

Produkt-Cybersicherheit Bedingungen für Lieferanten
Product Cyber Security Terms for Suppliers

MTQ 5014

Englische Fassung ab Seite 9 / English version from page 9

Ersatz für
Ausgabe 05.2023

Inhaltsverzeichnis	Seite
1 Anwendungsbereich	2
2 Normative Verweisung	2
3 Zweck	2
4 Mitgeltende Unterlagen	2
5 Organisation und Informationssicherheitsmanagement	3
6 Organisatorische Anforderungen an das Vertragsprodukt	3
7 Audits und Sicherheitsanalysen	4
8 Schwachstellenmanagement	6
9 Sicherheitsaktualisierungen	7
10 Mitwirkung des Auftragsnehmers	7
11 Härtung des Vertragsproduktes und Risikomitigation	8

Fortsetzung Seite 2 bis 16
Continued on pages 2 to 16

Fachbereich:	Redaktionell geprüft:	Freigegeben:	ICS-Nr.
Specialist department:	Editorially checked by:	Approved by:	ICS-No.
T. Daniel, TRY	A. Nitschke-Werner, TQCD	J. Mühlwerth, TQCD	25.040.40, 35.110

1 Anwendungsbereich

Dieser Standard beschreibt grundlegende rechtliche und organisatorische Anforderungen an die Produkt-Cybersicherheit für Lieferanten, Entwicklungsdienstleister und Partner (nachfolgend Auftragnehmer, AN genannt).

Dementsprechend kann er bei Lastenheften, Projektverträgen und Bestellungen herangezogen und referenziert werden, so dass er Vertragsbestandteil wird.

Abweichende Regelungen zu diesem Dokument bedürfen gesonderter schriftlicher Vereinbarung zwischen Auftragnehmer und RRS (nachfolgend Auftraggeber, AG genannt) vor einer Beauftragung.

Der Standard beschreibt keine Geheimhaltungspflichten, entsprechende Vereinbarungen zwischen Auftragnehmer und Auftraggeber müssen gesondert in einer Geheimhaltungsvereinbarung getroffen werden.

2 Normative Verweisung

Soweit projektspezifisch nichts anderes vorgegeben finden insbesondere folgende Normen / Standards branchenspezifisch Anwendung:

- IEC 62443 Normenreihe
- ISO/IEC 2700x (Normenreihe, IT-Sicherheit)
- Stand der Technik (z.B. BSI Richtlinien)

3 Zweck

Der Standard ist insbesondere einzuhalten von Lieferanten von komplexen, softwarebasierten, elektronischen Zukaufkomponenten wie Steuergeräten, Netzwerkkomponenten, Industrierechnern, speicherprogrammierbaren Steuerungen oder ähnlichem sowie von kritischen Bauteilen und Baugruppen und sonstigen Produkten mit digitalen Elementen im Sinne des EU Cyber Resilience Act (CRA, [2]).

4 Mitgeltende Unterlagen

[1] Lieferantenselbstauskunft Produkt-Cybersicherheit

[2] VERORDNUNG (EU) 2024/2847 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)

5 Organisation und Informationssicherheitsmanagement

Der AN ist dazu verpflichtet, ein Informationssicherheitsmanagementsystem (ISMS) zu betreiben.

1. Das Informationssicherheitsmanagement muss hierbei auch die IT-Sicherheit der IT-Infrastruktur des AN sowie die Angriffssicherheit seiner Vertragsprodukte (Produkt-Cybersicherheit) abdecken. Das ISMS des AN findet Anwendung in allen Unternehmensbereichen und an allen Standorten in denen Vertragsprodukte für den AG entwickelt, hergestellt oder gewartet werden.

Insbesondere sollen im ISMS die Prozesse für eine Risiko- und Bedrohungsanalyse sowie ein Konzept zur unverzüglichen Reaktion auf Zwischenfälle nebst einer zeitnahen Wiederherstellung (Recovery) eines angemessenen Sicherheitsniveaus enthalten sein.

2. Der AN sichert zu und gewährleistet, dass er die geltenden Gesetze, Vorschriften und Industriestandards in Bezug auf die IT-Sicherheit kennt, insbesondere diejenigen, die sich auf das Hacken von IT oder OT-Systemen, den unrechtmäßigen Zugriff auf ein IT oder OT-System, die absichtliche Störung des IT-Systembetriebs und die missbräuchliche Verwendung von Daten beziehen, und verpflichtet sich, diese einzuhalten.
3. Falls der AN Geheimnisse wie Passwörter oder Zugangsdaten liefert, so sind diese über einen gesonderten, vereinbarten Kanal bereit zu stellen. Die Lieferung und Dokumentation von Passwörtern und Zugangsdaten in Handbüchern ist nicht gestattet, solange das Vertragsprodukt nicht bei Inbetriebnahme zum Passwortwechsel zwingt.
4. Der AN ist verpflichtet, die Lieferantenselbstauskunft zur Produkt-Cybersicherheit auszufüllen (bezogen auf dieses Dokument – MTQ 5014) und die Compliance zu den Anforderungen in der Lieferantenselbstauskunft zu dokumentieren. Falls Abweichungen zu den Anforderungen vorhanden sind, werden diese dokumentiert, mit dem AG abgestimmt und proaktiv aufgelöst.
5. Der AN stellt sicher, dass nur potenzielle Sub-AN (Drittanbieter) beauftragt werden, die die EU Cyber Resilience Act (CRA,[2]) -Anforderungen mit einem angemessenen Sicherheitsniveau erfüllen, das auf dieses Dokument (MTQ5014) abgestimmt ist.
6. Der AN benennt eine verantwortliche Person als Ansprechpartner für Produkt-Cybersicherheit für die vom AG verwendeten Vertragsprodukte des AN. Eine Änderung des Verantwortlichen ist dem AG umgehend mitzuteilen.

6 Organisatorische Anforderungen an das Vertragsprodukt

1. Der AN gewährleistet und bestätigt auf Verlangen des AG mit einem Protokoll, dass das Vertragsprodukt zum Zeitpunkt der Bereitstellung an den AG keine bekannten, ausnutzbaren Schwachstellen aufweist, auf Malware und sonstige Schadsoftware geprüft wurde und frei von dergleichen ist. Das Vertragsprodukt wird mit einer sicheren Standardkonfiguration ausgeliefert, soweit nichts anderes vereinbart wurde.
 2. Der AN gewährleistet, dass das Vertragsprodukt so gestaltet ist, dass gespeicherte, übermittelte oder anderweitig verarbeitete Daten, einschließlich personenbezogener Daten, hinsichtlich ihrer Vertraulichkeit, Integrität und Verfügbarkeit angemessen geschützt werden. Dies erfolgt insbesondere durch geeignete technische Maßnahmen, Schutz vor unautorisierter Manipulation oder Veränderung sowie Mechanismen zur Meldung entsprechender Vorfälle, und durch Beachtung der Grundsätze der Datenminimierung. Das Vertragsprodukt muss so konzipiert sein, dass es eine automatische Aufzeichnung sicherheitsrelevanter Ereignisse (Protokollierung) ermöglicht, soweit nichts anderes vereinbart wurde.
 3. Der AN stellt dem AG eine umfassende technische Beschreibung des Vertragsprodukts zur Verfügung, die alle Informationen enthält, die der AG zur Erstellung der technischen Dokumentation gemäß Anhang VII des EU Cyber Resilience Act (CRA,[2]) benötigt. Die Dokumentation umfasst insbesondere eine Beschreibung der vorgesehenen Nutzung (intended use), der wesentlichen Funktionen (essential functions), eine etwaige Einstufung als „wichtiges Produkt“ im Sinne des EU Cyber Resilience Act (CRA, [2]) sowie bekannte Bedrohungen und Risiken für das Vertragsprodukt und die Erfüllung der Essential Requirements des EU Cyber Resilience Act (CRA, [2]) Anhang I Teil 1. Die Dokumentation für das Vertragsprodukt wird mindestens über den Supportzeitraum gepflegt.
-

Die Dokumentation umfasst zudem sicherheitsrelevante Eigenschaften, Hinweise zur sicheren Konfiguration sowie eine Darstellung von Risiken, die sich aus vorhersehbarem Fehlgebrauch und dem Einsatzkontext ergeben. Handbücher enthalten die Informationen nach Anhang II des EU Cyber Resilience Act (CRA, [2]).

4. Der AN gewährleistet, dass sein Vertragsprodukt nach einem anerkannten Standard der IT oder OT-Sicherheit, z.B. IEC 62443-4-1 entwickelt und hergestellt wurde, wobei ein strukturierter, sicherer Entwicklungsprozess einschließlich Konfigurationsmanagement und Qualitätssicherung zugrunde liegt. Produkt-Cybersicherheitsrisiken wurden durch den AN bei der Planung, Entwicklung und Herstellung des Vertragsproduktes berücksichtigt.
5. Der AN stellt dem AG die EU-Konformitätserklärung (CE-Konformitätserklärung) einschließlich der entsprechenden Nachweisdokumente zur Verfügung, damit der AG dies prüfen kann.
6. Der AN stellt dem AG eine Softwarestückliste (Software Bill of Material, SBOM) in einem gängigen maschinenlesbaren Format mit den Informationen nach einem anerkannten SBOM Standard, z.B. Software package data exchange format SPDX) oder CycloneDX zur Verfügung.
7. Der AN stellt dem AG ein Verzeichnis der in seinem Vertragsprodukt verwendeten Open Source Software und die entsprechenden Lizenzbedingungen zur Verfügung. Alle verwendeten (nicht selbstentwickelten) SW Bibliotheken, Tools, Entwicklungsumgebungen usw. müssen mit Versionsstand dokumentiert werden.
8. Softwarekomponenten, Open Source Komponenten und HW Komponenten, die aus einem sanktioniertem Land stammen oder bei denen ein erhöhtes Risiko zur Ausnutzung bzw. Ausspähung besteht, dürfen nicht verwendet werden (z.B. Sanktionsliste, Staatenliste im Sinne des Sicherheitsüberprüfungsgesetzes des Bundesministerium des Inneren). Falls eine Verwendung zwingend notwendig ist, so führt der AN eine ausführliche Security Analyse hinsichtlich data leakage und malware injection sowie eigene Tests durch, die er mit dem AG teilt.
9. Der AN stellt dem AG ein Verzeichnis der gelieferten Hardware mit der zugehörigen Software und Versionen zur Verfügung. Falls Software unabhängig von einem Vertragsprodukt geliefert wird, so liefert der AN den Hash der Software mit.
10. AG und AN prüfen ob ein Escrow-Agreement über alle Bestandteile (Software, Keys, Tools, Entwicklungsumgebung, Entwicklungsdokumente, HW-Layouts usw.) abgeschlossen werden muss. Es ist der Nachweis der Vollständigkeit aller Vertragsprodukt- und Entwicklungsbestandteile, die durch das Escrow-Agreement erfasst werden durch den AN zu führen und dem AG in dokumentierter Form zu übergeben.

7 Audits und Sicherheitsanalysen

Der AG kommt mit Audits und Sicherheitsanalysen seinen Sorgfaltspflichten im Sinne EU Cyber Resilience Act (CRA,[2]) nach.

1. Der AG ist berechtigt, ein Securityaudit für die angewendeten Prozesse der Organisation und der Projekte des AN vor Ort durchzuführen. Der AG kann damit auch Dritte beauftragen, die in seinem Namen dieses Audit durchführen. Falls vom AN gewünscht, kann das Audit durch einen unabhängigen Auditor einer akkreditierten Stelle durchgeführt werden. Der Bericht des Auditors ist dem AG vollständig vorzulegen. Der AN muss Security Audits an den betroffenen Standorten (z.B. Entwicklungs- oder Produktionsstandorte) innerhalb eines Monats thematisch vollumfänglich und ohne Einschränkungen der betroffenen Bereiche ermöglichen. Grundlage für Audits sind ISO 2700x oder IEC 62443-4-1.
 2. Der AN wird dem AG auf dessen Verlangen hin bereits vorliegende Nachweise einer Auditierung auf Grundlage eines anerkannten Standards (z.B. nach ISO 27001, IEC 62443-4-1 oder Cyber Essentials) liefern. Die Nachweise sind vollständig zu liefern und dürfen nicht älter als ein Jahr sein.
 3. Der AG ist berechtigt, eine Security Analyse (z.B. Technisches Audit, Code Review, Binäranalyse, Schwachstellenanalyse, Penetration Test) des Vertragsproduktes vorzunehmen. Der AN liefert dem AG die Binärsoftware zur Erstbemusterung und zu jeweiligen Updates. Bei einer Binäranalyse können Geheimnisse des AN offengelegt werden, insbesondere Schwachstellen.
-

4. Der AN gestattet dem AG Penetrationstests oder System Penetrationstests, unter Offenlegung aller hierzu erforderlichen internen Informationen des Systems (Entwicklungsdokumente), durchzuführen. Der AG kann dazu auch Dritte beauftragen.
5. Der AN wird den AG bzw. den vom AG beauftragten Dritten auf Anfrage angemessen bei der Durchführung des Security Audit bzw. der Security Analyse unterstützen und etwaige erforderliche Informationen bereitstellen.

8 Schwachstellenmanagement

Eine Schwachstelle ist eine Fehlfunktion in einer Software, Firmware, Hardware, Dienstkomponente oder einem Systemdesign, die (von einem Angreifer) ausgenutzt werden kann, um die Vertraulichkeit, Integrität oder Verfügbarkeit einer betroffenen Komponente oder eines betroffenen Systems bzw. eines Produkts mit digitalen Elementen zu beeinträchtigen (vergleiche IEC 62443-3-2 und Art. 3 Nr. 40 EU Cyber Resilience Act, [2]).

1. Der AN verpflichtet sich, ein Schwachstellenmanagement über die Laufzeit des gesamten Produktlebenszyklus zu pflegen. Das Schwachstellenmanagement beinhaltet auch eine regelmäßige, dokumentierte Analyse von Schwachstellendatenbanken und der Relevanz für die Vertragsprodukte.
 2. Der AN verpflichtet sich, die Sicherheit des Vertragsprodukts während des Produktlebenszyklus regelmäßig und wirksam zu testen und zu überprüfen und hierzu insbesondere Penetrationstests und Schwachstellenscans bzw. ein dauerhaftes Schwachstellenmonitoring durchzuführen. Der Produktlebenszyklus (Produkt-Supportzeitraum) des Vertragsprodukts wird von AN und AG einvernehmlich festgelegt. Dabei werden die voraussichtliche Nutzungsdauer, die berechtigten Erwartungen der Nutzer, die Art und Zweckbestimmung des Vertragsprodukts sowie etwaige einschlägige gesetzliche Vorgaben zur Lebensdauer von Produkten mit digitalen Elementen berücksichtigt. Die Ergebnisse der Penetrationstests und Schwachstellenscans werden mit dem AG vollständig und immer geteilt. Der AN legt dem AG dar, wie und in welchem zeitlichen Rahmen die Schwachstellen behoben werden. Funktionale Tests des AN berücksichtigen das Thema Angriffssicherheit.
 3. Der AN richtet einen strukturierten Prozess für die verantwortungsvolle Meldung von Schwachstellen (Responsible Disclosure) ein. Er stellt hierfür einen geeigneten Meldeweg (z. B. eine dedizierte E-Mail-Adresse oder ein Webformular) zur Verfügung, der öffentlich zugänglich dokumentiert ist. Der AN verpflichtet sich, eingehende Hinweise vertraulich zu behandeln, unverzüglich zu prüfen und – sofern erforderlich – geeignete Maßnahmen zu ergreifen.
 4. Der AN verpflichtet sich, etwaige ausnutzbare Schwachstellen seiner Vertragsprodukte, die ihm bekannt sind oder die bekannt werden, in einem angemessenen Zeitraum zu beheben. Ein angemessener Zeitraum ist < 90 Tage, falls kein anderer Zeitraum mit dem AG vereinbart ist. Bei Gefahr für Leib und Leben hat der Lieferant unverzüglich alles zu tun, um die von seinem Vertragsprodukt ausgehenden Gefahren zu begegnen bzw. kompensierende (auch betriebliche) Gegenmaßnahmen zu definieren, umzusetzen und zu kommunizieren. Nach Behebung liefert der AN einen Bericht über die Behebung.
 5. Der AN informiert den AG unverzüglich, jedenfalls aber innerhalb der Reaktionszeit, über bekannt gewordene Schwachstellen und Zwischenfälle (Security Incidents) an Vertragsprodukten, die an den AG geliefert wurden. Die Meldung hat unter Verwendung eines geeigneten Bewertungssystems (z. B. CVSS, EPSS, SSVC oder VPR) sowie unter Anwendung des Traffic Light Protocol (TLP) zu erfolgen. Darüber hinaus verpflichtet sich der AN, einen Prozess zur Erstellung und Bereitstellung von sicherheitsrelevanten Hinweisen (Advisories) im Common Security Advisory Framework (CSAF)-Format einzurichten und aufrechtzuerhalten. Entsprechende Advisories sind dem AG unverzüglich zur Verfügung zu stellen.
 6. Die Reaktionszeit für das Berichten von Schwachstellen nach Erkennung und Vorkommnissen an den AG durch den AN beträgt 24 Stunden, von Montag bis Freitag. Diese gilt unabhängig etwaiger Gewährleistungsfristen oder sonstiger gesetzlicher Verjährungsfristen über einen Zeitraum von 20 Jahren nach Lieferung, mindestens jedoch über den vereinbarten Produkt-Supportzeitraum.
 7. Der AN verwendet zur Meldung von Schwachstellen und Advisories die E-Mail Adresse PSIRT@ps.rolls-royce.com
-

9 Sicherheitsaktualisierungen

1. Der AN gewährleistet, dass dem AG Sicherheitsaktualisierungen unverzüglich, automatisch und unentgeltlich zur Verfügung gestellt werden, um bekannt gewordene Schwachstellen zu schließen. Dies gilt unabhängig etwaiger Gewährleistungsfristen oder sonstiger gesetzlicher Verjährungsfristen über einen Zeitraum von 20 Jahren nach Lieferung, mindestens jedoch über den vereinbarten Produkt-Supportzeitraum. Die Funktion für automatische Sicherheitsaktualisierungen im Sinne des CRA ist umgesetzt, soweit nichts anderes vereinbart wurde.
2. Der AN verpflichtet sich, jede dem AG bereitgestellte Sicherheitsaktualisierung nach ihrer Bereitstellung für mindestens zehn Jahre verfügbar zu halten.
3. Der AN verpflichtet sich, den AG bei End-of-Life des Vertragsproduktes mindestens 1 Jahr vor Produktionsende zu informieren. Sofern es dem AN aufgrund äußerer Umstände nicht möglich ist, erfolgt diese Information spätestens 48h nach Bekanntwerden.

10 Mitwirkung des Auftragnehmers

1. Der AN verpflichtet sich, konstruktiv an der sicheren Integration seines Vertragsproduktes in das System des AG mitzuwirken.
 2. Der AN verpflichtet sich, an Abstimmungen mit dem AG und dem Endkunden teilzunehmen, sowie aktiv an der Erstellung eines gesamtheitlichen Produkt-Cybersicherheitskonzeptes mitzuwirken, soweit es sein Vertragsprodukt betrifft. Ein ggf. vorhandenes Produkt-Cybersicherheitskonzeptes für das Vertragsprodukt ist mit dem Vertragsprodukt zu liefern. Das gesamtheitliche Produkt-Cybersicherheitskonzeptes bezieht sich auf den Lieferumfang des AG und kann sowohl technische Maßnahmen als auch organisatorische und personelle Maßnahmen beinhalten.
 3. Der AN verpflichtet sich, auf Anfrage des AG zusammen mit diesem eine Security Analyse des Vertragsproduktes, bei Bedarf, vorzunehmen. Insbesondere unterstützt der AN den AG bei der technischen Bewertung seines Vertragsproduktes gegenüber IEC 62443-4-2 und den Essential Requirements des EU Cyber Resilience Act (CRA, [2]) Anhang I Teil 1.
 4. Wenn der AN von einem tatsächlichen Vorfall innerhalb seiner IT Infrastruktur erfährt, die eine tatsächliche oder potenziell nachteilige Auswirkung auf die Infrastruktur des AN haben kann, in dem Daten des AG gespeichert sind (Cybervorfall) oder von einem sonstigen unbefugten Zugriff auf oder die Nutzung oder der Missbrauch, die Beschädigung oder die Zerstörung durch einen Dritten (sonstiger Vorfall) erfährt, muss der AN den AG unverzüglich und nicht später als 24 Stunden, nachdem er von dem Cybervorfall oder dem sonstigen Vorfall Kenntnis erlangt hat benachrichtigen. Der AN verwendet hierzu die E-Mail Adresse PSIRT@ps.rolls-royce.com
 5. Der AN verpflichtet sich, alle Anweisungen des AG im Zusammenhang mit dem Cybervorfall oder sonstigen Vorfall zu befolgen und die gesetzlichen Regelungen einzuhalten. Dies betrifft insbesondere die Dokumentation, die Beschaffung und Sicherung von Beweisen über den Cybervorfall, die Umsetzung von Abhilfestrategien, um die Auswirkungen des Cybervorfalles oder eines anderen Vorfalls oder die Wahrscheinlichkeit oder die Auswirkungen zukünftiger ähnlicher Vorfälle zu verringern und die Benachrichtigung von und Kooperation mit Behörden. Beweise sind für einen Zeitraum von mindestens 12 Monaten aufzubewahren.
 6. Der Daten- und Informationsaustausch kann geheimschutz- oder exportrechtlichen Einschränkungen unterliegen. Hier besteht Informationspflicht durch den AN.
-

11 Härtung des Vertragsproduktes und Risikomitigation

1. Der AN gewährleistet, dass das Vertragsprodukt so konzipiert, entwickelt und hergestellt wurde, dass es – insbesondere auch bei externen Schnittstellen – möglichst geringe Angriffsflächen bietet und über eine angemessene Resilienz gegenüber Cyberangriffen und Sicherheitsvorfällen verfügt. Auf Anfrage stellt der AN dem AG entsprechende Nachweisdokumente zur Verfügung.
2. Der AN liefert mit dem Vertragsprodukt Hinweise bzw. Handbücher zur sicheren Einstellung und Härtung des Vertragsproduktes, insbesondere für Netzwerk und/oder Betriebssystemeinstellungen.
3. Alle kryptographischen Funktionen sind nach Stand der Technik auszuführen (siehe z.B. technische Richtlinien des BSI, BSI TR-2102). Der AN bestätigt, dass er ein Verfahren implementiert, um kryptographische Schlüssel und andere Geheimnisse, die die Vertragsprodukte für den AG betreffen, nach dem Stand der Technik sicher zu schützen.
4. Wenn spezielle Hardware oder Software für Update-Aktivitäten, Diagnose, Operation, Konfiguration oder weitere Aktivitäten am Vertragsprodukt des AN, notwendig ist, so gilt diese Hardware oder Software ebenfalls als Vertragsprodukt und muss im Lieferumfang enthalten sein. Der AN räumt dem AG und dem Kunden das permanente Recht zur Nutzung der Software ein und wartet diese über die Lebensdauer des Vertragsprodukts. Die Software wird als Installationspaket mit Release Notes und Hash geliefert. Auf Anforderung durch den AG ist der AN dazu verpflichtet nachzuweisen, nach welchen Standards die Hardware oder Software entwickelt wurde.
5. Falls Standardbetriebssysteme im Vertragsprodukt benutzt werden, so stimmt der AN mit dem AG auf Anfrage ein Patchmanagementkonzept und ein Anti-Malwarekonzept ab und liefert dieses. Falls vereinbart, wird das Steuergerät des AN mit Anti-Malware geliefert.

Ergänzende Angaben

Frühere Ausgaben

05.2023

Änderungen

- Angepasst an die Anforderungen des EU Cyber Resilience Act
- Norm redaktionell überarbeitet

ENDE DER DEUTSCHEN FASSUNG!

The <i>English</i> version is a translation. In case of dispute the German original will govern.
--

Replaces
Edition 05.2023

CONTENTS

Page

1	Scope of application	10
2	Normative reference	10
3	Purpose	10
4	Applicable documents	10
5	Organisation and information security management	11
6	Organisational requirements for the scope of delivery	11
7	Audits and security analyses	13
8	Vulnerability Management	13
9	Security Updates	15
10	Cooperation of the Contractor	15
11	Product hardening and risk mitigation	16

1 Scope of application

This standard describes basic legal and organisational Product Cyber Security requirements for suppliers, development service providers and partners (hereinafter referred to as contractors, AN).

Accordingly, it can be referred to and referenced in specifications, project contracts and purchase orders so that it becomes part of the contract.

Deviating regulations to this document require a separate written agreement between the contractor and RRS (hereinafter referred to as the client, AG) before an order is placed.

The standard does not describe any confidentiality obligations; corresponding agreements between contractor and client must be made separately in a non-disclosure agreement.

2 Normative reference

Unless otherwise specified for a specific project, the following norms/standards in particular shall apply to the industry:

- IEC 62443 series
- ISO/IEC 2700x (series of standards, IT security)
- State of the art (e.g. BSI guidelines)

3 Purpose

The standard is to be complied with in particular by suppliers of complex, software-based, electronic bought-in components such as control units, network components, industrial computers, programmable logic controllers or similar, as well as critical components and assemblies and other products with digital elements within the meaning of the EU Cyber Resilience Act (CRA, [2]).

4 Applicable documents

[1] Supplier Self-Assessment on Product Cyber Security

[2] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

5 Organisation and information security management

The Contractor is obliged to operate an information security management system (ISMS).

1. The information security management must also cover the IT security of the Contractor's IT infrastructure and the attack security of its contractual products (product cyber security). The ISMS of the Contractor shall be applied in all divisions and at all locations where contractual products are developed, manufactured or maintained for the Client.

In particular, the ISMS shall contain the processes for threat and risk analysis as well as a concept for immediate reaction to incidents together with a timely recovery of an appropriate security level.

2. The Contractor represents and warrants that he is aware of and undertakes to comply with applicable laws, regulations and industry standards relating to IT security, in particular those relating to hacking of IT or OT systems, unlawful access to an IT or OT system, intentional disruption of IT system operations and misuse of data.
3. If the Contractor supplies secrets such as passwords or access credentials, these shall be provided via a separate, agreed channel. The delivery and documentation of passwords and access credentials in manuals is not permitted, as long as the contract product does not force you to change your password when you start it the first time.
4. The Contractor is obliged to complete the Supplier Self-Assessment on Product Cyber Security (to this document – MTQ 5014) and to document compliance with the requirements in the Supplier Self-Assessment. If there are deviations from the requirements, these are to be documented, coordinated with the Client and proactively resolved.
5. The Contractor will ensure that potential Sub-contractors (3rd party suppliers) are contracted to fulfill EU Cyber Resilience Act (CRA,[2]) requirements with an appropriate level of security, aligned with this document (MTQ5014).
6. The Contractor shall appoint a responsible person as contact person for product cyber security for the Contractor's contractual products used by the Client. The Client shall be informed immediately of any change in the person responsible.

6 Organisational requirements for the scope of delivery (contractual product)

1. The Contractor shall ensure and, upon the Client's request, confirm by means of a written record that, at the time of delivery to the Client, the contractual product does not contain any known exploitable vulnerabilities, has been scanned for malware and other malicious software and is free from such. The contractual product is delivered with a secure default configuration, unless otherwise agreed.
 2. The Contractor shall ensure that the contractual product is designed in such a way that stored, transmitted or otherwise processed data – including personal data – is protected with regard to confidentiality, integrity and availability in an appropriate way. This shall be ensured in particular through appropriate technical measures, protection against unauthorized manipulation or modification, mechanisms for reporting relevant incidents, and compliance with the principles of data minimization. The contractual product must be designed to enable the automatic recording of security-relevant events (logging) , unless otherwise agreed.
 3. The Contractor shall provide the Client with a comprehensive technical description of the contractual product containing all information required by the Client for the preparation of the technical documentation in accordance with Annex VII of the EU Cyber Resilience Act (CRA,[2]). The documentation shall include, in particular, a description of the intended use, the essential functions, any classification as a "important product" within the meaning of the EU Cyber Resilience Act (CRA, [2]), as well as known threats and risks associated with the contractual product and fulfillment the Essential Requirements of the EU Cyber Resilience Act (CRA, [2]) Annex I Part 1. The documentation is maintained throughout the support period. It shall further include security-relevant characteristics, guidance on secure configuration, and a description of risks arising from reasonably foreseeable misuse and operational context, and shall be made available to the Client. Manuals contain the information according to Annex II of the EU Cyber Resilience Act (CRA, [2]).
-

4. The Contractor ensures that its contractual product was developed and manufactured in accordance with a recognized standard of IT or OT security, e.g. IEC 62443-4-1, based on a structured, secure development process including configuration management and quality assurance. Product cybersecurity risks were taken into account by the Contractor in the planning, development and manufacture of the contract product.
 5. The Contractor shall provide the Client with the EU Declaration of Conformity (CE Declaration of Conformity), including the corresponding supporting documentation for the purpose of verification of the documentation by the Client.
 6. Upon request, the Contractor shall provide a software bill of material (SBOM) in a commonly used machine-readable format with the information according to a recognised SBOM standard, (e.g. software package data exchange format, SPDX or CycloneDX).
 7. The Contractor shall provide the Client with a list of the open source software used in its contractual product and the corresponding licence conditions. All (not self-developed) software libraries, tools, development environments etc. used must be documented with the version status.
 8. Software components or open source components that originate from a sanctioned country or that pose an increased risk of exploitation or spying must not be used (e.g. sanctions list, list of states within the meaning of the Sicherheitsüberprüfungsgesetz of the Bundesministerium des Inneren). If use is absolutely necessary, the Contractor will carry out an in-depth security analysis with regard to data leakage and malware injection as well as its own tests, which he shares with the Client.
 9. The Contractor undertakes to maintain a list of the hardware supplied with the associated software and versions for each contractual product and to make this available to the Client. If software is supplied independently of a contractual product, the Contractor shall also supply the hash of the software.
 10. The Contractor and client check if an escrow agreement for all components (software, keys, tools, development environment, development documents, hardware layouts, etc.) is necessary. The Contractor shall provide proof of the completeness of all contractual product and development components covered by the escrow agreement and hand them over to the Client in documented form.
-

7 Audits and security analyses

The Client fulfils its due diligence obligations within the meaning of the EU Cyber Resilience Act (CRA,[2]) with audits and security analyses.

1. The Client is entitled to carry out a security audit for the applied processes of the Contractor's organisation and projects on site. The Client may also commission third parties to carry out this audit on its behalf. If desired by the Contractor, the audit may be carried out by an independent auditor of an accredited body. The auditor's report shall be submitted in full to the Client. The Contractor must allow security audits to be carried out at the affected locations (e.g. development or production sites) within one month, fully covering the subject matter and without any restrictions on the affected areas. Basis for audits are ISO 2700x or IEC 62443-4-1.
2. At the Client's request, the Contractor shall provide the Client with existing evidence of an audit based on a recognised standard (e.g. in accordance with ISO 27001, IEC 62443-4-1 or Cyber Essentials). The evidence shall be provided in full and shall not be older than one year.
3. The Client is entitled to carry out a security analysis (e.g. technical audit, code review, binary analysis, vulnerability analysis, penetration test) of the contractual product. The Contractor shall deliver the binary software to the Client for initial sampling and for respective updates. During a binary analysis, secrets of the Contractor may be disclosed, in particular vulnerabilities.
4. The Contractor shall allow the Client to carry out penetration tests or system penetration tests, disclosing all internal system information (development documents) required for this purpose. The Client may also commission third parties for this purpose.
5. The Contractor shall, upon request, provide reasonable support to the Client or a third party appointed by the Client in the performance of the security audit or security analysis and shall make available any information required for this purpose.

8 Vulnerability management

A vulnerability is a malfunction in a software, firmware, hardware, service, component or system design that can be exploited (by an attacker) to compromise the confidentiality, integrity or availability of an affected component or system or the product with digital elements (see IEC 62443-3-2 and Article 3 No. 40 EU Cyber Resilience Act [2]).

1. The Contractor is obliged to maintain a vulnerability management system throughout the entire product life cycle. The vulnerability management also includes a regular, documented analysis of vulnerability databases and the relevance for the contractual products.
 2. The Contractor undertakes to regularly and effectively test and verify the security of the contractual product throughout its product lifecycle, including by carrying out regular penetration tests and vulnerability scans or permanent vulnerability monitoring. The product lifecycle (support period) of the contractual product shall be determined jointly by the Contractor and the Client. In doing so, the expected service life, the legitimate expectations of users, the nature and intended purpose of the contractual product, and any applicable legal requirements regarding the lifespan of products with digital elements shall be taken into account. The results of the penetration tests and vulnerability scans shall always be shared with the Client in full. The Contractor shall explain to the Client how and in what time frame the vulnerabilities will be remedied. Functional tests of the Contractor shall take into account the issue of attack security.
 3. The Contractor shall establish a structured process for the responsible disclosure of vulnerabilities. For this purpose, the Contractor shall provide an appropriate reporting channel (e.g. a dedicated email address or a web form), which shall be publicly documented and accessible. The Contractor undertakes to treat incoming reports confidentially, to review them without undue delay, and – where necessary – to take appropriate remedial action.
 4. The Contractor undertakes to remedy exploitable vulnerabilities in its contractual products that are known to it or become known within a reasonable period of time. A reasonable period of time is < 90 days if no other period of time has been agreed with the Client. In the event of danger to life and limb, the Contractor shall immediately do everything in its power to counter the dangers emanating from
-

its contractual product or to define, implement and communicate compensatory (including operational) countermeasures. After remediation, the Contractor provides a report on the remediation.

5. The Contractor shall inform the Client without delay, but in any case within the applicable response time, of any known vulnerabilities and incidents (security incidents) in contractual products delivered to the Client. For this purpose, a corresponding score (e.g. CVSS score or EPSS or SSVC or VPR) and the Traffic Light Protocol (TLP) shall be used. In addition, the Contractor undertakes to establish and maintain a process for the creation and provision of security advisories in the Common Security Advisory Framework (CSAF) format. Such advisories shall be made available to the Client without delay.
 6. The response time for reporting vulnerabilities after detection and incidents to the Client by the Contractor is 24 hours, from Monday to Friday. This applies irrespective of any warranty periods or other statutory limitation periods for a period of 20 years after delivery, but at least for the agreed product support period.
 7. The Contractor shall use the e-mail address PSIRT@ps.rolls-royce.com to report vulnerabilities and advisories.
-

9 Security updates

1. The Contractor undertakes to provide security updates to the Client without delay, automatically and free of charge in order to close any vulnerabilities that become known. This shall apply irrespective of any warranty periods or other statutory limitation periods for a period of 20 years after delivery, but at least for the agreed product support period. The function for automatic security updates as defined by the CRA has been implemented, unless otherwise agreed.
2. The Contractor undertakes to ensure that each security update provided to the Client remains available for a period of at least ten years after its release.
3. The Contractor undertakes to inform the Client of the end-of-life of the contractual product at least 1 year before the end of production. If it is not possible for the Contractor due to external circumstances, the information will be provided at the latest 48 hours after becoming known.

10 Cooperation of the Contractor

1. The Contractor undertakes to cooperate constructively in the secure integration of its contractual product into the Client's system.
 2. The Contractor undertakes to participate in coordination with the Client and the end customer and to actively participate in the creation of an overall product security concept, insofar as it concerns its contractual product. Any existing product security concept for the contractual product shall be delivered with the contractual product. The holistic product security concept refers to the Client's scope of delivery and may include technical measures as well as organisational and personnel measures.
 3. The Contractor undertakes to carry out a security analysis of the contractual product together with the Client, if required, at the Client's request. In particular, the Contractor shall support the Client in the technical evaluation of its contractual product against IEC 62443-4-2 and the Essential Requirements of EU Cyber Resilience Act (CRA, [2]) Annex I Part 1.
 4. If the Contractor learns of an actual incident within its IT infrastructure that may have an actual or potential adverse effect on the Contractor's infrastructure in which the Client's data is stored (Cyber Incident) or of any other unauthorised access to or use or misuse, damage or destruction by a third party (Other Incident), the Contractor shall notify the Client immediately and no later than 24 hours after it becomes aware of the Cyber Incident or Other Incident. The Contractor shall use the email address PSIRT@ps.rolls-royce.com for this purpose.
 5. The Contractor undertakes to comply with all instructions issued by the Client in connection with the cyber incident or other incident and to comply with the statutory regulations. This relates in particular to the documentation, the obtaining and preserving evidence about the cyber incident, the implementation of remediation strategies to reduce the impact of the cyber incident or other incident or the likelihood or impact of future similar incidents and the notification of and cooperation with authorities. Evidence shall be retained for a period of at least 12 months.
 6. The exchange of data and information may be subject to restrictions under export law or Regulations on the protection of classified information. In this case, the contractor is obliged to provide information pro-actively.
-

11 Contract product hardening and risk mitigation

1. The Contractor further ensures that the contractual product has been designed, developed and manufactured to minimise attack surfaces – particularly at external interfaces – and to provide an appropriate level of resilience against cyberattacks and security incidents. Upon request, the Contractor shall provide corresponding evidence documents.
2. The Contractor shall supply with the Contract Product instructions and manuals for the secure setting and hardening of the Contract Product, in particular for network and/or operating system settings.
3. All cryptographic functions shall be performed according to the state of the art (see e.g. technical guidelines of the BSI, BSI TR-2102). The Contractor confirms that it implements a procedure to securely protect cryptographic keys and other secrets relating to the contractual products for the Client in accordance with the state of the art.
4. If special hardware or software is required for update activities, diagnosis, operation, configuration or other activities on the Contractor's contractual product, this hardware or software shall also be deemed to be a contractual product and must be included in the scope of delivery. The Contractor shall grant the Client and the end customer the permanent right to use the software and shall maintain it over the lifetime of the contractual product. The software shall be delivered as an installation package with release notes and hash. Upon request by the Client, the Contractor shall be obliged to provide evidence of the standards according to which the hardware or software was developed.
5. If standard operating systems are used in the contractual product, the Contractor shall agree a patch management concept and an anti-virus concept with the Client on request and shall supply these. If agreed, the Contractor's control unit shall be supplied with anti-virus software.

Supplementary Information

Previous editions

05.2023

Changes

- Adapted to the requirements of the EU Cyber Resilience Act
 - Standard editorially revised
-