|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Kryptokonzept"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300001 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung (vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Kryptokonzept" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc78219978)

[Dokumentenhistorie 3](#_Toc78219979)

[Inhaltsverzeichnis 4](#_Toc78219980)

[Allgemeine Festlegungen 5](#_Toc78219981)

[Ziel / Zweck 5](#_Toc78219982)

[Geltungsbereich 5](#_Toc78219983)

[Zuständigkeiten 6](#_Toc78219984)

[Genehmigungs- und Änderungsverfahren 6](#_Toc78219985)

[Aufbau des Dokuments 6](#_Toc78219986)

[Sicherheitsrichtlinie "Kryptokonzept" 7](#_Toc78219987)

[Basismaßnahmen 7](#_Toc78219988)

[Auswahl geeigneter kryptographischer Verfahren (CON.1.A1) 7](#_Toc78219989)

[Datensicherung bei Einsatz kryptographischer Verfahren (CON.1.A2) 7](#_Toc78219990)

[Standardmaßnahmen 7](#_Toc78219991)

[Verschlüsselung der Kommunikationsverbindungen (CON.1.A3) 7](#_Toc78219992)

[Geeignetes Schlüsselmanagement (CON.1.A4) 8](#_Toc78219993)

[Sicheres Löschen und Vernichten von kryptographischen Schlüsseln (CON.1.A5) 8](#_Toc78219994)

[Bedarfserhebung für kryptographische Verfahren und Produkt (CON.1.A6) 8](#_Toc78219995)

[Maßnahmen bei erhöhtem Schutzbedarf 8](#_Toc78219996)

[Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte (CON.1.A8 - CIA) 9](#_Toc78219997)

[Auswahl eines geeigneten kryptographischen Produkts (CON.1.A9 - CI) 9](#_Toc78219998)

[Entwicklung eines Kryptokonzepts (CON.1.A10 - CI) 9](#_Toc78219999)

[Sichere Konfiguration der Kryptomodule (CON.1.A11 - CI) 9](#_Toc78220000)

[Sichere Rollenteilung beim Einsatz von Kryptomodule (CON.1.A12 - CI) 10](#_Toc78220001)

[Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen (CON.1.A13 - CI) 10](#_Toc78220002)

[Schulung von Benutzern und Administratoren (CON.1.A14 - CIA) 10](#_Toc78220003)

[Reaktion auf praktische Schwächung eines Kryptoverfahrens (CON.1.A15 - CI) 11](#_Toc78220004)

[Physische Absicherung von Kryptomodulen (CON.1.A16 - CI) 11](#_Toc78220005)

[Abstrahlsicherheit (CON.1A17 - C) 11](#_Toc78220006)

[Kryptographische Ersatzmodule (CON.1.A18 - CIA) 11](#_Toc78220007)

# Allgemeine Festlegungen

## Ziel / Zweck

Die Verschlüsselung von Informationen ist ein weit verbreitetes Mittel, um die Informationssicherheit in den Schutzzielen Vertraulichkeit, Integrität und Authentizität zu gewährleisten. Mit Hilfe von kryptografischen Verfahren werden Informationen verschlüsselt, sodass deren Inhalt ohne den zugehörigen Schlüssel nicht lesbar ist. Dabei können symmetrische Verfahren, d.h. es wird derselbe Schlüssel zum Verschlüsseln und Entschlüsseln verwendet, sowie asymmetrische Verfahren, d.h. es wird ein Schlüssel zum Verschlüsseln und ein anderer Schlüssel zum Entschlüsseln verwendet, eingesetzt werden.

In einer heterogenen Umgebung können dabei lokal gespeicherte Daten, die Daten in der SaaS-Lösung und auch die zu übertragenden Daten der <Institution> wirkungsvoll durch kryptografische Verfahren und Techniken geschützt werden.

Darüber hinaus werden weitergehende Maßnahmen auf organisatorischer und prozessualer Ebene benötigt. Der alleinige technische Einsatz von kryptografischen Verfahren genügt nicht, um die Vertraulichkeit, Integrität und Authentizität der verschlüsselten Informationen zu gewährleisten.

Die Gesamtheit der eingesetzten kryptografischen Verfahren und damit verbundenen Maßnahmen wird im Rahmen eines Kryptokonzeptes gebündelt betrachtet. Nur durch eine ganzheitliche Betrachtung der Thematik wird ein effektiver Schutz durch Kryptografie ermöglicht.

Eine Besonderheit stellen Kryptomodule dar, die für kryptografische Verfahren bei erhöhtem Schutzbedarf eingesetzt werden sollten. Mit einem Kryptomodul ist seitens der <Institution> ein Produkt gemeint, das die im Kryptokonzept dargelegte Sicherheitsfunktion bietet. Ein solches Produkt kann dabei aus Hardware, Software, Firmware oder aus einer Kombination daraus bestehen. Hinzu kommen noch notwendige Bauteile wie Speicher, Prozessoren, Busse und die Stromversorgung, um die Kryptoprozesse umzusetzen.

Diese Sicherheitsrichtlinie beschreibt, wie ein Kryptokonzept erstellt und wie Informationen kryptografisch abgesichert werden können. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Baustein CON.1 "Kryptokonzept" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Das Dokument "Sicherheitsrichtlinie Kryptokonzept“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie "Kryptokonzept"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Auswahl geeigneter kryptographischer Verfahren (CON.1.A1)

Es werden für den späteren Einsatz durch die Verantwortlichen Mitarbeitenden ausschließlich evaluierte und geeignete kryptographische Verfahren ausgewählt. Durch dieses Vorgehen wird sichergestellt, dass ausschließlich dem Stand der Technik sichere Algorithmen, Verfahren und Schlüssellängen verwendet werden. Sollten Algorithmen, Verfahren oder Schlüssellängen abweichen von den intern freigegebenen Verfahren verwendet werden, muss diese Ausnahme unter zur Hilfenahme des Dokument „Template für die Beantragung von Kryptographieausnahmen“ beantragt werden.

### Datensicherung bei Einsatz kryptographischer Verfahren (CON.1.A2)

Bei den Datensicherungsprozessen wird der Schutz der eingesetzten kryptographischen Mechanismen berücksichtigt. Aus diesem Grund findet eine geeignete Speicherung und Aufbewahrung von getätigten Datensicherungen statt, um die Zugriffe auf kryptographische Schlüssel durch unbefugte Dritte zu vermeiden. Alle langlebigen kryptographischen Schlüssel werden außerdem außerhalb der eingesetzten IT-Systeme aufbewahrt. Sofern eine Langzeitspeicherung von verschlüsselten Daten vorliegt, wird in regelmäßigen Abständen (mindestens einmal jährlich) überprüft, ob die verwendeten kryptographischen Algorithmen und Schlüssellängen dem aktuellen Stand der Technik und den intern freigegebenen Verfahren entsprechen.

Durch die Verantwortlichen für die Datensicherung ist sicherzustellen, dass auf verschlüsselt gespeicherte Daten auch nach längeren Zeiträumen noch zugegriffen werden kann. Des Weiteren müssen verwendete Kryptoprodukte archiviert und Konfigurationsdaten von Kryptoprodukten gesichert werden.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Verschlüsselung der Kommunikationsverbindungen (CON.1.A3)

Es ist sicherzustellen das mindestens auf Anwendungsebene mit vertretbarem Aufwand (Verhältnismäßigkeit) eine Verschlüsselung der Kommunikationsverbindungen etabliert ist.

Sollte eine Verschlüsselung der Kommunikationsverbindungen auf Anwendungsebene nicht möglich sein, ist durch die Verantwortlichen eine Verschlüsselung auf darunterliegende ISO/OSI-Layer zu vereinbaren.

### Geeignetes Schlüsselmanagement (CON.1.A4)

Die einzusetzenden kryptographischen Schlüssel werden gemäß dem Schlüsselmanagementprozess mit geeigneten Schlüsselgeneratoren und in sicheren Umgebungen erzeugt. Diese Schlüssel sollen dabei nach Möglichkeit nur einem Einsatzzweck dienen.

Für die Verschlüsselung und Signaturbildung müssen zum besseren Schutz unterschiedliche Schlüssel benutzt werden. Beim Einsatz von erzeugten Schlüsseln sind die authentische Herkunft und die Integrität der Schlüsseldaten durch den Anwender zu prüfen.

Der regelmäßige Wechsel von kryptographischen Schlüsseln richtet sich nach den Vorgaben der <Institution>.

Für den Fall das kryptographische Schlüssel ungewollt offengelegt werden, müssen zeitnah Vorfallbehandlungsmaßnahmen eingeleitet werden, die sicherstellen, dass ein unmittelbarer Schlüsselaustausch eingeleitet wird und eine Prüfung auf korrumpierte oder abgeflossene Informationen erfolgt. Alle erzeugten kryptographischen Schlüssel sind in unter der Hoheit der <Institution> sicher aufzubewahren und zu verwalten.

### Sicheres Löschen und Vernichten von kryptographischen Schlüsseln (CON.1.A5)

Nicht mehr benötigte Schlüssel und Zertifikate sind sicher zu löschen beziehungsweise zu vernichten. Auf Produkte mit unkontrollierbarer Schlüsselablage wird seitens der <Institution> generell verzichtet.

### Bedarfserhebung für kryptographische Verfahren und Produkt (CON.1.A6)

Es wird im Rahmen von Bedarfserhebungen festgelegt, für welche Aufgaben kryptographische Verfahren einzusetzen sind. Anschließend werden die Anwendungen, IT-Systeme und Kommunikationsverbindungen identifiziert, die notwendig sind, um diese Aufgaben zu erfüllen. Diese werden wie festgelegt kryptographisch abgesichert.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte (CON.1.A8 - CIA)

Bevor eine Entscheidung getroffen werden kann, welche kryptographischen Verfahren und Produkte bei erhöhtem Schutzbedarf eingesetzt werden, sind unter anderem folgende Einflussfaktoren zu ermitteln:

* Sicherheitsaspekte,
* Technische Aspekte,
* Personelle und organisatorische Aspekte,
* Wirtschaftliche Aspekte,
* Lebensdauer von kryptographischen Verfahren und der eingesetzten Schlüssellängen,
* Zulassung von kryptographischen Produkten und
* Gesetzliche Rahmenbedingungen.

### Auswahl eines geeigneten kryptographischen Produkts (CON.1.A9 - CI)

Vor der Auswahl eines kryptographischen Produkts legt die <Institution> mindestens folgende Anforderungen an das gewünschte Produkt fest:

* Funktionsumfang,
* Interoperabilität,
* Wirtschaftlichkeit,
* Fehlbedienungs- und Fehlfunktionssicherheit

Zusätzlich wird geprüft, ob zertifizierte Produkte vorrangig einzusetzen sind. Auch die zukünftigen Einsatzorte werden bei der Auswahl beachtet, da es z. B. Export- und Importbeschränkungen für kryptographische Produkte geben kann.

### Entwicklung eines Kryptokonzepts (CON.1.A10 - CI)

Das Kryptokonzept wird regelmäßig an die Kryptoanforderungen des Informationssicherheitsmanagements der <Institution> und der Fachwelt angepasst. Die Aktualisierung des Kryptokonzepts erfolgt mindestens einmal im Jahr.

Alle im Kryptokonzept beschriebenen technischen und organisatorischen Vorgaben werden durch die <Institution> spezifiziert. Bei der Entwicklung des Kryptokonzeptes wird der Lebenszyklus des jeweiligen Zielobjekts im Rahmen der Planungssicherheit und des wirtschaftlichen Betriebs berücksichtigt.

### Sichere Konfiguration der Kryptomodule (CON.1.A11 - CI)

Die Kryptomodule werden sicher installiert und konfiguriert. Dabei werden unter anderem voreingestellten Schlüssel gemäß den Anforderungen der <Institution> geändert. Anschließend sind Tests erforderlich, die Aufschluss darüber geben, ob die Kryptomodule korrekt funktionieren und vom Benutzer bedient werden können.

Bei allen IT-System-Änderungen wird getestet, ob die eingesetzten kryptographischen Verfahren noch greifen. Die Konfigurationen der Kryptomodule sind dokumentiert und werden regelmäßig (mindestens einmal jährlich) überprüft.

Weiterhin sind durch die Verantwortlichen Architekten und Betriebsverantwortlichen die Anforderungen an die Einsatzumgebung festgelegt.

### Sichere Rollenteilung beim Einsatz von Kryptomodule (CON.1.A12 - CI)

Bei der Konfiguration von Kryptomodulen sind Benutzerrollen festzulegen. Die damit einhergehende Sicherstellung von berechtigten Zugriffen auf gewünschte Dienste durch Mitarbeiter wird mit Zugriffskontroll- und Authentisierungsmechanismen verifiziert. Das Kryptomodul ist so konfiguriert, dass bei jedem Rollenwechsel oder bei Inaktivität nach einer bestimmten Zeitdauer die Authentisierungsinformationen erneut eingegeben werden müssen.

### Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen (CON.1.A13 - CI)

Für den sicheren Einsatz von Kryptomodulen sind auch die Anforderungen an die Betriebssysteme zu berücksichtigen. Es sollten nur geeignete, kompatible und gehärtete Betriebssysteme zum Einsatz kommen. Das Zusammenwirken von Betriebssystemen und Kryptomodulen gewährleistet, dass:

* Die installierten Kryptomodule nicht unbemerkt abgeschaltet oder umgangen werden können,
* Die angewendeten oder gespeicherten Schlüssel nicht kompromittiert werden können,
* Die zu schützenden Daten nur mit Wissen und unter Kontrolle des Benutzers auch unverschlüsselt auf Datenträgern abgespeichert werden bzw. das informationsverarbeitende System verlassen können und
* Manipulationsversuche am Kryptomodul erkannt werden.

### Schulung von Benutzern und Administratoren (CON.1.A14 - CIA)

Es werden regelmäßige Benutzer- und Administratorenschulungen durchgeführt, in denen der Umgang mit den von ihnen zu bedienenden Kryptomodulen vermittelt wird.

Den Benutzern wird unter anderem genau erläutert, was die spezifischen Sicherheitseinstellungen von Kryptomodulen bedeuten und warum sie wichtig sind. Außerdem werden sie auf die Gefahren hingewiesen, sollten die Sicherheitseinstellungen aus Bequemlichkeit umgangen oder deaktiviert werden.

Die Administratoren werden hinsichtlich der Installation, Konfiguration, dem korrekten Einsatz, Umgang mit Hilfsmitteln zur Untersuchung kryptographischer Einstellungen und zur regelmäßigen Wartung von kryptographischen Verfahren und Produkten geschult. Sie erhalten zusätzlich einen Überblick über kryptographische Grundbegriffe.

Die Schulungsinhalte werden immer den jeweiligen Einsatzszenarien entsprechend angepasst.

### Reaktion auf praktische Schwächung eines Kryptoverfahrens (CON.1.A15 - CI)

Durch den etablierten Prozess zur Reaktion auf praktische Schwächung eines Kryptoverfahrens wird die Informationssicherheit im Bereich Kryptographie in der <Institution> gewährleistet. Dabei wird sichergestellt, dass geschwächte kryptographische Verfahren abgesichert oder durch geeignete Alternativen abgelöst werden.

### Physische Absicherung von Kryptomodulen (CON.1.A16 - CI)

Ein unautorisierter physischer Zugriff auf Modulinhalte des Kryptomoduls ist untersagt. Hard- und Softwareprodukte, die als Kryptomodule eingesetzt werden, führen nach Möglichkeit einen Selbsttest durch.

### Abstrahlsicherheit (CON.1A17 - C)

Es sind keine zusätzlichen Maßnahmen hinsichtlich der Abstrahlsicherheit notwendig. Diese könnten bei Notwendigkeit in der zukünftigen Planung berücksichtigt werden, sofern staatliche Verschlusssachen (VS) der Geheimhaltungsgrade VS-VERTRAULICH und höher verarbeitet sollen.

### Kryptographische Ersatzmodule (CON.1.A18 - CIA)

In der <Institution> sind aus Verfügbarkeitsgründen Ersatzkryptomodule vorrätig zu halten, sofern Kryptomodule zum produktiven Einsatz kommen.