Inhaltsverzeichnis

1. Geltungsbereich 1
2. Anmeldung und Zulassung zur Prüfung 1
3. Durchführung der Prüfung 2
4. Bewertung 3
5. Wiederholung der Prüfung 3
6. Zertifizierungsentscheidung 3
7. Überwachung 3
8. Rezertifizierung 3
9. Prüfungsunterlagen 4
10. Kosten 4
11. Änderungsdienst 4
Anlage 1 - Mindestanforderungen an IT-Forensik-Berichte 5
Anlage 2 – Mindestanforderungen an IT-Gutachten 6

1. Geltungsbereich

Diese Prüfungs- und Zertifizierungsordnung (PZO) gilt für die Zertifizierungsverfahren

- **IT-Forensic-Analyst (Windows Betriebssysteme**)
- **IT-Forensic-Analyst (Mobile Devices)**
- **Sachverständiger IT-Forensic (lokale und mobile Systeme)**

entsprechend dem Programm zur Zertifizierung von Personen der DEKRA Certification GmbH (DCG) und auf der Grundlage der DIN EN ISO 17024 in der jeweils gültigen Fassung.

Zusätzlich gelten die Allgemeinen Geschäftsbedingungen (AGB) (D-030-18) und die Allgemeinen Zertifizierungsbedingungen (AZB) (D-030-19) der DEKRA Certification GmbH.

Die Dienstleistungen der Zertifizierungsstelle stehen allen interessierten Personen offen und die DEKRA Certification GmbH garantiert die Gleichbehandlung aller Antragsteller durch die Festlegung objektiver Kriterien für die Zulassung, die Prüfung und die Zertifizierung.

Aus Vereinfachungsgründen wurde für Bezeichnungen durchgängig die männliche Form gewählt. Damit soll keine Benachteiligung eines Geschlechts verbunden sein; die Bezeichnungen erfassen die jeweilige weibliche Form ebenso.

2. Anmeldung und Zulassung zur Prüfung

Die Anmeldung zu einer Prüfung und Zertifizierung erfolgt schriftlich anhand des Antrags zur Zertifizierung „IT-Forensic-Analyst/Sachverständiger“ (F-03S-59) und Bestätigung der PZO, AZB und AGB der DEKRA Certification GmbH. Die Antragstellung muss spätestens 1 Woche vor dem geplanten Prüfungstermin erfolgen.

Die Teilnahme an der unter Punkt 1 genannten Prüfung unterliegt nachfolgenden Zulassungsvoraussetzungen-

2.1 Zulassungsvoraussetzungen IT-Forensic-Analyst (Windows Betriebssysteme) / (Mobile Devices)

- einschlägiges, abgeschlossenes Studium, z. B. (Wirtschafts-)Informatik, Ingenieurstudiengang und mindestens 3 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 5 Jahre

oder

- abgeschlossene Berufsausbildung im Bereich EDV/IT, z. B. Informatiker, Informations- und Systemelektroniker und mindestens 5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre.

2.2 Zulassungsvoraussetzungen Sachverständige IT-Forensic (lokale und mobile Systeme)

- einschlägiges, abgeschlossenes Studium, z. B. (Wirtschafts-)Informatik, Ingenieurstudiengang und mindestens 5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre

oder

- abgeschlossene Berufsausbildung im Bereich EDV/IT, z. B. Informatiker, Informations- und Systemelektroniker und mindestens 8 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 10 Jahre

sowie

- Abschluss zum IT-Forensic Analyst (Windows Betriebssysteme) (Prüfungsteil 1) und ITForensic Analyst (Mobile Devices) (Prüfungsteil 1) oder gleichwertiger Nachweis.

Die Zertifizierungsstelle prüft die Vollständigkeit und formale Richtigkeit der Anmeldeunterlagen und entscheidet über die Zulassung zur Prüfung.

3. Durchführung der Prüfung

3.1 Prüfung zum IT-Forensic-Analyst (Windows Betriebssysteme) / (Mobile Devices)

Die Prüfung besteht jeweils aus zwei Teilen:

Teil 1: Schriftliche Prüfung, bestehend aus Multiple-Choice-Fragen (MC-Fragen) und offenen Prüfungsfragen gemäß den in der Kompetenzmatrix *(siehe Homepage)* beschriebenen Prüfungsinhalten. Die Dauer der Prüfung beträgt 45 Minuten. Zugelassene Hilfsmittel: Keine.

Bei den MC-Fragen ist immer mindestens eine Antwort richtig. Bitte kreuzen Sie alle richtigen Antworten an. Jede richtige Antwort wird mit einem Punkt bewertet. Achtung! Bei einer Aufgabe wird für jedes falsch gesetzte Kreuz (Antwort) ein Punkt abgezogen. Bei den offenen Aufgaben werden jeweils maximal 5 Punkte je nach Erfüllungsgrad der Beantwortung vergeben.

Teil 2: Auswertung eines Datenträger-Images und Berichterstellung (in Heimarbeit).

Der Teilnehmer erhält eine Aufgabenerstellung und Datenträgerabbild. Der Teilnehmer muss selbstständig eine Auswertung durchführen und innerhalb von 14 Tagen per (Post oder per E-Mail) einen forensischen Auswertebericht an die DEKRA Certification zur Bewertung einreichen. Bei der Erstellung des Auswerteberichts sind die Mindestanforderungen an IT-Forensik-Berichte *gemäß Anlage 1* zu beachten. Später eingehende Prüfungsleistungen werden als nicht bestanden gewertet. Eine Fristverlängerung ist nur mit Vorlage eines ärztlichen Attests möglich.

Die Prüfung erfolgt grundsätzlich in deutscher Sprache. Die Organisation der Prüfung liegt in der Verantwortung der Zertifizierungsstelle. Die Prüfung führt ein zugelassener und von der DEKRA Certification GmbH für diese Durchführung beauftragter Prüfer durch. Die Organisation der Prüfung vor Ort obliegt dem eingesetzten Prüfer.

3.2 Prüfung zum Sachverständiger IT-Forensic (lokale und mobile Systeme)

Die Prüfung besteht jeweils aus zwei Teilen:

Teil 1: Schriftliche Prüfung, bestehend aus Multiple-Choice-Fragen (MC-Fragen) und offenen Prüfungsfragen gemäß den in der Kompetenzmatrix *(siehe Homepage)* beschriebenen Prüfungsinhalten. Die Dauer der Prüfung beträgt 75 Minuten. Zugelassene Hilfsmittel: Taschenrechner.

Bei den MC-Fragen ist immer mindestens eine Antwort richtig. Bitte kreuzen Sie alle richtigen Antworten an. Jede richtige Antwort wird mit einem Punkt bewertet. Achtung! Bei einer Aufgabe wird für jedes falsch gesetzte Kreuz (Antwort) ein Punkt abgezogen. Bei den offenen Aufgaben werden jeweils maximal 5 Punkte je nach Erfüllungsgrad der Beantwortung vergeben.

Teil 2: Erstellung eines IT-Gutachtens (in Heimarbeit).

Der Teilnehmer erhält aus dem Pool verschiedener Fallstellungen eine Fallaufgabe. Das Gutachten zu dieser Fallaufgabe muss nach Abschluss der schriftlichen Prüfung (Teil 1) innerhalb von 8 Wochen bei DEKRA Certification zur Bewertung vorliegen (Datum des Poststempels). Bei der Erstellung des Gutachtens sind die Mindestanforderungen an IT-Gutachten *gemäß Anlage 2* zu beachten. Später eingereichte Gutachten werden als nicht bestanden bewertet. Eine Fristverlängerung ist nur mit Vorlage eines ärztlichen Attests möglich.

Die Prüfung erfolgt grundsätzlich in deutscher Sprache. Die Organisation der Prüfung liegt in der Verantwortung der Zertifizierungsstelle. Die Prüfung führt ein zugelassener und von der DEKRA Certification GmbH für diese Durchführung beauftragter Prüfer durch. Die Organisation der Prüfung vor Ort obliegt dem eingesetzten Prüfer.

4. Bewertung

Die Auswertung der Prüfung erfolgt durch den beauftragten Prüfer.

Die Prüfung gilt als bestanden, wenn in beiden Teilen mindestens 66 % der möglichen Höchstpunktzahl erreicht werden. Bei weniger als 66 % gilt die Prüfung als nicht bestanden.

Das Prüfungsergebnis und die Prüfungsunterlagen werden der Zertifizierungsstelle übermittelt und gegen geprüft.

5. Wiederholung der Prüfung

Eine nicht bestandene Prüfung bzw. ein nicht bestandener Prüfungsteil kann einmal wiederholt werden. Sonderregelung auf schriftlichen Antrag. Die Anmeldung zu einer Wiederholungsprüfung erfolgt schriftlich anhand des Antrags zur Wiederholungsprüfung (F-03S-09) und Bestätigung der PZO, AZB und AGB der DEKRA Certification GmbH.

Die Wiederholungsprüfung muss im Regelfall innerhalb von 60 Tagen nach der Zertifizierungsentscheidung (Datum des Entscheides) beantragt werden. Der Termin der Wiederholungsprüfung wird von der DEKRA Certification GmbH festgelegt.

6. Zertifizierungsentscheidung

Das Zertifizierungsgremium trifft die Zertifizierungsentscheidung in der Regel innerhalb von max. 4 Wochen nach dem Prüfungstermin. Weicht das Zertifizierungsgremium vom Votum des Prüfers ab, ist dies schriftlich zu begründen.

Bei bestandener Prüfung und erfolgreicher Zertifizierung wird das DEKRA Zertifikat in deutscher Sprache für die Laufzeit von max. 3 Jahren erteilt. Das Zertifikat beinhaltet die folgenden Angaben: vollständiger Name, Geburtsdatum und Titel (falls vorhanden) der zertifizierten Person, die erworbene Qualifikationsstufe, der Hinweis auf das Zertifizierungsprogramm, nachgewiesene Kenntnisse und Kompetenzen, DEKRA Logo, DEKRA Zeichen, Angaben zur Zertifizierungsstelle, Prüfungsdatum, Prüfungsort, Ausstellungsdatum, Ausstellungsort, Ablaufdatum des Zertifikates, eindeutige Zertifikatsnummer sowie die Unterschrift der verantwortlichen Person.

Die Zertifikatsinhaber werden in das zur Veröffentlichung für berechtigte Personen bestimmte Verzeichnis der zertifizierten Personen der DEKRA Certification GmbH aufgenommen. Das Zertifikat bleibt das Eigentum der DEKRA Certification GmbH. Die Nutzungsbedingungen für das Zertifikat sind in den AZB geregelt.

7. Überwachung

Die zertifizierte Person hat eigenverantwortlich ihren Kompetenzerhalt sicherzustellen. Die DEKRA Certification GmbH überwacht die Einhaltung der Nutzungsbedingungen für das Zertifikat. Dazu gehören – sofern im Gültigkeitszeitraum des Zertifikats eintretend – die Auswertung von Informationen von Aufsichtsbehörden, die Bewertung von Beschwerden und Informationen von interessierten Kreisen sowie von eingeleiteten rechtlichen Schritten in Bezug auf die zertifizierte Person. Der Kodex für IT-Sachverständige und IT-Analysten (*siehe Homepage*) ist einzuhalten.

8. Rezertifizierung

Eine Rezertifizierung kann vom Zertifikatsinhaber spätestens bis zu 3 Monaten nach dem Ablauf der Gültigkeit des aktuellen Zertifikates unter Verwendung des Antrags zur Rezertifizierung (F-03S-17) schriftlich bei DEKRA Certification GmbH beantragt werden. Dabei sind die nachfolgenden geforderten Nachweise mit einzureichen.

8.1 Nachweise für IT-Forensic-Analyst (Windows Betriebssysteme) / (Mobile Devices)

- 2 unterschiedliche IT-Forensic-Berichte entsprechend der Zertifizierungsstufe, die im Laufe der Zertifikatsgültigkeit durch den Antragsteller selbst ausgearbeitet und erstellt wurden

  sowie

- Nachweis über mindestens 16 Weiterbildungspunkte im zertifizierten Bereich im Zeitraum der Zertifikatsgültigkeit. Die Weiterbildung sowie der Bildungsdienstleister sind frei wählbar. Eine U-Std. entspricht 45 Min. (vgl. auch Kodex für IT-Sachverständige und IT-Analysten, *siehe Homepage*)

8.2 Nachweise für Sachverständige IT-Forensic (lokale und mobile Systeme)

- 2 verschiedene Gutachten entsprechend der Zertifizierungsstufe, die im Laufe der Zertifikatsgültigkeit durch den Antragsteller selbst ausgearbeitet und erstellt wurden

  sowie

- Nachweis über mindestens 24 Weiterbildungspunkte im zertifizierten Bereich im Zeitraum der Zertifikatsgültigkeit. Die Weiterbildung sowie der Bildungsdienstleister sind frei wählbar. Eine U-Std. entspricht 45 Min. (vgl. auch Kodex für IT-Sachverständige und IT-Analysten, *siehe Homepage*)

Die Nachweise sind zusammen mit dem Antrag zur Rezertifizierung (F-03S-17) einzureichen. Später eingereichte Anträge werden nicht akzeptiert.

Voraussetzung für eine Rezertifizierung sind ein vollständiger und korrekter Antrag und die positive Bewertung der eingereichten Nachweise. Das Ergebnis der Dokumentenprüfung wird dem Antragsteller mitgeteilt. Bei erfolgreicher Dokumentenprüfung wird ein neues Zertifikat für weitere max. 3 Jahre ausgestellt. Das bisherige Zertifikat verliert seine Gültigkeit.

9. Prüfungsunterlagen

Alle Unterlagen zur Prüfung werden von der Zertifizierungsstelle elektronisch oder in Papierform archiviert aufbewahrt. Die Aufbewahrungsfrist beträgt 10 Jahre.

10. Kosten

	IT-Forensic Analyst Preis zzgl. USt	**Sachverständiger IT-Forensic** Preis zzgl. USt
Erstzertifizierung		
Erstzertifizierung inkl. Zertifikatserstellung:	**319,00 EURO**	**695,00 EURO**
Erstzertifizierung mit gültigem DEKRA-Zertifikat	**---**	**619,00 EURO**
Wiederholungsprüfungen		
Prüfungsteil 1 schriftliche Prüfung:	**175,00 EURO**	**175,00 EURO**
Prüfungsteil 2 Bericht/Gutachten-Prüfung:	**225,00 EURO**	**255,00 EURO**
Rezertifizierung (inkl. Zertifikatserstellung)	**219,00 EURO**	**475,00 EURO**

11. Änderungsdienst

Der Teilnehmer bzw. die zertifizierte Person hat sich laufend eigenverantwortlich über Änderungen an den für den Zertifizierungsprozess relevanten Verfahren, Beschreibungen, Dokumenten und Formularen zu informieren. Die aktuellen Unterlagen sind auf der Website der DEKRA Certification GmbH erhältlich.

Anlage 1 - Mindestanforderungen an IT-Forensik-Berichte

Formalia

Der Auswertebericht muss u. a. Angaben zum Auswerter/Analysten (Titelseite), Auftraggeber, Geschäftszeichen, Untersuchungszeitraum, Anzahl der Ausfertigungen, Auftrag, Untersuchungsgegenstand, eingesetzte Hard- und Software, IT-forensische Vorgehensmethode, Verifizierungsmaßnahmen, Anlagen und Originalunterschrift enthalten.

Der Bericht muss gut lesbar sein, sowie einwandfreie Rechtschreibung und Grammatik aufweisen. Der Bericht ist in einem repräsentativen Layout zu halten.

Ziel, Aufgabe

Aus dem Bericht muss klar die Beantwortung der Fragen und die Grundsätze einer IT-forensischen Beweissicherung hervorgehen.

Vorgehensweise

Im Bericht sind kurze Ausführungen zur Arbeitsplatzumgebung (Laborsituation) sowie die Nennung von entsprechend eingesetzten Hard- und Software-Tools zu treffen.

Feststellungen

Der Bericht muss eindeutige Aussagen treffen zum vorliegenden Untersuchungsgegenstand (Beweismittel).

Aussagen

Im Bericht zu nennen sind Ergebnisse mit Angabe des

- Dateinamen
- Speicherpfad
- Prüfsumme (Hashwert – mind. MD5)

Schlussbemerkungen

Der Bericht muss Schlussbemerkungen zu der Archivierung, Verbleib von Sicherungskopien sowie die Originalunterschrift des Analysten enthalten.

Stand: 08/2019

Anlage 2 – Mindestanforderungen an IT-Gutachten

für

- IT-Sachverständige
- Sachverständige IT-Forensic
- Sachverständige IT-Security

zu finden auf der Homepage der DEKRA Certifikation GmbH.

Stand: 08/2019