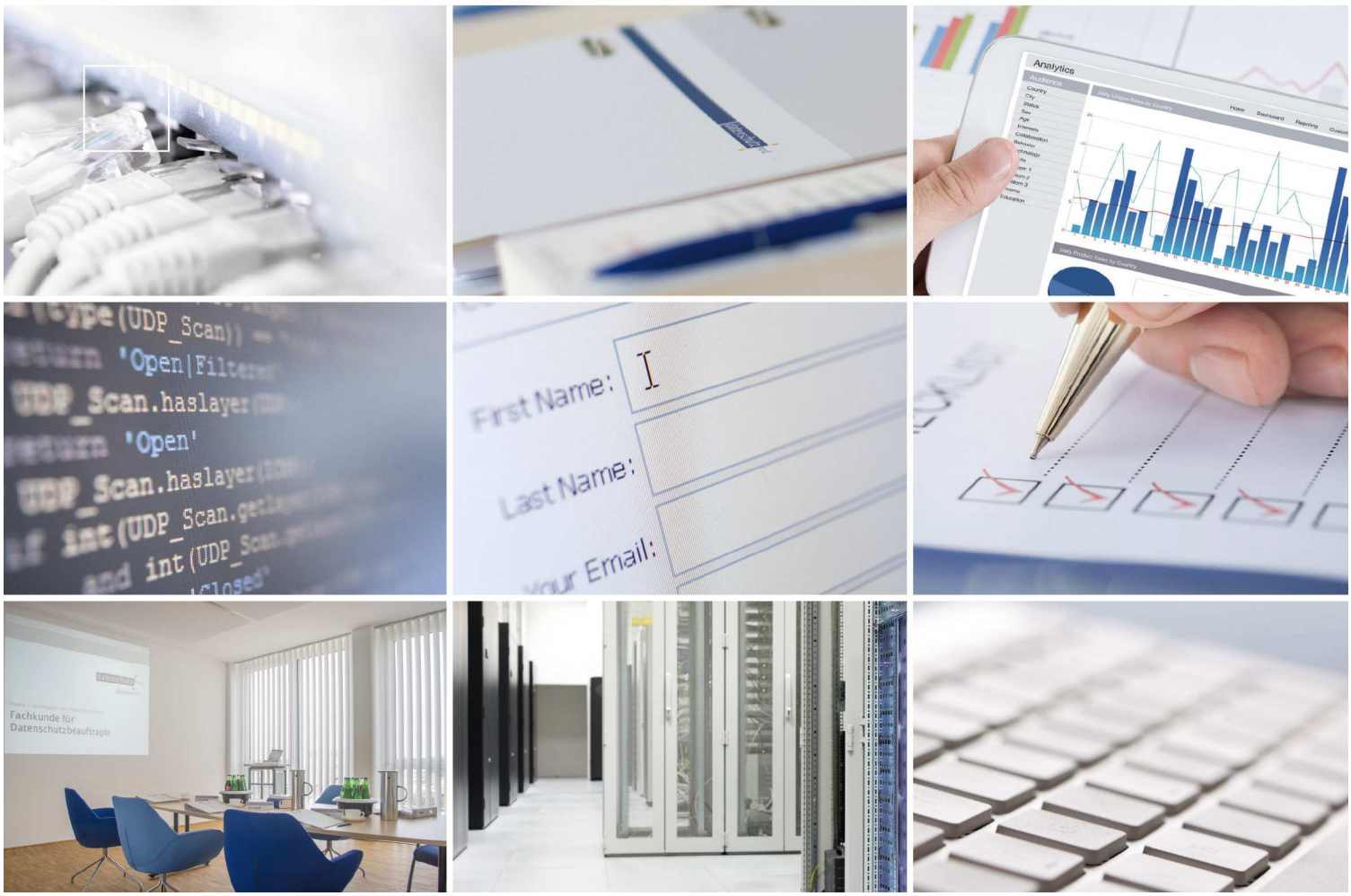

Kriterienkatalog und Vorgehensweise zur Auditierung und Zertifizierung gemäß ETSI

datenschutz cert GmbH

Version 1.5

datenschutz cert

Inhaltsverzeichnis

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
1.0	27.02.2013		Finalisierung nach Abnahme durch Zertifizierungsstelle	IK, SM
1.1	22.08.2013		Aktualisierung	IK, SM
1.2	04.07.2018		Designanpassung und letztes Kapitel	CS
1.3	26.03.2019		Aktualisierung	SM
1.4	12.11.2019		Aktualisierung	SM
1.5	07.12.2021		Aktualisierung AGB und KBO	HH

Dokumenten-Überwachungsverfahren

Status	Prozess-/Dokumentenbesitzer	Version
Final	Dr. Maseberg	1.5

1. Anforderungen an ETSI

Zur Förderung des elektronischen Geschäftsverkehrs, insbesondere innerhalb der Europäischen Gemeinschaften, erließen das Europäische Parlament und der Europäische Rat im Jahr 1999 die Direktive 1999/93/EC. Die Direktive regelt den Rahmen, in dem elektronische Signaturen, Zertifikate und Zeitstempel herausgegeben und verwendet werden. Zur praktischen Umsetzung dieses Rahmens entstanden in der Folge mehrere Normen.

Die Norm ETSI EN 319 411-2 definiert die Anforderungen, die an einen Zertifizierungsdiensteanbieter (englisch: Certification Authority, CA) gestellt werden, der qualifizierte Zertifikate herausgeben will.

Die Norm ETSI EN 319 411-1 definiert die Anforderungen, die an eine CA gestellt werden, der allgemeine, z. B. fortgeschrittene Zertifikate herausgeben will. Die Zertifizierung nach dieser Norm hat einen weiteren Vorteil: die Hersteller von Internet-Browsern akzeptieren diese Zertifizierung als Vorbedingung für die Aufnahme der CA in den Zertifikatsspeicher ihres jeweiligen Internet-Browsers.

Die Norm ETSI EN 319 421 definiert die Anforderungen, die an einen Zeitstempeldienst (englisch: Time-stamp Provider, TSP) gestellt werden, der elektronische Zeitstempel herausgeben will.

Die datenschutz cert GmbH bietet die Auditierung und Zertifizierung von Unternehmen an, die nach einer oder mehreren ETSI-Normen zertifiziert werden möchten.

Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) akkreditierte Zertifizierungsstelle für ETSI EN 319 411-2, ETSI EN 319 421 sowie ETSI EN 319 411-1.

Das vorliegende Dokument beschreibt den Auditierungs- und Zertifizierungsprozess und ist ein Extrakt aus dem vollständigen Zertifizierungsschema der datenschutz cert GmbH.

Bremen, den 12.11.2019

Dr. Sönke Maseberg
Geschäftsführer
datenschutz cert GmbH

2. ETSI

2.1. Hintergrund

Technisch hochwertige und vertrauenswürdige elektronische Zertifikate werden unter anderem von Internet-Browsern benötigt, um sichere Verbindungen zwischen Servern und Klienten im Internet on-line herstellen zu können. Die Herausgeber solcher Zertifikate benötigen ihrerseits technisch hochwertige und vertrauenswürdige elektronische Zertifikate, die von den Herstellern der Internet-Browser in die Internet-Browser integriert werden. Um die erforderliche Vertrauenswürdigkeit und Sorgfalt von Zertifikatsherausgebern nachzuweisen, verlangen die Hersteller von Internet-Browsern z. B. eine Zertifizierung nach der ETSI-Norm ETSI EN 319 411-1.

Für qualifizierte Zertifikate kann die ETSI-Norm ETSI EN 319 411-2 angewendet werden. Sie stellt die Anforderungen auf, die ein Zertifizierungsdiensteanbieter erfüllen sollte, wenn er qualifizierte elektronische Zertifikate herausgeben will.

Die ETSI-Norm ETSI EN 319 421 wurde geschaffen, um Zeitpunkte auf vertrauenswürdige Weise gegenüber Dritten ausweisen zu können. Die Anwendungsgebiete elektronischer Zeitstempel sind vielfältig und reichen von Anwendungen in Übertragungsprotokollen bis zur Angabe von Vorlagezeitpunkten elektronischer Dokumente. Anbieter elektronischer Zeitstempel können die Qualität der von ihnen herausgegebenen elektronischen Zeitstempel in technischer und organisatorischer Hinsicht z. B. durch eine Zertifizierung nach der ETSI-Norm ETSI EN 319 421 nachweisen.

Die datenschutz cert GmbH führt für Unternehmen, die technisch hochwertige und vertrauenswürdige elektronische Zertifikate anbieten, die erforderlichen Prüfungen als unabhängige Instanz durch und vergibt bei Normkonformität ein Zertifikat. Mit diesem Zertifikat zur ETSI-Normkonformität kann der Zertifikatsherausgeber (Zertifizierungsdiensteanbieter) zeigen, dass die erforderliche Normkonformität durch eine unabhängige Instanz geprüft und bestätigt wurde. Das elektronische Zertifikat des Zertifikatsherausgebers kann damit von den Herstellern der Internet-Browser in die Internet-Browser integriert werden.

2.1. Vorteile einer ETSI-Zertifizierung

Als Zertifikats- oder Zeitstempelanbieter ist ihre Dienstleistung eine der wesentlichen Voraussetzungen für eine sichere und vertrauenswürdige Kommunikation über das Internet. Mit dem ETSI-Zertifikat weisen Sie nach, dass Ihre Zertifizierungs- oder Zeitstempeldienstleistung vertrauenswürdig erbracht wird. In puncto Sicherheit erfüllen Sie alle Anforderungen, die dem aktuellen Stand der Technik entsprechen.

Wenn im Rahmen der Prüfung nach ETSI TS auch die „Network and Certificate System Security Requirements“ des CA/Browser Forums berücksichtigt werden, kann ihr Root-Zertifikat auch in die gängigen Internet-Browser integriert werden. Dadurch werden letztlich sichere Verbindungen im Internet bei der Darstellung im Browser besonders gekennzeichnet.

3. Kriterienkatalog

Für eine ETSI-Auditierung und -Zertifizierung stellen die internationalen Normen den Kriterienkatalog dar:

- „Policy and security requirements for Trust Service Providers issuing certificates“ gemäß ETSI EN 319 411-2;
- „Policy and security requirements for trust service providers issuing time-stamps“ gemäß ETSI EN 319 421;
- „Policy and security requirements for Trust Service Providers issuing certificates“ gemäß ETSI EN 319 411-1.

4. Auditierungs- und Zertifizierungsprozess

Der Audit- und Zertifizierungsprozess wird analog zum ISO/IEC 27001-Kritierienkatalog durchgeführt, vgl. dazu Download unter www.datenschutz-cert.de.

In Übereinstimmung mit ETSI EN 319 403 werden vorliegende Auditierungen und Zertifizierungen von Managementsystemen des Kunden berücksichtigt, soweit und sofern die erforderlichen Unterlagen durch den Kunden zur Verfügung gestellt werden und aus ihnen hervorgeht, welche im Rahmen der Konformitätsprüfung zu den relevanten Normen ETSI EN 319 411-2, ETSI EN 319 421 und ETSI EN 319 411-1 zu erfüllenden Anforderungen in welcher Weise geprüft wurden und erfüllt sind. Die Berücksichtigung erfolgt, um unnötige Doppelprüfungen zu vermeiden.

Nicht berücksichtigungsfähig sind vorliegende Auditierungen und Zertifizierungen, wenn

- die erforderlichen Nachweise durch den Kunden nicht oder nicht rechtzeitig zur Verfügung gestellt werden oder
- die Qualität der aktuell durchzuführenden Auditierung darunter leiden oder nachteilig beeinflusst würde.

Das Betreiben eines anderen Managementsystems, etwa eines Informationssicherheitsmanagementsystems nach ISO/IEC 27001, ist nicht Voraussetzung für die Konformitätsprüfung nach ETSI EN 319 411-2, ETSI EN 319 421 und ETSI EN 319 411-1.

4.1. Laufzeiten

Die Laufzeiten eines Zertifikats für die Konformität zu einer der ETSI-Normen ETSI EN 319 411-2, ETSI EN 319 421 und ETSI EN 319 411-1 sind identisch zu den Laufzeiten eines ISO/IEC 27001-Zertifikats: 3 Jahre Gültigkeit mit jährlichem Überwachungsaudit.

4.2. Zertifikatsliste

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

4.3. Entzug 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
- 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.

4.4. 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.

4.5. 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.

4.6. AGB und KBO

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 auch 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.

6.3. Kontakt

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen
Tel.: 0421.69 66 32-550
Fax: 0421.69 66 32-551
E-Mail: office@datenschutz-cert.de
Internet: www.datenschutz-cert.de