Curriculum für

# Certified Professional for Software Architecture (CPSA)®
*Advanced Level*

## Modul
## EMBEDDEDSEC

## Embedded Security for Architects

2025.1-rev0-DE-20250912

# Inhaltsverzeichnis

Die Abkürzung "e. V." ist Teil des offiziellen Namens des iSAQB und steht für "eingetragener Verein", der seinen Status als juristische Person nach deutschem Recht beschreibt. Der Einfachheit halber wird iSAQB e. V. im Folgenden ohne die Verwendung dieser Abkürzung als iSAQB bezeichnet.

# Einführung: Allgemeines zum iSAQB Advanced Level

## Was vermittelt ein Advanced Level Modul?

Das Modul kann unabhängig von einer CPSA-F-Zertifizierung besucht werden.

- Der iSAQB Advanced Level bietet eine modulare Ausbildung in drei Kompetenzbereichen mit flexibel gestaltbaren Ausbildungswegen. Er berücksichtigt individuelle Neigungen und Schwerpunkte.
- Die Zertifizierung erfolgt als Hausarbeit. Die Bewertung und mündliche Prüfung wird durch vom iSAQB benannte Expert:innen vorgenommen.

## Was können Absolventen des Advanced Level (CPSA-A)?

CPSA-A-Absolventen können:

- eigenständig und methodisch fundiert mittlere bis große IT-Systeme entwerfen
- in IT-Systemen mittlerer bis hoher Kritikalität technische und inhaltliche Verantwortung übernehmen
- Maßnahmen zur Erreichung von Qualitätsanforderungen konzeptionieren, entwerfen und dokumentieren sowie Entwicklungsteams bei der Umsetzung dieser Maßnahmen begleiten
- architekturrelevante Kommunikation in mittleren bis großen Entwicklungsteams steuern und durchführen

## Voraussetzungen zur CPSA-A-Zertifizierung

- erfolgreiche Ausbildung und Zertifizierung zum Certified Professional for Software Architecture, Foundation Level® (CPSA-F)
- mindestens drei Jahre Vollzeit-Berufserfahrung in der IT-Branche; dabei Mitarbeit an Entwurf und Entwicklung von mindestens zwei unterschiedlichen IT-Systemen
    - Ausnahmen sind auf Antrag zulässig (etwa: Mitarbeit in Open-Source-Projekten)
- Aus- und Weiterbildung im Rahmen von iSAQB-Advanced-Level-Schulungen im Umfang von mindestens 70 Credit Points aus mindestens drei unterschiedlichen Kompetenzbereichen
- erfolgreiche Bearbeitung der CPSA-A-Zertifizierungsprüfung

# Grundlegendes

## Was vermittelt das Modul „EMBEDDEDSEC“?

Das Modul präsentiert den Teilnehmerinnen und Teilnehmern Embedded Security for Architects als … Am Ende des Moduls kennen die Teilnehmerinnen und Teilnehmer … und können …

## Struktur des Lehrplans und empfohlene zeitliche Aufteilung

| Inhalt | Empfohlene Mindestdauer (min) |
|---|---|
| 1. Thema mit Einleitung | 180 |
| 2. Thema über xz | 150 |
| 3. Thema mit viel Theorie | 120 |
| 4. Thema mit xy und Beispiel | 180 |
| 5. Thema mit abc und d | 210 |
| 6. Thema mit Abschlussbeispiel | 120 |
| | |
| Summe | 960 (16h) |

## Dauer, Didaktik und weitere Details

Die unten genannten Zeiten sind Empfehlungen. Die Dauer einer Schulung zum Modul EMBEDDEDSEC sollte mindestens 3 Tage betragen, kann aber länger sein. Anbieter können sich durch Dauer, Didaktik, Art und Aufbau der Übungen sowie der detaillierten Kursgliederung voneinander unterscheiden. Insbesondere die Art der Beispiele und Übungen lässt der Lehrplan komplett offen.

Lizenzierte Schulungen zu EMBEDDEDSEC tragen zur Zulassung zur abschließenden Advanced-Level-Zertifizierungsprüfung folgende Credit Points) bei:

| | |
|---|---|
| Methodische Kompetenz: | 20 Punkte |
| Technische Kompetenz: | 10 Punkte |
| Kommunikative Kompetenz: | 0 Punkte |

## Voraussetzungen

Teilnehmerinnen und Teilnehmer **sollten** folgende Kenntnisse und/oder Erfahrung mitbringen:

- Voraussetzung 1
- Voraussetzung 2, etc.

**Hilfreich** für das Verständnis einiger Konzepte sind darüber hinaus:

- Kenntnisgruppe 1:
  - Kenntnis 1
  - Erfahrung 2
  - Kenntnis 3

- Erfahrung 4
- Wissen 5

## Gliederung des Lehrplans

Die einzelnen Abschnitte des Lehrplans sind gemäß folgender Gliederung beschrieben:

- **Begriffe/Konzepte**: Wesentliche Kernbegriffe dieses Themas.
- **Unterrichts-/Übungszeit**: Legt die Unterrichts- und Übungszeit fest, die für dieses Thema bzw. dessen Übung in einer akkreditierten Schulung mindestens aufgewendet werden muss.
- **Lernziele**: Beschreibt die zu vermittelnden Inhalte inklusive ihrer Kernbegriffe und -konzepte.

Dieser Abschnitt skizziert damit auch die zu erwerbenden Kenntnisse in entsprechenden Schulungen.

## Ergänzende Informationen, Begriffe, Übersetzungen

Soweit für das Verständnis des Lehrplans erforderlich, haben wir Fachbegriffe ins iSAQB-Glossar aufgenommen, definiert und bei Bedarf durch die Übersetzungen der Originalliteratur ergänzt.

# 1. Einführung

| | |
|---|---|
| Dauer: XXX Min. | Übungszeit: XXX Min. |

## 1.1. Begriffe und Konzepte

Begriff 1, Begriff 2, Begriff 3

## 1.2. Lernziele

**LZ 1-1: Dies ist das erste Lernziel, in Kategorie xy**

## 1.3. Referenzen

[IEC 62443], [ISO/SAE 21434], [ISO/IEC 25010], [NIST SP 800]

# 2. Analyse

| Dauer: XXX Min. | Übungszeit: XXX Min. |
|---|---|

## 2.1. Begriffe und Konzepte

Begriff 1, Begriff 2, Begriff 3

## 2.2. Lernziele

### LZ 2-1: Lorem ipsum dolor sit amet, consectetur adipiscing elit

Hier wird beschrieben, was Teilnehmer:innen in diesem Lernziel lernen sollen. Das kann in Prosa-Text in ganzen Sätzen oder in Aufzählungen mit Unterpunkten erfolgen. Dabei kann auch unterschieden werden, wie wichtig einzelne Aspekte des Lernziels sind. Es kann hier bereits auf Literatur verwiesen werden.

- Erstes Teilziel
- Zweites Unterthema
- Dritter Aspekt

### LZ 2-2: Hier ist ein zweites Lernziel in diesem Kapitel

tbd.

## 2.3. Referenzen

[Coley 2020], [Common Vulnerability Scoring System], [ISO/SAE 21434], [Shostack 2014]

# 3. Verifikation

| Dauer: XXX Min. | Übungszeit: XXX Min. |
|---|---|

## 3.1. Begriffe und Konzepte

Begriff 1, Begriff 2, Begriff 3

## 3.2. Lernziele

### LZ 3-1: Dies ist das erste Lernziel in Kapitel 3, das mit xyz

Hier wird beschrieben, was Teilnehmer:innen in diesem Lernziel lernen sollen. Das kann in Prosa-Text in ganzen Sätzen oder in Aufzählungen mit Unterpunkten erfolgen. Dabei kann auch unterschieden werden, wie wichtig einzelne Aspekte des Lernziels sind. Es kann hier bereits auf Literatur verwiesen werden.

- Erstes Teilziel
- Zweites Unterthema
- Dritter Aspekt

### LZ 3-2: Hier ist ein zweites Lernziel in diesem Kapitel

tbd.

## 3.3. Referenzen

[iSAQB AL Formal Methods], [iSTQB Glossary]

# 4. Kryptographie

| | |
|---|---|
| Dauer: XXX Min. | Übungszeit: XXX Min. |

## 4.1. Begriffe und Konzepte

Begriff 1, Begriff 2, Begriff 3

## 4.2. Lernziele

### LZ 4-1: Dies ist das erste Lernziel in Kapitel 4, das mit xyz

Hier wird beschrieben, was Teilnehmer:innen in diesem Lernziel lernen sollen. Das kann in Prosa-Text in ganzen Sätzen oder in Aufzählungen mit Unterpunkten erfolgen. Dabei kann auch unterschieden werden, wie wichtig einzelne Aspekte des Lernziels sind. Es kann hier bereits auf Literatur verwiesen werden.

- Erstes Teilziel
- Zweites Unterthema
- Dritter Aspekt

### LZ 4-2: Hier ist ein zweites Lernziel in diesem Kapitel

tbd.

## 4.3. Referenzen

[Ferguson 2010]

# 5. Angriffe

| Dauer: XXX Min. | Übungszeit: XXX Min. |
|---|---|

## 5.1. Begriffe und Konzepte

Begriff 1, Begriff 2, Begriff 3

## 5.2. Lernziele

### LZ 5-1: Dies ist das erste Lernziel in Kapitel 4, das mit xyz

Hier wird beschrieben, was Teilnehmer:innen in diesem Lernziel lernen sollen. Das kann in Prosa-Text in ganzen Sätzen oder in Aufzählungen mit Unterpunkten erfolgen. Dabei kann auch unterschieden werden, wie wichtig einzelne Aspekte des Lernziels sind. Es kann hier bereits auf Literatur verwiesen werden.

- Erstes Teilziel
- Zweites Unterthema
- Dritter Aspekt

### LZ 5-2: Hier ist ein zweites Lernziel in diesem Kapitel

tbd.

## 5.3. Referenzen

[CVE-Database], [CWE-Database], [OWASP Top 10], [OWASP IoT Top 10]

# 6. Lösungsansätze

| | |
|---|---|
| Dauer: XXX Min. | Übungszeit: XXX Min. |

## 6.1. Begriffe und Konzepte

Begriff 1, Begriff 2, Begriff 3

## 6.2. Lernziele

### LZ 6-1: Dies ist das erste Lernziel in Kapitel 4, das mit xyz

Hier wird beschrieben, was Teilnehmer:innen in diesem Lernziel lernen sollen. Das kann in Prosa-Text in ganzen Sätzen oder in Aufzählungen mit Unterpunkten erfolgen. Dabei kann auch unterschieden werden, wie wichtig einzelne Aspekte des Lernziels sind. Es kann hier bereits auf Literatur verwiesen werden.

- Erstes Teilziel
- Zweites Unterthema
- Dritter Aspekt

### LZ 6-2: Hier ist ein zweites Lernziel in diesem Kapitel

tbd.

## 6.3. Referenzen

[Fernandez-Buglioni 2013], [Schumacher 2006]

# 7. Lösungsansätze

| Dauer: XXX Min. | Übungszeit: XXX Min. |
|---|---|

## 7.1. Begriffe und Konzepte

Begriff 1, Begriff 2, Begriff 3

## 7.2. Lernziele

### LZ 7-1: Dies ist das erste Lernziel in Kapitel 4, das mit xyz

Hier wird beschrieben, was Teilnehmer:innen in diesem Lernziel lernen sollen. Das kann in Prosa-Text in ganzen Sätzen oder in Aufzählungen mit Unterpunkten erfolgen. Dabei kann auch unterschieden werden, wie wichtig einzelne Aspekte des Lernziels sind. Es kann hier bereits auf Literatur verwiesen werden.

- Erstes Teilziel
- Zweites Unterthema
- Dritter Aspekt

### LZ 7-2: Hier ist ein zweites Lernziel in diesem Kapitel

tbd.

## 7.3. Referenzen

[Fernandez-Buglioni 2013], [Schumacher 2006]

# Referenzen

Dieser Abschnitt enthält Quellenangaben, die ganz oder teilweise im Curriculum referenziert werden.


**C**

- [CVE-Database] The MITRE Cooperation: Common Vulnerabilities and Exposures. https://www.cve.org/
- [Common Vulnerability Scoring System] Common Vulnerability Scoring System SIG. Forum of Incident Response and Security. https://www.first.org/cvss/
- [CWE-Database] The MITRE Cooperation: Common Weakness Enumeration. https://cwe.mitre.org/

**F**

- [Ferguson 2010] Ferguson, N., Schneier, B., Kohno, T: Cryptography Engineering: Design Principles and Practical Applications. Wiley, 2010
- [Fernandez-Buglioni 2013] Fernandez-Buglioni, F: Security Patterns in Practice: Designing Secure Architectures Using Software Patterns. Wiley, 2013

**I**

- [IEC 62443] IEC 62443-1-1: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models. International Electrotechnical Commission, Geneva, Switzerland.
- [iSAQB AL Formal Methods] iSAQB e.V. : The CPSA Advanced Level Module Formal Methods. iSAQB e.V., 2024
- [ISO/SAE 21434] ISO/SAE 21434:2021: Road vehicles - Cybersecurity engineering. International Organization for Standardization, Geneva, Switzerland.
- [ISO/IEC 25010] ISO/IEC 25010:2023: Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Product quality model. International Organization for Standardization, Geneva, Switzerland.
- [iSTQB Glossary] iSTQB: iSTQB Glossary. iSTQB, https://glossary.istqb.org/en_US/home

**M**

- [Coley 2020] Coley, S.C., Chase, P.: Rubric for Applying CVSS to Medical Devices. MITRE Corporation, 2020

**N**

- [NIST SP 800] NIST Special Publication 800 Series. National Institute of Standards and Technology, Gaithersburg, MD, USA. https://csrc.nist.gov/publications/sp800

**O**

- [OWASP Top 10] Open Web Application Security Project: Top 10 Web Application Security Risks. https://owasp.org/www-project-top-ten/, 2021
- [OWASP IoT Top 10] Open Web Application Security Project: OWASP Top 10 Internet of Things 2018.

https://owasp.org/www-project-internet-of-things/, 2018

**S**


- [Shostack 2014] Shostack, A.: Threat Modeling Designing for Security. Wiley, 2014
- [Schumacher 2006] Schumacher, M., Fernandez-Buglioni, F., et al.: Security Patterns: Integrating Security and Systems Engineering. Wiley, 2006