DB NETZE

Digitaler Befehl
Anforderungen an Tf-Endgeräte & EVU-Schnittstelle

Projekt „Digitaler Befehl“

Anforderungen an Tf-Endgeräte

EVU-Schnittstelle

Stand: 28.06.2023

Inhaltsverzeichnis

Dokumentenhistorie

Version	Datum	Autor	Bemerkungen
1.0	22.12.2022	Markus Haupt	Erstfassung
1.1	31.01.2023	Markus Haupt	Aufnahme Anforderung wegen Jailbreak bzw. Rooten
1.2	21.03.2023	Markus Haupt	Einarbeitung Hinweise, Erweiterung um mögliche Gerätetypen wie Notebooks unter Windows oder Linux, Aufnahme organisatorischer Anforderungen
1.3	26.04.2023	Markus Haupt	Anforderungen den aktuellen Erfordernissen angepasst Redaktionelle Anpassungen
1.4	25.05.2023	Markus Haupt	Aufnahme nicht-sicherheitsrelevanter Anforderungen
1.5	01.06.2023	Markus Haupt	Konkretisierung Anforderung Konnektivität auf LTE-fähige Endgeräte
1.6	06.06.2023	Markus Haupt	Anforderung Konnektivität auf stabile Internetverbindung mit mindestens 1 Mbit/s geändert
1.61	28.06.2023	Björn Norwig	Zusammenfassung Anforderungen an Tf-Endgerät und EVU-Schnittstelle

1 Einleitung

Ziel des Dokuments ist die Definition von Anforderungen an mobile Endgeräte und deren Softwareausstattung um den sicheren Betrieb des Digitalen Befehls zu gewährleisten.

Unter mobile Endgeräte sind sowohl Notebooks, Smartphones als auch Tablets zu verstehen. Die Anforderungen sind herstellerunspezifisch definiert und sind sowohl für Windows, Linux, Android- als auch iOS-Plattformen umzusetzen.

Die hier aufgeführten Anforderungen stellen das notwendige Sicherheitsniveau sicher.

2 Anforderungen an das Endgerät

Thema	Anforderung
Authentisierung	Das Gerät muss mindestens eines der folgenden Mechanismen zur Entsperrung umgesetzt haben: alphanumerisches Passwort, Fingerprint, Gesichtserkennung, Hochsicherheits-Biometrie Scan.
Hardware	Es dürfen keine Hardwarekomponenten, bzw. Bauteile, Chips, etc. für Schnittstellen zum Einsatz kommen, die bekannte Schwachstellen beinhalten. Die Überwachung der Schwachstellen liegt in der Verantwortung des Endgeräte ausgebenden Unternehmens. Siehe unter organisatorische Anforderungen.
Kryptografie	Der interne Speicher (z.B. Flash oder HDD/SSD) des Endgeräts muss voll verschlüsselt sein. Die Verschlüsselung muss neben dem Nutzerkennwort auch auf einem gerätespezifischen Merkmal basieren, wie z.B. TPM bei Notebooks.
Kryptografie	Verfügt das Gerät über die Möglichkeit der Einbindung eines Wechseldatenträgers wie einen USB-Stick oder SD-Karte, so muss dieser verschlüsselt sein. Es gelten die gleichen Verschlüsselungsanforderungen wie bei einem internen Speicher.
Kryptografie	Neugeräte müssen mit aktuellen und sicheren Verschlüsselungsalgorithmen bzw. -technik ausgestattet sein. Z.B. TPM 2.0 in Notebooks.
Lifecycle	Bei Smartphones und Tablets müssen Neugeräte aus aktuellen Modellreihen bezogen werden. Diese sind aus den aktuell gültigen Produktkatalogen der Hersteller zu beziehen, um einen möglichst langen Lifecycle zu bieten. Hierbei sind auch Angaben des Herstellers zum End-of-Life und End-of-Service zu beachten. Es ist sicherzustellen, dass Smartphones und Tablets, sowie Betriebssysteme vom Hersteller mit Sicherheitsupdates versorgt werden
Rechte	Standard-Benutzer und -Gruppen sind zu löschen oder zu deaktivieren.
Umgebung	Telemetriedaten die an den Hersteller des Endgeräts gesendet werden sind auszuschalten bzw. müssen zumindest auf ein Minimum begrenzt werden. Hierbei dürfen keine Daten aus Anwendungen übermittelt werden.
Umgebung	Bei Notebooks muss das Betriebssystem entsprechend abgesichert sein (Sicherheitseinstellungen, Benutzereinschränkungen, Virenschutz, etc.), dass Schadcode in seiner Wirksamkeit eingeschränkt wird.
Konnektivität	Das Endgerät muss eine stabile Internetverbindung aufbauen können. Die Übertragungsgeschwindigkeit muss mindestens 1 Mbit/s betragen.
Darstellung	Das Endgerät muss eine Mindestbildschirmgröße nach Skalierung von 360px(dp) besitzen.

3 Anforderungen an die eingesetzte Software

Thema	Anforderung
Apps	Apps sind zentral zu verwalten, es ist sicherzustellen, dass die Apps keine Zugriffsmöglichkeiten auf Informationen aus dem Verfahren Digitaler Befehl erlangen können.
Apps	Installierte Apps sind auf einem aktuellen Versionsstand zu halten. Neue Versionen von Apps sind innerhalb 4 Wochen nach Veröffentlichung zu installieren. Sicherheitsupdates sind innerhalb einer Woche nach Veröffentlichung zu installieren. In den Updateprozess sind alle notwendigen Beteiligten mit einzubinden. Bei einer zentralen Lösung sind die Benutzer über anstehende Updates zu informieren. Der Endgeräte-Nutzer muss den Updateprozess unterstützen und den Anweisungen bezüglich Updates Folge leisten.
Apps	Browser Apps müssen auf aktuellem Versionsstand gehalten werden.
Apps	Es sind die für die Anwendung freigegebenen Browser einzusetzen (Chrome, Edge, Firefox und Safari für iOS). Sollte für den eingesetzten Browser gravierende Schwachstellen auftreten so ist ein anderer Browser aus der Aufzählung zu nutzen, bis die Schwachstelle behoben bzw. der Patch eingespielt ist.
Betriebssystem	Neugeräte müssen mit dem zum Zeitpunkt des Kaufes aktuellsten Betriebssystem ausgestattet sein. Das Betriebssystem muss im Lauf des Lebenszyklus des Endgerätes regelmäßig aktualisiert werden, so dass sich das Betriebssystem des Endgeräts im Nutzungszeitraum immer auf dem aktuellen Stand befindet.
Betriebssystem	Geräte deren OS nicht mehr mit Sicherheitsupdates versorgt werden, dürfen nicht mehr eingesetzt werden.
Betriebssystem	Die Einrichtung der Endgeräte, die Installation des Betriebssystems und der Apps müssen zentral erfolgen. Der Anwender darf weder Betriebssysteme selbst installieren, die wesentlichen sicherheitsrelevanten Konfigurationen des Endgerätes verändern, noch Apps aus anderen als den zentral zur Verfügung gestellten Quellen installieren.
Virenschutz	Alle Endgeräte sind mit einem Virenschutz zu versehen. Ausnahmen wie z.B. Linux oder iOS sind zu begründen und regelmäßig zu überprüfen.
Virenschutz	Der installierte Virenschutz ist aktuell zu halten, Virendefinitionen sind regelmäßig, mindestens einmal täglich, zu aktualisieren.
Virenschutz	Der Virenschutz darf durch den Benutzer nicht deaktiviert werden können.

4 Organisatorische Anforderungen

Thema	Anforderung
Passwort	Es sind Passwortvorgaben zu definieren, die ausreichend sichere Passwörter definiert, triviale Passwörter verbietet und die Mitarbeiter zur Geheimhaltung der Passwörter verpflichtet. Sofern technisch nicht durchsetzbar, sind diese organisatorisch anzuweisen.
Rechte	Benutzer dürfen auf den Endgeräten keine Administrator- oder Root-Berechtigung erhalten.
Schwachstellenmanagement	Die Verantwortung für die Überwachung von Schwachstellen in Apps und OS, sowie die Ausbringung von Sicherheitsupdates liegen bei den Endgeräten ausgebenden Unternehmen, der Benutzer hat sich an die Anweisungen bezüglich Schwachstellen und Updates zu halten.
Virenschutz	Ein Virenschutzkonzept ist zu erstellen, in dem die Verantwortlichkeiten festgelegt werden. Die Benutzer sind zu schulen, wie sie sich im Fall eines Virenbefalls korrekt verhalten.

5 EVU-Schnittstelle

5.1 Allgemeines

Seitens DB Netz AG wird, neben der Nutzung in der projekteigenen DB Tf-App, auch eine API Dritten zur Verwendung in eigenen Tf-App Implementierungen zur Verfügung stehen. Die zur Verfügung gestellte, öffentlich zugängliche API wird die Schnittstelle der Kommunikation seitens der Triebfahrzeugführer-Applikation zum gemeinsamen Backend darstellen.

5.2 Zugriffsmöglichkeiten

Die API kann über folgende Portale bezogen werden. Im Suchfeld ist die API über den Suchbegriff „Digitaler Befehl“ aufrufbar.

Hinweis: Die Links zu den API-Portalen werden noch veröffentlicht.