Zertifizierungsprogramm „eIDAS“

datenschutz cert GmbH
05.04.2024

Inhaltsverzeichnis

Historie

Version	Datum	Geänderte Kapitel	Grund der Änderung	Geändert durch
1.0	01.06.2016		Erstellung	Dr. Sönke Maseberg
1.1	15.06.2016		kleine und editorielle Anpassungen	Dr. Sönke Maseberg
1.2	03.03.2021	5	Aktualisierung Normen; keine inhaltliche Anpassung	Dr. Sönke Maseberg
1.3	05.04.2024	5	Aktualisierung Normen; keine inhaltliche Anpassung	Dr. Sönke Maseberg

1. Zweck

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 das Zertifizierungsprogramm 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 05.04.2024

Dr. Sönke Maseberg

datenschutz cert GmbH

2. Zertifizierungsprogramm

2.1. Angebotsanfrage und Zertifizierungsvereinbarung

Der Kunde für die Zertifizierung richtet seine Anfrage zum Zertifizierungsvorgang an die Zertifizierungsstelle. Die Zertifizierungsstelle informiert über das Zertifizierungsverfahren und der Kunde erhält auf Wunsch folgende Unterlagen:

- ein Zertifizierungsangebot,
- die Allgemeinen Geschäftsbedingungen (AGB) mit den Sonderbedingungen für die Durchführung von Zertifizierungsdienstleistungen.

Der Kunde erteilt auf der Grundlage des Angebotes der Zertifizierungsstelle den Auftrag zur Zertifizierung und erkennt durch Unterzeichnung des Formblatts Zertifizierungsvereinbarung die Zertifizierungsbedingungen an.

2.2. Zertifizierung mit Auditierung und Überwachung

Nach Auftragseingang für die Zertifizierung vergibt die Zertifizierungsstelle eine Zertifizierungs-Vorgangsnummer und benennt dem Kunden den verantwortlichen Zertifizierer und den verantwortlichen Auditteamleiter.

Die Auditierung wird von einem Auditteam unter Verantwortung des Auditteamleiters gemäß den Anforderungen und Vorgaben der Zertifizierungsstelle durchgeführt. Der verantwortliche Zertifizierer plant mit dem Kunden und dem Auditteam den zeitlichen Ablauf des Auditierungs- und Zertifizierungsvorgangs und räumt bei Bedarf in Vorgesprächen letzte Unklarheiten bezüglich des Auditierungs- und Zertifizierungsablaufs aus.

Die Auditierung umfasst alle Tätigkeiten, um zu vollständigen Informationen über die Erfüllung der festgelegten Anforderungen durch den Zertifizierungsgegenstand zu gelangen. Dies schließt planende und vorbereitendende Tätigkeiten sowie Dokumentenprüfungen, Ermittlung von Produktmerkmalen nach festgelegten Verfahren, Prüfungen, Inspektionen und Audits mit ein.

Nach erfolgter Auditierung erstellen die Auditoren einen Auditreport (Konformitätsbewertungsbericht gemäß Artikel 20 Absatz 1 eIDAS), der die Grundlage für die Zertifizierungsentscheidung darstellt. Seitens der Zertifizierungsstelle erfolgen eine Bewertung der Auditierung anhand des erstellten Auditreport und eine Überwachung der Einhaltung der Verfahrensvorgaben auf Basis der DIN EN ISO/IEC 17065.

Die Zertifizierungsentscheidung wird protokolliert. Der Kunde wird über die Zertifizierungsentscheidung informiert.

Bei positiver Zertifizierungsentscheidung wird das Zertifikat ausgestellt, das den Geltungsbereich der Zertifizierung und eine Gültigkeit von 2 Jahren wiedergibt sowie das Prüfzeichen darstellt. Ein gültiges Zertifikat berechtigt zur öffentlichen Nutzung des Prüfzeichens im Zusammenhang mit dem zertifizierten qualifizierten Vertrauensdienst gemäß den Zertifizierungsbedingungen (AGB).

Die Arbeiten der Zertifizierungsstelle werden überwiegend in den Geschäftsräumen der datenschutz cert GmbH durchgeführt. Darüber hinaus werden Prüfungen, Audits und Inspektionen auch beim Kunden durchgeführt.

Die Übergabe des Zertifikats erfolgt grundsätzlich in den Räumlichkeiten der Zertifizierungsstelle. Auf Wunsch kann das Zertifikat auch an anderen Orten übergeben werden.

Die Zertifizierungsstelle der datenschutz cert GmbH bietet qualifizierten Vertrauensdiensteanbietern im Sinne der EU-Verordnung Nr. 910/2014 vom 23.07.2014 (eIDAS) die Bewertung und Zertifizierung der folgenden qualifizierten Vertrauensdienste an:

A. Erstellung von:

1. qualifizierten Zertifikaten für elektronische Signaturen
2. qualifizierten Zertifikaten für elektronische Siegel
3. qualifizierten Zertifikaten für die Website-Authentifizierung
4. qualifizierten elektronischen Zeitstempeln
5. qualifizierten elektronischen Signaturen
6. qualifizierten elektronischen Siegeln

B. Überprüfung und Validierung von:

1. qualifizierten elektronischen Signaturen, Siegeln, Zeitstempeln und zugehörigen qualifizierten Zertifikaten
2. qualifizierten Zertifikaten für die Website-Authentifizierung

C. (Auf-)Bewahrung von:

1. qualifizierten elektronischen Signaturen, Siegeln oder zugehörigen qualifizierten Zertifikaten

D. Zustellung von:

1. Elektronischen Einschreiben.

Die Bewertung und Zertifizierung erfolgt auf der Grundlage relevanter Normen der ETSI:

- ETSI EN 319 401 stellt allgemeine Anforderungen an TSPs, die einen oder mehrere der oben genannten qualifizierten Vertrauensdienste (A – D) anbietet.
- ETSI EN 319 411-2 stellt zusätzliche Anforderungen an TSPs, die qualifizierte Zertifikate herausgeben. Diese Anforderungen sind relevant für die qualifizierten Vertrauensdienste A.1 – A.3.
- ETSI EN 319 411-2 verweist auf Anforderungen der ETSI EN 319 411-1 und unterscheidet zwischen den folgenden Zertifizierungspolitiken:
  - QCP-n

    Zertifizierungspolitik für EU qualifizierte Zertifikate für natürliche Personen,

  - QCP-n-qscd

    Zertifizierungspolitik für EU qualifizierte Zertifikate für natürliche Personen, welche die Verwendung qualifizierter elektronischer Signaturerstellungseinheiten (QSCD) fordert,
  - QCP-l

    Zertifizierungspolitik für EU qualifizierte Zertifikate für juristische Personen,
  - QCP-l-qscd

    Zertifizierungspolitik für EU qualifizierte Zertifikate für juristische Personen, welche die Verwendung qualifizierter elektronischer Signaturerstellungseinheiten (QSCD) fordert,
  - QCP-w

    Zertifizierungspolitik für EU qualifizierte Zertifikate für Webseiten-Authentifizierung.
- ETSI EN 319 421 stellt Anforderungen an TSPs, die qualifizierte elektronische Zeitstempel ausstellen. Diese Anforderungen sind relevant für den qualifizierten Vertrauensdienst A.4.
- Die Durchführung der Zertifizierung erfolgt auf Basis der ETSI EN 319 403. Die Auditierung wird von Auditoren durchgeführt, die Mitarbeiter der Zertifizierungsstelle sind oder durch die Zertifizierungsstelle zugelassen sind.

Die Auditoren untersuchen den TSP bzgl. der Konformität zu den für den qualifizierten Vertrauensdienst relevanten eIDAS-Anforderungen unter Berücksichtigung der Anforderungen der o. g. ETSI-Normen. Im Rahmen des Audits wird festgestellt, ob die organisatorischen und technischen Maßnahmen des TSP den Anforderungen genügen.

Das Audit des Zertifizierungsdienstes unterteilt sich in zwei Phasen:

- die Dokumentationsprüfung und das daran anschließende
- Audit vor Ort.

Der verantwortliche Zertifizierer und die Auditoren stimmen mit dem Kunden den zeitlichen Ablauf des Zertifizierungsvorgangs ab.

In der ersten Phase des Audits des TSP wird die in den Normen geforderte Dokumentation durch die Auditoren analysiert und auf Konformität überprüft. Falls die Prüfung zeigt, dass der Vertrauensdienst die Anforderungen nicht erfüllt, wird kein Audit vor Ort durchgeführt. Der Kunde hat Gelegenheit die Dokumentation des TSP an die Anforderungen anzupassen und erneut durch die Auditoren prüfen zu lassen. Kommen die Auditoren nach der Bewertung der TSP-Dokumentation zu dem Schluss, dass die Dokumentation die Anforderungen der anzuwendenden Normen erfüllt, so folgt die zweite Phase der Auditierung, das Audit vor Ort. Ziel dieses Audits ist es festzustellen, dass der Vertrauensdienst so wie in den Dokumentationen beschrieben implementiert ist und den Anforderungen entspricht. Das Audit vor Ort wird an einem vorher mit dem Kunden abgestimmten Termin beim TSP durchgeführt.

Das Audit vor Ort umfasst die Überprüfung der organisatorischen, baulichen und technischen Umsetzung der in der Dokumentation beschriebenen Maßnahmen zur Erfüllung der Anforderungen. Dabei werden von den Auditoren stichprobenhaft Nachweise

durch Befragungen, Prüfungen von Unterlagen, Beobachtungen von Tätigkeiten und Bedingungen und durch technische Tests gesammelt. Soweit vorhanden können auch Bewertungen anderer unabhängiger Stellen zu einzelnen Teilen des zu beurteilenden Dienstes herangezogen werden. Zum Beispiel ist es nicht notwendig, dass die Auditoren eigene Evaluationen von technischen Komponenten durchführen. Sie können für ihre Beurteilung Prüfberichte und Zertifikate anderer unabhängiger Stellen heranziehen. Ist der im Rahmen der Zertifizierung betrachtete TSP im Sinne von § 15 Signaturgesetz (SigG) freiwillig akkreditiert, so können Auditergebnisse aus der Akkreditierung nach SigG für die Zertifizierung des qualifizierten Vertrauensdiensteanbieters und der von ihm erbrachten qualifizierten Vertrauensdienste nach eIDAS wiederverwendet werden, um unnötige Redundanz in den Prüfungen und damit Kosten für den TSP zu vermeiden. Die Wiederverwendung ist aufgrund der gesetzliche Anforderungen gemäß § 15 Abs. SigG, nach denen das Sicherheitskonzept des TSP umfassend auf seine Eignung und praktische Umsetzung durch eine nach § 18 SigG anerkannte Bestätigungsstelle geprüft worden sein muss, grundsätzlich möglich.

Der Umfang der Wiederverwendung wird zwischen dem verantwortlichen Zertifizierer und den Auditoren abgestimmt. Dabei ist sicherzustellen, dass die wiederverwendeten Ergebnisse für die Zertifizierung des qualifizierten Vertrauensdiensteanbieters und der von ihm erbrachten qualifizierten Vertrauensdienste nach eIDAS anwendbar sind.

Nach erfolgtem Audit vor Ort erstellen die Auditoren auf Grundlage der Dokumentenprüfung und dem Audit einen Konformitätsbewertungsbericht gemäß Artikel 20 Absatz 1 eIDAS mit einer Aussage über die Übereinstimmung des Vertrauensdienstes zu den relevanten eIDAS-Anforderungen und ETSI-Normen. Dieser Bericht bildet die Grundlage für die Entscheidung über die Zertifizierung. Die Entscheidung über die Zertifizierung wird von der Leitung der Zertifizierungsstelle getroffen und im Protokoll der Zertifizierungsentscheidung dokumentiert. Das Zertifikat wird mit einer Gültigkeitsdauer von zwei Jahren ausgestellt.

Innerhalb des letzten Halbjahres des ersten Jahres nach Zertifikatsausstellung muss ein erneutes Audit vor Ort erfolgen, um die Zertifikatsgültigkeit zu verlängern bzw. zu erhalten. Bei diesem Überwachungsaudit wird wie beim Erstaudit in Form einer Stichprobe überprüft, ob die Konformität des Vertrauensdienstes zu den relevanten eIDAS-Anforderungen weiterhin gegeben ist. Der Umfang der jeweiligen Stichprobe beträgt bei Überwachungsaudits mindestens 50% des Stichprobenumfangs des Erstaudits. Dabei soll die Stichprobe alle seit dem letzten Audit durchgeführten Änderungen umfassen. Der TSP muss die Zertifizierungsstelle unverzüglich über Änderungen, die Auswirkung auf die Zertifizierung haben, informieren und eine Beschreibung der Änderungen zur Verfügung stellen. Die Zertifizierungsstelle entscheidet anhand der Beschreibung, ob ein erneutes Audit notwendig ist oder ob die Änderungen im Rahmen des nächsten Überwachungs- bzw. Re-Zertifizierungsaudits überprüft werden können.

Es ist maximal ein Überwachungsaudit möglich. Nach spätestens 2 Jahren ist gemäß Artikel 20 Absatz 1 eIDAS ein vollständiges Audit notwendig, um die Zertifikatsgültigkeit zu verlängern.

2.3. Zertifikatsveröffentlichung und Prüfzeichennutzung

Zur Unterstützung der Transparenz der Zertifizierungen führt die Zertifizierungsstelle eine Liste der zertifizierten Produkte, die der Öffentlichkeit zur Verfügung gestellt wird. Neue Zertifikate werden kurzfristig nach positiver Zertifizierungsentscheidung auf den Web-Seiten veröffentlicht.

Der Kunde ist berechtigt, das Zertifikat und das Prüfzeichen in Verbindung mit dem zertifizierten Produkt in Veröffentlichungen, Katalogen etc. entsprechend der Vorgaben der Zertifizierungsbedingungen der Zertifizierungsstelle datenschutz cert GmbH (AGB) zu verwenden. Bei inkorrekter Bezugnahme oder irreführender Verwendung des Zertifikates oder des Prüfzeichens durch den Kunden ist die Zertifizierungsstelle berechtigt, das Zertifikat zu entziehen.

Mitarbeiter der Zertifizierungsstelle überwachen regelmäßig, dass der Kunde bei der Nutzung der Zertifikate und Prüfzeichen die Zertifizierungsbedingungen einhält. Bei Feststellung von inkorrekter Bezugnahme oder irreführender Verwendung des Zertifikates oder des Prüfzeichens wird der Kunde aufgefordert, dies unverzüglich zu korrigieren. Es erfolgt eine Wiederholungskontrolle auf korrekte Nutzung durch die Zertifizierungsstelle innerhalb von drei Monaten.

2.4. Zertifizierungsaufwände

Die Aufwände für

- die Durchführung der Zertifizierung,
- die Durchführung von Auditierungen,
- die Übergabe von Zertifikaten an anderen Orten

sowie ggf. weitere Tätigkeiten der Zertifizierungsstelle sind der Kosten- und Gebühren-Übersicht auf den Webseiten der datenschutz cert GmbH zu entnehmen.

3. Beschwerden und Einsprüche

Die datenschutz cert GmbH ist offen für Beschwerden und Einsprüche. Die Kontaktdaten sind auf den Internet-Seiten verfügbar; dort findet sich auch unser Verständnis für Beschwerden und Einsprüche.

Allen Eingaben wird objektiv – unter Beachtung einer personellen Trennung - nachgegangen; verantwortlich ist der Leiter der Zertifizierungsstelle, sofern befangen, kann der Ausschuss kontaktiert werden. Der Meldende wird keine Nachteile aus seiner Eingabe erfahren, und es wird Vertraulichkeit zugesichert.

Der Meldende erhält Feedback über Eingang, Fortgang und Ergebnis der Eingabe sowie eine Information, ob die Beschwerde sich auf Zertifizierungstätigkeiten bezieht, für die die datenschutz cert GmbH verantwortlich ist.

Alle Eingaben werden eingehend untersucht und entsprechend dokumentiert. Beschwerden und Einsprüche werden intern im Rahmen der kontinuierlichen Verbesserung bearbeitet.

4. Zuordnungsmatrix

Die ETSI TS 119 612 V2.1.1 (2015-07), die in Kapitel 2 des Durchführungsbeschlusses (EU) 2015/1505 zitiert ist, benennt in Abschnitt 5.5.1.1 die folgenden 8 „qualified trust service types“:

- (a) URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC
- (b) URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
- (c) URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
- (d) URI: http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST
- (e) URI: http://uri.etsi.org/TrstSvc/Svctype/EDS/Q
- (f) URI: http://uri.etsi.org/TrstSvc/Svctype/ EDS/REM/Q
- (g) URI: http://uri.etsi.org/TrstSvc/Svctype/PSES/Q
- (h) URI: http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

Die ETSI TS 119 612 V2.2.1 (2016-04) kennt noch zusätzlich

- (i) URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q

Dieser Diensttyp (i) wird für Signierdienste benötigt. Dazu muss der Durchführungsbeschluss noch aktualisiert werden.

Damit ergibt sich folgende Zuordnung:

1. Ausstellen von qualifizierten Zertifikaten (für qualifizierte Siegel, Signaturen oder Websites) einschließlich CRL/OCSP-Auskunftsdiensten sowie (ggf.) Signier/Siegeldiensten, Prüfdiensten, Aufbewahrungsdiensten:

   (a) URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC

   (b) URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC

   (c) URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC

   (g) URI: http://uri.etsi.org/TrstSvc/Svctype/PSES/Q

   (h) URI: http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

   (i) URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q

2. Ausstellen qualifizierter Zeitstempel:

   (d) URI: http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

3. Zustellen elektronischer Einschreiben:

   (e) URI: http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

   (f) URI: http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q

Ferner ergibt sich folgendes Mapping zu den verschiedenen Vertrauensdiensten:

- A1. Erstellung von qualifizierten Zertifikaten für elektronische Signaturen
  - (a) .../CA/QC
  - (b) .../Certstatus/OCSP/QC
  - (c) .../Certstatus/CRL/QC
- A2. Erstellung von qualifizierten Zertifikaten für elektronische Siegeln
  - (a) .../CA/QC
  - (b) .../Certstatus/OCSP/QC
  - (c) .../Certstatus/CRL/QC
- A3. Erstellung von qualifizierten Zertifikaten für die Website-Authentifizierung
  - (a) .../CA/QC
  - (b) .../Certstatus/OCSP/QC
  - (c) .../Certstatus/CRL/QC
- A4. Erstellung von qualifizierten elektronische Zeitstempeln
  - (d) .../TSA/QTST
- A5. Erstellung von qualifizierten elektronische Signaturen
  - (i) .../RemoteQSCDManagement/Q
- A6. Erstellung von qualifizierten elektronische Siegeln
  - (i) .../RemoteQSCDManagement/Q
- B1. Überprüfung und Validierung von qualifizierten elektronischen Signaturen, Siegeln, Zeitstempeln und zugehörigen qualifizierten Zertifikaten
  - (h) .../QESValidation/Q
- B2. Überprüfung und Validierung von qualifizierten Zertifikaten für die Website-Authentifizierung
  - (h) .../QESValidation/Q
- C1. (Auf-)Bewahrung von qualifizierten elektronischen Signaturen, Siegeln oder zugehörigen qualifizierten Zertifikaten
  - (g) .../PSES/Q
- D1. Zustellung von elektronischen Einschreiben
  - (e) .../EDS/Q
  - (f) .../EDS/REM/Q

5. Normen

[1] DIN EN ISO/IEC 17065:2013-01 „Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren“

[2] (gelöscht)

[3] 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

[4] ETSI EN 319 401, v2.3.1: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[5] ETSI EN 319 411-1, v 1.4.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements

[6] ETSI EN 319 411-2, v 2.5.1: 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

[7] ETSI EN 319 421, v 1.2.1: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[8] ETSI EN 319 521 V1.1.1 (2019-02): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers

[9] ETSI TS 119 511 V1.1.1 (2019-06): 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

[10] ETSI EN 319 531 V1.1.1 (2019-01): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers

6. Kontakt

datenschutz cert GmbH

Konsul-Smidt-Str. 88a

28217 Bremen

Tel.: 0421.69 66 32-550

Fax: 0421.69 66 32-551

E-Mail: zertifizierung@datenschutz-cert.de

Internet: www.datenschutz-cert.de