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

Template "Antrag auf Kryptographieausnahme"

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 Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | TMP400001 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung (vergeben] |
| Name des Dokuments | Template "Antrag auf Kryptographieausnahme" | [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](#_Toc78553392)

[Dokumentenhistorie 3](#_Toc78553393)

[Inhaltsverzeichnis 4](#_Toc78553394)

[Beantragung von Kryptographieausnahmen 5](#_Toc78553395)

[Betrachtungsgegenstand 5](#_Toc78553396)

[interne Ansprechpartner 5](#_Toc78553397)

[externe Ansprechpartner 5](#_Toc78553398)

[Anwendungsbereich und Abgrenzung 5](#_Toc78553399)

[Krypto-Bedarfsanalyse 5](#_Toc78553400)

[Technische Sicherheit 6](#_Toc78553401)

[Kryptographische Geräte 8](#_Toc78553402)

[Organisatorische Sicherheit 9](#_Toc78553403)

[Sonstiges 9](#_Toc78553404)

[Anpassung der Algorithmen und Schlüssellängen 10](#_Toc78553405)

[Maßnahmen 10](#_Toc78553406)

[Maßnahme 1: <Titel 1> 10](#_Toc78553407)

[Maßnahme n: <Titel n> 10](#_Toc78553408)

# Beantragung von Kryptographieausnahmen

## Betrachtungsgegenstand

<An dieser Stelle muss textuell die Beschreibung des Betrachtungsgegenstandes hinterlegt werden>

## interne Ansprechpartner

Innerhalb der <Institution> sind mit dem Einsatz von kryptographischen Systemen folgende Mitarbeitenden befasst.

| **Name** | **Verantwortlichkeiten** |
| --- | --- |
|  |  |

Tabelle 1: interne Ansprechpartner

## externe Ansprechpartner

Folgende externe Dienstleister bzw. Lösungsanbieter sind am Einsatz kryptographischer Systeme beteiligt.

| **Name** | **Verantwortlichkeiten** |
| --- | --- |
|  |  |

Tabelle 2: externe Ansprechpartner

## Anwendungsbereich und Abgrenzung

<An dieser Stelle muss textuell die Beschreibung des Anwendungsbereichs und eventueller Abgrenzungen hinterlegt werden>

## Krypto-Bedarfsanalyse

Die nachfolgende Tabelle spiegelt das Ergebnis der Vertraulichkeits-/Integritätsanalyse und der Krypto-Bedarfsanalyse wider. Die Vertraulichkeits- und Integritätsanalyse setzt dabei auf die Schutzbedarfsfeststellung auf und verwendet die dort entwickelte Kritikalitätsmatrix. Die Krypto-Bedarfsanalyse orientiert sich an den Ergebnissen des BSI IT-Grundschutz-Checks.

|  |  |
| --- | --- |
| **Vertraulichkeits-/Integritätsanalyse** | **Krypto-Bedarfsanalyse** |
| Kommunikationsverbindungen | Art der Daten | Integrität | Vertraulichkeit | Eingesetzte Produkte bzw. Verfahren | Referenzen |
|  |  |  |  |  |  |

Tabelle 3: Krypto-Bedarfsanalyse

### Technische Sicherheit

#### Kryptographische Software

|  |  |
| --- | --- |
| **Produkt** | Welches Produkt kommt zum Einsatz? In welcher Version? |
|  |
| **Hersteller** | Wer ist der Hersteller? |
|  |
| **Funktion** | Was ist der Einsatzzweck? |
|  |
|  |
| **Algorithmus** | Welche kryptographischen Algorithmen und Schlüssellängen kommen zum Einsatz? |
|  |
|  |
| **Eignung** | Verfügt die Lösung über eine Zertifizierung, welche durch das europäische Abkommen zur Anerkennung von CC- und ITSEC- Zertifikate (SOGIS-MRA) oder durch das weltweite Abkommen (CCRA) zur Anerkennung von CC-Zertifikaten ebenfalls vollumfänglich in Deutschland gültig ist? |
|  |
|  |
| **Einsatzumgebung** | Wo sind die Geräte aufgestellt bzw. die Applikation zur Verfügung gestellt? Wie ist der Zugang gesichert? Wer hat Zugang? Bei Software bzw. SaaS: Auf welchen Systemen kommt die Software zum Einsatz? |
|  |
|  |
| **Installation** | Wer ist für die Aufstellung der Geräte/Installation der Software verantwortlich? Wer hat dies durchgeführt? Wer ist für die Bereitstellung der SaaS, IaaS, PaaS zuständig? |
|  |
|  |
| **Betrieb** | Wer ist für Wartung und Betrieb der Geräte/Software/Funktionen verantwortlich? |
|  |
|  |
| **Schulung und Einweisung** | Welche Qualifikationsmaßnahmen sind für Anwender und Administratoren durchgeführt worden? Sind diese ausreichend? |
|  |
|  |
| **Schlüsselmanagement** | Wer ist für das Schlüsselmanagement verantwortlich? |
|  |
|  |
| **Schlüsselerzeugung** | Wo und wie wurden die Schlüssel erzeugt? Von wem wurden die Schlüssel erzeugt? Besteht die Gefahr, dass Behörden Zugriff auf den Schlüssel verlangen können? |
|  |
|  |
| **Schlüsseltrennung** | Falls Schlüssel außerhalb des Geräts erzeugt werden, wie werden diese in das Gerät eingebracht? Wie werden öffentliche Schlüssel oder Zertifikate ausgetauscht/veröffentlicht? |
|  |
|  |
| **Schlüsselspeicherung** | Wo sind die kryptographischen Schlüssel gespeichert? Falls Krypto-Token zum Einsatz kommen (Chipkarten, USB-Token), wo werden diese verwahrt? Besteht die Gefahr, dass Behörden Zugriff auf den Schlüssel verlangen können? |
|  |
|  |
| **Schlüsselarchivierung** | Werden Schlüssel zur Wiederherstellung von Daten hinterlegt oder archiviert? |
|  |
|  |
| **Zugriffsregelung** | Wer hat Zugang bzw. Zugriff zu den Krypto-Systemen bzw. Zugriff auf die Software? |
|  |
|  |
| **Schlüsselwechsel** | Wie lange sind die verwendeten Schlüssel/Zertifikate gültig? Wie wird eine rechtzeitige Verlängerung sichergestellt? Wer ist dafür verantwortlich? |
|  |
|  |
| **Schlüsselvernichtung** | Werden alte Schlüssel gelöscht bzw. alte Token vernichtet? Wie? |
|  |
|  |
| **Protokollierung** | Welche Ereignisse werden protokolliert (z. B. Schlüsselwechsel, Verbindungsaufbau)? Wer hat Zugriff auf die Protokolle? Erfolgt eine Auswertung? |
|  |
|  |
| **Ausfall bzw. Notfallvorsorge** | Behindert der Ausfall der kryptographischen Geräte die Arbeitsfähigkeit? Wenn ja, welche Maßnahmen zur Vorsorge sind getroffen worden (z. B. Redundanzen, Ersatzgeräte, Service Levels)? |
|  |

Tabelle 4: technische Sicherheit - kryptographische Software

### Kryptographische Geräte

Zum Zwecke der kryptographischen Absicherung werden die folgenden Geräte-Modelle eingesetzt:

* <Modell A>
* <Modell n>

### Organisatorische Sicherheit

#### Einsatzbedingungen kryptographischer Produkte

<An dieser Stelle bitte textuell die Beschreibung der Einsatzbedingungen kryptographischer Produkte hinterlegen>

#### Sicherheitspolitik und Sicherheitsregelungen

Die Verantwortlichkeiten für den Betrieb der einzelnen kryptographischen Produkte können den Tabellen beim jeweiligen Produkt entnommen werden.

Die Umsetzung der Sicherheitsmaßnahmen wird im Rahmen von Sicherheitsaudits überprüft. Aktuelle Informationen zur Sicherheit von kryptographischen Verfahren und Produkten beziehen die Verantwortlichen aus den entsprechenden Mitteilungen bspw. vom Hersteller oder öffentlichen CERTS.

Angaben zur Protokollierung durch die einzelnen kryptographischen Produkte sind in den Tabellen beim jeweiligen Produkt mit aufgeführt.

#### Qualifikation und Schulung

Angaben zu den Qualifikationsmaßnahmen zu den einzelnen Lösungen finden sich in den entsprechenden Tabellen beim jeweiligen Produkt.

Für die Verantwortlichen des Betriebes und der Planung erfolgen Schulungen entsprechend des vorliegenden Bedarfs und nach Rücksprache mit dem Vorgesetzten.

#### Reaktion auf Verletzung der Sicherheitspolitik

Die Vorsorgemaßnahmen gegen den Ausfall von Krypto-Geräten richten sich je nach der eingesetzten Lösung und der zugrundeliegenden Verfügbarkeitsanforderungen gemäß der Schutzbedarfsfeststellung. Die Maßnahmen sind jeweils in den entsprechenden Tabellen beim jeweiligen Produkt mit aufgeführt.

Bei Sicherheitsvorfällen, insbesondere beim Verdacht auf vorsätzliche Handlungen, werden die Sicherheitsverantwortlichen informiert. Diese leiten die entsprechenden Maßnahmen zur Untersuchung, Aufklärung und Verfolgung der Fälle ein.

Eine Evaluierung der Aktualität und Eignung der eingesetzten kryptographischen Lösungen erfolgt jeweils bei der Aktualisierung dieser Betrachtung. Eine vorzeitige Überprüfung kann anlassbezogen erfolgen, z. B. wenn neue Angriffsmethoden auf kryptographische Verfahren publiziert werden.

### Sonstiges

#### Entsorgung von Altgeräten und Speichermedien

Bei ausgemusterten IT-Komponenten werden alle gespeicherten Daten gelöscht und vorhandene Speichermedien sollen mit einem BSI zugelassenen Tool gesäubert werden. Nähere Angaben zur Entsorgung der eingesetzten Geräte mit kryptographischen Funktionen finden sich in den Tabellen beim jeweiligen Produkt unter dem Punkt „Schlüsselvernichtung“.

#### Umgang mit Garantiefällen

Im Garantiefall werden die kryptographischen Geräte an den Hersteller im Rahmen eines Austausches oder einer Reparatur zurückgegeben. Die Schlüssel und die gespeicherten Informationen werden sofern noch möglich vorher aus dem System entfernt.

### Anpassung der Algorithmen und Schlüssellängen

Die Anpassung der zur Verfügung stehenden Algorithmen und Schlüssellängen erfolgt über entsprechende Updates der Hersteller.

## Maßnahmen

Die im Rahmen dieses Dokumentes durchgeführte Erhebung des Krypto-Einsatzes hat ergänzende Handlungsbedarfe der eingesetzten kryptographischen Lösungen oder zur Verbesserung ihrer Einsatzbedingungen ergeben. Diese Maßnahmen sind hier abschließend zusammengefasst.

### Maßnahme 1: <Titel 1>

<xxx>

### Maßnahme n: <Titel n>

<xxx>