9; ETSI EN 319 411-2, Abs. 6.4.9</p>
Abs. 2 j)	<p>identity Trust Management GmbH verarbeitet personenbezogene Daten gemäß Richtlinie 95/46/EG.</p> <p>Evaluation Reports zu ETSI EN 319 401, Abs. 7.13; ETSI EN 319 411-1, Abs. 6.8.4; ETSI EN 319 411-2, Abs. 6.8.4</p>

Für den Identitätsfeststellungsdienst sind keine speziellen Anforderungen gemäß der Verordnung (EU) Nr. 910/2014 (eIDAS) zu berücksichtigen.

4.2 Erfüllung der Anforderungen des Vertrauensdienstegesetzes

Das Modul zur Identitätsfeststellung natürlicher Personen für einen Vertrauensdiensteanbieter zur Ausstellung von qualifizierten Zertifikaten erfüllt die folgenden Anforderungen gemäß dem Vertrauensdienstegesetz (VDG), das im „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)“ enthalten ist.

Referenz	Erfüllung durch den Vertrauensdienst
§ 7	Barrierefreie Dienste
Abs. 1	<p>identity Trust Management GmbH bietet seinen Identitätsfeststellungsdienst soweit möglich auch Personen mit Behinderung an. Die Bereitstellung von Endnutzerprodukten zur Nutzung des Vertrauensdienstes ist generell nicht erforderlich und wird durch identity Trust Management GmbH nicht angeboten.</p> <p>Durch die Vielfalt der Identifizierungsverfahren (sowohl online als auch offline) wird soweit möglich ein barrierefreier Service</p>

Referenz	Erfüllung durch den Vertrauensdienst
----------	--------------------------------------

angeboten. In den Prozessen gibt es Möglichkeiten, den Dienst für Menschen mit Behinderungen zugänglich zu machen. Weiterhin hat der Endnutzer die Möglichkeit, das Identifizierungsverfahren zu wechseln, wenn das gewählte Verfahren nicht geeignet ist.

Evaluation Report zu ETSI EN 319 401, Abs. 7.13

Abs. 2

identity Trust Management GmbH informiert auf ihrer Internetseite in ihrem CPS über die von ihnen vorgenommenen Maßnahmen zur Barrierefreiheit des Identitätsfeststellungsdienstes. Diese Informationen und Hinweise sind barrierefrei zugänglich und nutzbar. Die Bereitstellung von Endnutzerprodukten zur Nutzung des Vertrauensdienstes ist generell nicht erforderlich und wird durch identity Trust Management GmbH nicht angeboten.

Evaluation Report zu ETSI EN 319 401, Abs. 7.13

§ 8	Datenschutz
-----	-------------

Abs. 5

identity Trust Management GmbH übermittelt die personenbezogenen Identifikationsdaten nach Beendigung eines Auftrags an den jeweiligen Vertrauensdiensteanbieter und löscht diese Daten spätestens 7 Werktage danach. Die Historie zu den Daten (Auftragsdaten), ohne personenbezogene Identifizierungsdaten, wird durch identity Trust Management GmbH für zwölf Monate verwahrt. Die Aufbewahrung der Daten bis zur Einstellung des Betriebs obliegt dem Vertrauensdiensteanbieter.

Evaluation Reports zu ETSI EN 319 401, Kap. 7.13; ETSI EN 319 411-1, Abs. 6.2.2, 6.4.5, 6.8.4; ETSI EN 319 411-2, Abs. 6.2.2, 6.4.5, 6.8.4

§ 10	Deckungsvorsorge
------	------------------

identity Trust Management GmbH verfügt über eine Haftpflichtversicherung der ERGO Versicherung AG sowie eine durch Markel International betreute Haftpflichtversicherung. Die Versicherungssumme je Schadensfall beträgt 4 Millionen Euro (ERGO) bzw. 6 Millionen Euro (Markel) und übersteigt die Anforderung an die erforderliche Deckungssumme von 250.000 Euro je Schadensfall um ein Vielfaches.

Evaluation Report zu ETSI EN 319 401, REQ-7.1.1-04

§ 11	Identitätsprüfung
------	-------------------

Abs. 1

identity Trust Management GmbH erfüllt die Anforderungen des Amtsblatts der Bundesnetzagentur für Elektrizität, Gas,

Referenz**Erfüllung durch den Vertrauensdienst**

Telekommunikation, Post und Eisenbahnen, Mitteilung Nr. 208/2018, Verfügung gemäß §11 Absatz 1 VDG.

Evaluation Reports zu ETSI EN 319 411-1, Abs. 6.2.2; ETSI EN 319 411-2, Abs. 6.2.2

Prüfbericht zur Erfüllung der Anforderungen gemäß der Verfügung gemäß § 11 Absatz 1 VDG

Abs. 3

identity Trust Management GmbH erfüllt mit dem Identifizierungsverfahren identity autoID die Anforderungen der vorläufigen Anerkennung einer innovativen Identifizierungsmethode gemäß § 11 Absatz 3 VDG.

Evaluation Reports zu ETSI EN 319 411-1, Abs. 6.2.2; ETSI EN 319 411-2, Abs. 6.2.2

Komponenten-Konformitätsbewertungsbericht von „Autoident Qualified Electronic Signature“

§ 16**Beendigungsplan; auf Dauer prüfbare Dienste**

Abs. 1

identity Trust Management GmbH übergibt die gemäß VDG § 16 Abs. 1 geforderten Zertifikatsinformationen, im vorliegenden Fall die Identifizierungsdaten, nach Beendigung des Auftrags an den Vertrauensdiensteanbieter. Die Identifizierungsdaten werden bei identity Trust Management GmbH nicht länger als 7 Werkzeuge vorgehalten.

Evaluation Reports zu ETSI EN 319 401, Abs. 7.12; ETSI EN 319 411-1, Abs. 6.4.9; ETSI EN 319 411-1, Abs. 6.4.9

Abs. 4

identity Trust Management GmbH übermittelt die personenbezogenen Identifikationsdaten nach Beendigung eines Auftrags an den jeweiligen Vertrauensdiensteanbieter und löscht diese Daten spätestens 7 Werkzeuge danach. Die Historie zu den Daten (Auftragsdaten), ohne personenbezogene Identifizierungsdaten, wird durch identity Trust Management GmbH für zwölf Monate verwahrt. Die Aufbewahrung der Daten bis zur Einstellung des Betriebs obliegt dem Vertrauensdiensteanbieter.

Evaluation Reports zu ETSI EN 319 401, Kap. 7.10; ETSI EN 319 411-1, Abs. 6.4.5, 6.8.4; ETSI EN 319 411-2, Abs. 6.4.5, 6.8.4

4.3 Erfüllung der Anforderungen der Vertrauensdiensteverordnung

Das Modul Identitätsfeststellung für einen Vertrauensdiensteanbieter zur Ausstellung von qualifizierten Zertifikaten erfüllt die folgenden Anforderungen gemäß der Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung – VDV).

Referenz	Erfüllung durch den Vertrauensdienst
§ 1	Anforderungen an die Barrierefreiheit
	<p>identity Trust Management GmbH bietet seinen Identitätsfeststellungsdienst soweit möglich auch Personen mit Behinderung an. Der Identitätsfeststellungsdienst ist, soweit technisch möglich, für Menschen mit Behinderungen wahrnehmbar, bedienbar, verständlich und robust. Die Bereitstellung von Endnutzerprodukten zur Nutzung des Vertrauensdienstes ist generell nicht erforderlich und wird durch identity Trust Management GmbH nicht angeboten. Hinweise und Informationen zur Barrierefreiheit nach § 7 Absatz 2 des Vertrauensdienstegesetzes sind barrierefrei, wahrnehmbar und verständlich.</p> <p>Evaluation Report zu ETSI EN 319 401, Abs. 7.13</p>
§ 2	Ausgestaltung der Deckungsvorsorge für qualifizierte Vertrauensdiensteanbieter
Abs. 1	<p>identity Trust Management GmbH verfügt in Bezug auf das Haftungsrisiko für Schäden gemäß Artikel 13 der Verordnung (EU) Nr. 910/2014 über eine Gewerbe-Haftpflichtversicherung mit der Policen-Nr. SV 75034477-777 der ERGO Versicherung AG sowie eine durch Markel International betreute Vermögensschadenhaftpflichtversicherung mit der Policen-Nr. MPD 52528579-1. Die Policen liegen der Konformitätsbewertungsstelle vor.</p> <p>Die Deckungsvorsorge nach Artikel 24 Abs. 2 Buchstabe c zweite Alternative der Verordnung (EU) Nr. 910/2014 in Verbindung mit § 10 des Vertrauensdienstegesetzes wird somit durch eine Vermögensschadens-Haftpflichtversicherung gemäß VDV § 2 Abs. 1 Nr. 1 erbracht.</p> <p>Evaluation Report zu ETSI EN 319 401, REQ-7.1.1-04</p>
Abs. 2 Nr. 1	<p>Nicht relevant, da die von identity Trust Management GmbH abgeschlossenen Versicherungen keine Pflichtversicherungen sind. Gemäß § 6 des Vertrauensdienstegesetzes haftet der Vertrauensdiensteanbieter für beauftragte Dritte wie für eigenes Handeln. Eine mögliche Versicherungspflicht obliegt somit dem Vertrauensdiensteanbieter.</p>
Abs. 2 Nr. 2	<p>Es sind Jahreshöchstleistungen in Höhe von 8 Millionen Euro (ERGO) sowie von 12 Millionen Euro (Markel) vereinbart, die das Vierfache der Mindestversicherungssumme deutlich übersteigen.</p> <p>Evaluation Report zu ETSI EN 319 401, REQ-7.1.1-04</p>
Abs. 2 Nr. 3	<p>Hinsichtlich des räumlichen Geltungsbereich liegen keine Einschränkungen vor.</p>

Referenz	Erfüllung durch den Vertrauensdienst
Abs. 2 Nr. 4	<p>Evaluation Report zu ETSI EN 319 401, REQ-7.1.1-04</p> <p>Über die in VDV § 2 Abs. 2 Nr. 4 genannten Ausschlüsse für Ersatzansprüche aus vorsätzlich begangener Pflichtverletzung liegen keine weiteren Ausschlüsse vor.</p>
Abs. 2 Nr. 5	<p>Evaluation Report zu ETSI EN 319 401, REQ-7.1.1-04</p> <p>Die in der Gewerbe-Haftpflichtversicherung der ERGO Versicherung AG vereinbarte Selbstbeteiligung liegt bei 5.000 Euro je Schadensfall, das bei einer Deckungssumme je Schadensfall in Höhe von 4 Millionen deutlich unter einem Prozent liegt.</p>
	<p>Für die durch Markel International betreute Vermögensschadenhaftpflichtversicherung wurde eine Selbstbeteiligung ausgeschlossen und eine Höhe von Null Euro festgelegt.</p>
	<p>Evaluation Report zu ETSI EN 319 401, REQ-7.1.1-04</p>
§ 3	Dokumentation der Ausgabe qualifizierter Zertifikate für Vertrauensdienste
Abs. 1	<p>Die Überprüfung der Identität bzw. von Attributen erfolgt durch identity Trust Management GmbH nicht an Hand von öffentlichen und auf Dauer zugänglichen Registern oder Dokumenten.</p>
Abs. 2	<p>Evaluation Reports zu ETSI EN 319 411-1, Abs. 6.2.2; ETSI EN 319 411-2, Abs. 6.2.2</p> <p>Angaben über die Vertretungsmacht des Antragstellers für eine dritte Person, amts- und berufsbezogene oder sonstige Angaben zur Person des Antragsstellers sowie weitere personenbezogene Angaben werden zur Ausweisung in einem qualifizierten Zertifikat für elektronische Signaturen nicht erhoben.</p>
	<p>Evaluation Reports zu ETSI EN 319 411-1, Abs. 6.2.2; ETSI EN 319 411-2, Abs. 6.2.2</p>
§ 4	Vorsorge für die dauerhafte Prüfbarkeit qualifizierter Zertifikate
Abs. 3	<p>Eine beabsichtigte Betriebseinstellung im Sinne des § 16 Abs. 1 Satz 1 VDG wird der Bundesnetzagentur unverzüglich mitgeteilt.</p>
	<p>Evaluation Report zu ETSI EN 319 401, Kap. 7.12</p>

5. Prüfergebnis

Zusammenfassung der Ergebnisse

Der Identitätsfeststellungsdienst wurde einer Konformitätsbewertung gemäß den relevanten Anforderungen der Verordnung (EU) Nr. 910/2014 [eIDAS-VO] unterzogen. Die relevanten gesetzlichen Anforderungen an den Dienst zur Identitätsfeststellung werden erfüllt. Dabei wurden zusätzlich die relevanten Anforderungen des nationalen eIDAS-Durchführungsgesetzes bzw. dem darin enthaltenen Vertrauensdienstegesetz, der Vertrauensdiensteverordnung sowie die Anforderungen der Verfügung gemäß § 11 Absatz 1 VDG und der vorläufigen Anerkennung einer innovativen Identifizierungsmethode gemäß § 11 Absatz 3 VDG berücksichtigt.

Die Konformitätsbewertungsstelle bestätigt gemäß eIDAS Art. 24 (1) d), dass die Identifizierungsverfahren identity Video und identity autold eine gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten.

Aus Sicht der Konformitätsbewertungsstelle hat identity Trust Management GmbH im Verfahren identity Video ausreichende Maßnahmen umgesetzt, um dem Erfolg eines Angriffes wie in [CCC] beschrieben entgegenzuwirken.

Die jeweiligen Verfahren müssen auf nationaler Ebene anerkannt sein.

Die Konformitätsbewertung erfolgte in den zwei Schritten

- Stage 1: Dokumentenprüfung (Zeitraum 12.07.2022 bis 22.07.2022).
- Stage 2: Remote-Auditierung des Standorts Düsseldorf (25.07.2022 und 26.07.2020), Vor-Ort Audit des Rechenzentrums, in dem die zentralen Komponenten des Identitätsfeststellungsdienstes technisch betrieben werden (27.07.2022), sowie des Videocallcenters Zagreb (09.08.2022) und die Identifizierung im Verfahren identity Shop (02.08.2022).

Für das Verfahren identity Video können die Videocallcenter in Düsseldorf (identity Trust Management GmbH), und Zagreb, Kroatien (Videocallcenter M.S.S. Vertriebsgesellschaft mbH Co. KG) zum Einsatz kommen. Das Videocallcenter in Düsseldorf wird derzeit nicht produktiv genutzt und kommt nur in Notfällen (z.B. Ausfall des Callcenters in Zagreb) zum Einsatz. Das Callcenter in Düsseldorf wird im Rahmen des Überwachungsaudits geprüft.

Als Grundlage für Prüfung der Dokumente und die Durchführung der Audits wurden die aufgeführten gesetzlichen Anforderungen sowie die europäischen Standards ETSI EN 319 401, ETSI EN 319 411-1 und ETSI EN 319 411-2 herangezogen.

Die detaillierten Prüfergebnisse sind in den folgenden separaten Berichten enthalten:

- Bericht, Identifizierung von natürlichen Personen gemäß Verordnung (EU) 910/2014, identity Management, Erfüllung der Anforderungen des Amtsblatts der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Mitteilung Nr. 208/2018, Verfügung gemäß § 11 Absatz 1 VDG, Version 1.0, Datum 26.08.2022

- Evaluation Report, Identification of natural persons according to Regulation (EU) 910/2014, identity Management, Fulfilment of Requirements according ETSI EN 319 401, Version 1.0, Date 26.08.2022
- Evaluation Report, Identification of natural persons according to Regulation (EU) 910/2014, identity Management, Fulfilment of Requirements according ETSI EN 319 411-1, Version 1.0, Date 26.08.2022
- Evaluation Report, Identification of natural persons according to Regulation (EU) 910/2014, identity Management, Fulfilment of Requirements according ETSI EN 319 411-2, Version 1.0, Date 26.08.2022

Die Konformitätsbewertung wurde von Frau Karina Kutzmutz und den Herren Thomas Hueske, Christoph Sesterhenn und Sascha Zielke durchgeführt und seitens identity Trust Management GmbH durch die Herren Erkan Ciftci, Harald Jacobs und Timo Tegtmeier begleitet.

Mit Ausstellung des vorliegenden Konformitätsbewertungsberichts liegt **keine kritischen Nichtkonformitäten** oder **nicht-kritische Nichtkonformitäten** vor.

Die folgenden **Empfehlungen** wurden in der Konformitätsbewertung gegeben und in den o.g. Prüfberichten dokumentiert.

Nr.	Empfehlung	Referenz
1	In der IDvos Umgebung sollte eine Netzwerksegmentierung eingeführt werden, um sensitive Systeme (Datenbank Systeme, Filesysteme) von öffentlich erreichbaren Systemen (Applikationsserver) zu trennen.	ETSI EN 319 401, REQ-7.8-02

Verwendung von Modulen

Aufgrund der Einbindung von Modulen Dritter ergeben sich die folgenden zeitlichen Einschränkungen für das Modul zur Identitätsfeststellung natürlicher Personen für VDA. Die Überwachung der Fristen obliegt identity Trust Management GmbH.

Typ	Bezeichnung	Registrierungsnummer	Gültigkeitsende
Modul	Autoident Qualified Electronic Signature	TUVIT.97174.TSP.06.2021	28.06.2023

Nächste Konformitätsbewertung

Die nächste Konformitätsbewertung ist spätestens bis zum 27. August 2024 durchzuführen.

6. Referenzen

Gesetze

[eIDAS-VO] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic

- transactions in the internal market and repealing Directive 1999/93/EC.
- [eIDAS-DFG] 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).
- [VDV] Verordnung zur Vertrauensdiensten (Vertrauensdiensteverordnung – VDV) vom 15. Februar 2019, Bundesgesetzblatt Jahrgang 2019 Teil I Nr. 5, ausgegeben zu Bonn am 27. Februar 2019
- [Nr. 208/2018] Amtsblatt der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Mitteilungen, Qualifizierte elektronische Signatur, Teil A, Mitteilungen der Bundesnetzagentur, Mitteilung Nr. 208/2018, Verfügung gemäß § 11 Absatz 1 VDG
- [EBK KBS] Ergänzende Bewertungskriterien für Konformitätsbewertungsstellen zur Prüfung der Vorgaben der Verfügung gemäß § 11 Absatz 1 VDG, Version 1.1, Stand 13.06.2018
- [Verfügung Autold] Bundesnetzagentur für Elektrizität, Gas, Telekommunikationen, Post und Eisenbahnen, Vorläufige Anerkennung einer innovativen Identifizierungsmethode gemäß § 11 Absatz 3 VDG, Identifizierung einer natürlichen Person im Rahmen der Beantragung eines qualifizierten Zertifikates unter Nutzung einer Videoübertragung (Videoidentifizierung) mit automatisiertem Verfahren

Standards und von Interessengruppen veröffentlichte Dokumente

- [ETSI EN 319 401] ETSI EN 319 401:2018: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, V2.3.1, 2021-05.
- [ETSI EN 319 403] ETSI EN 319 403-1 V2.3.1 (2020-06): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI TS 119 403-3 V1.1.1 (2019-03): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers.
- [ETSI EN 319 411-1] ETSI EN 319 411-1 V1.3.1 (2021-05): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements.
- [ETSI EN 319 411-2] ETSI EN 319 411-2 V2.3.1 (2021-05): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

- [ETSI EN 319 412-5] ETSI EN 319 412-5 V2.3.1 (2020-04): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- [SOGIS] SOG-IS Crypto Working Group, SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Algorithms, Version 1.2, 2020-01.
- [ISO/IEC 27002] ISO/IEC 27002:2013 "Information technology – Security techniques – Code of practise for information security controls".
- [KBB AutolD] TÜV Informationstechnik GmbH, Komponenten-Konformitätsbewertungsbericht, Konformitätsbewertung einer Komponente eines Vertrauensdienstes gemäß eIDAS, Registration number: TUVIT.97174.TSP.06.2021, 28.06.2021, gültig bis 28.06.2023.
- [Zertifikat AutolD] TÜV Informationstechnik GmbH, Zertifikat für die Komponente eines Vertrauensdienstes AutolDent Qualified Electronic Signature die Erfüllung aller relevanten Anforderungen der Verordnung VO (EU) Nr. 910/2014 (eIDAS) für die Identitätsfeststellung von natürlichen Personen, Certificate ID: 97174.21, 28.06.2021, gültig bis 28.06.2023.
- [Report AutolD] TÜV Informationstechnik GmbH, Audit Report – Re-Certification – ETSI EN 319 411-2, Project ID TUVIT.97174.TSP, 2021-06-18.
- [CCC] Praktischer Angriff auf Video-Ident, Demonstration inhärenter Schwächen der videobasierten Echtheitsprüfung physischer ID-Dokumente, Martin Tschirsich, Chaos Computer Club, Version 1.2, 8. August 2022

Öffentliche Dokumente der identity Trust Management GmbH

- [AGBs Kurier Shop] Allgemeine Geschäftsbedingungen der identity Trust Management GmbH für Identifizierungsdienstleistungen in den identity Kurier Verfahren sowie identity Shop Verfahren (jeweils Stand Januar 2022)
- [AGBs IDnow] Allgemeine Geschäftsbedingungen für die Nutzung des Identifizierungsdienstes der Unternehmen der IDnow-Gruppe, Stand Januar 2022
- [CPS] Certification Practice Statement of identity Trust Management GmbH for the identification procedures identity Shop, identity Video, identity eID, identity autolD and the document signing procedures identity eSign and identity PoS version 1.7 as of 2022-05-30.

Vertrauliche Dokumente der identity Trust Management GmbH

- [ISP] Informationssicherheitsleitlinie der identity Trust Management GmbH, Version 9, 26.07.2022
- [ISP Anhang A] Informationssicherheitsleitlinie – Anhang A, Version 7, 22.02.2022
- [SiKo] Sicherheitskonzept der identity Trust Management GmbH für die Identifizierungs-Verfahren identity Shop, identity PoS, identity Video,

	identity eID, identity autoID - Allgemeiner Teil - Version 3.2 vom 28.07.2022.
[SiKo_Anlage 1]	Anlage 1 zum Sicherheitskonzept der identity Trust Management GmbH für das Identifizierungs-Verfahren identity Shop vom 28.07.2022.
[SiKo Anlage 2]	Anlage 2 zum Sicherheitskonzept der identity Trust Management GmbH für die Identifizierungs-Verfahren identity PoS vom 28.07.2022.
[SiKo Anlage 3]	Anlage 3 zum Sicherheitskonzept der identity Trust Management GmbH für das Identifizierungs-Verfahren identity Video vom 28.07.2022.
[SiKo Anlage 4]	Anlage 4 zum Sicherheitskonzept der identity Trust Management GmbH für das Identifizierungs-Verfahren identity eID vom 28.07.2022.
[SiKo Anlage 5]	Anlage 5 zum Sicherheitskonzept der identity Trust Management GmbH für das Identifizierungs-Verfahren identity autoID vom 28.07.2022.
[Rechtskatastar]	Verzeichnis der anwendbaren, rechtlichen, regulatorischen, selbst-aufgelegten und vertraglichen Anforderungen, Version 4 vom 06.01.2022
[ArbeitsplatzRL]	Richtlinie zum Verhalten am Arbeitsplatz, Version 8 vom 20.01.2022
[Termination Plan]	Termination Plan für die Verfügbarkeit der Räumlichkeiten und des Personals, Version 2.0 vom 01.02.2022
[BCM-Richtlinie]	Richtlinie zur Aufrechterhaltung der Informationssicherheit bei Notfällen, Version 1, 22.02.2022
[Entwicklungs_RL]	Richtlinie zur sicheren Softwareentwicklung, Version 9, 25.02.2022
[Change-MGMT]	Richtlinie zum Change-Management, Version 6, 06.01.2022
[Zutritt-Zugang]	Richtlinie zur Regelung des Zutritts zu Räumen, Gebäuden und Liegenschaften, sowie dem Zugang zu technischen Systemen, Version 10, 22.02.2022
[Risiko-Richtlinie]	Richtlinie zum Risikomanagement, Version 6, 06.01.2022
[Risikomatrix]	Risikomatrix, Version 20, 14.07.2022
[Risikoübernahme]	Risikoübernahme, 13.01.2022
[Bestellungen_Roles]	Bestellungen von Personen in Trusted Roles: Sicherheitsbeauftragter (20.12.2012), stellvertretenden Sicherheitsbeauftragten (20.08.2020) System Administratoren (21.09.2020), System Auditor (20.08.2020).
[Vertrag ScanPlus]	Vertrag über Managed IT-Services, dated 17.03.2014

- [TOM ScanPlus] Technische und organisatorische Maßnahmen ScanPlus, dated March 2018
- [Pentest] SRC, Zusammenfassung der Ergebnisse des externen Penetrations-tests, identity Trust Management GmbH, Version 1.0, 25.04.2022
- [Vertrag IDnow] Framework Agreement zwischen IDnow GmbH und identity Trust Manamagent AG, unterzeichnet am 04.11.2021

Vertrauliche Dokumente der ScanPlus GmbH

- [Zugriffskontrolle] ScanPlus GmbH, Richtlinie Zugriffskontrolle, Version 3.1
- [Zugriffsverwaltung] ScanPlus GmbH, Zuteilung von Benutzerzugängen, Version 4.0, 04.03.2021
- [Zugriffswiderruf] ScanPlus GmbH, Entzug oder Anpassung von Nutzerzugängen, Version 5.0, 13.07.2021

Evaluation Reports der Konformitätsbewertungsstelle

- [ER VFG] Bericht, Identifizierung von natürlichen Personen gemäß Verordnung (EU) 910/2014, identity Management, Erfüllung der Anforderungen des Amtsblatts der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Mitteilung Nr. 208/2018, Verfügung gemäß § 11 Absatz 1 VDG, Version 1.0, Datum 26.08.2022
- [ER EN 319 401] SRC, Evaluation Report, Identification of natural persons according to Regulation (EU) 910/2014, identity Management, Fulfilment of Requirements according ETSI EN 319 401, Version 1.0, Date 26.08.2022
- [ER EN 319 411-1] SRC, Evaluation Report, Identification of natural persons according to Regulation (EU) 910/2014, identity Management, Fulfilment of Requirements according ETSI EN 319 411-1, Version 1.0, Date 2022-08-26
- [ER EN 319 411-2] SRC, Evaluation Report, Identification of natural persons according to Regulation (EU) 910/2014, identity Management, Fulfilment of Requirements according ETSI EN 319 411-2, Version 1.0, Date 2022-08-26

Ende des Konformitätsbewertungsberichts.