EIN TRUSTTROIAI-WERKZEUG

Required Core Artefacts.

Vierzehn konkrete Dokumente, die zwingend existieren müssen, damit Ihre technische Dokumentation nach Anhang VII vollständig ist. Operative Perspektive statt Legal-Perspektive.

VERSION	SPRACHE	ARTEFAKTE	BASIS
1.0 · August 2026	Deutsch	14 in 5 Phasen	CRA · Anhang VII

Diese Liste nennt vierzehn konkrete Dokumente, die zwingend existieren müssen, damit die technische Dokumentation nach Anhang VII vollständig ist. Sie ist die **operative Übersetzung** der Board Assurance Checklist: aus Board-Fragen werden konkrete Dateien in Repository, Wiki und Ticket-System.

INHALT

PHASE 1 VON 5

Design

Die Design-Phase legt die Grundlage für alle späteren Konformitätsnachweise. Drei Artefakte müssen hier existieren, sonst hat die technische Dokumentation keine Basis.

Artefakt 1-1 Product Security Context Note

ZWECK

Definiert den Scope, die Annahmen und die Sicherheits-Ziele des Produkts. Grundlage jeder späteren Risikobewertung.

INHALT

Beabsichtigter Verwendungszweck, Einsatzumgebungen, Nutzer- und Admin-Rollen, Daten-Typen und -Sensitivität, wichtige externe Abhängigkeiten.

WO ES LEBT

docs/security/product-context.md im Repository oder Wiki-Seite.

AKTUALISIERUNGS-TRIGGER

Neuer Verwendungszweck, wesentliche Änderung der Einsatzumgebung, neue kritische Abhängigkeit.

QUELLE · CRA Annex VII (points 1 and 2)

Artefakt 1-2 Architecture and Trust-Boundary Diagram

ZWECK

Zeigt die System-Struktur mit Trust-Boundaries, Datenflüssen und Angriffsflächen. Basis für Threat Modelling.

INHALT

Hauptkomponenten, externe Entitäten, Datenspeicher, Einstiegspunkte, Trust-Boundaries.

WO ES LEBT

docs/architecture/trust-boundaries.md mit eingebettetem Diagramm oder Wiki-Seite mit Draw.io-Referenz.

AKTUALISIERUNGS-TRIGGER

Neue Schnittstelle, neue Abhängigkeit, größere Architekturänderung.

QUELLE · CRA Annex I, Part 1 (PT1.1, PT1.2.d, e, f, j)

Artefakt 1-3 Top Threats and Mitigations List

ZWECK

Priorisierte Liste der wichtigsten Bedrohungen mit zugeordneten Mitigationen und Verifikationstests.

INHALT

Fünf bis zehn Top-Threats mit Priorität (H/M/L), zugeordnete Mitigation, Verifikations-Test, Refresh-Trigger.

WO ES LEBT

docs/security/top-threats.md oder Jira-Board mit dediziertem Label.

AKTUALISIERUNGS-TRIGGER

Neuer Threat-Modelling-Zyklus, neuer Incident, neue Vulnerability in ähnlichen Produkten.

QUELLE · CRA Annex I, Part 1

PHASE 2 VON 5

Development

Während der Entwicklung entstehen die Artefakte, die zeigen, dass Cybersicherheit im Code selbst verankert ist, nicht nur in der Dokumentation.

Artefakt 2-1 Secure Coding Baseline

ZWECK

Einseitiger Standard für sicheres Programmieren im Haupt-Stack, plus Liste verbotener Muster.

INHALT

Regeln zu Input-Validierung, Auth-Prüfungen, Fehler-Behandlung, Krypto-Verwendung, Logging. Verbotene Muster wie String-basiertes SQL, eval-artige Funktionen, TLS-Verifikation-Deaktivierung.

WO ES LEBT

docs/security/coding-baseline.md und .gitattributes oder ähnliche Repo-Konfiguration.

AKTUALISIERUNGS-TRIGGER

Neue Tech-Stack-Version, neue verbotene Muster aus Incident-Learnings.

QUELLE · CRA Annex I, Part 1 (PT1.2.a), Part 2 (PT2.3)

Artefakt 2-2 CODEOWNERS or Equivalent

ZWECK

Erzwingt Peer Review für sicherheitsrelevante Änderungen durch geschützte Branches.

INHALT

Datei mit Zuordnung von Pfaden (Auth, Krypto, Update-Mechanismus, externe Schnittstellen) zu verantwortlichen Reviewern.

WO ES LEBT

.github/CODEOWNERS oder äquivalente Datei in der Repository-Wurzel.

AKTUALISIERUNGS-TRIGGER

Team-Wechsel, neue sensitive Module.

QUELLE · CRA Annex I, Part 2 (PT2.3)

Artefakt 2-3 SBOM per Release

ZWECK

Maschinenlesbares Inventar aller Software-Komponenten in einem Release, Basis für Vulnerability-Antwort.

INHALT

SPDX- oder CycloneDX-Format, alle direkten und transitiven Abhängigkeiten mit Version und Lizenz.

WO ES LEBT

Als Build-Artefakt im Release-Ordner, verlinkt aus der Release-Notes-Seite.

AKTUALISIERUNGS-TRIGGER

Jeder Release-Build, automatisch aus der Build-Pipeline.

QUELLE · CRA Annex I, Part 2 (PT2.1, explicit SBOM requirement)

PHASE 3 VON 5

Verification

Verifikation ist der Punkt, an dem Belege entstehen. Zwei Artefakte machen aus Tests und Reviews auditfähige Nachweise.

Artefakt 3-1 Release Security Checklist

ZWECK

Standard-Prüfliste vor jedem Release mit Pass/Fail-Kriterien und dokumentierten Ausnahmen.

INHALT

SAST-Scan-Ergebnis, Dependency-Scan-Ergebnis, Threat-Modell aktualisiert, negative Tests bestanden, Vulnerability-Triage abgeschlossen.

WO ES LEBT

.github/pull_request_template.md oder Release-Ticket-Template.

AKTUALISIERUNGS-TRIGGER

Neue Prüfungs-Kategorie, Änderung der Release-Kadenz.

QUELLE · CRA Annex I, Part 2 (PT2.3)

Artefakt 3-2 Known Issues and Residual Risk Log

ZWECK

Registriert bekannte Schwachstellen, die im aktuellen Release nicht behoben wurden, mit Begründung und Ablauf-Datum.

INHALT

Vulnerability-ID, Schwere, Grund für Nicht-Behebung, kompensierende Kontrolle, Verantwortlicher, Review-Datum.

WO ES LEBT

docs/security/residual-risk-log.md oder dediziertes Jira-Board mit Label.

AKTUALISIERUNGS-TRIGGER

Jedes neu identifizierte, nicht sofort behebbare Risiko.

QUELLE · CRA Annex I, Part 2 (PT2.2)

PHASE 4 VON 5

Deployment

Deployment ist der Übergang vom Bau zum Betrieb. Drei Artefakte müssen den Übergang begleiten, damit Nutzer und Board wissen, worauf sie sich einlassen.

Artefakt 4-1 Support Period Decision Record

ZWECK

Dokumentiert den festgelegten Unterstützungszeitraum je Produkt mit Begründung.

INHALT

Produkt-Name, Support-Startdatum, Support-Enddatum (Monat und Jahr), Begründung basierend auf erwarteter Nutzungsdauer, Review-Datum.

WO ES LEBT

docs/lifecycle/support-period-{product}.md oder Produktmanagement-System.

AKTUALISIERUNGS-TRIGGER

Produkt-Roadmap-Änderung, Marktentwicklung.

QUELLE · CRA Article 13(8), Article 13(19)

Artefakt 4-2 Secure Update Process Description

ZWECK

Beschreibt den End-to-End-Prozess für die Auslieferung von Sicherheitsupdates.

INHALT

Signierungs-Prozess, Verteilungs-Mechanismus, Integritätsprüfung, Rollback-Verfahren, Nutzer-Benachrichtigung.

WO ES LEBT

docs/lifecycle/update-process.md

AKTUALISIERUNGS-TRIGGER

Änderung des Update-Mechanismus, neue Signierungs-Anforderung.

QUELLE · CRA Annex I, Part 1 (PT1.2.c), Part 2 (PT2.7, PT2.8)

Artefakt 4-3 User Information and Instructions

ZWECK

Sicherheits-relevante Informationen und Anweisungen, die dem Produkt beiliegen (nach Anhang II).

INHALT

Sicherheits-Konfigurations-Anleitung, End-of-Life-Datum, sichere Deprovisionierung, Melde-Kontakt für Schwachstellen.

WO ES LEBT

Als Beilage zum Produkt oder auf der Produkt-Support-Seite.

AKTUALISIERUNGS-TRIGGER

Änderung der Sicherheits-Standardkonfiguration, Ende des Supports.

QUELLE · CRA Annex II

PHASE 5 VON 5

Maintenance

Nach dem Release beginnt der längste Teil des Produktlebens. Drei Artefakte tragen die Konformität durch den Unterstützungszeitraum.

Artefakt 5-1 Vulnerability Handling Process

ZWECK

Intake-to-Fix-Workflow für Schwachstellen, mit SLAs pro Schwere.

INHALT

Meldekanäle (CVD, interne Scans, Kundenberichte), Triage-Verantwortliche, SLA-Matrix (Critical/High/Medium/Low), Eskalations-Pfad.

WO ES LEBT

docs/security/vulnerability-process.md

AKTUALISIERUNGS-TRIGGER

Änderung der SLAs, neue Meldekanäle.

QUELLE · CRA Annex I, Part 2 (PT2.2, PT2.5, PT2.6, PT2.7, PT2.8)

Artefakt 5-2 Article 14 Reporting Playbook

ZWECK

Handlungs-Anleitung für die 24-Stunden-Frühwarnung, 72-Stunden-Meldung und den Abschluss-Bericht an ENISA.

INHALT

Entscheidungs-Baum für Meldepflicht, Vorlagen für die drei Meldungen, Zugangs-Daten zur ENISA-Meldeplattform, Verantwortliche.

WO ES LEBT

docs/security/article14-playbook.md mit Verweis auf einen geschützten Zugangs-Store.

AKTUALISIERUNGS-TRIGGER

Änderung der Melde-Plattform, Erkenntnis aus einem realen Vorfall.

QUELLE · CRA Article 14, applies from 11 September 2026

Artefakt 5-3 Security Changelog

ZWECK

Öffentliches Register aller Sicherheits-relevanten Änderungen mit CVE-Referenzen und Betroffenheits-Angaben.

INHALT

Release-Version, Datum, Behobene Schwachstellen (CVE-IDs), betroffene Produktversionen, Behebungs-Hinweise.

WO ES LEBT

Sicherheitsempfehlungen-Seite auf der Produktwebsite, plus Advisory-Mailingliste.

AKTUALISIERUNGS-TRIGGER

Jeder Release mit Sicherheits-Auswirkung.

QUELLE · CRA Annex I, Part 2 (PT2.4, PT2.8)

VIERZEHN ARTEFAKTE, EIN PROZESS

Der Inspektor erkennt, welche Artefakte fehlen, direkt in Ihrem Projekt.

Jedes der vierzehn Artefakte entspricht einem konkreten Ort im Repository, im Wiki oder im Ticket-System. Der Inspektor prüft die Existenz und Aktualität dieser Artefakte kontinuierlich und erzeugt Jira-Tickets für fehlende oder veraltete Elemente, mit signierten Werkstücken zur direkten Umsetzung.

Der Inspektor liest nur, was Ihr Team ohnehin sehen kann. Die Installation ist kostenfrei. Jeder Skill trägt die Signatur einer Compliance-Expertin oder eines Compliance-Experten über Cronos.

Inspektor für Jira installieren →

Über dieses Dokument. Die Required Core Artefacts sind eine TrustTroiAI-Ressource, gebaut auf Basis des Cyber Resilience Act (Verordnung EU 2024/2847), insbesondere Anhang VII, und der ENISA Secure by Design and Default Playbook v1.0 (CC BY 4.0). Dieses Dokument ist ein Orientierungs-Instrument, keine Rechtsberatung und kein Konformitätsbewertungsverfahren.