FRAUNHOFER-GESELLSCHAFT

ZERTIFIZIERUNGSHANDBUCH UND PRÜFUNGSORDNUNG

Personenzertifizierungen im Bereich Cyber Security

(Normatives Dokument)

Revision 1

Gültig ab Dezember 2023

Fraunhofer-Personenzertifizierungsstelle
Schloss Birlinghoven
53757 Sankt Augustin

Fraunhofer

ZERTIFIZIERUNGSHANDBUCH UND PRÜFUNGSORDNUNG

Personenzertifizierungen im Bereich Cyber Security

Dorothea Kugelmeier

Leiterin der Fraunhofer-Personenzertifizierungsstelle
angesiedelt am

Fraunhofer-Institut für Angewandte Informationstechnik FIT
Schloss Birlinghoven
53757 Sankt Augustin

Inhalt

1 VORWORT

Im Folgenden wird das Verfahren für Personenzertifizierungen im Bereich »Cyber Security« in Anlehnung an die Vorgaben der EN ISO 17024 »Allgemeine Kriterien für Stellen, die Personen zertifizieren« beschrieben und damit ein einheitliches Zertifizierungssystem vorgegeben. Gleichzeitig dient dieses Zertifizierungshandbuch als Prüfungsordnung.

2 ANWENDUNGSBEREICH

Der Anwendungsbereich des vorliegenden Zertifizierungshandbuchs erstreckt sich auf die Personenzertifizierungen im Bereich »Cyber Security« durch die Fraunhofer-Personenzertifizierungsstelle.

Die Personenzertifizierungen im Bereich »Cyber Security« beziehen sich aktuell auf folgendes Zertifizierungsprofil:

- Level 1 (Basic): Security Champion (Software Security) – Basic Level

Eine detaillierte Beschreibung des Zertifizierungsprofils befindet sich in Anhang A

Mittel- bis langfristig sind weitere Zertifizierungsprofile im Bereich Cyber Security auf drei Stufen und für unterschiedliche Tätigkeitsbereiche geplant.

- Level 1 (Basic)
- Level 2 (Advanced)
- Level 3 (Senior)

Die verschiedenen Zertifizierungsprofile bauen wie folgt aufeinander auf:

Auf Level 1 (Basic) werden Zertifikate vergeben, die eine grundlegende Qualifikation in den wesentlichen inhaltlichen und methodischen Aspekten im Bereich Cyber Security für das jeweilige Aufgabenprofil / die jeweilige Rolle von Mitarbeitenden im Unternehmen darstellen.

Zugangsvoraussetzung für Prüfungen auf dem Level 1 können je nach Zertifizierungsprofil variieren und sind in den Anhängen beschrieben. In der Regel wird der Nachweis von Vorbildung sowie der Nachweis der Teilnahme an einer von der Fraunhofer-Personenzertifizierungsstelle anerkannten Weiterbildungsmaßnahme auf dem Basic Level gefordert. Das Zertifikat wird vergeben, wenn zusätzlich die Abschlussprüfung auf dem Basic Level bestanden wurde.

Level 2 (Advanced Level), beinhaltet vertiefte Kompetenzen und Erfahrung im Bereich Cyber Security.

Das Zertifikat wird vergeben bei Nachweis eines Zertifikats auf dem Level 1, dem Nachweis der Teilnahme an einer von der Fraunhofer-Personenzertifizierungsstelle anerkannten Weiterbildung auf dem Advanced Level, Vorlage eines Nachweises von Berufserfahrung sowie dem Nachweis, dass die Zertifizierungsprüfung auf dem Advanced Level bestanden wurde.

Level 3 (Senior Level) bescheinigt umfassende Kompetenzen in und Erfahrung mit der Durchführung von Cyber Security-Projekten im jeweiligen Aufgabenbereich.

Das Zertifikat »Cyber Security Senior Level« wird vergeben, wenn neben mehrjähriger Berufserfahrung das Zertifikat »Cyber Security Advanced Level« sowie die Kompetenzen im Rahmen der Vorstellung eines Cyber Security Projekts nachgewiesen werden können und eine zugehörige Abschlussprüfung bestanden wurden.

Nachfolgende Abbildung stellt die Zusammenhänge zwischen den einzelnen Zertifizierungsprofilen dar.

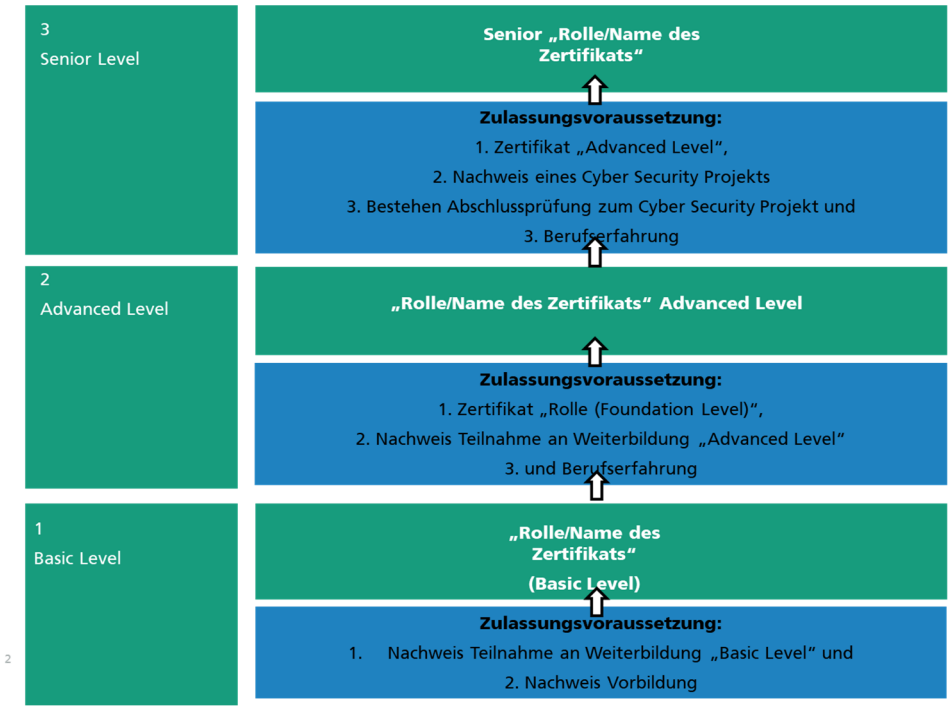

Abbildung 1: Zusammenhänge zwischen den Personenzertifizierungen im Bereich Cyber Security

Die Anforderungen der Zertifizierungsprofile sind in den Anlagen des vorliegenden Dokuments aufgeführt und sind Bestandteil der jeweiligen Personenzertifizierung.

3 ALLGEMEINGÜLTIGE BEGRIFFE

- **Fraunhofer-Personenzertifizierungsstelle**
  Stelle in der Fraunhofer-Gesellschaft, die Zertifizierungen der Konformität von normativen Vorgaben und der tatsächlichen Personenqualifikation durchführt.

- **Prüfungsbeauftragte (PB)**
  Fachkräfte, die im Auftrag der Fraunhofer-Personenzertifizierungsstelle tätig werden, um Personen zu prüfen. Sie sind in der Wahrnehmung ihrer Prüfungsaufgaben fachlich unabhängig. Die Anforderungen an die Prüfungsbeauftragten sind im jeweiligen Kompetenzprofil festgelegt.

- **Schriftführer*in (SchF)**
  Personen, die im Auftrag der Fraunhofer-Personenzertifizierungsstelle tätig werden, um während mündlichen Prüfungen Protokoll zu schreiben. Sie sind nicht an der Findung des Prüfungsergebnisses beteiligt. Die Anforderungen an die Schriftführenden sind im jeweiligen Kompetenzprofil festgelegt.

- **Fachausschüsse (FA)**
  Von der Fraunhofer-Personenzertifizierungsstelle berufene Gremien von Fachkräften, welche Prüfungsinhalte verifizieren und validieren, Prüfungsaufgaben erstellen, für Fachanfragen zuständig sind sowie die Fraunhofer-Personenzertifizierungsstelle hinsichtlich der fachlichen Qualität der Prüfungsbeauftragten beraten. Näheres zu Aufgaben und Befugnissen findet sich in der »Geschäftsordnung des Fachausschusses«. Für jedes Zertifizierungsprofil wird jeweils ein eigener Fachausschuss gebildet.

- **Begriff »kennen«**
  Befindet sich nach der Bloom'schen Lernzieltaxonomie (*Taxonomie von Lernzielen im kognitiven Bereich.* (Taxonomy of educational objectives, 1974. 5. Auflage. Beltz Verlag, Weinheim 1976) auf der ersten und zweiten Stufe der sechststufigen Skala. Kennzeichnend dafür ist die Wiedergabe aus dem Gedächtnis auf Abruf durch Stichworte. Die dafür ausgeprägten Fertigkeiten sind Wissen, Erkennen, Nachahmen, Vergleichen, Ableiten und Klassifizieren.
  Das Ziel »kennen« in Prüfungen im Bereich Cyber Security beinhaltet für jedes Zertifizierungsprofil unterschiedliche Inhalte. Diese werden in den Anhängen zu diesem Dokument beschrieben.

- **Begriff »anwenden«**
  Ist ein synonym verwendeter Begriff für die dritte und vierte Lernzielstufe der Bloom'schen Lernzieltaxonomie.
  Kennzeichnend dafür ist die eigene Verarbeitung und Einordnung des Gelernten. Die dafür ausgeprägten Fertigkeiten sind Verstehen, Reagieren und Üben.
  Das Ziel »anwenden« in Prüfungen im Bereich Cyber Security beinhaltet für jedes Zertifizierungsprofil unterschiedliche Inhalte. Diese werden in den Anhängen zu diesem Dokument beschrieben.

■ **Begriff »beurteilen«**

Ist ein synonym verwendeter Begriff für die Lernzielstufe »Transfer« und »Problemlösendes Denken«. Ist ein synonym verwendeter Begriff für die fünfte und sechste Lernzielstufe der Bloom'schen Lernzieltaxonomie.

Kennzeichnend dafür ist die Übertragung der Grundprinzipien auf neue, ähnliche Aufgaben bzw. auf für die Lernenden neue Leistungen. Die dafür ausgeprägten Fertigkeiten sind Beurteilen, Werten, Koordinieren bzw. Problemlösen, Werte leben, Automatisieren.

Das Ziel »beurteilen« in Prüfungen im Bereich Cyber Security beinhaltet für die Zertifizierungsprofile unterschiedliche Inhalte. Diese werden in den Anhängen zu diesem Dokument beschrieben.

4 VORGABEN FÜR DAS ZERTIFIZIERUNGSVERFAHREN

Nachfolgend werden Vorgaben für das Zertifizierungsverfahren beschrieben.

4.1 Ziel

Durch Zertifizierungen werden anhand von definierten Anforderungsprofilen Qualifikationsmerkmale geprüft und deren Qualität durch ein Kompetenzzertifikat attestiert.

4.2 Antragstellung

Zertifiziert werden können Personen, die eine Prüfung der Fraunhofer-Personenzertifizierungsstelle im Bereich Cyber Security erfolgreich bestehen und die definierten Zugangsvoraussetzungen entsprechend den Anlagen dieses Zertifizierungshandbuchs erfüllen.

Personen, welche an der Zertifizierungsprüfung / Wiederholungsprüfung teilnehmen möchten, müssen bei der Fraunhofer-Personenzertifizierungsstelle dazu einen schriftlichen Antrag. Dieser Antrag muss folgende Angaben des Prüfungsteilnehmenden enthalten:

- Name, Geburtsdatum und private Postanschrift
- Tätigkeit
- zu zertifizierendes Zertifizierungsprofil
- Angabe, ob es sich um eine Erstprüfung oder Wiederholungsprüfung handelt.

Die Prüfungstermine werden von der Fraunhofer-Personenzertifizierungsstelle festgelegt.

4.3 Zugangsvoraussetzungen

Um zur Prüfung zugelassen zu werden, müssen die Teilnehmenden einen Nachweis über die für jedes Zertifizierungsprofil im Anhang definierten Zugangsvoraussetzungen erbringen. Die geforderten Zugangsvoraussetzungen unterscheiden sich je nach Zertifizierungsprofil.

Die Prüfungsteilnehmenden haben die Möglichkeit, fehlende Berufserfahrung innerhalb von einem Jahr nach Ablegen der jeweiligen Zertifizierungsprüfung (Zertifizierungsprofile in den Anhängen) nachzuweisen.

4.4 Prüfungsdurchführung

Nachfolgend wird die Prüfungsdurchführung für die bestehenden Zertifizierungsprofile im Bereich Cyber Security beschrieben. Das vorliegende Zertifizierungshandbuch wird jeweils um das Prüfungsvorgehen von neuen Zertifizierungsprofilen erweitert, sobald diese vom Fachausschuss verabschiedet wurden.

Zertifizierungsprofil »Security Champion (Software Security) - Basic Level«:
Bei den Prüfungen auf Level 1 (Basic Level) zum »Security Champion (Software Security) - Basic Level« handelt es sich um mündliche Prüfungen mit theoretischen und praxisnahen Prüfungsaufgaben.

4.4.1 Zusammenstellung und Bereitstellung der Prüfungsunterlagen und Beauftragung der Prüfungsbeauftragten

Zusammenstellung der Prüfungsunterlagen

Mündliche Prüfungen

Die Fraunhofer-Personenzertifizierungsstelle stellt den Prüfungsbeauftragten die theoretischen und praxisnahen Prüfungsfragen für die mündlichen Zertifizierungsprüfungen aus einem vom zuständigen Fachausschuss bestätigten Prüfungsfragenpool für das jeweilige Zertifizierungsprofil zur Verfügung.

Die Prüfungsfragen- und aufgaben werden den Prüfungsbeauftragten ausreichend frühzeitig vor der Prüfung zur Verfügung gestellt, damit sie die Prüfung zum festgesetzten Termin durchführen können. Die Bereitstellung der Prüfungsfragen und -aufgaben erfolgt geschützt vor unbefugtem Zugriff.

Beauftragung der Prüfungsbeauftragten und Schriftführer

Die Leitung der Fraunhofer-Personenzertifizierungsstelle beauftragt die Prüfungsbeauftragten mit der Abnahme und der Bewertung der mündlichen Prüfung sowie die Schriftführer mit der Protokollführung während der Prüfung.

Alle benötigten Dokumente für die Prüfungsvorbereitung und Abnahme werden den Prüfungsbeauftragten und Schriftführern rechtzeitig vor der Prüfung zur Verfügung gestellt.

4.4.2 Durchführung von mündlichen Prüfungen

Bei mündlichen Prüfungen handelt es sich in der Regel um Präsenzprüfungen. Diese finden an einem von der Fraunhofer-Personenzertifizierungsstelle abgenommenen Ort statt, der die von der Fraunhofer-Personenzertifizierungsstelle festgelegten Bedingungen erfüllt.

Die mündlichen Prüfungen können jedoch auch als online-Prüfungen durchgeführt werden, sofern die Vergleichbarkeit der Prüfungssituation (in Präsenz vs. online) gegeben bleibt.

Bei mündlichen Prüfungen werden den Teilnehmenden offene Fragen gestellt, die die teilnehmende Person zu Beginn der Prüfung zufällig aus dem Prüfungsfragenpool auswählt. Dabei wird vorgegeben, aus welchem Themenbereich wie viele Aufgaben / Fragen gezogen werden müssen.

Bei den Prüfungsfragen / -aufgaben handelt es sich um offene Fragenformate, für die jeweils auch ein Erwartungshorizont vorliegt.

Die Prüfungsfragen /- aufgaben bei mündlichen Prüfungen sind sowohl bei Präsenzprüfungen als auch bei Online-Prüfungen mündlich zu beantworten.

Die mündliche Prüfung erfolgt in der Regel in Form einer Einzelprüfung, kann aber auch als Gruppenprüfung mit bis zu drei Teilnehmenden durchgeführt werden.

Die mündlichen Prüfungen auf Level 1 dauern 30 Minuten pro Person.
Die Dauer der Prüfungen auf Level 2 und 3 wird noch festgelegt.

Hilfsmittel sind grundsätzlich keine zugelassen.

Es wird sichergestellt, dass für die Beantwortung der Fragen der mündlichen Prüfung ausreichend Zeit zur Verfügung steht. Hierzu wird bereits bei der Konzeption der Fragen vom zuständigen Fachausschuss überprüft, wie viel Zeit die Beantwortung der Fragen ungefähr in Anspruch nimmt.

Für Teilnehmende, die die Prüfung aufgrund einer Beeinträchtigung nicht in der vorgesehenen Form durchführen können, sind individuelle Ausnahmeregelungen vorgesehen.

4.5 Prüfungsfragen und -aufgaben

Der Prüfungsfragenpool unterscheidet sich je nach Zertifizierungsprofil. Gleiches gilt für die Anzahl der Aufgaben und Fragen für die theoretischen und praktischen Prüfungsteile von mündlichen Prüfungen.

Der Prüfungsfragenpool beinhaltet sowohl die theoretischen Prüfungsaufgaben und -fragen als auch die praxisnahen Aufgabenstellungen.

Die Fragen sind eindeutig dem Zertifizierungsprofil und Themenbereichen zugeordnet. Jedem Prüfungsteilnehmenden dürfen nur Fragen und Aufgaben gestellt werden, die seinem fachlichen Anforderungsprofil entsprechen.

4.6 Auswertung und Bewertung von Prüfungen

Die Bewertung von mündlichen Prüfungen erfolgt während bzw. unmittelbar im Anschluss an die Prüfung durch fachlich qualifizierte Prüfungsbeauftragte und wird den Teilnehmenden in der Regel am Prüfungstag, spätestens eine Woche nach der Prüfung bekanntgegeben.

Für jede Frage und Aufgabe der mündlichen Prüfungen werden den Prüfungsbeauftragten Erwartungshorizonte vorgegeben, die als Richtlinie für die Beurteilung der Frage verwendet werden. Zusätzlich wird für jede Frage und Aufgabe die Vergleichbarkeit und zu erreichende Punktzahl durch den Fachausschuss bestätigt.

Die Prüfungsteilnehmenden müssen einen Mindesterfüllungsgrad von 67% erreichen.

Erreichen die Teilnehmenden weniger als 67%, wird kein Zertifikat erteilt.

Bei Nichtbestehen kann die Prüfung maximal zweimal innerhalb von zwei Jahren nach der letzten Teilprüfung wiederholt werden.

4.7 Zertifizierung

Nach erfolgreich abgelegter Prüfung und Erfüllung der Zugangsvoraussetzungen wird dem Prüfungsteilnehmenden von der Fraunhofer-Personenzertifizierungsstelle das für das jeweilige Zertifizierungsprofil vorgesehene Zertifikat ausgehändigt.

Die Prüfungsteilnehmenden haben die Möglichkeit, fehlende Berufserfahrung innerhalb von einem Jahr nach Ablegen der jeweiligen Zertifizierungsprüfung (Zertifizierungsprofile in den Anhängen) nachzuweisen.

Die Zertifikatserteilung erfolgt, sobald die Berufserfahrung nachgewiesen wurde. Die Zertifikatserteilung muss spätestens ein Jahr nach Ablegen der letzten Prüfung erfolgen.

Zertifikate im Zertifizierungsbereich »Cyber Security« (unabhängig vom Zertifizierungsprofil) sind drei Jahre gültig.

4.8 Rezertifizierung

Für alle Zertifizierungsprofile ist nach einer Zertifikatslaufzeit von drei Jahren minus einem Tag nach der letzten Teilprüfung eine Rezertifizierung erforderlich.

Die Rezertifizierung ist jeweils nur für das Zertifikat des höchsten erworbenen Levels notwendig.

Zu erbringende Nachweise für die Rezertifizierung

- Nachweis von Berufserfahrung auf dem Gebiet des zu rezertifizierenden Profils während der Zertifikatslaufzeit durch:
  - Einreichen von Nachweisen über die Durchführung von Cyber Security Aufgaben und Projekten im Kontext des jeweiligen Zertifizierungsprofils

und

- Nachweis der Teilnahme an einer von der Fraunhofer-Personenzertifizierungsstelle anzuerkennenden Weiterbildungsveranstaltung während der Zertifikatslaufzeit, in der nachweislich aktuelle fachspezifische Informationen bezüglich des im Zertifizierungshandbuch Cyber Security definierten Kompetenzprofils oder aktuelle weiterführende Themen im Kontext von Cyber Security vermittelt werden.

Mindestanforderungen an die nachzuweisende Weiterbildungsveranstaltung:

Es muss sich um eine mindestens zweitägige Veranstaltung handeln, die sich mit Themen der Cyber Security beschäftigt.

Ablauf der Rezertifizierung

Die zertifikatstragende Person muss in dem Zeitraum von zwei Jahren minus einem Tag nach der letzten Teilprüfung bis 2,5 Jahren minus einem Tag nach der letzten Teilprüfung (Das bedeutet: ab 2 Jahre bis spätestens 2,5 Jahre nach der Zertifizierung; also bis sechs Monate vor Ablauf des Zertifikats) die Rezertifizierung formal beantragen und sowohl die Berufserfahrung als auch die Teilnahme an einer Weiterbildungsveranstaltung nachweisen.

Über die Anerkennung der Berufserfahrung sowie der Weiterbildungsveranstaltung entscheidet die Leitung der Fraunhofer-Personenzertifizierungsstelle.

In Ausnahmefällen können Berufserfahrung und Teilnahme an einer Weiterbildungsveranstaltung auch innerhalb der letzten sechs Monate vor Ablauf des Zertifikats anerkannt

werden. Dies muss bis 2,5 Jahre minus einem Tag nach der letzten Teilprüfung bei der Fraunhofer-Personenzertifizierungsstelle schriftlich beantragt und begründet werden. Über die Gewährung dieser Ausnahmeregelung entscheidet die Leitung der Fraunhofer-Personenzertifizierungsstelle im Einzelfall.

Werden die Rezertifizierungsbedingungen nicht eingehalten, erlischt die Gültigkeit des Zertifikats mit dem Ablaufdatum. Das Zertifikat muss neu erworben werden (siehe Erstzertifizierung).

In begründeten Ausnahmefällen kann ein Aufschub von maximal sechs Monaten gewährt werden (z.B. im Falle von schwerer Krankheit oder Elternzeit). Auch dieser Aufschub muss schriftlich beantragt und begründet werden. Die Entscheidung über die Gewährung eines Aufschubs liegt bei der Leitung der Fraunhofer-Personenzertifizierungsstelle.

Nachweis von Berufserfahrung und Teilnahme an einer Weiterbildungsveranstaltung

Der Nachweis der **Berufserfahrung** kann beispielsweise durch eine Bescheinigung des Arbeitgebers erfolgen.

Der Nachweis der **Teilnahme an der Weiterbildungsveranstaltung** erfolgt durch eine Teilnahmebescheinigung des Weiterbildners sowie die Einreichung einer Agenda, aus der die fachspezifischen Themen hervorgehen, die behandelt wurden.

Rezertifizierung

Bei Erfüllung der Rezertifizierungsanforderungen wird das jeweilige Zertifikat für weitere drei Jahre minus einen Tag verlängert.

Bei Nicht-Erfüllen der Rezertifizierungsanforderungen erlischt die Gültigkeit des jeweiligen Zertifikats.

5 RECHTE UND PFLICHTEN (Stand Dezember 2023)

Die Erteilung des Zertifikats ist mit einigen Rechten und Pflichten verbunden, auf die wir bereits im Vorfeld hinweisen möchten. Diese Regelungen werden Ihnen mit der späteren Erteilung des Zertifikats nochmals ausgehändigt.

5.1 Bekanntmachung

Die Fraunhofer-Personenzertifizierungsstelle darf auf schriftliche *Anfrage, (z.B. von potentiellen Auftraggebern einer zertifikatstragenden Person) unter Angabe der Zertifikatsnummer Auskunft darüber erteilen, ob diese Person das* Zertifikat rechtmäßig trägt. Zur Identifikation der zertifikatstragenden Person werden deren Name, Geburtsdatum und Geburtsort gespeichert. Mit der Anmeldung erklären Teilnehmende durch ihre Unterschrift ihre Absicht, diese Regelungen im Falle der Erteilung des Zertifikats zu akzeptieren. Die Fraunhofer-Personenzertifizierungsstelle ist an die Bestimmungen des deutschen Bundesdatenschutzgesetzes gebunden.

5.2 Rechte

Die zertifikatstragende Person ist berechtigt, im Rahmen ihrer Tätigkeit im Bereich »Cyber Security«:

- auf persönlichen Briefbögen, in sonstigen Drucksachen in Zusammenhang mit ihrer Person sowie im Internet im Zusammenhang mit ihrer Person auf ihre Zertifizierung wie folgt hinzuweisen: »zertifizierter NAME DES ZERTIFIKATS, geprüft durch die Fraunhofer-Personenzertifizierungsstelle« oder »zertifizierter »NAME DES ZERTIFIKATS« (z.B. »certified Security Champion (Software Security) - Basic Level« oder in der Kurzbezeichnung »certified Security Champion – Basic Level«). Bei Verwendung der Variante 1 ist darauf zu achten, dass die Bezeichnung »geprüft durch die Fraunhofer-Personenzertifizierungsstelle« nicht größer ist als der zugehörige Name der Person.r
- die ausgehändigte Zertifizierungs-Urkunde zu verwenden, allerdings nur im Ganzen.
- das Zertifizierungshandbuch »Personenzertifizierungen im Bereich Cyber Security« einzusehen, welches das Zertifizierungssystem im Bereich Cyber Security der Fraunhofer-Personenzertifizierungsstelle erläutert.

Näheres ist unter den Pflichten geregelt.

5.3 Pflichten

Folgende Pflichten sind bei der Ausübung der Aufgaben im Bereich » Cyber Security« von der zertifikatstragenden Person einzuhalten:

5.3.1 Gewissenhaftigkeit und Fortbildung

Die zertifikatstragende Person hat die in ihrem zertifizierten Profil genannten Tätigkeiten unter Berücksichtigung des Standes der anerkannten Regeln im Bereich Cyber Security zu erledigen.

Das Handeln der zertifikatstragenden Personen ist von dem Grundsatz geprägt, stets ein fehlerfreies und qualitativ hochwertiges Arbeitsergebnis zu erzielen.

Sie ist verpflichtet, die Zertifizierung nicht in einer missbräuchlichen Art und Weise zu verwenden und keinerlei Aussagen zu treffen, die von der Fraunhofer-Personenzertifizierungsstelle als irreführend oder unbefugt betrachtet werden müssen.

5.3.2 Unabhängigkeit

Die zertifikatstragende Person hat insbesondere darauf zu achten, dass sie ihr Handeln ohne Rücksicht auf dienstliche Beziehungen im Unternehmen, die übrigen Beschäftigten und / oder deren Ergebniswünschen ausrichtet (persönliche Unabhängigkeit).

5.3.3 Persönliche Aufgabenerfüllung

Die zertifikatstragende Person hat die von ihr geforderten Leistungen bei der Vorbereitung, Durchführung und Bewertung von Projekten persönlich zu erbringen bzw. zu überwachen. Sie darf ihre Zertifizierungsurkunde nicht in missbräuchlicher Weise verwenden.

5.3.4 Zulässige Verwendung von Zertifikaten

Folgende Regelungen gelten bezüglich der Verwendung von Zertifikaten:

- Das Zertifikat wird zwar der jeweiligen zertifikatstragenden Person erteilt; die Zertifikatsurkunde bleibt jedoch Eigentum der Fraunhofer-Personenzertifizierungsstelle.
- Es dürfen nur gültige Zertifikate verwendet werden.
- Das Zertifikat darf nicht missbräuchlich verwendet werden.
- Die Zertifizierungs-Urkunde darf nicht verändert werden und nur im Ganzen verwendet werden.
- Das Zertifikat ist der Fraunhofer-Personenzertifizierungsstelle zurückzugeben, nachdem das Zertifikat ausgelaufen ist, oder sobald die zertifikatstragende Person durch die Fraunhofer-Personenzertifizierungsstelle über den Entzug des Zertifikats informiert wurde
- Bei Aussetzung, Erlöschen oder Entzug von Zertifikaten ist die Verwendung des Zertifikats unverzüglich einzustellen; etwaige Hinweise auf das Zertifikat und die Fraunhofer-Personenzertifizierungsstelle sind unverzüglich zu löschen. Etwaige noch vorhandene Briefbögen und sonstige Drucksachen sind, im Falle der Aussetzung für deren Dauer nicht zu verwenden, ansonsten sind sie zu vernichten.
- Die Nutzung des Zertifikats bzw. Hinweise auf das Zertifikat sind nur im Geltungsbereich des Zertifikats gestattet.
- Das Zertifikat darf ausschließlich im Zusammenhang mit der darin zertifizierten Person verwendet werden.
- Die Verwendung des Zertifikats und Hinweise auf das Zertifikat sind nur zulässig, wenn für den Betrachter eindeutig erkennbar ist, welche Person in welchem Bereich geprüft und zertifiziert wurde.
- Durch die Verwendung des Zertifikats und Hinweise auf das Zertifikat darf nicht der Eindruck entstehen, dass die zertifizierte Person zum Personal der Fraunhofer-Gesellschaft gehört oder sie in ihrem Auftrag handelt.
- Die zertifikatstragende Person ist für die korrekte Verwendung des Zertifikats verantwortlich; etwaige Zweifel gehen zu ihren Lasten.

5.3.5 Verwendung des Fraunhofer-Logos

Das Zertifikat der Fraunhofer-Personenzertifizierungsstelle enthält auch das Fraunhofer-Logo. Das Logo darf ausschließlich als Teil des Zertifikats verwendet werden und zwar dergestalt, dass die Zertifizierungs-Urkunde im Ganzen als Nachweis der ausstellenden Fraunhofer-Personenzertifizierungsstelle für z. B. Kunden oder Arbeitgeber kopiert bzw. im Internet eingestellt werden kann. Jedwede darüber hinaus gehende Nutzung des Fraunhofer-Logos oder die markenmäßige Verwendung des Namens Fraunhofer ist ausdrücklich untersagt und kann im Falle von Zuwiderhandlungen Schadensersatzansprüche der Fraunhofer-Gesellschaft nach sich ziehen.

5.3.6 Anzeigepflicht

Die zertifikatstragende Person hat der Fraunhofer-Personenzertifizierungsstelle unverzüglich schriftlich anzuzeigen:
- Namensänderung (z. B. durch Hochzeit),
- die Änderung ihres Wohnsitzes,
- den Verlust des Zertifikates.

Zudem muss die zertifikatstragende Person die Fraunhofer-Personenzertifizierungsstelle unmittelbar über Angelegenheiten informieren, die ihre Fähigkeit weiterhin die Zertifizierungsanforderung zu erfüllen, beeinträchtigt können (z. B. neu auftretende körperliche Einschränkungen).

5.3.7 Auskunftspflicht

Die zertifikatstragende Person hat auf Verlangen der Fraunhofer-Personenzertifizierungsstelle die Einhaltung ihrer Pflichten erforderlichen Auskünfte (mündlich / schriftlich) innerhalb der gesetzten Fristen und unentgeltlich zu erteilen sowie angeforderte Unterlagen auf ihre Kosten vorzulegen.

Sie kann die Auskunft auf solche Fragen verweigern, deren Beantwortung sie selbst oder einen ihrer Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

5.4 Verstoß gegen die Pflichten als zertifikatstragende Person

Ein Verstoß gegen die unter Punkt 5.3.1 bis 5.3.7 aufgeführten Pflichten führt je nach Schwere zur Aussetzung oder zum Entzug der Zertifizierung, welche der zertifikatstragenden Person schriftlich mitgeteilt wird. Für die Dauer der Aussetzung bzw. nach erfolgtem Entzug der Zertifizierung ist es der zertifikatstragenden Person untersagt, auf die Zertifizierung und die Fraunhofer-Personenzertifizierungsstelle hinzuweisen.

ANLAGE A: »SECURITY CHAMPION (SOFTWARE SECURITY) - BASIC LEVEL«

A 1 Verweis auf andere Normen und Dokumente

- EN ISO 17024

A 2 Anforderungsprofil

A 2.1 Bestimmung des Anforderungsprofils

Das Anforderungsprofil eines »Security Champion (Software Security) - Basic Level« ergibt sich aus der Charakteristik und Beschreibung seines Tätigkeitsfeldes.

Ein zertifizierter »Security Champion (Software Security) - Basic Level« …

- können die Rolle des Security Champions erklären inkl. notwendigen Kompetenzen und Pflichten,
- sind sensibilisiert für das Thema Software Security und kennen die dazugehörige Terminologie,
- können Software Security-Anforderungen für ihr Produkt definieren und eine Risikoanalyse durchführen,
- kennen die Prinzipien des Secure Design und des Defensive Coding,
- kennen die Maßnahmen im Kontext Security Testing, z.B. Code Review und statische Codeanalyse,
- können Security-Awareness schaffen und in ihrem Team als Multiplikator agieren.

Die Bezeichnung lautet: »Certified Security Champion (Software Security) - Basic Level«

Die Kurzbezeichnung lautet: »Certified Security Champion - Basic Level«

A 2.2 Zugangsvoraussetzungen

A 2.2.1 Vorbildungen

Ein zertifizierter »Security Champion (Software Security) - Basic Level« muss nachweisen:

Ein erfolgreich abgeschlossenes Studium an
- einer deutschen wissenschaftlichen Hochschule,
- einer deutschen staatlichen oder staatlich anerkannten Hochschule oder
- einer von der zuständigen Stelle des Landes als gleichwertig anerkannten ausländischen Hochschule

oder

- eine mindestens 2-jährige Tätigkeit im Bereich Informatik.

und

- die Teilnahme an einer von der Fraunhofer-Personenzertifizierungsstelle anerkannten Weiterbildung zum Security Champion (Software Security) - Basic Level.

Die Zugangsvoraussetzungen müssen rechtzeitig vor der Prüfung eingereicht werden, spätestens eine Woche vor dem Prüfungstermin.

Im zu prüfenden Einzelfall hat die antragstellende Person die Möglichkeit, fehlende Zugangsvoraussetzungen innerhalb von einem Jahr nach Ablegen der Prüfung nachzuweisen.

Nach Prüfung der eingereichten Unterlagen entscheidet die Fraunhofer-Personenzertifizierungsstelle über die Voraussetzung. Sollten Zugangsvoraussetzungen nicht erfüllt sein, teilt die Fraunhofer-Personenzertifizierungsstelle dies der antragstellenden Person unverzüglich über das Sekretariat der Fraunhofer-Personenzertifizierungsstelle mit.

Grundsätzlich kann die Fraunhofer-Personenzertifizierungsstelle in begründeten Ausnahmefällen davon abweichende Nachweise akzeptieren. Diese Nachweise und die Entscheidung der Fraunhofer-Personenzertifizierungsstelle sind zu dokumentieren.

A 2.2.2 Zusätzliche Ausbildungen/Berechtigungen und praktische Tätigkeiten

Keine.

A 2.2.3 Persönliche Voraussetzungen

Keine.

A 2.3 Geforderte Kompetenzen (Lernziele)

Grundlage für die Prüfung zum »Security Champion (Software Security) - Basic Level« sind folgende Kompetenzen (Lernziele):

Themenbereich	**Kompetenzen (Lernziele)** **Die Zertifikatstragenden können…**	**Kennen** (Wissen und Verstehen)	**Anwenden** und Analysieren	Synthese und **Beurteilen**
01 - Security Champion (Theorie)	erklären welche Rolle der Security Champion einnimmt und dabei auf Aufgaben und Kompetenzen eingehen.	x		
02 - Motivation & Awareness (Theorie)	Dritte für Software Security sensibilisieren.	x		
03 - Secure Requirements und Risk Management (Theorie)	die Risikoanalyse inkl. ihrer Bestandteile erklären.	x		
04 - Secure Requirements und Risk Management (Praxis)	für ein gegebenes kurzes Szenario eine Risikoanalyse durchführen.	x	x	
05 - Secure Design (Theorie und Praxis)	die Prinzipien des Secure Design erklären.	x		
05 - Secure Design (Theorie und Praxis)	die Prinzipien des Secure Design in einem gegebene Szenarien analysieren.	x	x	
06 - Defensive Coding (Theorie)	die Prinzipien des Defensive Coding erklären.	x		
07 - Vulnerabilities (Theorie)	typischen Vulnerabilities im Code erklären und wie man sie verhindert.	x		
08 - Kryptographie (Theorie)	kryptographische Konzepte kurz erklären.	x		

Themenbereich	**Kompetenzen (Lernziele)** **Die Zertifikatstragenden können…**	**Kennen** (Wissen und Verstehen)	**Anwenden** und Analysieren	Synthese und **Beurteilen**
09 - Security Testing & Incident Response (Theorie)	Maßnahmen im Kontext Security Testing erklären.	x		
09 - Security Testing & Incident Response (Theorie)	für das Thema Incident Response sensibilisieren und hierhin Konzepte erläutern.	x		
10 - Softskills (Praxis)	ein gegebenes fiktives Szenario im Alltag eines Security Champion analysieren und ihre Softskills unter Beweis stellen.	x	x	

Der »Security Champion« umfasst noch keine Themenbereiche, die er beurteilen können muss.