

TeleTrust-EBCA "PKI-Workshop" 2025

Berlin, 18.09.2025

"Die Rolle der PKI bei der erfolgreichen Umsetzung des Cyber Resilience Act"

Andreas Philipp, SITS

Der Cyber Resilience Act im Überblick

EU-Verordnung

Legt ein Mindestmaß an Cybersicherheit für alle vernetzten Produkte auf dem EU-Markt fest

Zielsetzung

Erhöhung der Cybersicherheit innerhalb der EU, im Zusammenspiel mit weiteren Maßnahmen wie der NIS2-Richtlinie

Umsetzung

Mapping auf Normen (ENISA-Paper als Guide) oder BSI-Rahmenwerk (TR-03183) sowie spezifische Normen z.B. IEC 62443, ..



Zielsetzung des Cyber Resilience Act

Sichere Produktgestaltung und -entwicklung

für alle digitalen Produkte, die in der EU in Verkehr gebracht werden, wobei Cybersicherheit eine Kernanforderung von der Produktentwicklung bis zum Ende des Lebenszyklus sein muss.

Erhöhung der Transparenz

hinsichtlich der Sicherheitsmerkmale und Schwachstellen digitalen Produkte, damit Verbraucher und Unternehmen fundierte Entscheidungen treffen können.

Sicherstellung, dass Wirtschaftsakteure (Hersteller, Importeure, Vertreiber) ihre Verantwortung für die Cybersicherheit von Produkten wahrnehmen,

einschließlich der Bereitstellung von Sicherheitsupdates und der Verwaltung von Schwachstellen während der gesamten Lebensdauer (mind. 5 Jahre) eines Produkts, und dass ein Rahmen für die Marktüberwachung und Durchsetzung vorhanden ist.

Grundlegende Maßnahmen

- Datenintegrität & Security by Default
- Schutz der Daten & Zugriffsschutz
- Sicherheitsupdates & Systemverfügbarkeit
- Absicherung der Lieferkette
- Datenverschlüsselung
- Minimierung der Angriffsfläche

PKI – Infrastruktur-Technologie

Public-Key-Infrastruktur (PKI) und Key Management sind grundlegende Technologien, die der Infrastruktur und nicht der Anwendung zuzuordnen sind.

i PKI arbeitet oft im Hintergrund und wird erst durch die konkrete Anwendung im Kontext verständlich.

Um die essenzielle Rolle einer PKI für die Absicherung von Produkten unter dem CRA zu verstehen, müssen wir die damit verknüpften Anwendungen betrachten.



PKI-basierende Sicherheitsverfahren

Gesicherte Geräte Identität

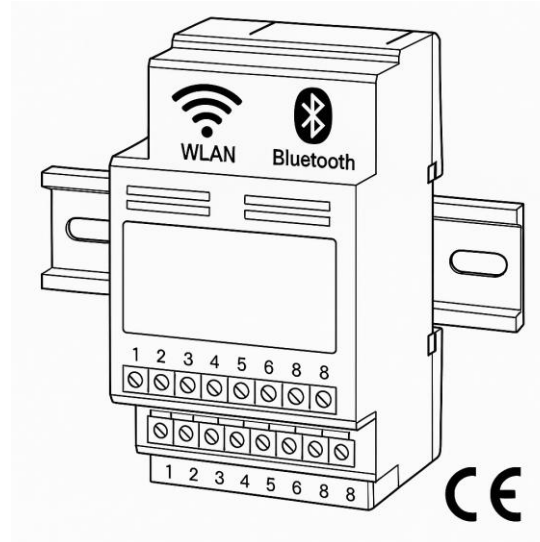
Eindeutige und kryptografisch gesicherte Identitäten für vernetzte Geräte

Secure Boot

Sicherstellung, dass nur vertrauenswürdige Software beim Startvorgang geladen wird

Secure Update

Code-Signing-Verfahren zur Absicherung von Softwareupdates und Konfigurationen



Vertrauensanker

Grundlegendes Element für die Etablierung von Vertrauensketten

Gesicherter Remote-Zugang

Authentifizierte und verschlüsselte Fernzugriffe auf Geräte

Gesicherte SBOM

Kryptografisch signierte Software Bill of Materials zur Transparenz der Komponenten

Kommunikationsabsicherung

Verschlüsselte und integritätsgeschützte Datenübertragung

Security by Design und by Default

Um PKI-basierte Verfahren und Technologien effizient einzusetzen, müssen sie im Kontext des gesamten Produktlebenszyklus betrachtet werden.

- **Nur durch diese ganzheitliche Betrachtung wird die wesentliche Rolle einer PKI für die CRA-Konformität deutlich.**

Die Integration von Sicherheitsmaßnahmen muss von Beginn an in den Entwicklungsprozess eingebettet sein, nicht als nachträgliche Ergänzung.



PKI-Anwendungen im Produktlebenszyklus

Die PKI fungiert als übergreifende Infrastruktur, die mit den Sicherheitsverfahren in jeder Phase interagiert.



Fazit: PKI als Schlüsselement des CRA

Zentrale Bedeutung

Die Public-Key-Infrastruktur bildet das Fundament für zahlreiche Sicherheitsmaßnahmen, die für die CRA-Konformität unerlässlich sind.

Ohne eine robuste PKI können wesentliche Schutzziele wie Authentisierung, Integrität und Nicht-Abstreitbarkeit nicht erreicht werden.

Handlungsempfehlungen

- Frühzeitige Integration der PKI in den Produktentwicklungsprozess
- Ganzheitliche Betrachtung über den gesamten Produktlebenszyklus
- Regelmäßige Überprüfung und Aktualisierung der PKI-Komponenten





Fragen?

Wir helfen Ihnen gerne!



Andreas Philipp

Head of Applied Crypto –
Business Development
Swiss IT Security Group

Andreas.Philipp@sits.com
+49 151 67001952