Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: +43 1 503 19 63–0
Fax: +43 1 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: +43 316 873-5514
Fax: +43 316 873-5520

https://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461 ZVR: 948166612 UID: ATU60778947

A-SIT Konformitätsbewertungsstelle
Tel.: +43 1 503 19 63-0
E-Mail: office@a-sit.at

Merkblatt: Konformitätsbewertung gemäß Art. 20 eIDAS-VO

Tätigkeiten der Konformitätsbewertungsstelle

A-SIT führt Konformitätsbewertungen unter Art. 20 eIDAS-VO[1] als durch die Akkreditierung Austria gemäß ÖVE/ÖNORM EN ISO/IEC 17065[2] iVm ETSI EN 319 403-1[3] (inkl. ETSI TS 119 403-2[4] und ETSI TS 119 403-3[5]) akkreditierte Konformitätsbewertungsstelle durch. In einem Konformitätsbewertungsverfahren wird die Konformität qualifizierter Vertrauensdiensteanbieter (VDA) und der von ihnen erbrachten qualifizierten Diensten mit den Anforderungen geprüft und bewertet. Die Anforderungen umfassen die Art. 15, Art. 19 und Art. 24 eIDAS-VO, sowie je nach angebotenem Vertrauensdienst auch Art. 28, Art. 32, Art. 34, Art. 38, Art. 42, Art. 44, Art. 45, Anhang I, Anhang III und Anhang IV eIDAS-VO, aber auch mitgeltende Normen bzw. international anerkannte Standards von geeigneten und den Mitgliedstaaten benannten öffentlichen oder privaten Stellen. Darüber hinaus bescheinigt A-SIT die Resultate gegenüber der Aufsichtsstelle. Wenn keine Normen für die Sicherheitsbewertung vorliegen, die durch die Kommission im Wege von Durchführungsrechtsakten festgelegt wurden, wird das Verfahren gemäß Art. 24 eIDAS-VO durchgeführt und nach dem Stand der Technik beurteilt.

Zweck dieses Merkblatts

Zum Erlangen einer positiven Bewertung sind der Konformitätsbewertungsstelle im Regelfall organisatorische, technische und rechtliche Dokumente vorzulegen, die sowohl formale als auch inhaltliche Anforderungen erfüllen müssen (siehe (C)).

---

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

2 Konformitätsbewertung - Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren (ISO/IEC 17065:2012)

3 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers

4 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates

5 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

Das Merkblatt soll den Antragstellern die Vorbereitung dieser Dokumente und damit eine zügige Abwicklung des Verfahrens zur Konformitätsbewertung qualifizierter VDAs erleichtern. Daher enthält dieses Merkblatt generelle Hinweise; die tatsächlichen Erfordernisse hängen vom konkreten Einzelfall ab.

(A) Warum eine Konformitätsbewertung?

Für die Verleihung des Status „qualifizierter Vertrauensdiensteanbieter“[6] sind eine positive Konformitätsbewertung, sowie eine Vorlage des Konformitätsbewertungsberichts bei einer Aufsichtsstelle gemäß Art. 17 eIDAS-VO erforderlich. Qualifizierte Vertrauensdienste werden in Vertrauenslisten gem. Art. 22 eIDAS-VO geführt und sind EU- bzw. EWR-weit anerkannt. Darüber hinaus werden qualifizierte Vertrauensdienste mit dem „EU trust mark“ als anerkannte, vertrauenswürdige Online-Service eingestuft, welche die Anforderungen der eIDAS-VO erfüllen. Zum Erhalt dieses Status ist ein Überwachungsaudit innerhalb eines Jahres erforderlich und die Konformität muss mindestens alle 24 Monate neu überprüft und bestätigt werden.

Art. 20 Abs. 1 eIDAS-VO: Qualifizierte Vertrauensdiensteanbieter werden mindestens alle 24 Monate auf eigene Kosten von einer Konformitätsbewertungsstelle geprüft. Zweck dieser Prüfung ist es nachzuweisen, dass sie und die von ihnen erbrachten qualifizierten Vertrauensdienste die in dieser Verordnung festgelegten Anforderungen erfüllen. Die qualifizierten VDAs legen der Aufsichtsstelle den entsprechenden Konformitätsbewertungsbericht innerhalb von drei Arbeitstagen nach Empfang vor.

Art. 3 lit. 16 eIDAS-VO: Ein Vertrauensdienst ist ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und aus Folgendem besteht:

a) Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, und Diensten für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten oder

b) Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder

c) Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten.

Art. 3 lit. 17 eIDAS-VO: Qualifizierter Vertrauensdienst ist ein Vertrauensdienst, der die einschlägigen Anforderungen dieser Verordnung erfüllt.

Art. 3 lit. 19 eIDAS-VO: Vertrauensdiensteanbieter (VDA) ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter VDA erbringt.

Art. 3 lit. 20 eIDAS-VO: Qualifizierter VDA ist ein VDA, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde.

Im Rahmen der Konformitätsbewertungen nach eIDAS werden ausschließlich qualifizierte Vertrauensdiensteanbieter (bzw. Anbieter die den Status eines qualifizierten Vertrauensdiensteanbieters anstreben) gemäß Art. 20 der eIDAS-VO geprüft.

Die Konformitätsbewertung nach eIDAS wird von einem qualifizierten VDA (bzw. einem VDA der diesen Status anstrebt) beauftragt, der einen Konformitätsbewertungsbericht gemäß Art. 20 Abs. 1 und Art. 21 Abs. 1 eIDAS-VO der Aufsichtsstelle vorlegen muss.

Die Ausstellung einer positiv bewerteten Konformitätsbewertung setzt die Erbringung hinreichender Nachweise voraus, dass im Antrag festgelegte sowie gesetzliche, normative oder darüber hinaus spezifizierte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Dienstleistung oder eine Stelle erfüllt sind.

Nach erfolgter Prüfung wird ein Konformitätsbewertungsbericht und eine Konformitätsbewertungs-bescheinigung ausgefertigt. Der Konformitätsbewertungsbericht dient i.S.d. Artikels 20 der eIDAS-VO zur Vorlage an eine Aufsichtsstelle.

[6] Vgl. Art. 3 Z 20 VO (EU) Nr. 910/2014 (eIDAS) „Qualifizierter Vertrauensdiensteanbieter“ ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde.

(B) Welche Unterlagen sind für die Konformitätsbewertung vom Antragsteller beizubringen?

Ein formeller Antrag auf Konformitätsbewertung, welcher enthält:

(i) Name, Anschrift und Rechtsform des Antragstellers

(ii) Elektronische Erreichbarkeit des Antragstellers

(iii) Name, Anschrift und Rechtsform des Herstellers bzw. Anbieters der zu bewertenden Produkte, Prozesse oder Dienstleistungen

(iv) Beschreibung der zu bewertenden Produkte, Prozesse oder Dienstleistungen

(v) Das Konformitätsbewertungsverfahren, das anzuwenden ist

(vi) Erklärung des Antragstellers der zu bewertenden Produkte, Prozesse oder Dienstleistungen, dass er damit einverstanden ist, die Konformitätsbewertungsanforderungen zu erfüllen und alle für die Begutachtung der zu bewertenden Prozesse oder Dienstleistungen erforderlichen Informationen zur Verfügung zu stellen. Dies beinhaltet auch Informationen über alle ausgegliederten Prozesse, die vom Antragsteller genutzt werden und die die Konformität mit den Anforderungen beeinflussen

(vii) Sowie falls anwendbar: anerkennbare Zertifikate, Prüfberichte oder Konformitätsbewertungs-bescheinigungen anderer Konformitätsbewertungsstellen.

Angabe (im Antragsformular anzukreuzen), welche Anforderungen aus relevanten Europäischen Normen auf Grund der erbrachten Dienste neben denen der eIDAS-VO erfüllt werden:

- **ETSI EN 319 401 V2.3.1 (2021-05):** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (Anmerkung: generell für alle Vertrauensdienste anwendbar)
- **ETSI EN 319 411-1 V1.4.1 (2023-10):** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- **ETSI EN 319 411-2 V2.5.1 (2023-10):** 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 319 421 V1.2.1 (2023-05):** Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- **ETSI EN 319 521 V1.1.1 (2019-02):** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
- **ETSI EN 319 531 V1.1.1 (2019-01):** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers
- **ETSI TS 119 431-1 V1.2.1 (2021-05):** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
- **ETSI TS 119 441 V1.2.1 (2023-10):** Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services
- **ETSI TS 119 461 V1.1.1 (2021-07):** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
- **ETSI TS 119 495 V1.6.1 (2022-11):** Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking

Für die Durchführung der Konformitätsbewertung ist die Bereitstellung ausführlicher Unterlagen zum Vertrauensdiensteanbieter und den angebotenen Vertrauensdiensten notwendig, insbesondere:

(i) Zertifizierungsrichtlinie (CP), Zertifizierungspraxisrichtlinie (CPS)

(ii) Sicherheitskonzept bzw. ISMS-Richtlinie

(iii) Risikoanalyse

(iv) PKI Hierarchie

(v) Angaben zu verwendeten Sicherheitsmodulen

(vi) Angaben zu externen Dienstleistern (Verträge, SLA, …)

(vii) Vereinbarungen mit Kunden (AGB, Signaturvertrag, Unterweisung, …)

(viii) Verträge mit Registrierungsstellen

(ix) Nachweis der Haftpflichtversicherung

(x) Gegebenenfalls PKI Disclosure Statement

Darüberhinausgehende Unterlagen sind abhängig von der Art und Umsetzung der angebotenen Vertrauensdienste.

Alle eingereichten Unterlagen sind mit einem Deckblatt zum Antrag kurz aber vollständig, mit Referenzen auf eingereichte Unterlagen oder andere relevante Dokumente (inkl. relevante Kapitel/Abschnitte falls angebracht) darzustellen.

Zertifikate nach Evaluierungsnormen zu einzelnen Komponenten sind dabei allein nicht ausreichend. Das bedeutet, es ist der Nachweis zu erbringen, dass die zu bewertenden Eigenschaften erfüllt sind (z.B. durch Sicherheitsvorgaben, Evaluierungs- bzw. Zertifizierungsberichte etc.).

Auch sind alle weiteren Umstände zu erklären und zu belegen, welche die technisch begründete Entscheidung über die Gültigkeitsdauer der Konformitätsbewertung beeinflussen.

Sind die vorgelegten Materialien in formaler oder inhaltlicher Hinsicht unzureichend, ist die Ausstellung einer positiven Konformitätsbewertung nicht möglich.

(C) Wie wird die Konformitätsbewertung durchgeführt?

1) Antragsbewertung: Die Konformitätsbewertungsstelle prüft den Antrag. Etwaige Unklarheiten werden mit dem Antragsteller geklärt und ggf. wird der Antragsteller zur Übermittlung eines nachgebesserten Antrags aufgefordert.

Bevor ein neues Konformitätsbewertungsverfahren gestartet wird, muss sichergestellt sein, dass:

- alle notwendigen Informationen zum Antragsteller und Hersteller bzw. Anbieter sowie auch über die zu bewertenden Produkte, Prozesse oder Dienstleistungen vorliegen
- das anzuwendende Konformitätsbewertungsverfahren und damit die relevanten Normen bzw. normativen Vorgaben klar definiert sind
- das anzuwendende Konformitätsbewertungsverfahren in den Kompetenzbereich der Konformitätsbewertungsstelle fällt und ausreichende Ressourcen zur Durchführung des Verfahrens verfügbar sind.

Sind diese Voraussetzungen nicht vollständig erfüllt, ist die Konformitätsbewertungsstelle berechtigt, den Antrag abzuweisen.

2) Inhaltliche Prüfung und Bewertung: Die Konformitätsbewertungsstelle ist verantwortlich für die Durchführung des Konformitätsbewertungsverfahrens gemäß der akkreditierten Vorgehensweise und die Ausfertigung des Konformitätsbewertungsberichts auf der Grundlage der vorgelegten Unterlagen, des durchgeführten Vor-Ort-Audits und der Checkliste aus ETSI TR 119 411-4.

Die Konformitätsbewertungsstelle ist berechtigt, vom Antragsteller oder vom Hersteller zu bewertender Komponenten, Methoden oder Verfahren ergänzende Informationen und Nachweise zu fordern, die zur zuverlässigen Wahrnehmung der Aufgaben als Konformitätsbewertungsstelle dienen.

(D) Was beinhalten Konformitätsbewertungsberichte und -bescheinigungen?

Konformitätsbewertungsbericht. Ein detaillierter Konformitätsbewertungsbericht wird für jedes Konformitätsbewertungsverfahren angefertigt und dient zur Vorlage an eine Aufsichtsstelle. Konformitätsbewertungsberichte enthalten detaillierte Beschreibungen der durchgeführten Begutachtungen und deren Ergebnisse.

Konformitätsbewertungsbescheinigung. Konformitätsbewertungsbescheinigungen sind Dokumente, die die Erfüllung der Konformität mit den festgelegten Anforderungen bestätigen. Eine Konformitätsbewertungsbescheinigung wird auf Wunsch des Antragstellers ausgefertigt. Sie kann auf Wunsch des Antragstellers mit Einverständnis des Herstellers bzw. Anbieters veröffentlicht werden.

Ein Konformitätsbewertungsbericht bzw. eine Konformitätsbewertungsbescheinigung enthält mindestens folgende Angaben:

- Bezeichnung des Dokuments (Konformitätsbewertungsbericht oder Konformitätsbewertungsbescheinigung)
- Datum der Ausstellung und eindeutige Identifizierung des Dokuments
- Bezeichnung der Konformitätsbewertungsstelle: „Konformitätsbewertungsstelle A-SIT“
- Bezeichnung des Auftraggebers und Herstellers bzw. Anbieters (falls unterschiedlich)
- Bezeichnung des angewendeten Konformitätsbewertungsverfahrens
- Bezeichnungen der bewerteten Produkte, Prozesse bzw. Dienstleistungen
- Geltungsbereich der durchgeführten Konformitätsbewertung
- Geltungszeitraum der durchgeführten Konformitätsbewertung
- Ergebnisse der Konformitätsbewertung einschließlich einer Konformitätserklärung zu den vereinbarten Kriterien, sowie Angabe aller Fehler und Abweichungen von den vereinbarten Kriterien
- Das A-SIT Logo, das Akkreditierungszeichen der Konformitätsbewertungsstelle, sowie Name und elektronische Signatur des Gesamtleiters

Auf Anfrage kann eine Liste mit von A-SIT durchgeführten Konformitätsbewertungen angefordert werden. Sowohl Konformitätsbewertungsberichte als auch –bescheinigungen werden von A-SIT jedoch nicht an Dritte weitergegeben oder veröffentlicht (Ausnahme: Bericht an Aufsichtsstelle).

(E) Gültigkeit der Konformitätsbewertung

Die eIDAS-VO sieht keine formelle Gültigkeitsdauer für Konformitätsbewertungen vor, sondern es werden gemäß Art. 20 Abs. 1 der eIDAS-VO qualifizierte Vertrauensdiensteanbieter mindestens alle 24 Monate von einer Konformitätsbewertungsstelle erneut geprüft. Spätestens ein Jahr nach Durchführung der Konformitätsbewertung ist ein Überwachungsaudit durch die Konformitätsbewertungsstelle vorgesehen.

Sofern sich Umstände ergeben, welche den Aussagen der Konformitätsbewertung widersprechen, sind diese der Aufsichtsstelle unverzüglich zur Kenntnis zu bringen.

(F) Geheimhaltung durch A-SIT

A-SIT verfolgt eine strenge Politik der Vertraulichkeit.

Das Non-Disclosure-Statement (NDS) ist auf der Webseite von A-SIT verfügbar (https://www.a-sit.at/pdfs/nds_asit.pdf).

Um den Anforderungen seitens der betroffenen Vertrauensdiensteanbieter gerecht zu sein, händigt A-SIT auf Wunsch eine unterfertigte Fassung des NDS aus. Andere Non-Disclosure-Agreements (NDAs) geht A-SIT nicht ein. Das bedeutet, vom VDA oder seinen Lieferanten selbst erstellte Vertraulichkeitserklärungen bzw. NDAs sind daher nicht notwendig.

Wien, Oktober 2023

A-SIT Zentrum für sichere Informationstechnologie – Austria