



Kriterienkatalog und Vorgehensweise zur Auditierung und Zertifizierung gem. ETSI-Standards

datenschutz cert GmbH
Version 1.6

Inhaltsverzeichnis

1. Einleitung.....	4
2. ETSI.....	5
2.1. Hintergrund	5
2.2. Vorteile einer ETSI-Zertifizierung.....	5
3. Kriterienkatalog.....	6
4. Auditierungs- und Zertifizierungsprozess	7
4.1. Laufzeiten	7
4.2. Zertifikatsliste	7
4.3. Entzug eines Zertifikates.....	7
4.4. Ablauf eines Zertifikates	8
4.5. Anfrageformular	8
4.6. AGB und KBO.....	8
5. Über die datenschutz cert GmbH.....	9
5.1. Was wir tun.....	9
5.2. Leitlinien.....	9
5.3. Anerkennungen und Akkreditierungen	10

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
1.6	18.02.2026		Aktualisierung	SM

Dokumenten-Überwachungsverfahren

Status	Prozess-/Dokumentbesitzer	Version
Final	Dr. Sönke Maseberg	1.6

1. Einleitung

Public-Key-Infrastrukturen (PKI) ermöglichen eine sichere Kommunikation über unsichere Netze: Signaturen gewährleisten die Integrität von Nachrichten, Zertifikate geben Auskunft über die Authentizität von Kommunikationspartnern, und eine Verschlüsselung schafft Vertraulichkeit bei der Übermittlung sensibler Informationen. Ebenso wichtig: Einheitliche Standards, damit etwa Kommunikationsprotokolle, Tools, Schnittstellen und Formate aufeinander abgestimmt sind. Ein solcher Standard wird über die Standardisierungsorganisation ETSI (European Telecommunications Standards Institute) zur Verfügung gestellt.

Grundlage einer PKI ist stets Vertrauen: Vertrauen in die Kryptographie. Vertrauen in die Zertifikate, dass diese tatsächlich den richtigen kryptographischen Schlüssel der richtigen Kommunikationspartnern enthalten. Und damit insbesondere Vertrauen in Vertrauensdienste – sogenannte Trust Service Provider.

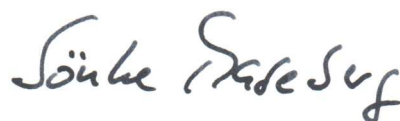
Eine Möglichkeit, um Vertrauen aufzubauen und nach außen hin zu dokumentieren, sind Prüfungen und Zertifizierungen. Die ETSI bietet dazu verschiedene Standards an. So enthält ETSI 319 401 allgemeine Anforderungen an einen Trust Service Provider (TSP), dieser Standard stellt die Basisnorm für nachfolgende themenspezifische Ergänzungen dar. ETSI 319 411-1 beschreibt eine Certification Authority (CA) – also einen TSP, der Zertifikate herausgibt; ETSI 319 411-2 ergänzt die 411-1 um zusätzliche Anforderungen, wenn qualifizierte Zertifikate erstellt werden sollen. Für Zeitstempel bietet sich die ETSI 319 421 an. ETSI 119 431-1 adressiert Anbieter von Fernsignaturen und -siegeln, während Validierungsdienste ETSI 119 441 nutzen. Für Bewahrungsdienste bietet sich ETSI 119 511 an. Wichtig auch ist die ETSI 119 461 zur Identitätsprüfung.

Die ETSI-Normen sind interessant für Trust Service Provider sowie für deren Kunden, um einen geeigneten Dienst auszuwählen.

Die datenschutz cert GmbH prüft und zertifiziert Trust Service Provider nach diesen ETSI-Normen. Dazu ist die datenschutz cert GmbH bei der DAkkS als eIDAS-Konformitätsbewertungsstelle akkreditiert. Damit sind wir Ihr Partner für eine Zertifizierung Ihres Trust Services nach ETSI-Standards.

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

Bremen, den 18.02.2025



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.

2.2. 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:

Allg. Anforderungen:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

Zertifikate:

- ETSI EN 319 411-1: Electronic Signatures and Trust 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: Requirements for trust service providers issuing EU qualified certificates

Zeitstempel:

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

Fernsignaturen/remote:

- ETSI TS 119 431-1: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev

Validierung:

- ETSI TS 119 441: Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services

Bewahrung:

- 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

Identifizierung/Identitätsprüfung:

- ETSI TS 119 461: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

4. Auditierungs- und Zertifizierungsprozess

Der Audit- und Zertifizierungsprozess wird analog zum ISO/IEC 27001-Kriterienkatalog 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. Über die datenschutz cert GmbH

5.1. Was wir tun

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 DSN Group. Sitz der Gesellschaft ist Bremen. Geschäftsführer ist Dr. Sönke Maseberg. Die Unternehmen der DSN Group sind inhabergeführt.

5.2. Leitlinien

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

5.2.1. 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.

5.2.2. Vertraulichkeit

Wir sichern Ihnen Vertraulichkeit zu.

5.2.3. 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 zertifiziert 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.

5.2.4. 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.

5.3. Anerkennungen und Akkreditierungen

Die datenschutz cert GmbH ist bei der **Deutschen Akkreditierungsstelle GmbH (DAkkS)** zu folgenden Regelwerken akkreditiert:

- ISO/IEC 27001 für Informationssicherheits-Managementsysteme (ISMS)
- „IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG“ (§ 5c EnWG) für Strom- und Gasnetzbetreiber
- „IT-Sicherheitskatalog gemäß § 11 Abs. 1b EnWG“ (§ 5c EnWG) für Energieanlagenbetreiber
- ISO/IEC 27701 für Datenschutz-Managementsysteme (DSMS)
- eIDAS für Vertrauensdiensteanbieter
- „ips-VSS-IT“ für Videosprechstunden
- Zertifizierungsstandard ‚DSGVO – information privacy standard‘ gem. Art. 42 DSGVO

„ips-VSS-IT“ für Videosprechstunden und „DSGVO – information privacy standard“ sind von der datenschutz cert GmbH erstellte, **behördlich genehmigte Zertifizierungsstandards**.

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 und IT-Sicherheitsdienstleister beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt.

Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-Auditoren. 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.

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

Aufgrund der Akkreditierung bei der DAkkS und der Anerkennung beim BSI darf die datenschutz cert GmbH im Kontext von BSIG/KRITIS-VO/NIS-2-Verfahren die Rolle der „**prüfenden Stelle**“ einnehmen. Ferner sind die Auditoren der datenschutz cert GmbH beim BSI als Prüfer anerkannt; dies umfasst auch die Prüfung von Systemen zur Angriffserkennung (SzA).

datenschutz



datenschutz cert GmbH

Hauptsitz Bremen

Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: +49 421 69 66 32-550

Standort Offenbach

Mainstraße 143
63065 Offenbach am Main
Tel.: +49 69 870 07 83-580

office@datenschutz-cert.de

www.datenschutz-cert.de

