Kriterienkatalog und Vorgehensweise zur Zertifizierung von Vertrauensdiensten gemäß eIDAS

datenschutz cert GmbH

Version 1.0

datenschutz cert

Inhaltsverzeichnis

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
1.0	07.12.2021		Erstellung	SM

Dokumenten-Überwachungsverfahren

Status	Prozess-/Dokumentbesitzer	Version
Final	Dr. Sönke Maseberg	1.0

1. Zertifizierung von Vertrauensdiensten

Die eIDAS-Verordnung regelt EU-weit Vertrauensdienste. Damit gibt eIDAS den Rechtsrahmen für elektronische Signaturen, Siegel, Zeitstempel sowie Dienste für Zustellung elektronischer Einschreiben und Dienste für Website-Authentisierung vor. Die qualifizierten Vertrauensdiensteanbieter müssen mit den qualifizierten Vertrauensdiensten geprüft werden – durch akkreditierte Konformitätsbewertungsstellen. Die datenschutz cert GmbH ist einer der bei der DAkkS akkreditierten Konformitätsbewertungsstellen nach Artikel 3 Nummer 18 der Verordnung (EU) Nr. 910/2014.

Darüber hinaus regelt die eIDAS-Verordnung auch die Feststellung der Konformität qualifizierter elektronischer Signatur- oder Siegelerstellungseinheiten mit den Anforderungen des Anhangs II der Verordnung (EU) 910/2014 – durch eine eIDAS-Zertifizierungsstelle. Die datenschutz cert GmbH ist eine bei der Bundesnetzagentur anerkannte Zertifizierungsstelle nach Art. 30 Abs. 1 der Verordnung (EU) 910/2014 i.V.m. § 17 des Vertrauensdienstegesetzes (VDG).

Die Zertifizierungsstelle der datenschutz cert GmbH bietet Unternehmen die Zertifizierung von Produkten, Systemen, Dienstleistungen und Prozessen aus dem Bereich Informationstechnik und Datenschutz an. Im Folgenden wird vereinfachend von der Zertifizierung von Produkten gesprochen. Die Zertifizierung erfolgt auf der Grundlage von normativen Dokumenten wie Rechtsvorschriften, Normen oder technischen Spezifikationen, welche Anforderungen an Produkte festgelegen. Die Unternehmen haben mit einer Zertifizierung durch einen unabhängigen Dritten die Möglichkeit zu dokumentieren, dass ihre Produkte die festgelegten Anforderungen erfüllen.

Die Zertifizierungsstelle der datenschutz cert GmbH ist auf Basis der DIN EN ISO/IEC 17065 für die Zertifizierung von Produkten akkreditiert.

Das vorliegende Dokument beschreibt die Vorgehensweise für die Vergabe der Zertifikate für qualifizierte Vertrauensdiensteanbieter und der von ihnen erbrachten qualifizierten Vertrauensdienste, die in diesen akkreditierten Bereich fallen. Es soll Unternehmen, die eine Zertifizierung bei der datenschutz cert GmbH durchführen lassen wollen, alle notwendigen Informationen geben.

Bremen, den 07.12.2021

Dr. Sönke Maseberg
Geschäftsführer
datenschutz cert GmbH

2. eIDAS

eIDAS steht für „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 regelt elektronische Identifizierungsmittel für natürliche und juristische Personen sowie Vertrauensdienste. Damit gibt eIDAS den Rechtsrahmen für elektronische Signaturen, Siegel, Zeitstempel sowie Dienste für Zustellung elektronischer Einschreiben und Dienste für Website-Authentisierung vor.

eIDAS sieht im Detail folgende Dienste vor:

- Erstellung
  - qualifizierter Zertifikate für elektronische Signaturen
  - qualifizierter Zertifikate für elektronische Siegel
  - qualifizierter Zertifikate für die Website-Authentifizierung
  - qualifizierter elektronischer Zeitstempel
  - qualifizierter elektronischer Signaturen
  - qualifizierter elektronischer Siegeln
- Überprüfung und Validierung
  - qualifizierter elektronischer Signaturen, Siegeln, Zeitstempeln und zugehöriger qualifizierter Zertifikate
  - qualifizierter Zertifikate für die Website-Authentifizierung
- Aufbewahrung
  - qualifizierter elektronischer Signaturen, Siegeln oder zugehöriger qualifizierter Zertifikate
- Zustellung
  - elektronischer Einschreiben

3. Kriterienkatalog

Für die Prüfung und Zertifizierung von Vertrauensdiensteanbietern und den von ihnen angebotenen Vertrauensdiensten werden ETSI-Normen herangezogen:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for Trust Service Providers issuing EU qualified certificates
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing time-stamps
- ETSI EN 319 521: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI TS 119 511: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- ETSI EN 319 531: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers

4. Konformitätsbewertung

4.1. Laufzeiten

Jedes Zertifizierungsverfahren besteht aus folgenden Phasen:

- Erst-Begutachtung;
- Überwachung (1 Jahr nach Erst-Begutachtung);
- Re-Begutachtung (2 Jahre nach Erst-Begutachtung).

4.2. Konformitätsbewertung

Die Konformitätsbewertung wird als Prozess mit vier Phasen durchgeführt.

- Phase 1: Angebotsannahme und Einreichung der erforderlichen Dokumente

  Das Projekt beginnt mit der Angebotsannahme. Im Anschluss daran wird die datenschutz cert GmbH eine Identifikationsnummer (ID) für das Verfahren vergeben, unter der alle Informationen zum Projekt ausgetauscht werden sollen. Es wird ein Zeitplan abgestimmt. Es wird die Referenzdokumentation zur Verfügung gestellt.
- Phase 2: Erstellung des Stage-1 Berichtes

  Nach Bereitstellung der erforderlichen Dokumentation, die die Art und Weise beschreibt, in der der Vertrauensdienst erbracht wird, prüft die datenschutz cert GmbH die Dokumentation auf der Grundlage der Verordnung (EU) 910/2014 und der anwendbaren europäischen Normen und stellt dabei fest, ob, und wenn ja, welche Abweichungen vorhanden sind oder welche Informationen fehlen.
- Phase 3: Audit und Stage-2 Bericht

  Nachdem mit dem Stage-1 Bericht festgestellt wurde, dass durch die vorgesehene Art und Weise der Diensterbringung des Vertrauensdienstes alle normativen und regulatorischen Anforderungen erfüllt werden können, wird in einem Audit vor Ort die Umsetzung der in den zur Verfügung gestellten Dokumenten beschriebenen Maßnahmen geprüft. Die Prüfergebnisse werden in einem Auditbericht (Stage-2 Bericht) festgehalten. Im Audit wird festgestellt, ob die in der Dokumentation beschriebenen Verfahren, Regeln und Maßnahmen tatsächlich angewendet werden. Abweichungen werden aufgezeichnet und bewertet und führen ggf. zu einem Nachbesserungsverlangen.
- Phase 4: Konformitätsbewertungsbericht

  Der Konformitätsbewertungsbericht über den Vertrauensdienst wird parallel zu den Aktivitäten der Phasen 1 bis 3 erstellt. Für den Fall, dass weder der Stage-1 Bericht noch der Stage-2 Bericht Hauptabweichungen feststellen und die Summe der ggf. vorhandenen Nebenabweichungen nicht gegen eine ordnungsgemäße Erbringung des Dienstes spricht, stellt der Konformitätsbewertungsbericht die Erfüllung der Anforderungen der Verordnung (EU) 910/2014 fest. Andernfalls stellt er fest, welche Anforderung nicht erfüllt ist, und gibt eine Begründung für diese Feststellung an.

4.3. Zertifikatsliste

Eine Liste unserer erteilten Zertifizierungen kann abgerufen werden unter: https://www.datenschutz-cert.de/zertifikatslisten. Aus der Liste sind der Antragsteller, der Geltungsbereich, die Zertifikats-ID sowie die Gültigkeit der Zertifizierung ersichtlich.

4.4. Entzug, Aussetzen oder Einschränken eines Zertifikates

Das Zertifikat wird entzogen, wenn der Antragsteller nachhaltig gegen die Zertifizierungsvoraussetzungen verstößt. Ein solcher Verstoß liegt insbesondere vor, wenn

- der zertifizierte Untersuchungsgegenstand in der beschriebenen Weise verändert wurde und der Anbieter keine Prüfung ermöglicht,
- im Rahmen der Prüfung nicht die für die Vergabe des Zertifikats erforderlichen Voraussetzungen erfüllt werden,
- der Antragsteller aufgrund drohender oder eingetretener Insolvenz einen zuverlässigen Geschäftsbetrieb nicht mehr aufrechterhalten kann oder
- die Zertifizierungskosten nicht spätestens innerhalb von 4 Wochen nach Abschluss der Zertifizierung gegenüber der Zertifizierungsstelle beglichen werden.

Die Zertifizierungsstelle teilt dem Antragsteller die Gründe des Zertifikatsentzugs mit. Im Falle des Entzuges wird das über die Zertifikatsliste online unter www.datenschutz-cert.de veröffentlichte Zertifikat auf den Status als entzogen gesetzt und spätestens nach 4 Wochen aus der Liste entfernt. Der Entzug des Zertifikates kann auch anderweitig veröffentlicht werden.

Ferner kann die datenschutz cert GmbH Zertifikate aussetzen, wenn eine wesentliche Anforderung des Regelwerkes nicht erfüllt wird (max. Aussetzung: 6 Monate), oder einschränken, wenn für diesen ausgeschlossenen Teil wesentliche Anforderung des Regelwerkes nicht erfüllt werden (Einschränkung des Geltungsbereiches). Im Anschluss an eine Aussetzung erfolgt entweder die Behebung unter Berücksichtigung entsprechender Nachweise (mit Wiederherstellung) oder die Zurückziehung des Zertifikates.

4.5. Ablauf eines Zertifikates

Soweit das Zertifikat nach Ablauf der Gültigkeit entfällt, hat der Anbieter dafür zu sorgen, dass das Logo und sämtliche Hinweise auf eine gültige Zertifizierung aus den genutzten Medien unverzüglich entfernt werden.

4.6. Kosten und Gebühren

Kosten fallen einerseits für die Auditierung, andererseits für die Zertifizierung an.

Für die Zertifizierung veranschlagt die datenschutz cert GmbH Kosten/ Gebühren. Die einmaligen Zertifizierungskosten gelten für die gesamte Laufzeit des Zertifikats (i.d. R. drei Jahre) und umfassen

- Prüfbegleitung des Auditors durch die Zertifizierungsstelle;

- Ausstellung des international gültigen Zertifikats, sofern das ISMS zertifizierungsfähig ist, in deutscher Sprache;
- Darstellung Ihres Zertifikats in der Zertifikatsliste unter www.datenschutz-cert.de;
- Übergabe Ihres Zertifikats.

Neben den Zertifizierungskosten fallen Kosten für die Auditierung an, wobei der Aufwand für die Auditierung stark von der Komplexität des Untersuchungsgegenstands und der Anzahl der Mitarbeiter im Geltungsbereich abhängt. Als Orientierung bietet sich die für alle akkreditierten Zertifizierungsstellen bindende Norm ISO/IEC 27006 an, in der Richtwerte für die Audittage vor Ort angegeben werden. Zu beachten ist, dass diese Werte in der Tabelle für die Audittage vor Ort nur einen Anhaltspunkt darstellen und dass der Aufwand für die Vor- und Nachbereitung, den ausführlichen Auditreport sowie das Projektmanagement zusätzlich zu berücksichtigen sind. Da diese Werte nur einen Anhaltspunkt bieten können, sprechen Sie uns für ein konkretes Angebot bitte einfach an!

Jährliche Überwachungsaudits zur Aufrechterhaltung mit dem Auditor werden separat berechnet; alternativ können wir diese gerne in die Kalkulation aufnehmen, so dass wir Ihnen ein Angebot zur Auditierung und Zertifizierung über die gesamte Laufzeit des Zertifikats unterbreiten können.

4.7. Anfrageformular

Sofern Sie Interesse an einer Zertifizierung haben, sprechen Sie uns bitte an! Sie können auch das Anfrageformular ausfüllen, das die für uns wichtigen Angaben enthält. Das Anfrageformular können Sie herunterladen unter: http://www.datenschutz-cert.de.

4.8. AGB und KBP

Im Falle eines Vertragsschlusses gelten ausschließlich unsere Allgemeinen Geschäftsbedingungen (AGB) sowie unsere Konformitätsbewertungsordnung (KBO), die Sie unter https://www.datenschutz-cert.de/ueber-uns/agb.html abrufen können.

5. Anforderungen an einen Auditreport

Ein Auditreport zur Vorlage bei der Zertifizierungsstelle muss inhaltlich mindestens zu folgenden Aspekten Stellung beziehen:

- Organisatorische und formale Angaben zum Audit:
  - das mit der Auditierung angestrebte Zertifikat;
  - untersuchte Organisation, Name, Anschrift, Standort;
  - genaue Bezeichnung des Untersuchungsgegenstands, Abgrenzung zu den nicht auditierten Bereichen;
  - Auditoren (Recht/Technik), Name, Anschrift;
  - Zeitraum der Auditierung;

- Angewandte Methodik: z.B. Prüfung von Dokumenten des Auftraggebers, Führung von Mitarbeitergesprächen, Durchführung von Stichproben vor Ort (Site Visit) oder Plausibilitätstests;
- Grundlagen der Auditierung:
  - eingesehene Dokumente;
  - befragte Abteilungen/Arbeitsbereiche/Unternehmensorgane;
  - Gegenstand der Stichproben;
  - Ortsbesichtigung, Standort, Adresse, Dauer, Teilnehmer;
- Erklärung der Auditoren zur Unabhängigkeit und Unparteilichkeit;
- Kurzdarstellung des Untersuchungsgegenstands;
- Zusammenstellung des für den konkreten Auditgegenstand anwendbaren Prüfkriterien/Anforderungen;
- Auditergebnisse:
  - Prüfung und Bewertung aller Prüfpunkte des Kriterienkatalogs;
- Votum des Auditors mit:
  - Zusammenfassung der Auditergebnisse / Management Summary;
  - Vorschlag an die Zertifizierungsstelle.

6. Über die datenschutz cert GmbH

Die datenschutz cert GmbH bietet Konformitätsbewertungen auf dem Gebiet des Datenschutzes und der Informationssicherheit an. Diese Konformitätsbewertungen schließen sowohl Prüfaktivitäten als auch Zertifizierungstätigkeiten ein – einerseits für IT-Systeme und -Produkte und andererseits für Verfahren und Managementprozesse.

Die datenschutz cert GmbH ist ein Unternehmen der datenschutz nord-Gruppe. Sitz der Gesellschaft ist Bremen. Geschäftsführer ist Dr. Sönke Maseberg. Die Unternehmen der datenschutz nord Gruppe sind inhabergeführt.

6.1. Leitlinien

Die datenschutz cert GmbH bietet Konformitätsbewertungen unter folgenden grundsätzlichen Leitlinien an:

6.1.1. Unabhängigkeit und Unparteilichkeit

Wir sind unabhängig und unparteilich. Es gilt das übergeordnete Interesse und die vorrangige Pflicht, Auditierungen, Evaluierungen, Zertifizierungen und Bestätigungen entsprechend den Vorgaben frei von internen und externen kommerziellen, finanziellen und sonstigen Zwängen durchzuführen. Maßstab ist das jeweilige Kriterienwerk. Zudem führen wir keinerlei Beratung durch.

Wir haben einen "Ausschuss zur Sicherstellung der Unparteilichkeit der datenschutz cert GmbH" (Ausschuss) etabliert, mit dem die grundsätzlichen Regelungen zur

Unabhängigkeit und Unparteilichkeit der Zertifizierungstätigkeiten diskutiert und durchgeführte Zertifizierungsprozesse auf ihre Unabhängigkeit hin überprüft werden.

Zur Gewährleistung der Unabhängigkeit und Unparteilichkeit unserer erteilten Zertifikate setzen wir für den Auditierungs- und Zertifizierungsprozess darüber hinaus regelmäßig externe Fachbegutachter ein.

6.1.2. Vertraulichkeit

Wir sichern Ihnen Vertraulichkeit zu.

6.1.3. Offenheit und Transparenz

Wir sind offen und transparent hinsichtlich unserer Tätigkeiten, d.h.

- wir kommunizieren klar und unmissverständlich, was und nach welchen Regeln geprüft und zertifizieren wird;
- unsere Zertifikate und Auditreports sind klar und verständlich formuliert;
- wir veröffentlichen die zugrundeliegenden Regelwerke – sofern nicht durch Copyright geschützt;
- wir benennen klar, wofür wir akkreditiert sind;
- wir lassen uns selber regelmäßig auditieren;
- wir sind offen für alle Anfragen und Beschwerden: Wenn Sie Fragen zu einem von uns erteilten Zertifikat haben oder potentiell den Missbrauch eines Zertifikats vermuten: Bitte sprechen Sie uns an. Wir sichern Ihnen Vertraulichkeit zu und gehen der Sache nach. Wir informieren Sie über den Stand der Untersuchung sowie den Abschluss.

6.1.4. Datenschutz

Wir kommen aus dem Datenschutz. Jede Art von Konformitätsprüfung wird – im Rahmen des jeweiligen Untersuchungsgegenstands – unter den besonderen Aspekten des Datenschutzes beleuchtet. Dadurch stellen wir sicher, dass die von uns geprüften und bewerteten IT-Produkte und -Systeme den Anforderungen des Datenschutzes genügen.

Unser Anspruch ist, dass sich "datenschutz cert-ifizierte" Produkte und Prozesse etablieren und für unsere Kunden einen Mehrwert zu einem besseren Datenschutz darstellen und dass unser Zertifikat eine entsprechende Anerkennung genießt.

6.2. Anerkennungen und Akkreditierungen

Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) gemäß ISO/IEC 27006 akkreditierte Zertifizierungsstelle und darf danach international gültige Zertifikate für ISO/IEC 27001-konforme Informationssicherheits-Managementsysteme (ISMS) erteilen. Die Akkreditierung der DAkkS umfasst ferner das Regelwerk „IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG“.

Ferner ist die datenschutz cert GmbH bei der DAkkS für Produkte und Dienstleistungen gemäß ISO/IEC 17065 akkreditiert und darf danach Zertifikate für Vertrauensdienste gemäß eIDAS erteilen.

Auditoren der datenschutz cert GmbH sind beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Auditoren für die TR-03109-6 (Smart Meter Gateway Administratoren) sowie BSI TR-03145 (Secure CA Operation) zertifiziert.

Die datenschutz cert GmbH ist als Prüfstelle für IT-Sicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt.

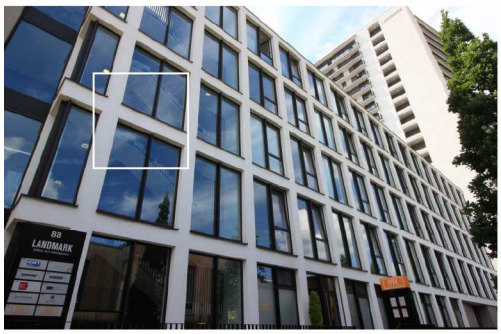
Die datenschutz cert GmbH ist bei der Bundesnetzagentur anerkannte Zertifizierungsstelle nach eIDAS gem. Vertrauensdienstegesetz (VDG) sowie Konformitätsbewertungsstelle nach eIDAS.

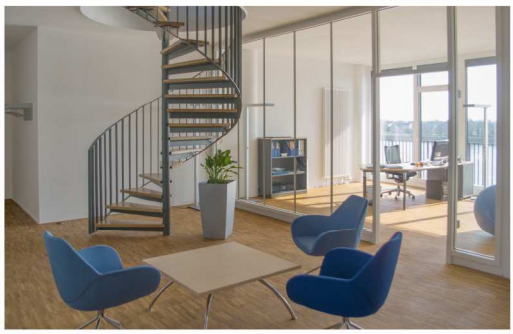
Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-Auditoren und IS-Revisoren. Die datenschutz cert GmbH stellt eines der beiden GS-Zertlabs, die für das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Prüfbegleitung in den IT-Grundschutz-Verfahren durchführt.

Ferner ist die datenschutz cert GmbH beim BSI anerkannter IT-Sicherheitsdienstleister für Penetrationstest.

Auditoren der datenschutz cert GmbH sind zudem anerkannte EuroPriSe Experten für Recht und Technik.

Aufgrund der Akkreditierung bei der DAkkS und der Anerkennung beim BSI darf die datenschutz cert GmbH im Kontext von §8a-Verfahren die Rolle der „prüfenden Stelle“ einnehmen. Ferner sind die Auditoren der datenschutz cert GmbH beim BSI als Prüfer für § 8a BSIG anerkannt.









datenschutz cert GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: 0421 69 66 32 50

Standort Offenbach am Main
Mainstraße 143
63065 Offenbach am Main
Tel.: 069 87 00 783 580

office@datenschutz-cert.de
www.datenschutz-cert.de

datenschutz cert