Bundesamt
für Sicherheit in der
Informationstechnik

Musterkryptokonzept

Verfasser: BSI – Sicherheitsberatung

Version: 1.2

Stand: 15.04.2010

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-333
E-Mail: sicherheitsberatung@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

Management Summary und Einordnung des Dokumentes in den Kontext

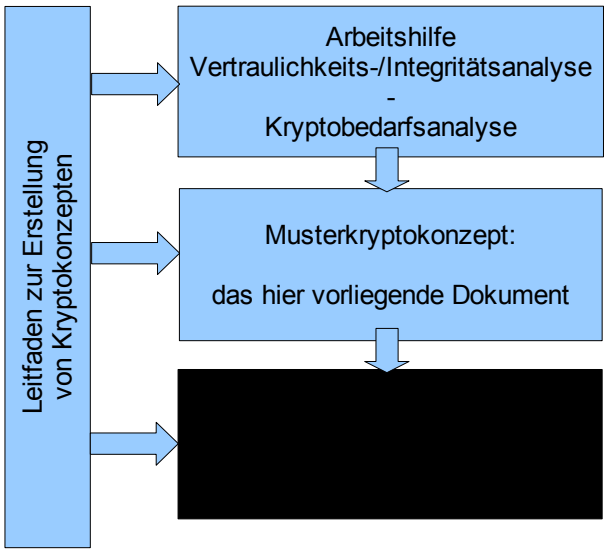
In der heutigen vernetzten IT-Welt steigt die Quantität der Informationen, die ausgetauscht werden, stetig und sie werden damit für „Angreifer“ zugänglicher und deutlich attraktiver. Insbesondere die Vertraulichkeit und die Integrität der Daten sind bei der Nutzung von IT-Systemen von besonderer Bedeutung.

Im „Umsetzungsplan BUND“ werden in Kapitel 4 - „Vertraulichkeit gewährleisten“ besondere Anforderungen gestellt, die insbesondere die Durchführung einer Vertraulichkeits-/Integritätsanalyse, einer Kryptobedarfsanalyse und die Erstellung von Kryptokonzepten umfassen. Um hier eine Hilfestellung anzubieten, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im September 2008 den Leitfaden zur Erstellung von Kryptokonzepten veröffentlicht.

Im Januar 2009 hat das BSI eine Arbeitshilfe herausgegeben, die über die Informationen des Leitfadens hinaus eine ergänzende und praxisorientierte Unterstützung für alle Personen, die für die Informationssicherheit verantwortlich sind, bietet.

Das hier vorliegende Musterkryptokonzept setzt **exemplarisch** den Leitfaden nach dem Vorgehen der Arbeitshilfe um und veranschaulicht den konkreten Aufbau eines Kryptokonzeptes.

Nachfolgende Graphik stellt den Zusammenhang aller zur Erstellung des Kryptokonzeptes der Behörde erforderlichen und hilfreichen Dokumente dar.



Die Gliederung des Musterkryptokonzeptes entspricht dabei der Vorgehensweise und Gliederung des Leitfadens zur Erstellung von Kryptokonzepten und verwendet dazu die Arbeitsschritte aus der Arbeitshilfe.

Die Musterbehörde wird im Folgenden mit „Bundesamt für Konzeption“ (BfK) bezeichnet.

1. Einführung

1.1 Allgemeine Angaben

Das Bundesamt für Konzeption (BfK) ist gesetzlich mit der Erstellung von projektspezifischen Konzepten beauftragt worden. Die Konzepterstellung erfolgt überwiegend IT-gestützt, dabei werden sowohl sensitive Daten, als auch Verschlusssachen verarbeitet. Daher verfolgt das Amt das Ziel, hierfür eine sichere IT-Umgebung bereitzustellen, um die zu verarbeitenden Daten und Informationen vor Verlust von Vertraulichkeit, Integrität und Verfügbarkeit zu schützen.

Dieses Ziel wird im BfK durch die Umsetzung der BSI-Standards 100-1 bis 100-4 sichergestellt. Hierfür wurde im BfK die Funktion des IT-Sicherheitsbeauftragten (IT-SiBe) eingerichtet. Der ITSibe wird an allen IT-Projekten beteiligt, wobei die Gesamtzuständigkeiten der für die Planung/Beschaffung und den IT-Einsatz zuständigen Stellen erhalten bleiben (siehe auch „Dienstanweisung IT-SiBe“ vom 21. Juli 1998). Der IT-Sicherheitsbeauftragte hat Vorgaben, Informationen und Komponenten zur Einhaltung der Informationssicherheit der Benutzer-APC’s in geeigneter Form bereit zu stellen.

Neben dem IT-Sibe des BfK waren die folgenden Parteien bei der Erstellung des Kryptokonzeptes beteiligt:

- Datenschutzbeauftragter gemäß § 4 des Bundesdatenschutzgesetzes
- Geheimschutzbeauftragter gemäß § 5 Abs. 3 Verschlusssachenanweisung des Bundes (VSA)
- Abteilungsleiter der Abteilung IT
- Amtsleitung

1.2 Zweck des Dokumentes

1.2.1 Zielgruppe

Dieses Kryptokonzept richtet sich an alle Verantwortlichen der Informationssicherheit, sowie an alle Mitarbeiterinnen und Mitarbeiter des BfK, die in Ihrer täglichen Arbeit Kryptosysteme nutzen oder sie administrieren.
Die in dieser Richtlinie enthaltenen Sicherheitsregelungen haben für die o.g. Personenkreise bindenden Charakter.

1.2.2 Gültigkeitszeitraum des Dokumentes

Das Kryptokonzept wird jährlich im ersten Quartal des Jahres und bei Sicherheitsvorfällen auf seine Aktualität hin geprüft. Änderungen im Aufbau der IT-Landschaft, der verwendeten IT-Systeme und Anwendungen, sowie der eingesetzten kryptographischen Verfahren fließen unmittelbar in das Kryptokonzept ein.

1.3 Referenzierte Dokumente

Das vorliegende Kryptokonzept ist Bestandteil der aktuellen IT-Sicherheitskonzeption. Es wurde auf der Basis der BSI-Standards 100-2 (Version 2.0) sowie des Leitfadens zur Erstellung von Kryptokonzepten (Version 1.0) und der Arbeitshilfe zur Vertraulichkeits-/Integritätsanalyse und Kryptobedarfsanalyse (Version 1.0) erstellt.

2. Überblick über das Gesamtsystem

2.1 Überblick

Als Untersuchungsgegenstand wird das über zwei Liegenschaften erstreckte Hausnetz des BfK betrachtet (siehe Abbildung 1: IT-Verbund des BfK).

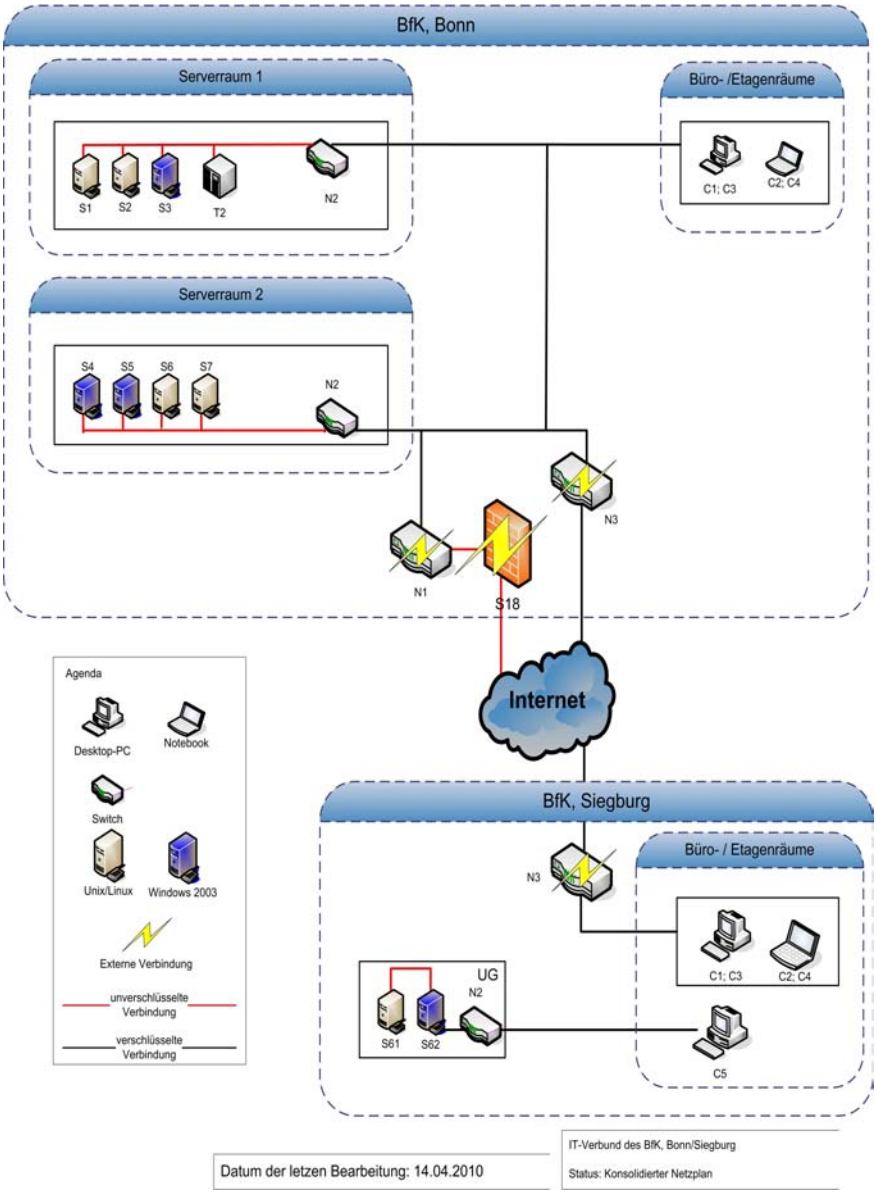


Abbildung 1: Informationsverbund BfK

Die Abbildung 1 zeigt den im Rahmen des Kryptokonzeptes zu betrachtenden Informationsverbund. Die dort gezeigten IT-System werden in der Vertraulichkeits-/Integritätsanalyse und Kryptobedarfsanalyse mit den entsprechenden Bezeichnungen weiter betrachtet.

Mobile Speichermedien sind in der Abbildung 1 nicht visualisiert, werden aber im Kryptokonzept mit betrachtet.

2.2 Beteiligte Parteien

2.2.1 Interne Parteien

Folgende Personengruppen sind mit dem Einsatz von kryptographischen Systemen befasst:

- Der IT-Sicherheitsbeauftragte, der Geheimschutzbeauftragte und Mitarbeiter der Abteilung IT sind mit der Auswahl geeigneter Produkte betraut.
- Mitarbeiter der Abteilung IT sind für die Beschaffung, Betrieb, Administration und Aussonderung von Kryptosystemen zuständig.
- Der Kryptoverwalter, der für die nachweispflichtigen Kryptomittel des BSI zuständig ist.
- Mitarbeiter, die auf Ihren Arbeitsplatz-PCs Verschlüsselungsprodukte einsetzen.

Die Aufbauorganisation des BfK kann dem Organigramm entnommen werden, welches im Intranet des BfK veröffentlicht ist.

2.2.2 Externe Parteien

Folgende externe Parteien (Dienstleister) werden vom BfK eingebunden:

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt dem BfK nachweispflichtige Kryptomittel für den Betrieb der Kryptogeräte zur Verfügung.
- Die IVBB-CA stellt für die sichere E-Mail-Kommunikation Zertifikate und kryptographische Schlüssel zur Verfügung.
- Die Hersteller von Kryptosystemen stellen die Produkte und den Support zur Verfügung.

2.3 Zielsetzung und Anwendungsbereich

Das Kryptokonzept betrachtet den Informationsverbund des BfK. Hierbei werden von öffentlich zugänglichen bis hin zu nach VSA eingestuften Daten alle Informationen in das Kryptokonzept einbezogen. Die Bearbeitung, Übertragung und Speicherung von personenbezogenen Daten steht dabei im besonderen Fokus in der Zusammenarbeit mit dem Datenschutzbeauftragten. Ziel ist es ein angemessenes Maß an Vertraulichkeit und Integrität zu gewährleisten, ohne die Verfügbarkeit einzuschränken.

2.4 Abgrenzung

Die Abgrenzung des Kryptokonzeptes geht aus der zugrunde liegenden Sicherheitskonzeption hervor.

2.5 Umsetzung

Das BfK verfügt über eine sichere IT-Infrastruktur. Diese basiert auf den in den Grundschutz-Katalogen geforderten Konzepten, z.B.

Konzeption:

- IT-Sicherheitskonzept (nach BSI-Standards 100-1 bis 100-4)
- Datensicherungskonzept
- das vorliegende Kryptokonzept

Auswahl kryptographischer Verfahren erfolgt auf der Grundlage der technischen Richtlinien des BSI (Kürzel: BSI TR-02102)

Auswahl und Beschaffung kryptographischer Geräte und Programme:

- Hier findet eine Auswahl nach den Vorgaben der VSA und unter Anwendung des Beschaffungsleitfadens (BSI - L04001) bzw. aufgrund von Empfehlungen des BSI statt.
- Der Markt der Krypto-Produkte bzw. IT-Sicherheitsprodukte wird beim BSI abgefragt.

3. Vertraulichkeits-/Integritätsanalyse und Kryptobedarfsanalyse

Die Ergebnisse aus der Vertraulichkeits-/Integritätsanalyse und der Kryptobedarfsanalyse (siehe Schritt 2 und 3 der Arbeitshilfe zur Vertraulichkeitsanalyse und Kryptobedarfsanalyse) sind für das BfK in Tabelle 1 dargestellt. Die im IT-Sicherheitskonzept enthaltene Risikoanalyse nach BSI-Standard 100-3 wurde dabei berücksichtigt und angepasst.

Arbeitsschritt 2					Arbeitsschritt 3
IT-Systeme / Datenträger / Kommunikations-verbindungen	Anzahl	Art der Daten (z.B. E-Mail, Dateien)	Schutzbedarf (Anm. 4)	VS-Einstufung (maximal)	eingesetztes Kryptoprodukt
C1 (Windows-Desktop) C2 (Windows-Notebook)	100	Dateien, E-Mails	Hoch (Vertraulichkeit) Hoch (Integrität)	VS-NfD	Compusec, Chiasmus, GPG4Win (Anm.1), cv act s/mail, OpenVPN (Anm.2)
C3 (Linux-Desktop) C4 (Linux-Notebook)	100	Dateien, E-Mails, personenbezogene Daten	Hoch (Vertraulichkeit) Hoch (Integrität)	Keine VS	Compusec, Kleopatra, OpenVPN
C5 (VS-Clients)	10	Dateien	Sehr Hoch (Vertraulichkeit) Hoch (Integrität)	VS-V	Noch auszuwählen
S1 (DB-Server)	1	Personaldatenbank (personenbezogene Daten)	Sehr Hoch (Vertraulichkeit) Sehr Hoch (Integrität)	Keine VS	Noch auszuwählen
S2 (File-Server unter Linux)	1	Dateien, personenbezogene Daten	Hoch (Vertraulichkeit) Hoch (Integrität)	Keine VS	Noch auszuwählen
S3/S4/S5 (File-Server unter Windows)	3	Dateien	Hoch (Vertraulichkeit) Hoch (Integrität)	VS-NfD	Entbehrlich durch materielle und organisatorische Maßnahmen (Anm. 3)

Arbeitsschritt 2					Arbeitsschritt 3
IT-Systeme / Datenträger / Kommunikations-verbindungen	Anzahl	Art der Daten (z.B. E-Mail, Dateien)	Schutzbedarf (Anm. 4)	VS-Einstufung (maximal)	eingesetztes Kryptoprodukt
S61/S62 (VS-File-Server)	2	Dateien	Sehr Hoch (Vertraulichkeit) Hoch (Integrität)	VS-V	Entbehrlich durch materielle und organisatorische Maßnahmen (Anm. 3)
S6/S7 (E-Mail Gateway)	2	E-Mails	Hoch (Vertraulichkeit) Hoch (Integrität)	keine VS	Julia Mail-Office (Mail-VPS)
N2 VPN Gateways	2	Datenpakete	Hoch (Vertraulichkeit) Hoch (Integrität)	VS-NfD	OpenVPN (Anm.2)
N3 IPSEC VPN Gateway	2	Datenpakete	Hoch (Vertraulichkeit) Hoch (Integrität)	VS-NfD	SINA-Box S
Server-Netz	2	Datenpakete	Hoch (Vertraulichkeit) Hoch (Integrität)	VS-NfD	Entbehrlich durch materielle und organisatorische Maßnahmen (Anm. 3)
VS-Netz	1	Datenpakete	Sehr Hoch (Vertraulichkeit) Hoch (Integrität)	VS-V	Noch auszuwählen
Bonn - Siegburg	1	Datenpakete	Hoch (Vertraulichkeit) Hoch (Integrität)	VS-NfD	SINA-Box S
Client-Netz	1	Datenpakete	Hoch (Vertraulichkeit) Hoch (Integrität)	VS-NfD	OpenVPN (Anm.2)
Transport über USB-Stick	100	Dateien	Hoch (Vertraulichkeit) Hoch (Integrität)	keine VS	Noch auszuwählen

Tabelle 1: Vertraulichkeits- und Integritätsanalyse

Anmerkungen zur Tabelle 1:
1) GPG4Win wird für die Verschlüsselung von nicht VS-eingestuften Daten verwendet.
2) OpenVPN dient zur logischen Trennung in einem für VS-NfD freigegebenen Netzwerk.
3) Die Maßnahmen sind im IT-Sicherheitskonzept dokumentiert.
4) Die Festlegung des Schutzbedarfs wird aus dem IT-Sicherheitskonzept übernommen

Somit besteht ein offener Kryptobedarf bei folgenden IT-Systemen:

Nr.	Beschreibung der Anforderungen an das Produkt	Übertagungs-protokoll	VS-Einstufung	Anzahl
1.	VS-Netz	IP	VS-V	1
2.	VS-Clients (C 5)	Dateien	VS-V	10
3.	Datenbankserver (S 1)	Personaldatenbank	Keine VS	1
4.	File-Server unter Linux (S 2)	Personenbezogene Daten	Keine VS	1
5.	USB-Sticks	Dateien	Keine VS	100

Tabelle 2: Kryptobedarf

Zur Deckung des festgestellten offenen Kryptobedarfs (Stand: Q1/2009) befindet sich das BfK in engem Kontakt mit der Sicherheitsberatung des BSI, um den oben aufgeführten Bedarf zu decken und ein angemessenes Sicherheitsniveau zu erreichen.

4. Technische Sicherheit

4.1 Kryptographische Softwareprodukte

Im BfK wird eine Vielzahl von kryptographischen Produkten genutzt.

4.1.1 Auswahl

Produkt	Funktion	Krypto-Algorithmus	Eignung
Chiasmus für Windows (BSI)	Dateiverschlüsselung	Chiasmus mit 160-Bit Schlüssellänge	BSI-Entwicklung VS-Zulassung bis VS-NfD
GPG4Win (BSI)	Verschlüsselung und Signierung von Dateien und E-Mails	RSA mit 2048 Bit Schlüssellänge	BSI-Entwicklung Open Source
Compusec (CE-Infosys)	Festplattenver-schlüsselung USB-Verschlüsselung	AES mit 256 Bit Schlüssellänge	Produkt für Windows und Linux erhältlich.
OpenVPN (Open Source)	Netzabsicherung mittels SSL	RSA mit 2048 Bit Schlüssellänge AES mit 128 Bit Schlüssellänge	Netzwerkverschlüsselung im Hausnetz Open Source
cv act s/mail (Crypto-vision)	Verschlüsselung und Signierung von E-Mails	RSA mit 2048 Bit Schlüssellänge AES mit 128 Bit Schlüssellänge	S/MIME AddOn für Microsoft Outlook spezifische Einsatzempfehlung für VS-NfD
Kleopatra (BSI)	Verschlüsselung und Signierung von E-Mails	RSA mit 2048 Bit Schlüssellänge AES mit 128 Bit Schlüssellänge	S/MIME AddOn in Kontact für Linux
Julia Mail-Office (ICC)	Verschlüsselung und Signierung von E-Mails	RSA mit 2048 Bit Schlüssellänge AES mit 128 Bit Schlüssellänge	BSI Entwicklung Sicheres E-Mail-Gateway zur Kommunikation mit anderen Behörden

Tabelle 3: eingesetzte kryptographische Softwareprodukte

Bei der Anschaffung kryptographischer Produkte wird die BSI-Empfehlung BSI-TR 02102 „Kryptographische Verfahren" berücksichtigt.

4.1.2 Installation

Produkt	Zuständige Stelle
Chiasmus für Windows (BSI)	Chiasmus für Windows wird auf Antrag durch die Abteilung IT installiert. (Siehe Installationshandbuch der Abteilung IT)
GPG4Win (BSI)	GPG4Win wird auf Antrag durch die Abteilung IT installiert. (Siehe Installationshandbuch der Abteilung IT)
Compusec (CE-Infosys)	Compusec wird standardmäßig auf allen Laptops durch die Abteilung IT installiert. (Siehe Installationshandbuch der Abteilung IT)
OpenVPN (Open Source)	OpenVPN wird durch die Abteilung IT installiert. (Siehe Installationshandbuch der Abteilung IT)
cv act s/mail (Cryptovision)	cv act s/mail wird auf allen Clients standardmäßig installiert. (Siehe Installationshandbuch der Abteilung IT)
Kleopatra (BSI)	Kleopatra wird auf allen Clients standardmäßig installiert. (Siehe Installationshandbuch der Abteilung IT)
Julia Mail-Office (ICC)	Die VPS wird zentral durch die Abteilung IT eingerichtet und betrieben. (Siehe Installationshandbuch der Abteilung IT)

Tabelle 4: Installation kryptographischer Softwareprodukte

Das Installationshandbuch der Abteilung IT beschreibt, wie die Kryptoprodukte zu installieren sind. Das Handbuch umfasst mindestens folgende Punkte:

- minimale Hardwarevoraussetzungen
- erforderliches Betriebssystem
- erforderlicher Patchstand
- Installationsanleitung

4.1.3 Betrieb

Produkt	Zuständige Stelle
Chiasmus für Windows (BSI)	Die Mitarbeiter nutzen Chiasmus für Windows selbstständig und prüfen vor Versand / Weitergabe einer Datei, ob diese zu verschlüsseln ist. Die BSI-Rahmenbedingungen der Zulassung werden berücksichtigt. (Siehe Nutzerhandbuch)
GPG4Win (BSI)	Die Mitarbeiter nutzen GPG4Win selbstständig und prüfen vor Versand einer Nachricht, ob diese zu signieren und zu verschlüsseln ist. (Siehe Nutzerhandbuch)
Compusec (CE-Infosys)	Die verantwortungsvolle Nutzung von Compusec obliegt den Nutzern. Für die Lösung technischer Probleme ist die Abteilung IT zuständig. (Siehe Nutzerhandbuch)
OpenVPN (Open Source)	Zentraler Betrieb durch die Abteilung IT. (Siehe Administrationshandbuch der Abteilung IT)
cv act s/mail (Cryptovision)	Die Mitarbeiter nutzen cv act s/mail selbstständig und prüfen vor Versand einer Nachricht, ob diese zu signieren und zu verschlüsseln ist. (Siehe Nutzerhandbuch)
Kleopatra (BSI)	Die Mitarbeiter nutzen Kleopatra selbstständig und prüfen vor Versand einer Nachricht, ob diese mit dem genannten Produkt zu signieren und zu verschlüsseln ist. (Siehe Nutzerhandbuch)
Julia Mail-Office (ICC)	Die Julia Mail-Office Lösung wird zentral durch die Abteilung IT betrieben. (Siehe Administrationshandbuch der Abteilung IT)

Tabelle 5: Betrieb kryptographischer Softwareprodukte

4.1.4 Sonstiges

Die im BfK genutzten Produkte werden zentral durch die Abteilung IT installiert. Der Mitarbeiter selbst hat aufgrund fehlender Schreibrechte keine Möglichkeit, Softwareprodukte auf seinem APC zu installieren. Sobald die Hersteller Sicherheitsupdates oder neue Versionen der Verschlüsselungs-Software zur Verfügung stellen, werden diese nach einer Testphase im BfK ausgerollt.

4.2 Kryptographische Geräte

Bei kryptographischen Geräten sind die Algorithmen in entsprechender Hardware (z.B. Kryptoprozessoren) implementiert und das Auslesen der geheimen Schlüssel wird in diesen Systemen verhindert.

4.2.1 Auswahl

Produkt	Funktion	Krypto-Algorithmus	Eignung
SINA-Box S (secunet)	Leitungsverschlüsselung	AES mit 128 bzw. 256 Bit Schlüssellänge oder Chiasmus mit 160 Bit Schlüssellänge	Bei der SINA-Box S handelt es sich um ein Produkt, welches ein IP-basiertes IT-Netz mit Hilfe von IPSec absichert. Die eingesetzte SINA-Box S hat eine entsprechende BSI-Zulassung.

Tabelle 6: Eingesetzte kryptographische Geräte

Soweit möglich, wird bei der Anschaffung kryptographischer Produkte die BSI-Empfehlung BSI-TR 02102 „Kryptographische Verfahren" berücksichtigt, und sie Auswahl sollte grundsätzlich auf der Basis der BSI-Schrift 7164 „Liste der zugelassenen IT-Sicherheitsprodukte und -Systeme“ erfolgen.

4.2.2 Einrichtung

Produkt	Zuständige Stelle
SINA-Box S (secunet)	Gemäß Rollenkonzept des BfK erfolgt die Einrichtung durch Mitarbeiter der Abteilung IT. Die erforderlichen Schlüsselmittel werden vom BSI erstellt, und an den Kryptoverwalter übergeben, der sie vereinnahmt und in das Kryptogerät einbringt. (Siehe Administrationshandbuch der Abteilung IT)

Tabelle 7: Einrichtung kryptographischer Geräte

4.2.3 Betrieb

Produkt	Zuständige Stelle
SINA-Box S (secunet)	Der Betrieb der SINA-Komponenten wird durch die Abteilung IT wahrgenommen. Bei technischen Problemen ist für alle SINA-Komponenten die Abteilung IT zuständig. Die Einsatz- und Betriebsbedingungen in der Zulassungsurkunde des BSI werden beachtet.

Tabelle 8: Betrieb kryptographischer Geräte

Die für die Installation der Hardware-Produkte notwendigen Einsatz- und Betriebsbedingungen in der Zulassungsurkunde des BSI werden unter Berücksichtigung des IT-Sicherheitskonzepts des BfK beachtet.

4.2.4 Sonstiges

Die im BfK eingesetzten Produkte werden zentral durch die Abteilung IT eingerichtet.

4.3 Schlüsselmanagement

In der folgenden Tabelle wird der jeweilige Verantwortliche für das Schlüsselmanagement der einzelnen Kryptoprodukte im BfK festgelegt.

Produkt	Verantwortlicher für Schlüsselmanagement
Chiasmus für Windows (BSI)	Benutzer.
GPG4Win (BSI)	Benutzer.
Compusec (CE-Infosys)	Abteilung IT.
OpenVPN (Open Source)	Abteilung IT.
cv act s/mail (Cryptovision)	Verwaltungs-PKI und IVBB-CA.
Kleopatra (BSI)	Verwaltungs-PKI und IVBB-CA.
Julia Mail-Office (ICC)	Verwaltungs-PKI und IVBB-CA.
SINA-Box S (secunet)	Kryptoverteilerstelle des BSI und Kryptoverwalter des BfK

Tabelle 9: Verantwortliche für Schlüsselmanagement

4.3.1 Schlüsselerzeugung

Es werden im BfK folgende Methoden zur Schlüsselerzeugung genutzt:

Produkt	Schlüsselerzeugung
Chiasmus für Windows (BSI)	Der Benutzer muss seine Schlüssel selbst erzeugen. Innerhalb der Software stehen die entsprechenden Funktionen zur Verfügung. (Siehe Nutzerhandbuch)
GPG4Win (BSI)	Der Benutzer muss seine Schlüssel selbst erzeugen. Innerhalb der Software stehen die entsprechenden Funktionen zur Verfügung. (Siehe Nutzerhandbuch)
Compusec (CE-Infosys)	Der Schlüssel wird zentral durch die Abteilung IT erstellt. (Siehe Administrationshandbuch der Abteilung IT)
OpenVPN (Open Source)	Schlüssel und die X.509 Zertifikate werden durch die Abteilung IT bei der IVBB-CA beantragt und der Abteilung IT per E-Mail zugesandt . (Siehe Administrationshandbuch der Abteilung IT)
cv act s/mail (Cryptovision)	Schlüssel und die X.509 Zertifikate werden durch die Abteilung IT bei der IVBB-CA beantragt und dem Benutzer auf einer Chipkarte zugesandt. (Siehe Administrationshandbuch der Abteilung IT)
Kleopatra (BSI)	Schlüssel und die X.509 Zertifikate werden durch die Abteilung IT bei der IVBB-CA beantragt und dem Benutzer per E-Mail zugesandt. (Siehe Administrationshandbuch der Abteilung IT)
Julia Mail-Office (ICC)	Schlüssel und die X.509 Zertifikate werden durch die Abteilung IT bei der IVBB-CA beantragt und der Abteilung IT per E-Mail zugesandt. (Siehe Administrationshandbuch der Abteilung IT)
SINA-Box S (secunet)	Schlüsselmittel für die SINA-Boxen des BfK werden vom BSI mittels SINA-Management erzeugt, und dem Kryptoverwalter des BfK zugestellt. (Siehe Administrationshandbuch der Abteilung IT)

Tabelle 10: Schlüsselerzeugung

4.3.2 Schlüsseltrennung

Eine Schlüsseltrennung ist produktspezifisch, und ist wie folgt realisiert:

Produkt	Schlüsseltrennung
Chiasmus für Windows (BSI)	Nicht anwendbar.
GPG4Win (BSI)	Produkt unterstützt unterschiedliche Zertifikate für verschiedene Einsatzzwecke (Signierfunktion vs. Verschlüsselungsfunktion). Das BfK verwendet allerdings derzeit keine Schlüsseltrennung.
Compusec (CE-Infosys)	Systemspezifische Schlüsseltrennung vorhanden (Siehe Administrationshandbuch der Abteilung IT)
OpenVPN (Open Source)	Systemspezifische Schlüsseltrennung vorhanden (Siehe Administrationshandbuch der Abteilung IT)
cv act s/mail (Cryptovision)	Produkt unterstützt unterschiedliche Zertifikate für verschiedene Einsatzzwecke (Signierfunktion vs. Verschlüsselungsfunktion).
Kleopatra (BSI)	Produkt unterstützt unterschiedliche Zertifikate für verschiedene Einsatzzwecke (Signierfunktion vs. Verschlüsselungsfunktion). Das BfK verwendet allerdings derzeit keine Schlüsseltrennung.
Julia Mail-Office (ICC)	Produkt unterstützt unterschiedliche Zertifikate für verschiedene Einsatzzwecke (Signierfunktion vs. Verschlüsselungsfunktion). Das BfK verwendet allerdings derzeit keine Schlüsseltrennung.
SINA-Box S (secunet)	Gerätespezifische Schlüsseltrennung vorhanden (Siehe Administrationshandbuch der Abteilung IT)

Tabelle 11: Schlüsseltrennung

4.3.3 Schlüsselverteilung und Schlüsselaustausch

Im BfK werden die notwendigen Schlüssel für die Kryptoprodukte wie folgt verteilt:

Produkt	Schlüsselverteilung und -austausch
Chiasmus für Windows (BSI)	Die Schlüsselverteilung des Chiasmus-Schlüssels erfolgt postalisch oder durch persönliche Übergabe an den Kommunikationspartner. (Siehe Nutzerhandbuch)
GPG4Win (BSI)	Der öffentliche Schlüssel wird per signierter E-Mail geschickt oder auf der Internetseite veröffentlicht. (Siehe Nutzerhandbuch)
Compusec (CE-Infosys)	Der Schlüssel wird durch die Abteilung IT auf einen USB-Token geschrieben und persönlich dem Mitarbeiter übergeben. (Siehe Administrationshandbuch der Abteilung IT)
OpenVPN (Open Source)	Schlüssel und Zertifikate werden durch die Abteilung IT auf den Arbeitsplatz-PCs und den VPN-Gateways gespeichert. (Siehe Administrationshandbuch der Abteilung IT)
cv act s/mail (Cryptovision)	Die X.509 Zertifikate mit den öffentlichen Schlüsseln werden auf dem Verzeichnisdienst der IVBB-CA bereitgestellt.
Kleopatra (BSI)	Die X.509 Zertifikate mit den öffentlichen Schlüsseln werden auf dem Verzeichnisdienst der IVBB-CA bereitgestellt.
Julia Mail-Office (ICC)	Die X.509 Zertifikate mit den öffentlichen Schlüsseln werden auf dem Verzeichnisdienst der IVBB-CA bereitgestellt.
SINA-Box S (secunet)	Die Verteilung erforderlicher Chipkarten erfolgt per Kurier durch die Kryptoverteilerstelle des BSI. (Siehe Administrationshandbuch der Abteilung IT)

Tabelle 12: Schlüsselverteilung und Schlüsselaustausch

4.3.4 Schlüsselinstallation und Schlüsselspeicherung

Produkt	Installation / Speicherung
Chiasmus für Windows (BSI)	Die Schlüssel werden als passwortgeschützte Schlüsseldateien lokal auf dem Arbeitsplatz-PC des Mitarbeiters gespeichert. (Siehe Nutzerhandbuch)
GPG4Win (BSI)	Die Schlüssel werden lokal in der Anwendung auf dem Arbeitsplatz-PC des Mitarbeiters gespeichert. Der private Schlüssel ist passwortgeschützt. (Siehe Nutzerhandbuch)
Compusec (CE-Infosys)	Der Schlüssel wird auf einem USB-Token gespeichert. (Siehe Administrationshandbuch der Abteilung IT)
OpenVPN (Open Source)	Schlüssel und Zertifikate werden durch die Abteilung IT auf den Arbeitsplatz-PCs und den VPN-Gateways gespeichert. (Siehe Administrationshandbuch der Abteilung IT)
cv act s/mail (Cryptovision)	Die Schlüssel und X.509-Zertifikate werden auf einer Chipkarte gespeichert. (Siehe Nutzerhandbuch)
Kleopatra (BSI)	Die Schlüssel und X.509-Zertifikate werden lokal im Zertifikatsspeicher der Anwendung auf dem Arbeitsplatz-PC des Mitarbeiters gespeichert. Der private Schlüssel ist passwortgeschützt. (Siehe Nutzerhandbuch)
Julia Mail-Office (ICC)	Die Schlüssel und X.509-Zertifikate werden lokal im Zertifikatsspeicher der Anwendung auf dem Arbeitsplatz-PC des Mitarbeiters gespeichert. (Siehe Administrationshandbuch der Abteilung IT)
SINA-Box S (secunet)	Der Schlüssel zur Authentisierung wird auf einer Chipkarte gespeichert. (Siehe Administrationshandbuch der Abteilung IT)

Tabelle 13: Schlüsselinstallation und Schlüsselspeicherung

4.3.5 Schlüsselarchivierung

Produkt	Art der Archivierung
Chiasmus für Windows (BSI)	Archivierung liegt in der Verantwortung des Mitarbeiters.
GPG4Win (BSI)	Archivierung liegt in der Verantwortung des Mitarbeiters.
Compusec (CE-Infosys)	USB-Token ist doppelt vorhanden. Ersatz-USB-Token wird im Safe der Abteilung IT aufbewahrt.
OpenVPN (Open Source)	Keine Archivierung vorgesehen.
cv act s/mail (Cryptovision)	Keine Archivierung vorgesehen.
Kleopatra (BSI)	Archivierung liegt in der Verantwortung des Mitarbeiters.
Julia Mail-Office (ICC)	Die Schlüssel und X.509-Zertifikate werden lokal im Zertifikatsspeicher der Anwendung auf dem Arbeitsplatz-PC des Mitarbeiters gespeichert.
SINA-Box S (secunet)	Chipkarte ist doppelt vorhanden. Ersatzchipkarte wird in der Kryptoverwaltung aufbewahrt.

Tabelle 14: Schlüsselarchivierung

4.3.6 Zugriffs- und Vertreterregelung/Secret Sharing

Zugriff- und Vertretungsregelung wird derzeit erarbeitet.

4.3.7 Schlüsselwechsel

Ein Schlüsselwechsel findet wie folgt statt:

Anwendung	Gültig-keitsdauer	Schlüssel-wechsel	Zeitliche Überschneidung der Schlüssel möglich?	Sperrung / Vernichtung des abgelaufenen Schlüssels	Umschlüsselung
Chiasmus für Windows (BSI)	max. 2 Jahre	Durch den Benutzer bei Bedarf oder nach Ablauf der Gültig-keitsdauer	Ja, jeder Schlüssel ist dabei eine eigene Datei.	Durch sicheres Löschen der entsprechenden Datei.	Liegt in der Verantwortung des Benutzers.
GPG4Win (BSI)	max. 2 Jahre	Durch den Benutzer bei Bedarf	Ja, jeder Schlüssel ist dabei eine eigene Datei.	Durch sicheres Löschen der entsprechenden Datei.	Liegt in der Verantwortung des Benutzers.
Compusec (CE-Infosys)	wie IT-System	Durch den Benutzer bei Bedarf	Nein	Durch sicheres Löschen der entsprechenden Einträge.	Nein, nicht notwendig.
OpenVPN (Open Source)	max. 2 Jahre	Durch Abteilung IT	Nein	Mitarbeiter der Abteilung IT kann das Zertifikat sperren.	Nein, nicht notwendig.
cv act s/mail (Cryptovision)	max. 3 Jahre	Durch den Benutzer bei Bedarf oder nach Ablauf der Gültig-keitsdauer	Nein	Mitarbeiter der Abteilung IT kann das Zertifikat sperren.	Liegt in der Verantwortung des Benutzers.
Kleopatra (BSI)	max. 3 Jahre	Durch den Benutzer bei Bedarf oder nach Ablauf der Gültig-keitsdauer	Nein	Mitarbeiter der Abteilung IT kann das Zertifikat sperren.	Liegt in der Verantwortung des Benutzers.
Julia Mail-Office (ICC)	max. 3 Jahre	Durch einen Mitarbeiter bei Support	Nein	Mitarbeiter der Abteilung IT kann das Zertifikat sperren.	Nein, nicht notwendig.
SINA-Box S (secunet)	Max. 2 Jahre	Durch Krypto-verwater	Nein	Kryptoverwalter kann das Zertifikat beim BSI sperren lassen.	Nein, nicht notwendig.

Tabelle 15: Schlüsselwechsel

4.3.8 Schlüsselvernichtung

Siehe Spalte 5 in Tabelle im Abschnitt 4.3.7.
Nach erfolgreicher Umschlüsselung sind die privaten Schlüssel sicher zu vernichten.

5. Organisatorische Sicherheit

5.1 Einsatzumgebungen und -bedingungen der kryptographischen Produkte

5.1.1 Absicherung der Standorte

Das Gelände ist alarmgesichert mit Polizeiaufschaltung. Während der Dienstzeiten erfolgt eine Einlasskontrolle durch Pförtner. Innerhalb des BfK-Gebäudes erfolgt die Zutrittskontrolle mittels kontaktloser Zutrittskarten. Sollten diese verlorengehen, hat sofort eine Meldung an den Objekt- und Geheimschutzbeauftragten zu erfolgen. Die Zutrittskarte wird dann sofort gesperrt und für den Mitarbeiter eine neue ausgestellt. Bei längerer Abwesenheit werden die Büroräume von den Mitarbeitern abgeschlossen.

5.1.2 Einsatz und Bedienung von kryptographischen Produkten

Produkt	Einsatz und Bedienung
Chiasmus für Windows (BSI)	Einsatz auf IT-Grundschutz abgesicherten APCs und Bedienung durch den Benutzer.
GPG4Win (BSI)	Einsatz auf IT-Grundschutz abgesicherten APCs und Bedienung durch den Benutzer.
Compusec (CE-Infosys)	Einsatz auf IT-Grundschutz abgesicherten APCs und Bedienung durch den Benutzer. Bei Nichtgebrauch wird der USB-Token sicher aufbewahrt.
OpenVPN (Open Source)	Einsatz auf IT-Grundschutz abgesicherten APCs und Router und Administration durch Mitarbeiter der Abteilung IT.
cv act s/mail (Cryptovision)	Einsatz auf IT-Grundschutz abgesicherten APCs und Bedienung durch den Benutzer. Bei Nichtgebrauch wird die Chipkarte sicher aufbewahrt.
Kleopatra (BSI)	Einsatz auf IT-Grundschutz abgesicherten APCs und Bedienung durch den Benutzer.
Julia Mail-Office (ICC)	Einsatz auf IT-Grundschutz abgesicherten Server und Administration durch Mitarbeiter der Abteilung IT.
SINA-Box S (secunet)	Einsatz auf spezieller Hardware und Administration durch Mitarbeiter der Abteilung IT. Bei Nichtgebrauch wird die Chipkarte i.d.R. sicher aufbewahrt.

Tabelle 16: Einsatz und Bedienung

5.1.3 Dokumentation

Folgende Dokumente werden vom IT-Sicherheitsbeauftragten bzw. dem Geheimschutzbeauftragten bereitgestellt:

- IT-Sicherheitskonzept
- Geheimschutzkonzept
- Rollenkonzept mit Vertretungsregelungen
- Installationshandbuch der Abteilung IT
- Administrationshandbuch der Abteilung IT
- produktspezifische Nutzerhandbücher

5.2 Sicherheitspolitik und Sicherheitsregeln

5.2.1 Festlegung der Hauptverantwortlichkeiten

Für die sichere Nutzung der Kryptokomponenten auf den APCs ist grundsätzlich der Benutzer verantwortlich. Die Abteilung IT ist für alle zentral administrierten IT-Systeme verantwortlich, das heißt, auch für die Kryptokomponenten auf den APC's der Mitarbeiter. Eine Vertreterregelung findet innerhalb der Abteilung IT statt und ist in einem Rollenkonzept detailliert geregelt.

5.2.2 Kontrolle der Sicherheitsmaßnahmen

Kontrollen des IT-Sicherheitsbeauftragten finden im Rahmen des Grundschutzes statt. Kontrollen des Geheimschutzbeauftragten finden aufgrund der Regelungen der VSA (§ 42 VSA) statt. Es ist zu prüfen, ob

- IT-Sicherheitskomponenten sicherheitsgerecht eingesetzt, gewartet und instand gesetzt werden,
- Zugriffsrechte in der erteilten Form korrekt zugewiesen und erforderlich sind,
- die Mittel zur Identifizierung/Authentisierung vorschriftsgemäß geschützt sind,
- die freigegebene Hard- und Software unverändert ist,
- anhand der protokollierten Daten Zugangs -/Zugriffsversuche abgewiesen wurden und Zugriffe auf VS-Daten offensichtlich ohne Befugnis erfolgten.

5.2.3 Informationsbeschaffung

Aktuelle Informationen zu sicheren kryptographischen Verfahren und sichere Kryptoprodukte werden vom BSI bereitgestellt. Für den Informationsfluss in das BfK sind der IT-Sicherheitsbeauftragte und der Geheimschutzbeauftragte verantwortlich.

5.2.4 Protokollierung

Produkt	Protokollierung
Chiasmus für Windows (BSI)	Keine Protokollierung
GPG4Win (BSI)	Keine Protokollierung
Compusec (CE-Infosys)	Keine Protokollierung
OpenVPN (Open Source)	Protokollierung durch das System: •Verbindungsauf- und -abbau •Aushandeln des Sitzungsschlüssels •Schlüsselwechsel
cv act s/mail (Cryptovision)	Keine Protokollierung
Kleopatra (BSI)	Keine Protokollierung
Julia Mail-Office (ICC)	Protokollierung durch das System: •Ver- und Entschlüsselung von E-Mails •Signaturerstellung und -prüfung von E-Mails •Zertifikatsprüfungen.
SINA-Box S (secunet)	Protokollierung durch das SINA Management: •Verbindungsauf- und -abbau •Aushandeln des Sitzungsschlüssels •Schlüsselwechsel Nachweisführung durch den Kryptoverwalter

Tabelle 17: Protokollierung

Eine Protokollierung des Zutritts in Räume findet nicht statt.

Die Nachweisführung der Kenntnisnahme von Verschlusssachen ab VS-V erfolgt auf der Basis der VSA.

5.3 Qualifikation und Schulung der Mitarbeitern

5.3.1 Kenntnisse und datenverarbeitungsspezifische Qualifikation der IT-Benutzer

Vor der Nutzung der Kryptosysteme (CryptoVision, Kleopatra, Chiasmus, GPG4WIN) werden die Benutzer geschult (oder erhalten zumindest eine kurze Einweisung in die Nutzung des Systems). Darüber hinaus befinden sich Dokumentationen (Nutzerhandbuch) zum Nachlesen im Intranet. Die restlichen Kryptosysteme arbeiten unsichtbar für den Benutzer. Das Bedien- und Administrationspersonal der Abteilung IT werden entsprechend geschult. Des weiteren sind Installations- und Administrationshandbücher für diese Mitarbeiter vorhanden.

5.3.2 Durchführung der personellen Maßnahmen

Die Mitarbeiter des BfK werden laufend durch Hinweise im Intranet auf Schwachstellen und Gefahren aufmerksam gemacht. Des Weiteren finden bei der Einstellung neuer Mitarbeiter sowie bei Einführung neuer Kryptoprodukte Schulungen statt. Das Schulungsskript ist im Intranet veröffentlicht.

5.3.3 Dokumentation

Die Teilnahme an Schulungen und VS-Belehrungen, sowie der Zulassungs- bzw. Ermächtigungsgrad der Mitarbeiter werden in der Personalakte bzw. in der Geheimschutzdokumentation dokumentiert.

5.4 Reaktion auf Verletzung der Sicherheitspolitik

5.4.1 Ausfall von Kryptogeräten

Für den Ausfall der SINA Boxen S und der Arbeitsplatz-PCs auf Grund technischer Defekte werden Ersatzgeräte vorgehalten. Die Ersatz-APCs sind mit einer Standardinstallation ausgestattet.

5.4.2 Vorsätzliche Handlungen

Bei Verstößen und Bloßstellungen von Kryptomitteln ist umgehend der Geheimschutzbeauftragte und der Kryptoverwalter zu informieren.

5.4.3 Evaluierung

Der IT-Sicherheitsbeauftragte und der Geheimschutzbeauftragte prüfen nach Sicherheitsvorfällen, mind. jedoch einmal jährlich, ob die im BfK eingesetzten Produkte noch den Anforderungen des BSI (z.B. BSI-TR 02102, BSI-Schrift 7164) genügen.

6. Sonstiges

6.1 Ausmusterung von Altgeräten

Die Aussonderung von Altgeräten (auch Speichermedien) ist im BfK geregelt (siehe Handlungsanweisung vom 12.08.2005).

6.2 Entsorgung von Speichermedien

Siehe Punkt 6.1

6.3 Umgang bei 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 vorher sicher gelöscht.

6.4 Anpassung an neue kryptographische Algorithmen und Schlüssellängen

Der IT-Sicherheitsbeauftragte und der Geheimschutzbeauftragte stellen sicher, dass die im BfK eingesetzten Produkte den Vorgaben und Anforderungen des BSI entsprechen.

6.5 Information für Endanwender

Siehe Punkt 5.3.1.

7. Literaturverzeichnis

[1] BMI, Nationaler Plan zum Schutz der Informationsinfrastrukturen, 2005
verfügbar unter http://www.bmi.bund.de

[2] BMI, Nationaler Plan zum Schutz der Informationsinfrastrukturen in Deutschland Umsetzungsplan Bund VS-NUR FÜR DEN DIENSTGEBRAUCH, 2005

[3] BSI, BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Version 2.0, 2008.
verfügbar unter http://www.bsi.bund.de/literat/bsi_standard

[4] BSI, IT-Grundschutzkataloge, jährlich neu.
verfügbar unter http://www.bsi.bund.de/gshb

[5] BSI, L04001 Leitfaden für die Auswahl von IT-Sicherheitssystemen für sensible Infrastrukturen, deren Schutz im nationalen Sicherheitsinteresse liegt, Version 2.0.05

[6] BSI, Leitfaden zur Erstellung von Kryptokonzepten, 2008.
verfügbar unter http://www.bsi.bund.de

[7] BSI, Arbeitshilfe zur Vertraulichkeits-/Integritätsanalyse und Kryptobedarfsanalyse

[8] BSI, Liste der zugelassenen IT-Sicherheitsprodukte und -Systeme, BSI-Schrift 7164.
auf Anfrage vom BSI erhältlich

[9] BSI, TR 02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen