Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheitsempfehlungen zur Konfiguration von Samsung Knox

Version 1.0 vom 28.11.2016

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	28.11.2016	secuvera GmbH	Erste veröffentlichte Version

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Autoren

Sebastian Fritsch (secuvera GmbH)

Kathrin Schäberle (secuvera GmbH)

Inhaltsverzeichnis

1 Beschreibung

1.1 Einführung

Mobile Endgeräte sind Teil der ständig voranschreitenden Digitalisierung des Alltags. Sie sind immer online, bieten jederzeit Zugriff auf Informationen und speichern selbst viele Daten ab. Die Kommunikation erfolgt dabei über Funkschnittstellen wie GSM/UMTS/LTE und im lokalen Bereich über WLAN und Bluetooth.

Aufgrund moderner und einfacher Bedienkonzepte sowie hoher Leistungsfähigkeit sind Smartphones und Tablets heutzutage weit verbreitet. Smartphones mit Android-Betriebssystem haben Stand 2016 einen weltweiten Marktanteil von mehr als 80 %. Die Android-Software wird von der Firma Google gepflegt und von Smartphone-Herstellern auf konkrete Endgeräte integriert. Der Hersteller mit der größten Verbreitung ist die Firma Samsung mit ihren Modellen der Galaxy-Serie.

Google hat über die verschiedenen Versionen von Android Zug um Zug Funktionen zum Endgeräte-Management durch zentrales Mobile Device Management (MDM) ergänzt. Zudem wurden Schutzfunktionen in das Betriebssystem integriert.

Die Firma Samsung bietet für auf Android basierende Galaxy-Smartphones und -Tablets die Sicherheitserweiterung Samsung Knox an. Samsung Knox bildet einen weitergehenden Satz an Schutzfunktionen und Möglichkeiten zum Endgeräte-Management. Knox-Geräte können in Organisationen (Behörden und Unternehmen der Privatwirtschaft) mit einem MDM-System betrieben werden. Insbesondere für private Nutzer (Bürger) bietet Samsung My Knox an. Allgemeine Informationen sowie Details zu Samsung Knox können in folgendem Samsung-Portal abgerufen werden:

http://www.samsungknox.com

1.2 Zielsetzung

Ziel dieses Dokuments ist es, aufzuzeigen, welche Möglichkeiten sich zur Absicherung von Android-Smartphones der Samsung-Galaxy-Serie durch die weitergehenden Knox-Funktionalitäten ergeben. Dazu werden Basis- und zusätzliche Maßnahmen aufgeführt, welche auf Knox-Geräte angewandt werden können.

Über eine einführende Planungsmaßnahme werden die Möglichkeiten von Samsung Knox dargestellt, sodass eine individuelle Strategie für die Nutzung von Samsung Knox abgeleitet werden kann.

Basierend auf technischen Maßnahmen wird sowohl für Organisationen als auch für private Nutzer anlassbezogen dargestellt, wie Samsung Knox zu konfigurieren ist. Für private Nutzer wird in Kapitel 5 beschrieben, wie das Endgerät unter Verwendung von My Knox sicher eingerichtet werden kann. Für Organisationen wird in Kapitel 4 anhand von zwei MDM-Systemen eine beispielhafte Konfiguration dargestellt.

1.3 Abgrenzung

Das Dokument enthält Basis- und zusätzliche Maßnahmen, die bei der Planung und dem Einsatz von Samsung-Knox-Geräten beachtet werden sollten. Die teilweise komplexe Integration mit weiteren Diensten wie Groupware und konkreten VPN-Systemen sowie der Rollout von Geräten wird nicht betrachtet.

Für den Einsatz in einer Organisation wird angenommen, dass ein MDM-System eingesetzt wird. Da Samsung Knox mittels My Knox auch im Standalone-Modus genutzt werden kann, beispielsweise bei Privatgeräten, wird dies ebenfalls informativ behandelt.

Allgemeine Aspekte zum sicheren Betrieb von Smartphones und Tablets unabhängig vom Betriebssystem finden sich im IT-Grundschutzkatalog in Baustein B 3.405 Smartphones, Tablets und PDAs.

2 Gefährdungen für mobile Android-Geräte

Aus der Vielzahl der Funktionen, Schnittstellen, Sensoren und Dienste auf mobilen Geräten resultieren eine Menge möglicher Schwachstellen. Im Folgenden sind die wesentlichen Gefährdungen, denen mobile und insbesondere Android-basierte Geräte sowie auch Samsung-Knox-Geräte ausgesetzt sein können, aufgeführt.

Weitere Informationen zu Gefährdungen und Gegenmaßnahmen bei Android enthalten das „Überblickspapier Android“ des BSI aus dem Bereich des IT-Grundschutz:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Android_pdf.html

Zusätzliche Hinweise enthält das Dokument „Android - Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit“ aus der Reihe der Cybersicherheits-Empfehlungen des BSI:

https://www.bsi.bund.de/ACS/DE/_/downloads/BSI-CS_109.html

2.1 Unsichere Entsperr-/Authentifizierungsmechanismen

Entsperrmechanismen für die Benutzeroberfläche des mobilen Endgerätes unterscheiden sich in Bezug auf ihre Stärken und Schwächen, die sich im Spannungsfeld zwischen Sicherheit und Komfort bewegen.

„Finger bewegen“ oder „Wischen“ ist die einfachste und zugleich unsicherste Variante, da lediglich eine intuitive Wischgeste das Gerät entsperrt.

Mehr Sicherheit bietet ein „Entsperrmuster“. Hierbei müssen auf einer 3x3-Matrix zwischen 4 und 9 Punkte durch eine zuvor vom Benutzer festgelegte Wischgeste miteinander verbunden werden. Anhand von Schmutzablagerungen auf dem Display des Geräts kann diese Wischgeste allerdings in gewissen Fällen mit relativ geringem Aufwand rekonstruiert werden.

Eine biometrische Authentisierung kann unter Verwendung des Fingerabdrucklesers erfolgen, welcher den Benutzer durch einen zuvor erfassten Fingerabdruck authentifiziert. Fingerabdruckleser sind mittlerweile in den Topmodellen der Hersteller von Android-Geräten eingebaut. Bei diesem Verfahren besteht die Möglichkeit, mit einem entsprechenden Aufwand einen Fingerabdruck zu fälschen (z. B. durch den Nachbau eines künstlichen Fingers auf Basis eines digital gesäuberten Fingerabdrucks).

Bei den klassischen Authentifizierungs- und Entsperrmechanismen durch Prüfung einer PIN oder eines Passworts hängt deren Wirksamkeit im Wesentlichen von der Qualität und Länge der verwendeten Authentisierungsinformation ab. Eine leicht zu erratende PIN (z. B. Trivial-PINs wie 0000, 1234 oder 2580) oder ein kurzes und triviales Passwort können das Sicherheitsniveau dieser Mechanismen massiv verschlechtern.

2.2 Daten

2.2.1 Bedrohungen der Schlüssel zur Datenverschlüsselung

Der Einsatz von Datenverschlüsselung bedingt die Nutzung entsprechender kryptografischer Schlüssel. Diese sind besonders stark zu schützen und dürfen das Endgerät niemals verlassen. Durch die Manipulation der Systemsoftware oder durch unberechtigten direkten Zugang zum Endgerät könnte ein Angreifer Zugriff auf diese Schlüssel erhalten.

2.2.2 Missbrauch sensitiver Daten im Sperrbildschirm

Auch auf einem gesperrten Endgerät werden teilweise Informationen auf dem Sperrbildschirm angezeigt, z. B. zugehörige Namen von verpassten Anrufen oder Betreffzeilen erhaltener E-Mails. Diese könnten für einen unberechtigten Benutzer bereits interessant sein.

2.2.3 Missbrauch gespeicherter Daten

Mobile Endgeräte speichern eine zunehmend große Menge an persönlichen Daten sowie im professionellen Einsatz schützenswerte Daten der Organisation. Die Art dieser Daten ergibt sich aus dem Anwendungseinsatz sowie den genutzten Applikationen (Apps). Über Eigenschaften des Android-Systems ist ein Zugriff auf Daten durch andere Apps in bestimmten Fällen möglich, z. B. der Zugriff auf Kontaktinformationen. Durch die Zugriffsmöglichkeiten ist z. B. ein Missbrauch wie der unentdeckte Transfer von Daten an einen Cloud-Dienst oder die Analyse von Daten für Werbezwecke möglich.

2.2.4 Mitlesen von Verbindungs-/Inhaltsdaten

Bei der Nutzung von Mobilfunknetzen, aber insbesondere bei WLAN-Verbindungen, können Verbindungs- und Inhaltsdaten mitgelesen werden. Inhaltsdaten können durch eine Kommunikationsverschlüsselung geschützt werden. Die Absicherung muss aber bereits durch den App-Anbieter umgesetzt worden sein. Verbindungsdaten, z. B. IP-Adresse und Datum der Verbindung, sind betrieblich anfallende Daten, welche weitaus schwieriger zu verschleiern sind.

2.2.5 Unzureichender Schutz abgelegter Daten in Cloud-Systemen

Die Nutzung von Cloud-Diensten bedingt generell immer eine zugehörige App, welche auf dem Endgerät installiert sein muss. Sobald eine App Daten an einen Cloud-Dienst gesendet hat, können diese nicht mehr durch das mobile Endgerät geschützt werden.

Insbesondere die Nutzung von Google-Apps setzt die Nutzung von Google-Cloud-Diensten voraus. Diese Dienste sind teilweise tief in die Plattform integriert, beispielsweise werden Push-Nachrichten über Google Cloud Messaging verschickt.

2.2.6 Datenabfluss aus der Zwischenablage

Unter Android können Daten ohne Beschränkungen in die Zwischenablage geschrieben und davon gelesen werden. Jede Anwendung kann somit auf Inhalte der Zwischenablage zugreifen. Dies wird problematisch, wenn in der Zwischenablage vertrauliche Informationen zeitweise abgelegt werden. Einzelne Apps zur Verwaltung von Passwörtern nutzen diese Möglichkeit.

Nach jeder Änderung der Zwischenablage findet eine systemweite Benachrichtigung statt. Hierdurch kann eine Schadsoftware die Inhalte der Zwischenablage mit relativ geringem Aufwand überwachen und so effektiv vertrauliche Inhalte auslesen.

2.2.7 Begrenztes Lizenz-Management

Die Nutzung von Samsung-Galaxy-Android-Geräten mit Samsung Knox und einem MDM erfordert die Aktivierung von MDM-Knox-Lizenzen, um verschiedene Funktionen von Samsung Knox nutzen zu können. Höherwertige MDM-Knox-Lizenzen haben in der Regel ein maximales Gültigkeitsdatum. Sobald dieses Datum überschritten wurde, werden die Knox-Endgerät-Lizenzen deaktiviert und Knox-Funktionen lassen sich nicht mehr nutzen. Durch E-Mails kurz vor Ende der Laufzeit weist beispielsweise Samsung allerdings auf den Ablauf der Lizenz hin.

2.2.8 Webbasierte Angriffe auf Browser

Browser als Teil der System- oder Anwendungssoftware von Android-Geräten zeigen regelmäßig Schwachstellen, welche es z. B. ermöglichen, Angriffe über den Browser auf dem mobilen Endgerät auszuführen. Ein Angreifer müsste dazu sein Opfer auf eine von ihm präparierte Webseite locken.

2.3 Endgerät

2.3.1 Fehlende Betriebssystem-Updates bei älteren Geräten oder neuen Android-Schwachstellen

Im Bereich von Android existiert eine große Fragmentierung des Endgeräte-Marktes, welche sich durch verschiedenste Hersteller und zahlreiche Gerätemodelle ergibt. Dies hat zu dem weithin bekannten Problem geführt, dass bei Schwachstellen in Android oder in Gerätetreibern trotz vorliegender Problemlösungen keine Updates für Endgeräte verfügbar werden. Selbst bei Herstellern mit guter Updatekultur wird mit zunehmendem Gerätealter immer seltener eine Aktualisierung der Geräte durchgeführt.

2.3.2 Lokale Bedrohungen des Geräts

Sofern ein Angreifer physische Kontrolle über das Gerät erhält, kann trotz eines Passwortschutzes versucht werden, lokal auf das Gerät zuzugreifen, um das Gerät zu manipulieren. Beispielsweise kann eine verfälschte Firmware aufgespielt werden, welche den Passwortschutz umgehen soll.

Ein weiterer lokaler Angriffspunkt ist ein Datenabfluss über die USB-Schnittstelle. Hierzu muss vorab keine spezielle Software installiert werden, da mit Bordmitteln des Betriebssystems auf die Daten des Android-Geräts zugegriffen werden kann. Falls dieser Zugriff in den Einstellungen des Geräts aktiviert wurde, kann trotz Bildschirmsperre auf die Daten des Android-Geräts zugegriffen werden.

2.3.3 Rooten des Endgeräts

Unter dem Rooten des Endgeräts wird verstanden, dass ein berechtigter Benutzer sich vollen Systemzugriff auf sein Gerät verschafft. Hiermit werden allerdings gleichzeitig Schutzmaßnahmen umgangen oder deaktiviert, was zu einem erhöhten Risiko im Umgang mit unbekannten Apps führen kann. Neben dem bewussten Rooten durch einen Benutzer ist auch unbemerktes Rooten durch eine nicht vertrauenswürdige App möglich, was einem Angreifer dann weitgehenden Zugriff auf das Gerät ermöglicht.

2.3.4 Nicht vertrauenswürdige Apps

Apps haben die unterschiedlichsten Funktionen und benötigen hierzu sehr verschiedene Zugriffsrechte. Um diesen Zweck zu erfüllen, müssen Apps teilweise auf die Hardware des mobilen Geräts sowie auf im System abgespeicherte Daten zugreifen. Bei unbekannten, fehlerbehafteten oder nicht vertrauenswürdigen Apps oder Malware ergeben sich hierdurch Gefährdungen für das Endgerät selbst, aber auch für die Sicherheit und den Schutz der gespeicherten Daten.

3 Härtungsmaßnahmen für Samsung Knox

Die im Folgenden dargestellten Härtungsmaßnahmen richten sich an die IT-Verantwortlichen und IT-Administratoren der Organisation, welche den operativen Einsatz von mobilen und insbesondere Knox-Endgeräten planen, umsetzen sowie betreuen.

Es ist möglich, Samsung-Galaxy-Android-Geräte mit Samsung Knox durch Konfigurationen zu härten. Die unterschiedlichen Themen der Konfiguration werden zur Sortierung in Härtungsmaßnahmen eingeteilt.

Die Maßnahmen, welche einen grundlegenden Schutz bieten und primär umgesetzt werden sollten, werden im Folgenden als Basismaßnahmen bezeichnet, diese sollten bei der sicheren Nutzung von Knox-Geräten umgesetzt werden.

Um einen zusätzlichen Schutz zu erreichen, z. B. falls der Datenverkehr vollständig über die Organisation abgewickelt werden soll oder falls z. B. keine Google-Dienste genutzt werden sollen, werden weitere Maßnahmen empfohlen. Diese werden als zusätzliche Maßnahmen bezeichnet. Durch die Erarbeitung eines organisationsspezifischen Sicherheitskonzepts kann, in der Regel, die Identifizierung und Auswahl der zusätzlichen Maßnahmen erleichtert werden.

Nachfolgend wird eine Übersicht über alle Maßnahmen gegeben:

Basismaßnahmen

- B.1 Strategie für die Knox-Nutzung,
- B.2 Konfiguration der Geräte- und Knox-Container-Sperre,
- B.3 Sichere Grundkonfiguration des Knox-Gerätes,
- B.4 Einrichten eines Knox-Containers,
- B.5 Planung von weiteren MDM-Policies,
- B.6 Verhinderung des unautorisierten Löschens des Geräteadministrators des MDM,
- B.7 Aktualisierung des Betriebssystems,
- B.8 Auswahl eines MDM-Systems für die Knox-Nutzung.

Zusätzliche Maßnahmen

- Z.1 Schutz des Netzwerkverkehrs mit einem VPN,
- Z.2 Schutz des Webdatenverkehrs mit einem HTTP-Proxy,
- Z.3 Application Whitelisting,
- Z.4 Freigabe von internen Apps,
- Z.5 Weitergehende Geräteabsicherung durch MDM-Policies,
- Z.6 Knox-Gerät ohne Google-Konto.

3.1 Basismaßnahmen

3.1.1 B.1 Strategie für die Knox-Nutzung

Samsung Knox stellt verschiedene Sicherheitsfunktionen für ausgewählte Samsung-Galaxy-Geräte zur Verfügung. Um zu prüfen, welche Geräte unterstützt werden und welche Knox-Version für diese bereitsteht, führt Samsung eine Liste, die regelmäßig aktualisiert wird:

https://www2.samsungknox.com/knoxportal/files/GalaxyDevicesSupportingKNOX.pdf

Generell kann empfohlen werden, dass möglichst alle verfügbaren optionalen Knox-Sicherheitsfunktionen aktiviert werden sollten, sofern diese anwendbar sind. Teilweise hängt dies von den zusätzlich zu erwerbenden Lizenzen ab. Details hierzu finden sich im Härtungsguide (siehe Kapitel 4).

Bei der Planung des Einsatzes von Samsung Knox müssen diverse Überlegungen angestellt werden, hierzu sollen die folgenden Hinweise eine Übersicht und Anregungen geben.

Nutzung des Knox-Containers

Der Knox-Container stellt eine abgetrennte Benutzerumgebung innerhalb des Android-Profils dar. Der Knox-Container kann entweder eingeblendet werden, ähnlich zur Gruppierungsfunktion des Android-Startbildschirms, oder es kann eine vollständige Umgebung simuliert werden, u. a. mit eigenem Hintergrundbild und einem eigenen Startbildschirm. Im letzteren Fall spricht man auch davon, „im Container“ und „außerhalb des Containers“ zu arbeiten. Beide Varianten verwenden den identischen Knox-Container, die Konfiguration kann auch zwischenzeitlich geändert werden.

Mithilfe eines Knox-Containers können verschiedene Nutzungsszenarien realisiert werden, die wichtigsten sind:

- **Work-&-Play-Konfiguration**: Dem Szenario liegt zugrunde, dass ein dienstliches mobiles Endgerät privat genutzt werden darf, wobei private und dienstliche App-Daten voneinander getrennt werden sollen. So könnten z. B. außerhalb des Knox-Containers Apps frei aus dem Play Store installiert werden, der Knox-Container selbst enthält aber nur freigegebene Apps.
- **Zwei Sicherheitszonen**: Ein ebenfalls dienstliches Gerät, welches auch vollständig gemanagt wird, erhält in diesem Szenario einen Knox-Container, um sensibel eingestufte Daten von den weniger sensibel eingestuften Daten zu trennen. In diesem Szenario werden sowohl innerhalb als auch außerhalb des Knox-Containers strikte Policies umgesetzt. Durch die Container-Grenze wird aber noch zusätzlich sichergestellt, dass eine weitere Trennung bei der Datenhaltung realisiert wird.
- **BYOD-Szenario**: In diesem Szenario stellt ein Benutzer sein privates Gerät seiner Organisation zur Verfügung. Durch den Knox-Container kann die Organisation Daten separiert ablegen. Auch ist es möglich, interne Android-Apps zu installieren (siehe Maßnahme Z.4). Falls der Benutzer die Organisation verlässt, können durch ein einfaches Löschen des Containers die Daten der Organisation wieder entfernt werden.

Für die Umsetzung dieser Nutzungsszenarien wird in der Regel ein MDM-System eingesetzt, welches in der Lage sein muss, einen Knox-Container einzurichten sowie diesen zu managen.

Alternativ kann ein Knox-Container durch Installation und Einrichtung der App My Knox erstellt werden. Hiermit wird ein nicht zentral gemanagter Knox-Container installiert, welcher ansonsten aber alle Funktionen eines Knox-Containers besitzt. My Knox bietet sich z. B. für kleine Unternehmen an, welche auf ein MDM verzichten und die Konfiguration per organisatorischer Regelung sicherstellen wollen. In diesem Fall muss das Gerät vom Administrator sicher voreingestellt werden, und der Benutzer darf diese Einstellungen nicht ändern, Letzteres muss geregelt werden.

Hauptsächlich adressiert My Knox aber den privaten Benutzer von Samsung-Galaxy-Geräten. Die Einrichtung von My Knox wird sogar mittlerweile während des Erstinstallations-Wizards des Geräts

vorgeschlagen. Ein privater Nutzer kann mittels My Knox das Modell der zwei Sicherheitszonen (siehe oben) auch für seine privaten Daten umsetzen.

Sofern nicht durch App-Installationsbeschränkungen verhindert, kann neben einem schon gemanagten Knox-Container ein zweiter durch My Knox angelegt werden.

Einsatzzweck bestimmen

Um den Umfang der Konfiguration von Samsung Knox zu planen, sollte zuerst der Einsatzzweck bestimmt werden. Folgende Fragen sollten hierbei beantwortet werden:

- Welche Daten der Organisation sollen auf dem Endgerät verfügbar sein, wie sollen diese übertragen werden?
- Haben gewisse Daten einen erhöhten Schutzbedarf? Reicht hier eine Separierung dieser Daten aus, um sie ausreichend zu schützen?
- Soll das Gerät frei nutzbar sein, z. B. beliebige Apps installierbar, oder sollen starke Restriktionen durchgeführt werden?
- Welcher Umfang an Flexibilität und Verantwortung wird dem Benutzer aus Usability-Gründen zugestanden, und kann der Benutzer hiermit umgehen?
- Welche technischen Schutzmaßnahmen können zusätzlich noch zur Absicherung eingesetzt werden?

Mit den Antworten auf diese Fragen kann ein passendes Nutzungsszenario (siehe oben) für den Knox-Container ausgewählt werden.

Knox-Lizenzen

Das Knox-Lizenzmodell ist nicht trivial. Um die richtigen Knox-Lizenzen zu erhalten und damit die benötigten Funktionen freischalten zu können, muss ein MDM-System mit den richtigen Lizenzen ausgewählt werden. Dies kann durchaus kompliziert sein und sollte im Zuge der Planung bei dem MDM-Hersteller oder einem Systemhaus abgefragt werden.

Bevor das MDM-System ausgewählt werden kann, sollte zunächst die Strategie für die Knox-Nutzung festgelegt werden. Wenn klar ist, welche Funktionen benötigt werden, sollte dann ein passendes MDM-System ausgewählt werden (siehe Maßnahme B.8).

Obiges gilt nicht für My Knox, hierzu benötigt man keine weiteren Lizenzen außer der Akzeptanz der Nutzungsbedingungen.

Google-Accounts

Die Nutzung von Google-Accounts (Google-Konto) bedingt die Annahme der Google-Lizenzbedingungen. Dies kann für einzelne Organisationen problematisch sein. An dieser Stelle soll nur auf diese Tatsache hingewiesen werden, ohne dabei eine exakte Prüfung der rechtlichen Konsequenzen durchzuführen.

Die Nicht-Nutzung eines Google-Accounts kann umgekehrt allerdings Funktionseinschränkungen mit sich bringen. Ohne aktivierten Google-Account ist beispielsweise die Nutzung des Play Stores zur Installation von Apps nicht verfügbar. Weitere Details zur Nutzung von Samsung-Galaxy-Geräten und insbesondere Samsung Knox ohne aktivierten Google-Account werden in Maßnahme Z.6 besprochen.

Knox-Nutzungsbedingungen

Für die Nutzung der Knox-Dienste, insbesondere des Knox-Containers, müssen ebenfalls die Nutzungsbedingungen durch den Lizenzvertrag (EULA) von Samsung akzeptiert werden. Vor dem Einsatz von Samsung Knox sollte daher geprüft werden, ob diese Nutzungsbedingungen für die eigene Organisation angenommen werden können. Die Lizenzverträge finden sich unter:

https://www.samsungknox.com/en/eula

3.1.2 B.2 Konfiguration der Geräte- und Knox-Container-Sperre

Um mobile Endgeräte vor unzulässigem Zugriff zu schützen, sollte eine Gerätesperre, z. B. durch ein Passwort, aktiviert werden. Samsung-Galaxy-Geräte mit Samsung Knox bieten verschiedene Möglichkeiten, diesen Geräte-Schutz umzusetzen.

Durch den Knox-Container ist es möglich, eine zweite Authentifizierungsebene neben der Gerätesperre zu konfigurieren. Beispielsweise kann das Gerät mit einem Fingerabdruck entsperrt werden, der Knox-Container kann aber erst durch Eingabe eines Passworts geöffnet werden.

Folgende Tabelle zeigt die technischen Möglichkeiten für die Geräte- und Container-Sperre und gibt gleichzeitig Hinweise, welche Methoden empfohlen werden.

Tabelle 1: Möglichkeiten und Empfehlungen zur Geräte- und Knox-Container-Sperre

Methode	Gerätesperre	Container-Sperre
kein Schutz (nur Wischen)	nicht empfohlen, mit Geräteverschlüsselung nicht möglich	nicht möglich
Muster	nicht empfohlen, mit Geräteverschlüsselung nicht möglich	nicht empfohlen
PIN	mit Einschränkungen empfohlen	mit Einschränkungen empfohlen
Passwort	empfohlen	empfohlen
Fingerabdruck	empfohlen mit Hinweis (siehe B.1), benötigt beim Start die Eingabe des Passworts	empfohlen mit Hinweis (siehe B.1)
Zwei-Faktor-Authentifizierung (Fingerabdruck und Passwort)	nicht möglich	empfohlen

Für den Geräteschutz und die Nutzung von Passwörtern sollten folgende weitere Einstellungen gesetzt werden:

- Minimale Passwortlänge: 8 Zeichen,
- Passworthistorie: 3 Passwörter,
- Passwortkomplexität:
  - mindestens eine Ziffer,
  - mindestens je ein Groß- und Kleinbuchstabe,
  - mindestens ein Sonderzeichen,
  - Nutzung von mindestens zwei der drei vorherigen Zeichenarten,
  - Verhinderung von zwei oder mehr aufeinanderfolgenden Zeichen oder Wiederholungen (z. B. 456, aaa),
- Automatische Sperrung nach spätestens: 5 Minuten,
- Passwortsperre nach Fehleingaben:
  - maximale Anzahl von Fehlversuchen, nach denen das Gerät deaktiviert wird: 10,
  - Zeitraum für Fehleingaben-Zähler, danach sind weitere Eingaben möglich: 30 Minuten,
- Passwortwechsel:
  - maximales Passwortalter: 90 Tage,
  - zulässige Zeit für Passwortwechsel: 14 Tage,

- Passworteingabe:
    - Die Möglichkeit, das Passwort bei der Eingabe anzuzeigen, sollte deaktiviert werden.

Die Vorgaben zur Nutzung der Passwörter wurden analog zu den Hinweisen der IT-Grundschutz-Kataloge in Maßnahme „M 2.11 Regelung des Passwortgebrauchs“ gewählt und bezogen auf den Fall mobiler Endgeräte ergänzt.

Für den Knox-Container sollten, je nach individuellem Szenario, Einstellungen für die Container-Sperre gesetzt werden. Wir geben nachfolgend Empfehlungen, welche gut auf das Nutzungsszenario Play & Work passen.

Nutzung des Fingerabdrucksensors

Die Nutzung von Fingerabdrucksensoren bringt neue Gefährdungen hinsichtlich des Einsatzes in Sicherheitsprodukten mit sich, gleichzeitig kann aber auch die Akzeptanz solcher Maßnahmen erhöht werden, insbesondere da es zu geringeren Fehlversuchen und schnellerer Authentifizierung führen kann. Zu diesem Ergebnis kam beispielsweise eine Studie im Jahr 2014 (Smartphone Fingerprint Authentication versus PINs: A Usability Study, Karthikeyan et al, 2014).

Für den Einsatz mit Samsung Knox ist daher zu entscheiden, inwieweit die Gefährdungen getragen werden können und welche Vorteile eine Nutzung haben kann. Samsung Knox bietet zudem die Möglichkeit, den Fingerabdruck erst für die zweite Ebene, den Knox-Container, zu nutzen.

Stärke des Knox-Container-Passworts

Der Knox-Container ist erst nutzbar, nachdem der Benutzer sich am Gerät selbst authentifiziert hat. Es ist daher denkbar, dass für den Knox-Container ein schwächeres Passwort genutzt werden kann, wenn ein angemessener automatischer Screen-Lock-Timeout gesetzt ist.

3.1.3 B.3 Sichere Grundkonfiguration des Knox-Gerätes

Ein gemanagtes Knox-Gerät sollte vor dem ersten Betrieb durch den Administrator über das MDM in einen sicheren Zustand versetzt werden, d.h. alle vom MDM-System vorgegebenen Geräterichtlinien sollten bereits aktiviert sein. Im Folgenden wird ein kurzer Überblick über eine sichere Grundkonfiguration gegeben.

Geräteverschlüsselung

Im Endgerät sollte eine vollständige Verschlüsselung aller Daten umgesetzt werden. Sofern das Gerät eine externe SD-Karte unterstützt und beinhaltet, sollte diese ebenfalls verschlüsselt werden.

Sideloading verhindern

Die Installation von Apps kann auch direkt über Installationsdateien per Download oder per USB auf Standard-Android-Geräten erfolgen, dies wird als „Sideloading“ bezeichnet. Durch die MDM-basierte Deaktivierung des Entwickler-Modus und Deaktivierung der Installation von Apps aus „unbekannten Quellen“ wird dies ausgeschlossen.

Firmware-Installation per USB verhindern

Auf Samsung-Geräten kann trotz Sicherheitsmaßnahmen durch den lokalen Firmware-Update-Modus (ODIN-Modus) andere Gerätefirmware aufgespielt werden, beispielsweise um Root-Zugriff zu erlangen. Damit dies nicht nur im Nachgang erkannt, sondern schon vorab unterbunden wird, sollte über das MDM die direkte Installation von Firmware verhindert werden. Diese Einstellung kann nur per MDM vorgenommen werden.

Sperrbildschirmdaten

Es sollte geprüft werden, ob die von der Organisation bereitgestellten Apps bereits im Sperrbildschirm schützenswerte Daten einblenden. Hiermit sind beispielsweise Kalender-, E-Mail- oder Push-Benachrichtigungen gemeint. Es wird empfohlen, diese Nachrichten zu deaktivieren oder die Detailinhalte auszublenden.

Entwickler-Modus verhindern

Für einen erweiterten Zugriff per USB-Schnittstelle auf das Endgerät wird häufig der ADB- oder Entwickler-Modus genutzt, z. B. können so zusätzliche Apps aus Installationsdateien und ohne Play Store installiert werden. Zudem kann auf die Daten des Endgeräts direkt zugegriffen werden. Über den Entwickler-Modus ergeben sich Gefährdungen für die Integrität des Geräts sowie für den Schutz der gespeicherten Daten. Daher wird die Deaktivierung des Entwickler-Modus empfohlen.

Verwendung von nicht-personalisierten Gerätenamen

Die Gerätenamen sollten keine Hinweise auf die Organisation enthalten. Zum Beispiel wird bei aktiviertem WLAN während der Suche nach Access Points der eigene Gerätename verschickt, der entsprechend anonym gehalten sein sollte.

3.1.4 B.4 Einrichten eines Knox-Containers

Die Aktivierung des Containers erfolgt per MDM; damit wird auf dem Knox-Gerät die Erstellung des Knox-Containers automatisch durchgeführt.

Bevor das Gerät ausgegeben wird, sollte die Aktivierung des Knox-Containers vom Administrator bereits durchgeführt worden sein, der Nutzer kann sein Passwort dann über einen erzwungenen Passwortwechsel individuell setzen.

Zusätzlich kann einem Benutzer erlaubt werden, einen separaten, persönlichen Knox-Container einzurichten. Hierzu muss durch den Administrator die Verwendung von My Knox zugelassen bzw. nicht unterbunden werden. Dieser My-Knox-Container und seine Restriktionen können durch den Administrator nicht gemanagt werden.

3.1.5 B.5 Planung von weiteren MDM-Policies

Auf einem per MDM verwalteten mobilen Endgerät kann die Nutzung von Schnittstellen (u. a. WLAN, Bluetooth, NFC) deaktiviert und der Umgang mit Daten auf dem Endgerät sowie die Nutzung von Funktionen über MDM-Policies konfiguriert werden.

Die exakte Planung dieser und weiterer Policies ist aufwendig und sollte in einer Organisation mit allen beteiligen Gruppen abgestimmt werden. Samsung Knox bietet hier weitgehende Möglichkeiten zur Restriktion der verschiedenen Funktionen des Geräts. Der Härtungsguide in Kapitel 4 gibt eine Übersicht sowie eine Empfehlung zu den konfigurierbaren Policies.

3.1.6 B.6 Verhinderung des unautorisierten Löschens des Geräteadministrators des MDM

Um das mobile Endgerät zentral konfigurieren zu können, muss ein MDM-Client installiert sein. Dieser registriert sich aus Sicht des Android-Betriebssystems als Geräteadministrator. Damit der Benutzer diese zentrale Steuerung und damit die Sicherheitseinstellungen nicht umgehen kann, darf es für den Benutzer nicht möglich sein, den Geräteadministrator zu deaktivieren oder den MDM-Client zu deinstallieren.

Bei der Auswahl des MDM-Systems für Samsung Knox muss darauf geachtet werden, dass die Deaktivierung des Geräteadministrators dediziert blockiert werden kann. Auf diese Funktion sollte bei der Auswahl des MDM-Systems für Samsung Knox geachtet werden.

3.1.7 B.7 Aktualisierung des Betriebssystems

Samsung verfolgt für Galaxy-Endgeräte mit Samsung Knox eine Update-Strategie, durch welche circa zwei Jahre lang Firmware-Updates für die Topmodelle des Herstellers bereitgestellt werden. Samsung hat 2016 außerdem das Enterprise-Device-Programm gestartet, welches zwei Jahre Geräteverfügbarkeit sowie monatliche Sicherheitsupdates für Firmen bereitstellen soll.

Die von Samsung bereitgestellten Betriebssystem-Updates werden als Firmware Over-The-Air (FOTA) verteilt und variieren in der Größe je nach Umfang. Ein Knox-Update wird nicht unabhängig, sondern als Teil eines Betriebssystem-Updates freigegeben.

Samsung veröffentlicht monatlich einen Security-Bulletin sowie die zugehörigen Sicherheitsupdates und lehnt sich dabei an den Security-Patchlevel von Google an. Bezüglich Samsung Knox veröffentlicht Samsung eine Liste aller Endgeräte mit der jeweils aktuellen Knox-Version.

Der Update-Vorgang selbst kann über ein MDM nur sehr rudimentär gesteuert werden. Entweder es werden Updates zugelassen oder diese werden verhindert. Um die Kontrolle über Updates zu haben, sollten diese per MDM-Policy deaktiviert werden.

Falls man mehrere Endgeräte des gleichen Typs per MDM verwaltet, dann bietet es sich an, ein Endgerät als Testgerät zu nutzen. Mit diesem lassen sich die Verfügbarkeit von Firmware-Updates und neue Firmware-Versionen prüfen. Nach einem positiven Test kann im Anschluss über eine Policy-Änderung das Update für die weiteren Endgeräte freigeschaltet werden.

Über die Konsole des MDM sollte abschließend geprüft werden, ob die Endgeräte die neuste Softwareversion erhalten haben. Danach sollte die Policy wieder zurück geändert werden.

Es wird empfohlen, für die Policies dieser Maßnahme eine separate Gruppe im MDM-System zu definieren, um diese Policies zeitweise an- und ausschalten zu können.

3.1.8 B.8 Auswahl eines MDM-Systems für die Knox-Nutzung

Der Einsatz von Samsung Knox in vollem Umfang erfordert ein MDM-System. Dieses muss entsprechend den zu nutzenden Funktionen ausgewählt werden. Die vorliegenden Vorgaben zur Härtung von Samsung Knox in Form eines Maßnahmenkatalogs sowie eines Härtungsguides geben Hinweise, welche Sicherheitskonfigurationen vorgenommen werden sollten. Auf Basis dieser Informationen sollten eine Knox-Strategie definiert sowie ein Satz an Maßnahmen ausgewählt werden.

Darauf aufbauend sollte ein Anforderungskatalog erstellt werden, der bei Auswahl und Test des MDM-Systems zugrunde gelegt wird.

Nach einer Vorauswahl sollten ein oder mehrere MDM-Systeme in Form von Teststellungen in Zusammenhang mit den relevanten Knox-Endgeräten konfiguriert werden. In diesem Schritt kann herausgearbeitet werden, welche Maßnahmen tatsächlich konfiguriert werden können und ob die erwarteten Reaktionen auf dem Endgerät erkennbar werden.

Zusammengefasst wird empfohlen, die MDM-Auswahl entsprechend der folgenden drei Schritte vorzunehmen:

1. Definition Knox-Strategie (entsprechend B.1),
2. Auswahl von Richtlinien für die Knox-Endgerätekonfiguration (unter Zuhilfenahme von B.2 bis B.7 und Z.1 bis Z.6) als Anforderungsliste für das MDM-System,
3. Teststellung eines oder mehrerer MDM-Systeme mit Tests an den Knox-Endgeräten, mit dem Ziel der Auswahl eines MDM-Systems.

3.2 Zusätzliche Maßnahmen

3.2.1 Z.1 Schutz des Netzwerkverkehrs mit einem VPN

Als Schutz gegen das Mitlesen von Daten über ein öffentliches Netzwerk, wie Mobilfunk oder ein WLAN-Hotspot, kann ein Virtual Private Network (VPN) genutzt werden. Ein VPN hat zudem noch weitere Vorteile, wie z. B. die Möglichkeit, Server nur in einem lokalen Netzwerk zu betreiben, aber diese gleichzeitig per VPN aus einem externen Netz erreichbar zu haben.

Um mit Knox-Geräten ein VPN nutzen zu können, werden von Samsung zwei Möglichkeiten angeboten: Zum einen kann der eingebaute VPN-Client genutzt werden, welcher das Standard-Protokoll IPSec für VPN nutzt, zum anderen können spezielle VPN-Clients von VPN-Herstellern installiert werden. Im letzteren Fall sollte man bei seinem VPN-Hersteller nachfragen, ob ein solcher VPN-Client angeboten wird.

Im Falle des VPN-Clients wird ein IPSec-kompatibler VPN-Server benötigt, welcher IKEv1, IKEv2 oder MOBIKE unterstützt. Da es sich um Standardprotokolle handelt, bieten viele VPN-Server die Unterstützung dieser Protokolle an.

Die Konfiguration des VPN-Clients kann über das MDM-System erfolgen, hierzu wird ein VPN-Profil angelegt und dem Endgerät zugeordnet. Genauere Details werden im Härtungsguide angegeben.

Wichtig ist, zu beachten, dass für jeden Bereich ein VPN-Tunnel aufgebaut werden muss. Dies bedeutet, wenn der gesamte Datenverkehr verschlüsselt werden soll, dann müssen sowohl ein VPN-Client außerhalb als auch ein VPN-Client innerhalb des Knox-Containers konfiguriert werden. Dies gilt auch für einen My-Knox-Container.

Um die gewünschte Konfiguration vornehmen zu können, muss diese im MDM-System einstellbar sein. Alternativ kann ein VPN-Client im gewünschten Bereich installiert und manuell konfiguriert werden.

3.2.2 Z.2 Schutz des Webdatenverkehrs mit einem HTTP-Proxy

Zum Schutz des Knox-Geräts vor Bedrohungen, welche über den Browser ausgenutzt werden, kann ein HTTP-Proxy mit Filterfunktionen einen weiteren Schutz bieten. Durch einen Proxy ist es möglich, eine Whitelisting- oder Blacklisting-Strategie umzusetzen.

Ein solcher HTTP-Proxy wird in der Regel im Unternehmen aufgebaut, sodass ebenfalls empfohlen wird, eine VPN-Verbindung zu konfigurieren (siehe Maßnahme Z.1). Der HTTP-Proxy kann mittels des MDM-Systems systemweit am Endgerät konfiguriert werden, sodass alle Zugriffe auf Webseiten über den Proxy geleitet werden.

3.2.3 Z.3 Application Whitelisting

Ein Schutz vor bösartigen Apps auf Knox-Geräten lässt sich nur durch eine restriktive Freigabe von Apps umsetzen. Als umfangreicher Schutz kann die Nutzung des gesamten Play Stores komplett unterbunden werden. Alternativ können über die eingesetzte MDM-Lösung gezielt Apps freigeschaltet werden. Verschiedene MDM-Systeme erlauben die Konfiguration eines White- und Blacklisting von Apps, was auf dem Knox-Endgerät umgesetzt wird. Hierdurch kann die generelle Nutzung des Play Stores unter Durchsetzung von Restriktionen zugelassen werden.

Es wird empfohlen, für die Beschränkung von Apps innerhalb und außerhalb des Containers eine Strategie festzulegen, diese kann restriktiv oder eher freizügig definiert werden. Beispielsweise sollte beim Einsatz eines restriktiv genutzten Knox-Containers die Installation von Apps innerhalb des Knox-Containers stark restriktiv gehandhabt werden.

3.2.4 Z.4 Freigabe von internen Apps

Um speziell für die Organisation entwickelte interne Apps auf die verwalteten Knox-Geräte zu installieren, kann in der Regel das MDM-System genutzt werden. Hierzu muss die APK-Datei in das MDM geladen und für die Installation ausgewählt werden.

Je nach Möglichkeit des MDM-Systems kann die Installation von internen Apps für den Knox-Container durchgeführt werden. Sofern dies erfolgt, findet eine Datenhaltung innerhalb des Knox-Containers statt, mit allen Vorteilen, die unter B.1 bereits genannt wurden.

Sofern die Installation von internen Apps innerhalb des Knox-Containers für die Organisation eine wichtige Funktionalität ist, sollte dies als Auswahlkriterium für das MDM-System herangezogen und im Detail getestet werden.

3.2.5 Z.5 Weitergehende Geräteabsicherung durch MDM-Policies

Im Rahmen einer Basisabsicherung des Knox-Geräts können die Funkschnittstellen (u. a. Bluetooth, WLAN, NFC) vollständig deaktiviert werden. Knox-Geräte ermöglichen allerdings auch eine feinere Konfiguration dieser Schnittstellen.

Die Nutzung von Bluetooth lässt sich auf einzelne Bluetooth-Profile beschränken. In diesem Fall ist es beispielsweise möglich, Bluetooth-Verbindungen mit einem Auto zur Nutzung der Freisprechfunktion zuzulassen und gleichzeitig die Übertragung von Kontaktdaten zu verhindern.

Insbesondere wenn für das mobile Gerät spezielle Bedrohungen bestehen, auf die mit einer ausgefeilten Sicherheitskonfiguration reagiert werden soll, können spezielle, aber auch aufwendigere Sicherheits-Policies definiert und erzwungen werden.

Es wird empfohlen, die Funkschnittstellen entsprechend der Sicherheitsbedürfnisse der Einsatzumgebung zu beschränken.

3.2.6 Z.6 Knox-Gerät ohne Google-Konto

Die Nutzung von Samsung-Galaxy-Geräten, welche auf Android aufbauen und Samsung Knox beinhalten, wird in der Regel mit einem Google-Konto gekoppelt. Aufgrund von Datenschutzbedenken sowie im Bereich von erhöhten Sicherheitsanforderungen kann eine Koppelung mit diesen Diensten nicht wünschenswert sein. Im Folgenden wird dargestellt, welche Funktionen durch eine fehlende Koppelung nicht mehr verfügbar sind. Danach wird skizziert, wie ein Knox-Gerät vollständig in Betrieb genommen werden kann, ohne ein Google-Konto bei der Installation angeben zu müssen.

Nach der standardmäßigen Installation des Knox-Geräts ist es möglich, Google-Konten wieder zu entfernen. Danach sind die folgenden Funktionen nicht mehr vorhanden:

- Neue Apps können nicht mehr aus dem Google Play Store installiert werden.
- Die MDM-App kann möglicherweise nicht mehr sofort die im MDM-System initiierten Aktionen auf dem Endgerät ausführen, wie z. B. Gerät sperren.
- Apps können keine Google-Dienste mehr nutzen, z. B. für Push-Nachrichten.

Installation ohne Google-Konto

Die Installation eines Knox-Geräts ohne Angabe eines Google-Kontos birgt die Schwierigkeit, dass der Play Store zur Installation der MDM-Client-App nicht genutzt werden kann.

Die MDM-App kann per ADB (Android Debug Bridge) auf das Gerät installiert werden. Hierzu muss während der Erstkonfiguration durch den Administrator ADB aktiviert werden. Sobald die Installation und die Anmeldung am MDM-Server erfolgt sind, werden die Vorgaben des MDM-Servers übernommen, hierbei wird die ADB-Schnittstelle deaktiviert (siehe Maßnahme B.3).

Installation und Einrichtung mit minimalen Google-Diensten

Aktiviert man ein Google-Konto auf dem Gerät, z. B. ein anonymes Konto für die einfache Nutzung auf dem mobilen Endgerät, ist es möglich, den Play Store zu nutzen und somit die MDM-Client-App zu installieren.

Nach der Installation der MDM-App sollten die folgenden Konfigurationen vorgenommen werden, um eine minimale Kommunikation zu den Google-Servern herzustellen:

- Einrichtung eines Google-Accounts ohne weitere Nutzung, erste Datenschutzeinstellungen sind unter https://myaccount.google.com/privacycheckup/ möglich.
- Die Synchronisation der Daten des Google-Accounts kann unter *Einstellungen → Konten → Google* nach Auswahl des Kontos für alle Dienste deaktiviert werden. Hierzu muss jeder Dienst separat deaktiviert werden.

4 Härtungsguide

Nachfolgend werden beispielhaft zwei MDM-Systeme konkret betrachtet, um Konfigurationseinstellungen möglichst exakt zu beschreiben.

CellWe EMM Cloud wurde ausgewählt, da auf diesem Weg schnell und ohne eigene Server-Installation Knox-Geräte mit einem MDM-System gemanagt werden können. Zudem wird CellWe EMM Cloud von Samsung bereitgestellt; ein Account kann über samsungknox.com angelegt werden. Ergänzend sei für den Wirkbetrieb darauf hingewiesen, dass der Einsatz einer Cloud-basierten MDM-Lösung nicht empfohlen wird.

BES12 On-Premise wurde ausgewählt, da Blackberry mit BES12 eine ausgereifte MDM-Lösung anbietet, welche bereits seit Jahren mehrere Betriebssystemplattformen unterstützt. Zudem hat Blackberry jahrelange Erfahrung in der Entwicklung von Sicherheitslösungen.

Mit der Auswahl der beiden MDM-Systeme geht keinerlei Empfehlung für eines dieser Systeme einher. Sie wurden ausgewählt, um möglichst konkrete Punkte im Bereich der Planung und Konfiguration beispielhaft adressieren zu können.

Vor Auswahl, Konfiguration und Inbetriebnahme sollte ein Konzept auf Basis der Härtungsmaßnahmen erstellt werden. Dieses Konzept kann danach anhand der folgenden Konfigurationsvorlagen umgesetzt werden.

Die Maßnahmen B.1 und B.8 sind dabei Planungsmaßnahmen und werden im Folgenden nicht weiter betrachtet. Für alle anderen Maßnahmen werden möglichst praktische Empfehlungen auf Basis der MDM-Systeme gegeben. Falls eine Konfigurationsoption nur durch die Organisation entschieden werden kann, dann ist dies in diesem Kapitel als „individuelle Entscheidung“ bezeichnet.

Die Konfigurationsoptionen sind insbesondere für den Knox-Container stark restriktiv gewählt. In konkreten Anwendungsfällen kann es notwendig sein, einzelne Einstellungen abweichend vorzunehmen, falls ansonsten ein Einsatz nicht möglich ist. Beispielsweise kann es im Einzelfall sinnvoll sein, eine Kamera-App für das Aufnehmen von dienstlichen Fotos im Knox-Container, entgegen der Empfehlung in dieser Vorlage, freizugeben, um die Fotos im separierten Bereich des Knox-Containers zusätzlich zu schützen.

4.1 Konfiguration des MDM für CellWe EMM Cloud

4.1.1 Konzeption

CellWe EMM Cloud unterscheidet zwischen Administratoren und Benutzern. Administratoren verwalten das System, legen Policies fest und richten Benutzer ein. Nachfolgend werden nur die Aufgaben der Administration beschrieben.

Vor der Konfiguration sollte ein Policy-Konzept erstellt werden. Eine Möglichkeit zur dauerhaft einfachen Verwaltung ist die thematische Gruppierung von Policies, sodass je nach Anforderungen für einzelne Nutzer auch Policies deaktiviert werden können.

4.1.2 Vorlage zur Konfiguration

Um die Konfiguration in CellWe EMM Cloud vorzunehmen, wird empfohlen, die englische Sprachversion zu nutzen, da die deutsche Übersetzung, insbesondere die Hilfe, teilweise missverständlich formuliert ist. Hierzu muss die Sprache des Browsers auf Englisch konfiguriert werden.

Hinweise zur Tabelle: Kursive Einträge geben Hinweise auf die Menüstruktur, in der die Einstellung zu finden ist. Generell wird allerdings empfohlen, mit der Suchfunktion (im linken Menü der CellWe-EMM-Cloud-Oberfläche) nach den Optionen zu suchen. Die folgenden Angaben beziehen sich auf die zum Zeitpunkt der Erstellung des Dokuments aktuelle Version von CellWe EMM Cloud (mittlerweile umbenannt in Samsung SDS IAM & EMM Cloud).

Tabelle 2: Vorlage zur Konfiguration von CellWe EMM Cloud

Maßnahme	Option	Empfohlene Einstellung	Minimale Lizenz
B.2 Geräte-/ Container-Schutz	Samsung KNOX Device Settings		
	Enable password visibility	No	Express
	Enable lock screen fingerprint authentication	Entscheidung entsprechend B.1	Express
	Maximum failed password attempt for disabled device	10	Express
	Timeout for password change enforcement	20160 14 Tage x 24 Stunden x 60 Minuten = 20160 Minuten	Express
	Samsung KNOX Workspace Settings (KNOX-Container)		
	Enable password visibility	No	Express
	Maximum number of failed attempts	10	Express
	Maximum passcode age (days)	180	Express
	Passcode history	3	Express
	Maximum password lock delay (seconds)	1800 30 Minuten x 60 Sekunden = 1800 Sekunden	Express
	Minimum number of complex characters	2	Express
	Enable fingerprint authentication	Entscheidung entsprechend B.2	Express

Maßnahme	Option	Empfohlene Einstellung	Minimale Lizenz
	Minimum passcode quality	1	Express
	Minimum password length	8	Express
	Require two-factor authentication	Entscheidung entsprechend B.2, sperrt alle anderen Varianten zur Authentifizierung	Express
B.3 Sichere Grundkonfiguration	Encrypt internal onboard storage	Yes, aber durch „Enable Common Criteria mode“ bereits mit aktiviert.	Express
	Enable ODE Trusted Boot verification	Yes	Premium
	Enable Common Criteria mode	Yes	Premium
	Enable TIMA Key Store	Yes	Express
	Require attestation verification	Yes	Premium
	Permit USB debugging	No	Express
	Permit installation of non-Google-Play apps	No	Express
	Permit firmware recovery	No	Express
B.4 Knox-Container	Enable KNOX Container	Yes	Express
	Samsung KNOX Workspace Settings (Knox-Container)		
	Allow applications to be moved into container	No	Workspace
	Allow Google apps in the container	No	Workspace
	Applications that can access SD Card	individuelle Entscheidung	Workspace
	Force secure keypad	Yes	Workspace
	Permit Bluetooth	No	Workspace
	Permit camera use	No	Workspace
	Permit display of share via list	No	Workspace
	Permit moving files into the container	individuelle Entscheidung	Workspace
	Permit moving files out of the container	No	Workspace
	Permit NFC	No	Workspace
	Permit screen capture	No	Workspace
	Permit user from changing app data sync setting	No	Workspace
	Permit user to delete the KNOX container	No	Workspace
	Configure applications that can sync with container	Yes	Workspace
	Preview KNOX notifications	No	Workspace
	Export to personal mode: Contacts	No	Workspace
	Export to personal mode: S Planner (Calendar)	No	Workspace
	Import to KNOX mode:	individuelle Entscheidung	Workspace

Maßnahme	Option	Empfohlene Einstellung	Minimale Lizenz
	Contacts		
	Import to KNOX mode: S Planner (Calendar)	individuelle Entscheidung	Workspace
B.5 Weitere MDM-Policies	Samsung KNOX Device Settings Hinweis: Diese Einstellungen betreffen den Bereich außerhalb des Knox-Containers.		
	Permit Bluetooth access	individuelle Entscheidung	Express
	Permit NFC use	individuelle Entscheidung	Express
	Permit audio recording	individuelle Entscheidung	Express
	Permit microphone use	individuelle Entscheidung	Express
	Permit video recording	individuelle Entscheidung	Express
	Permit Tethering	individuelle Entscheidung	Express
	Permit Wi-Fi use	individuelle Entscheidung	Express
	Permit device as a media player via USB	No	Express
	Permit SD card access	No	Express
	Permit Google backup	No	Express
	Permit S Beam use	No	Express
	Permit S Voice application use	No	Express
	Permit sending crash report to Google	No	Express
	Permit USB host storage	No	Express
	Permit multiple users	No	Express
	Permit mock GPS locations	No	Express
B.6 Verhinderung des Löschens	Permit user to unenroll devices	No	Express
B.7 Aktualisierung des Betriebssystems	Permit upgrading the operating system (OS) over-the-air (OTA)	No (siehe Kapitel 3.1.7 zur Update-Strategie)	Express
Z.1 VPN	Hinweis: Durch die verschiedenen Knox-Lizenzen können unterschiedliche VPN-Konfigurationen vorgenommen werden. Ein VPN innerhalb des Knox-Containers kann nur mit einer Knox-Workspace-Lizenz konfiguriert werden.		
	VPN mit eingeschränkten Funktionen, u. a. nur IKEv1, nur Pre-Shared-Key (beschränkte Optionen, wenn nur über MDM konfiguriert) *Samsung KNOX Device Settings → VPN Settings*		
	VPN profiles	Notwendige Konfigurationsoptionen: - Server (IP/DNS-Name), - VPN-Typ: IPSec PSK oder RSA, - Authentifizierungsdaten.	Express
	Erweitertes VPN *Samsung KNOX Workspace Settings → VPN Settings*		
	VPN profiles	Notwendige Konfigurationsoptionen: - Server (IP/DNS-Name),	Workspace

Maßnahme	Option	Empfohlene Einstellung	Minimale Lizenz
		- VPN-Typ: IPSec, - (Auswahl) VPN for all applications, - Authentifizierungsdaten, - Verschlüsselungsdaten sowie weitere Hersteller-spezifische Konfigurationsoptionen	
Z.2 Proxy	Proxy rules		Express
	(danach) IP Address	Proxy-Server-IP-Adresse	Express
	(danach) Port	Proxy-Server-Port	Express
Z.3 Application Whitelisting	Samsung KNOX Device Settings		
	Permission restrictions to block third-party apps	individuelle Entscheidung	Premium
	Allow applications to be moved into container	individuelle Entscheidung	Premium
	Applications that can be installed	individuelle Entscheidung	Premium
	Applications that the user cannot uninstall	individuelle Entscheidung	Premium
	Applications that user can/cannot clear from cache	individuelle Entscheidung	Premium
	Applications to be added to the home screen	individuelle Entscheidung	Premium
	Applications to be disabled	individuelle Entscheidung	Premium
	Samsung KNOX Workspace Settings		
	Allow applications to be moved into container	individuelle Entscheidung	Workspace
	Applications that can be installed	individuelle Entscheidung	Workspace
	Applications that the user cannot uninstall	individuelle Entscheidung	Workspace
	Applications that the user can/cannot clear from cache	individuelle Entscheidung	Workspace
	Applications to be added to the home screen	individuelle Entscheidung	Workspace
	Applications to be disabled	individuelle Entscheidung	Workspace
Z.4 Freigabe von internen Apps	Die Freigabe von internen Apps (APK-Dateien) erfolgt nicht über Policies, sondern über den Menüpunkt „Apps“ in der CellWe-EMM-Cloud-Administrationsoberfläche.		
Z.5 Weitergehende Geräteabsicherung	Bluetooth Settings		
	Devices that user can/cannot connect	individuelle Entscheidung	Express
	Enable Bluetooth discoverable mode	individuelle Entscheidung	Express
	Enable limited discoverable mode	individuelle Entscheidung	Express

Maßnahme	Option	Empfohlene Einstellung	Minimale Lizenz
	Features that user can/cannot use	individuelle Entscheidung	Express
	Permit data transfer via Bluetooth	individuelle Entscheidung	Express
	Permit desktop or laptop connection via Bluetooth	individuelle Entscheidung	Express
	Permit outgoing calls via Bluetooth headset	individuelle Entscheidung	Express
	Wi-Fi Restrictions		
	Permit user to add Wi-Fi networks	individuelle Entscheidung	Express
	Permit user to start an open (non-secured) Wi-Fi hotspot	individuelle Entscheidung	Express
Z.6 Knox-Gerät ohne Google-Konto	Hinweis: Dies wurde bereits im Maßnahmentext beschrieben und wird nicht über das MDM konfiguriert.		

Hinweise zu „Knox Premium“-Lizenz und Knox-Container

Bei CellWe EMM Cloud mit der „Knox Premium“-Lizenz und aktivem Knox-Container werden folgende Einstellungen bezüglich des Knox-Containers gesetzt:

- „Kontakte und Kalender freigeben“ deaktiviert,
- Verschieben von Dateien in den Knox-Container ist möglich, ein Verschieben aus dem Knox-Container heraus ist nicht möglich,
- „Anwendungen installieren“ deaktiviert.

4.1.3 Betrieb

Im laufenden Betrieb von CellWe EMM Cloud können nachstehende zentralen Administrationsaufgaben wie folgt ausgeführt werden.

Tabelle 3: Administrationsaufgaben in CellWe EMM Cloud

Aktion	Auswahl in Menü	Reaktionen
Löschen des gesamten Geräts	*Devices → Auswahl des Gerätes → Details → Wipe Device*	Startet das Gerät sofort neu und führt einen Factory Reset durch.
Passwortwechsel der Gerätesperre	*Devices → Gerät anwählen (Haken anklicken) → Actions (Drop-Down-Menü) → Force Password Change*	Sperrt das Gerät, fordert dann zur Eingabe des Passworts auf, danach muss ein neues Passwort gesetzt werden.
Sperren der CellWe-EMM-App-Oberfläche	*Devices → Gerät anwählen (Haken anklicken) → Actions (Drop-Down-Menü) → Administrative Lock*	Die CellWe-App zeigt nur noch die Möglichkeit, das Menü für Einstellungen zu öffnen, Details zur Richtlinie werden nicht mehr angezeigt. Über „Administrative Unlock“ kann die Oberfläche wieder freigegeben werden.
Löschen des Containers	*Devices → Gerät anwählen (Haken anklicken) → Actions (Drop-Down-Menü) → Remove Container*	In der Notification Bar wird angezeigt, dass ein Profil „Container entfernen“ geladen wird, danach wird der Container gelöscht. In der CellWe-App wird der Benutzer dann aufgefordert, einen neuen Knox-Container anzulegen, hierzu muss der Dialog zur Auswahl des Sperrtyps durchlaufen werden, siehe auch B.2.
Sperren und Entsperren des Knox-Containers	*Devices → Gerät anwählen (Haken anklicken) → Actions (Drop-Down-Menü) → Lock Container/Unlock Container*	Es wird eine neue Sicherheitsrichtlinie angewandt. Der Container muss zunächst gesperrt werden (durch manuelles Sperren oder durch einen Timeout), danach greift die neue Richtlinie. Statt der Möglichkeit zur Authentifizierung wird gemeldet, dass der Knox-Container gesperrt ist. Nach einem „Unlock Container“ ist eine Anmeldung am Knox-Container wieder möglich.
Passwortwechsel Knox-Container	*Devices → Gerät anwählen (Haken anklicken) → Actions (Drop-Down-Menü) → Reset Container Password*	Zeigt in der Notification Bar an, dass ein Profil zu „Container-Kennwort zurücksetzen“ empfangen wurde. Vor der weiteren Nutzung muss bei einem zuvor bereits geöffneten Knox-Container zuerst ein neues Kennwort angegeben werden.
Prüfen des Versionsstandes	*Devices → Auswahl des Gerätes → Details → Operating System*	

Zeit ohne Verbindung zum MDM-Server	*Devices → Auswahl des Gerätes → Details → Device Activity*	

4.2 Konfiguration des MDM für Blackberry Enterprise Server (BES12)

4.2.1 Konzeption

Über die Administrationskonsole von BES12 werden Benutzer angelegt. Benutzer mit Administratorrechten können die Konsole bedienen, hier werden IT-Richtlinien festgelegt und Benutzer eingerichtet. Nachfolgend werden nur die Aufgaben der Administration beschrieben.

Vor der Konfiguration sollte ein Policy-Konzept erstellt werden. Eine Möglichkeit zur dauerhaft einfachen Verwaltung ist die thematische Gruppierung von Policies, sodass je nach Anforderungen für einzelne Nutzer auch Policies deaktiviert werden können.

Bei der initialen Anmeldung der BES12-App werden im Anschluss die Policies umgesetzt. Falls ein sehr umfangreicher Satz an Policies definiert wurde, ist es möglich, dass die Aktivierung fehlschlägt, da einige Policies nicht automatisch umgesetzt werden können. Daher wird für die Aktivierung folgendes Vorgehen vorgeschlagen:

1. Anmeldung an BES12 mit Standard-Policy (IT-Richtlinie),
2. Aktivierung eines ersten Satzes an Policies, hier sollte die CC-Mode-Policy enthalten sein,
3. Aktivierung der vollständigen Policies.

4.2.2 Vorlage zur Konfiguration

Die folgende Konfigurationsvorlage zeigt die gesamte Einstellung der BES12-Konfigurationen für IT-Richtlinien an. Da die vollständige IT-Richtlinie in BES12 über eine lange Konfigurationsseite angezeigt wird, werden hier auch zur besseren Orientierung alle Konfigurationsoptionen angegeben.

In der Spalte „Empfohlene Einstellungen“ werden nur die Einstellungen aus den Basismaßnahmen und zusätzlichen Maßnahmen adressiert. Konfigurationseinträge mit dem Hinweis N/A werden innerhalb dieses Härtungsguides nicht betrachtet. Die folgenden Angaben beziehen sich auf BES12 in Version 12.5.0.

Tabelle 4: Vorlage zur Konfiguration der BES12-„IT-Richtlinie“

Kategorie 1	**Kategorie 2**	**Policy**	**Sub-Policy**	**Standard-einstellung**	**Empfohlene Einstellung** mit Referenz auf Maßnahme
Native OS	*Hinweis: Diese Optionen betreffen Kontrollfunktionen von anderen Android-Smartphones.*				
KNOX MDM					
		Password requirements		„Numeric“	Komplex (B.2)
			Minimum password length	4	8 (B.2)
			Minimum lowercase letters required in password	-	1 (B.2)
			Minimum uppercase letters required in password	-	1 (B.2)
			Minimum complex	-	1 (B.2)

Kategorie 1	Kategorie 2	Policy	Sub-Policy	Standard-einstellung	Empfohlene Einstellung mit Referenz auf Maßnahme
			characters required in password		
			Maximum character sequence length	-	2 (B.2)
			Maximum numeric sequence length	„“	2 (B.2)
			Maximum inactivity time lock	„“	5 Minuten (B.2)
			Maximum failed password attempts	0	10 (B.2)
			Password history restriction	„“	3 (B.2)
			Password expiration timeout	0	90 Tage (B.2)
		Allow password visibility		Yes	No (B.3)
		Allow fingerprint authentication		Yes	individuelle Entscheidung (B.2)
	Device functionality				
		Allow mobile data usage while roaming		Yes	N/A
		Allow WAP push while roaming		Yes	N/A
		Allow automatic sync while roaming		Yes	N/A
		Allow voice calls while roaming		Yes	N/A
		Allow users to modify location provide settings		Yes	individuelle Entscheidung (B.5)
		Allow SD card		Yes	individuelle Entscheidung (B.5)
		Allow camera		Yes	individuelle Entscheidung (B.5)
		Allow data on mobile network		Yes	N/A
		Allow Wi-Fi		Yes	individuelle Entscheidung (B.5)
		Allow users to modify Wi-Fi profile		Yes	individuelle Entscheidung

Kategorie 1	Kategorie 2	Policy	Sub-Policy	Standard-einstellung	Empfohlene Einstellung mit Referenz auf Maßnahme
		settings			(B.5)
		Allow Bluetooth		Yes	individuelle Entscheidung (B.5)
			Allow Bluetooth A2DP	Yes	individuelle Entscheidung (Z.5)
			Allow Bluetooth AVRCP	Yes	individuelle Entscheidung (Z.5)
			Allow Bluetooth HFP	Yes	individuelle Entscheidung (Z.5)
			Allow Bluetooth HSP	Yes	individuelle Entscheidung (Z.5)
			Allow Bluetooth PBAP	Yes	individuelle Entscheidung (Z.5)
			Allow Bluetooth SPP	Yes	individuelle Entscheidung (Z.5)
			Allow NFC	Yes	individuelle Entscheidung (Z.5)
		Allow microphone		Yes	individuelle Entscheidung (B.5)
		Allow audio recording		Yes	individuelle Entscheidung (B.5)
		Allow video recording		Yes	individuelle Entscheidung (B.5)
		Allow Media Transfer Protocol (MTP)		Yes	No (B.3)
		Allow USB host storage		Yes	No (B.3)
		Allow users to modify the Settings app		Yes	individuelle Entscheidung (B.3), siehe Hinweis für App-Aktivierung
		Allow date and time		Yes	individuelle

Kategorie 1	Kategorie 2	Policy	Sub-Policy	Standard-einstellung	Empfohlene Einstellung mit Referenz auf Maßnahme
		changes			Entscheidung (B.3)
			Force automatic time sync	Yes	individuelle Entscheidung (B.3)
		Allow OTA updates		Yes	No (B.7) (siehe Kapitel 3.1.7 zur Update-Strategie)
		Allow VPN		Yes	Yes (Z.1)
		Allow Wi-Fi Direct		Yes	No (B.5)
		Allow multiple user accounts		No	No (B.5)
		Allow adding email accounts		Yes	N/A
		Allow Google auto-sync		Yes	N/A
		Allow sending crash reports to Google		Yes	No (B.5)
	Apps				
		Allow Google Play		Yes	individuelle Entscheidung (B.5)
		Allow Android Backup Service		Yes	No (B.5)
		Allow S Voice		Yes	No (B.5)
		Allow browser cookies		Yes	N/A
		Allow autofill setting		Yes	N/A
		Enable JavaScript		Yes	N/A
		Enable pop-up browser setting		Yes	N/A
		Allow installation of non-Google-Play apps		Yes	No (B.5)
		Allow incoming MMS		Yes	N/A
		Allow incoming SMS		Yes	N/A
		Allow outgoing MMS		Yes	N/A
		Allow outgoing SMS		Yes	N/A

Kategorie 1	**Kategorie 2**	**Policy**	**Sub-Policy**	**Standard-einstellung**	**Empfohlene Einstellung** mit Referenz auf Maßnahme
		Allow phone		Yes	N/A
	Security and privacy				
		Require fast encryption		No	No (B.3)
		Require internal storage encryption		No	Yes (B.3)
		Require SD card encryption		No	Yes (B.3)
		Allow screen capture		Yes	individuelle Entscheidung
		Allow developer mode		Yes	No (B.3)
			Enable USB debugging	No	No (B.3)
			Allow users to modify the mock location	Yes	No (B.3)
		Allow firmware recovery		Yes	No (B.8)
		Allow factory reset		Yes	No (B.6)
	Tethering				
		Allow tethering		Yes	individuelle Entscheidung
			Allow Bluetooth tethering	Yes	individuelle Entscheidung
			Allow USB tethering	Yes	No (B.5)
			Allow Wi-Fi tethering	Yes	individuelle Entscheidung
KNOX Premium - Device					
	Security and privacy				
		Allow other device administration apps		Yes	No (B.6)
		Require certificate revocation (CRL) check for apps		No	Hinweis: Laut BES12-Hilfe Teil des CC-Mode.
			Require OCSP check for apps	-	Hinweis: Laut BES12-Hilfe Teil des CC-Mode.
		Enable NIAP		No	Yes (B.3)

Kategorie 1	**Kategorie 2**	**Policy**	**Sub-Policy**	**Standard-einstellung**	**Empfohlene Einstellung** mit Referenz auf Maßnahme
		Common Criteria functionality			
KNOX Premium - Workspace	-				
		Password requirements		„Numeric“	„Komplex“ (B.2)
			Minimum lowercase letters required in password		1 (B.2)
			Minimum uppercase letters required in password		1 (B.2)
			Minimum complex characters required in password		3 (B.2)
			Maximum character sequence length		2 (B.2)
			Minimum password length	4	8 (B.2)
			Maximum inactivity time lock	„“	5 Minuten (B.2)
			Maximum failed password attempts	10	10 (B.2)
			Password history restriction	„“	3 (B.2)
			Password expiration timeout	0	14 Tage (B.2)
			Minimum number of changed characters for new password	0	N/A
		Allow keyguard customizations		Yes	No (B.3)
			Allow keyguard trust agents	No	No (B.3) Hinweis: Verhindert Smart Unlock
		Allow password visibility		Yes	No (B.2)
		Enforce two-factor authentication		No	Entscheidung entsprechend B.2, sperrt alle anderen

Kategorie 1	**Kategorie 2**	**Policy**	**Sub-Policy**	**Standard-einstellung**	**Empfohlene Einstellung** mit Referenz auf Maßnahme
					Varianten zur Authentifizierung
		Allow fingerprint authentication		Yes	Entscheidung entsprechend B.2
	Device functionality				
		Allow camera		Yes	No (B.4)
		Allow Bluetooth		Yes	No (B.4)
		Allow NFC		Yes	No (B.4)
		Allow microphone		Yes	No (B.4)
		Allow audio recording		Yes	No (B.4)
		Allow video recording		Yes	No (B.4)
		Allow users to modify the Settings app in the KNOX Workspace		Yes	individuelle Entscheidung
		Allow adding email accounts		No	No (B.4)
		Allow Google auto-sync		Yes	No (B.4)
		Allow sending crash reports to Google		Yes	No (B.4)
	Apps				
		Allow Google services		Yes	No (B.4)
		Allow browser cookies		Yes	N/A
		Allow autofill setting		Yes	N/A
		Enable JavaScript		Yes	N/A
		Enable pop-up browser setting		Yes	N/A
	Security and privacy				
		Allow screen capture in KNOX Workspace		Yes	No (B.4)
		Allow work files into the personal space		No	No (B.4)

Kategorie 1	**Kategorie 2**	**Policy**	**Sub-Policy**	**Standard-einstellung**	**Empfohlene Einstellung** mit Referenz auf Maßnahme
		Allow „Share via“ list		Yes	No (B.4)
		Allow non-secure keypad		No	No (B.4)
		Allow personal files in the KNOX Workspace		No	individuelle Entscheidung
		Enable work and personal data synchronization		No	individuelle Entscheidung
			Allow contact synchronization	-	individuelle Entscheidung
			Import personal contacts	-	individuelle Entscheidung
			Allow export of work contacts	-	No (B.4)
			Allow calendar synchronization	-	individuelle Entscheidung
			Import personal calendar data	-	individuelle Entscheidung
			Export work calendar data	-	No (B.4)
			Allow notification synchronization	-	individuelle Entscheidung
		Allow user modifications of „Show detailed notifications“ setting		No	individuelle Entscheidung
		Enable Trusted Boot verification		No	Yes (B.3)
		Require certificate revocation (CRL) check for apps		No	Hinweis: Laut BES12-Hilfe Teil des CC-Mode.
			Require OCSP check for apps	-	Hinweis: Laut BES12-Hilfe Teil des CC-Mode.
Secure Workspace					
	Hinweis: Diese Optionen betreffen eine andere Funktion von BES12 und nicht Samsung Knox.				

Konfiguration „Aktivierung“

Als zulässige „Aktivierung“ sollte BES12 in folgender Reihenfolge konfiguriert werden; durch diese Einstellung werden die Knox-Workspace-Einstellungen auf dem Endgerät aktiviert:

- Work and personal – full control (Samsung KNOX),
- MDM controls.

Die folgenden drei Arten von Aktivierungen werden bezüglich Samsung Knox unterstützt:

- Work and personal – full control (Samsung KNOX),
- Workspace only (Samsung KNOX),
- Work and personal – user privacy (Samsung KNOX).

Knox-Workspace-Nachweisführung (Attestation)

Um eine regelmäßige Attestation von verwalteten Knox-Endgeräten durchzuführen, muss hierzu in BES12 die Option unter:

> *Einstellungen → Allgemeine Einstellungen → Nachweis → „Regelmäßige Nachweisabfragen für KNOX-Workspace-Geräte aktivieren“*

eingeschaltet werden. Die Standard-Zeitintervalle sind eine Abfragehäufigkeit von je 1 Tag sowie eine Übergangsfrist bei Nichterreichbarkeit von 3 Tagen, bis das Gerät als nicht mehr positiv attestiert gilt.

Maßnahme Z.1 Schutz des Netzwerkverkehrs mit einem VPN

BES12 erlaubt die Konfiguration von VPN-Verbindungen über VPN-Profile. Es werden die Client-Apps von Cisco und Juniper unterstützt. Für die Konfiguration der Apps sei auf die jeweiligen VPN-Lösungen verwiesen. Alternativ können VPN-Clients installiert und manuell konfiguriert werden.

Maßnahme Z.2 Schutz des Webdatenverkehrs mit einem HTTP-Proxy

BES12 erlaubt die Konfiguration der Proxy-Einstellungen über ein Proxy-Profil.

Maßnahme Z.3 Application Whitelisting

Die Freischaltung von Apps wird über das Menü „Apps“ durchgeführt. Hier können Apps aus dem Google Play Store oder als APK-Datei bereitgestellt werden. Um die Apps im Knox-Container verfügbar zu machen, müssen sie den „Samsung Workspace devices“ zugeordnet werden. So werden Apps ausgewählten Benutzern oder Gruppen zugeordnet.

Zum Blockieren von Apps wird ebenfalls das Menü „Apps“ genutzt. Hier können Apps mittels der App Package ID angegeben werden. Über eine Compliance-Richtlinie können aus der Liste der zuvor konfigurierten und zu blockierenden Apps diejenigen ausgewählt werden, welche nicht ausgeführt werden dürfen. Hierüber lässt sich auch der Knox-Container von vorinstallierten Apps bereinigen.

4.2.3 Betrieb

Im laufenden Betrieb des BES12 können folgende zentrale Administrationsaufgaben wie folgt ausgeführt werden.

Tabelle 5: Administrationsaufgaben im Betrieb von BES12

Aktion	**Auswahl in Menü** Das Menü kann wie folgt aufgerufen werden: *Users → Auswahl Benutzer → Auswahl Gerät (z. B. Samsung SM-928F)*	**Reaktionen**
Sperren des Geräts	*Lock device*	Das Gerät wird gesperrt.
Entsperren des Geräts	*Unlock device and clear password*	Statt dem Lockscreen wird die Eingabe eines neuen Passworts gefordert. Hinweis: Vorab sollte das Gerät mittels „Lock device“ gesperrt werden.
Setzen eines neuen Gerätepassworts	*Specify device password and lock*	Entsprechend der Passwort-Policy wird über die Oberfläche von BES12 ein Passwort gesetzt. Auf dem Gerät muss danach zur Nutzung das Passwort eingegeben werden.
Löschen des gesamten Geräts	*Delete all device data*	Startet das Gerät sofort neu und führt einen Factory Reset durch.
Löschen des Containers	*Delete only work data*	Nach einem Bestätigungsdialog erscheint die Meldung „Sucessful. This device will be removed from the system.“ Danach ist das Knox-Icon verschwunden, das Gerät ist aus BES12 entfernt und die BES12-App ist nicht mehr konfiguriert.
Passwortwechsel Knox-Container	*Reset work space password*	Nachdem der Knox-Container das nächste Mal gesperrt wurde, wird anschließend statt der Anmeldemaske die Aufforderung zum Setzen eines neues Passworts angezeigt.
Sperren des Knox-Containers	*Disable work space*	Die Anmeldemaske des Knox-Workspace zeigt an, dass dieser gesperrt ist.
Entsperren des Knox-Containers	*Enable work space*	Die Anmeldemaske wird nach einer Sperrung wieder erreichbar.
Zeit ohne Verbindung zum MDM-Server	*View device report → Last contacted*	
Prüfen des Versionsstandes	*View device report → OS version*	

5 Konfiguration von My Knox

5.1 Einrichtung

Die folgende Anleitung für private Nutzer und kleine Unternehmen erläutert die Einrichtung von My Knox auf Samsung-Galaxy-Endgeräten mit Samsung Knox. Dabei wird beschrieben, wie das Gerät in Betrieb genommen und die in Kapitel 3 dieses Dokuments definierten Maßnahmen umgesetzt werden können.

Dabei ist zu beachten, dass die Einstellungen nicht technisch erzwungen werden, sondern manuell von einem Benutzer (oder seinem Administrator) vorgenommen werden müssen. Eine Änderung der Einstellungen ist durch den Benutzer jederzeit möglich. Ziel ist es dabei, das Gerät gegen unberechtigte Benutzung oder Manipulation zu schützen.

Um einen eindeutigen Konfigurationsstand zu erhalten, kann das Gerät vor Beginn der Konfiguration über das Einstellungen-Menü *Sichern und Zurücksetzen → Auf Werkseinstellungen zurücksetzen* frisch initialisiert werden.

In der Ersteinrichtung wird ein Installations-Wizard angezeigt. Die Fragen sollten restriktiv beantwortet werden. Für die Installation der My-Knox-App wird zumindest zu Beginn ein aktiver Google-Account benötigt, siehe dazu Maßnahme Z.6. Im Rahmen der Einrichtung sollten keine weiteren Cloud-Dienste aktiviert werden. Die Geräte-Sperre sollte bereits eingestellt sein, für Vorgaben sei hier auf B.2 verwiesen.

Nach der Installation der My-Knox-App wird beim ersten Aufruf der Knox-Container eingerichtet, siehe Maßnahme B.1, hierzu muss insbesondere die Authentifizierungsmethode gewählt werden, hier sei auf die Vorgaben in B.2 und die Konfigurations-Schritte im folgendem Abschnitt verwiesen. Während der Einrichtung wird auch gefragt, welche Apps im Knox-Container verfügbar sein sollen. Die ausgewählten Apps können im Nachgang auch noch hinzugefügt oder wieder entfernt werden.

Bei der Aktivierung von My Knox muss eine E-Mail-Adresse eingegeben werden. An diese wird eine Aktivierungs-PIN verschickt, welche dann im Nachgang im Installationsdialog eingegeben wird. Anschließend wird noch eine weitere E-Mail-Adresse bei der Festlegung des Passworts für das My-Knox-Portal angegeben. Die Möglichkeiten des My-Knox-Portals werden in Kapitel 5.3 aufgelistet und erläutert.

Auf den Knox-Container kann über das Icon „My Knox“ zugegriffen werden. Zu Beginn sollten die Knox-Einstellungen durchgeführt werden, hier sei auf die Hinweise in B.4 und die Konfigurationsschritte im folgenden Abschnitt verwiesen.

Standardmäßig wird der Knox-Container im Modus „Ordner“ aktiviert. Über die Knox-Einstellungen kann dies geändert werden, sodass der Modus „Startprogramm“ genutzt wird, dadurch wird der Homescreen im Knox-Container aktiviert.

5.2 Konfigurationsschritte

Um die empfohlenen Maßnahmen auf einem manuell verwalteten Gerät durchführen zu können, wird in der folgenden Tabelle angegeben, wie die Konfigurationen über die Menüs des Knox-Geräts vorgenommen werden können. Die folgenden Angaben beziehen sich auf die zum Zeitpunkt der Erstellung des Dokuments aktuelle Version von My Knox sowie eines Knox-Endgeräts mit Samsung Knox Version 2.5.1.

Tabelle 6: Schritte zur manuellen Konfiguration der Endgeräte und Knox-Einstellungen

Maßnahme	Konfiguration	Weitere Hinweise
B.2 Konfiguration der Geräte- und Knox-Container-Sperre	*Einstellungen → Anzeige → Bildschirm-Timeout → 5 Minuten* *Einstellungen → Gerätesicherheit → Sichere Sperreinstellungen → Automatisch sperren → Sofort*	
B.3 Sichere Grundkonfiguration des Knox-Gerätes	Verschlüsselung *Einstellungen → Gerätesicherheit → Andere Sicherheitseinstellungen → Gerät Verschlüsseln*	
	Zusätzliche interne Sicherheitseinstellungen Durch die Installation der CC-Mode-App werden erweiterte Sicherheitseinstellungen im Endgerät aktiviert, welche im Rahmen von erfolgten Sicherheitszertifizierungen festgelegt wurden. Die App ist nach der Anmeldung mit einem Samsung-Account über folgenden Link erreichbar: https://www.samsungknox.com/en/content/common-criteria-mode-apk	
B.4 Einrichten eines Knox-Containers	Installation von My Knox aus dem Play Store. Die Konfiguration des Knox-Containers kann innerhalb von My Knox über die folgenden Wege erreicht werden: 1) *Optionen → KNOX-Einstellungen* (KNOX-Stil „Ordner“) oder 2) Icon „KNOX-Einstellungen“ (KNOX-Stil „Startprogramm“)	
	Knox-Container-Sperrzeit Die Sperrzeit des Knox-Containers kann innerhalb von My Knox über die Optionen angepasst werden: *Optionen → KNOX-Einstellungen → KNOX-Timeout* Die Sperrzeit kann dabei von "Wenn Bildschirm ausgeschaltet wird" sehr restriktiv bis zu 30 Minuten gesetzt werden.	Die Option "Beim Neustart" wird nicht empfohlen, da in diesem Fall nur noch die Gerätesperre vor Zugriffen auf den KNOX-Container bis zum nächsten Neustart des Endgeräts schützt.
	Manuelle Knox-Container-Sperre Eine manuelle Sperre des Knox-Containers im KNOX-Stil „Ordner“ kann wie folgt jederzeit durchgeführt werden: *Optionen → Sperre*	

	Im KNOX-Stil „Startprogramm“ ist ein Sperren des Knox-Containers über das Schlosssymbol in den Android-Benachrichtigungen jederzeit möglich.	
	<u>Benachrichtigungen</u> Folgende Optionen sind möglich: - Details anzeigen deaktiviert (Standard und empfohlen), - Details anzeigen aktiviert und Inhalte auf Sperrbildschirm ausblenden, - Details anzeigen aktiviert und Inhalte auf Sperrbildschirm nicht ausblenden.	Die Option „Details anzeigen deaktiviert“ ist die Standardeinstellung und wird empfohlen.
	<u>Kontakte und Kalender freigeben</u> Es wird empfohlen, die Einstellungen nur in der Richtung „aus Persönlich“ zu aktivieren und nicht in die Richtung „aus KNOX“.	Die Standard-Option ist restriktiver und verhindert die Synchronisation in beide Richtungen.
Z.1 Schutz des Netzwerkverkehrs mit einem VPN	Für die Einrichtung eines VPNs kann der integrierte VPN-Client und/oder eine zusätzliche VPN-App genutzt werden. Die Einstellungen hängen sowohl vom VPN-Server als auch von der gewählten VPN-Client-App ab. Integrierter VPN-Client: *Einstellungen → Weitere Verbindungseinstellungen → VPN → Mehr → VPN hinzufügen*	Die integrierte Möglichkeit zur Einrichtung einer VPN-Verbindung über die Standard-Endgeräte-Einstellungen aktiviert ein VPN, welches aber *nicht* den My-Knox-Container beinhaltet.
Z.2 Schutz des Webdatenverkehrs mit einem HTTP-Proxy	*Einstellungen → WLAN → Auswahl konfiguriertes WLAN (langes Halten, Menü → Netzwerkeinstellungen verwalten → Auswahl Erweiterte Einstellungen anzeigen → Proxy → Manuell* Danach erfolgt die Angabe von Proxy-Server-IP und -Port sowie optional von weiteren Daten.	
Z.6 Knox-Gerät ohne Google-Konto	Google-Synchronisation deaktivieren: *Einstellungen → Konten → Google→ aktives Google-Konto wählen → Erste Zeile wählen (Synchronisationseinstellungen) → alle Optionen deaktivieren* Google-Konto vom Gerät entfernen: *Synchronisationeinstellungen wählen (wie zuvor beschrieben) → mehr (oben rechts) → Konto entfernen → Bestätigungsdialog: Konto*	

	entfernen → Weiterer Bestätigungsdialog: OK → Geräte-Passwort eingeben Hinweis: Vor der Entfernung des Google-Kontos müssen alle notwendigen Apps installiert werden, da danach kein Zugriff auf den Google Play Store mehr möglich ist.	

Ergänzend zu B.3 wird empfohlen, die Standardeinstellungen zu nutzen und keine Änderungen vorzunehmen:

- „Unbekannte Quellen“ deaktiviert (Standardoption), dies verhindert die Installation von Apps ohne Play Store.
- Entwickler-Modus nicht aktivieren (Standardoption), dies verhindert unberechtigte Zugriffe per USB-Schnittstelle.

5.3 Hinweise zum Betrieb

Im Rahmen der Installation von My Knox wird ein My-Knox-Portal-Account eingerichtet. Über dieses Portal können die folgenden Aktionen ausgeführt werden, die zweite Spalte beschreibt die Reaktionen am Endgerät.

Tabelle 7: Funktionen des My-Knox-Portals und Reaktionen am Endgerät

Aktion	Reaktionen
Gerät sperren	Hierzu muss ein PIN-Freigabecode und optional eine Rufnummer und ein Hinweistext angegeben werden, über den PIN-Freigabecode kann dann das gesperrte Gerät wieder freigegeben werden.
KNOX sperren	Dies sperrt den Knox-Container, eine Authentifizierung ist dann nicht mehr möglich.
KNOX entsperren	Ermöglicht bei vorheriger Sperre wieder die Authentifizierung für den Knox-Container.
KNOX-Passwort zurücksetzen	Setzt das Passwort des Knox-Containers zurück, bei der nächsten Nutzung kann ohne vorherige Authentifizierung ein neues Passwort gesetzt werden.
KNOX abmelden	Dies entfernt My Knox und löscht damit auch den Knox-Container vom Gerät, danach kann keine Administration mehr über das My-Knox-Portal durchgeführt werden.
Gerät löschen	Dies setzt das Gerät auf Werkseinstellungen zurück, es wird sofort ein Neustart durchgeführt.

Stichwort- und Abkürzungsverzeichnis

ADB	Android Debug Bridge
App	Applikation
CC	Common Criteria
CellWe EMM	Samsung CellWe EMM (MDM Solution), umbenannt in Samsung SDS IAM&EMM
EULA	End-User License Agreement
FOTA	Firmware Update Over-The-Air
MDM	Mobile Device Management
ODE	On-Device Encryption
OS	Operating System
OTA	Over-The-Air
TIMA	TrustZone-based Integrity Measurement Architecture
VPN	Virtual Private Network

Hinweis: Für eventuelle Abkürzungen der MDM-Hersteller in den Konfigurationstabellen in Kapitel 4 sei auf die jeweiligen Hersteller-Dokumentationen verwiesen.