Leitfaden

Gerätekonfiguration
und
Einbindungsmöglichkeiten
der Datafox Geräte

Inhalt

1. Einleitung ... 1
2. Systemaufbau ... 1
2.1. Aufbau der Hardware / Gerät und Firmware ... 2
2.2. Unterstützte Zeichensätze ... 3
2.3. Mehrsprachenfähigkeit ... 4
2.4. Displaydesigner ... 5
2.4.1. Farbeinstellung für die Anzeigen im EVO 4.3 Multifunktionsterminal / 2.8 und 3.5 Pure ... 6
2.4.2. Standardeinstellungen ... 6
2.4.3. Funktionstasten im Display des EVO 4.3 Flex / 2.8 und 3.5 Pure anzeigen ... 7
2.4.4. Bilder für Funktionstasten des EVO 4.3 Flex / 2.8 / 3.5 Pure hochladen ... 7
2.4.5. Designbeispiele im Designer ... 8
2.5. Individuelle Touch-Layouts für EVO 5.0 Pure/Flex und EVO 7.0 Flex ... 9
2.6. Individuelle Display-Layouts V2 für EVO 5.0 Pure/Flex und EVO 7.0 Flex ... 10
3. Erstellung eines Setups (Programm) ... 12
4. Geräteschlüssel und Sicherheit ... 13
4.1. Gerätepasswörter ... 13
4.1.1. Kommunikationspasswort ... 13
4.1.2. Bios Menü Passwort ... 13
4.2. WLAN Sicherheit ... 14
4.2.1. M111_WLAN ESP32-c3 ML01 (WLAN-Modul DF-WL03) ... 14
4.2.2. Texas Instruments TI-CC3135 (Generation 2) ... 15
4.2.3. Redpine (Generation 1) ... 16
5. Beschreibung der einzelnen Kommunikationstechniken ... 17
5.1. Übersicht über die Kommunikationstechniken ... 17
5.2. Funktionsübersicht der Kommunikationstechniken ... 18
6. Kommunikation per DFCom API (DLL) ... 19
6.1. Programmbibliothek [Dynamic Link Library (DLL)] – Allgemeines ... 19
6.1.1. Was ist eine Programmbibliothek? ... 19
6.1.2. Vorteile einer Programmbibliothek in DLL- oder so-Form. ... 19
6.1.3. Die Kommunikations-Bibliothek ist für folgende Systeme verfügbar: ... 19
6.1.4. Programmbibliothek (DLL) - Einbindung Passiv-Mode (Polling) ... 20
6.2. Programmbibliothek (DLL) - Einbindung Active-Mode (Aktive Verbindung) ... 21
6.3. Verschlüsselung der Daten bei der Verwendung der DFCom.dll ... 22
6.3.1. Erstellung und Hinterlegen des Schlüssels im Gerät ... 23
6.3.2. Hinterlegen des Passwortes im Datafox StudioIV ... 24
6.3.3. Übergabe des Schlüssels in die DFComDLL ... 24
6.3.4. Löschen des Kommunikationsschlüssels ... 25
7. http Level 1 ... 26
7.1. Voraussetzungen ... 26
7.1.1. Request ... 26
7.1.1.1. Methode: GET ... 26
7.1.2. Response ... 27
7.1.2.1. Optionale Parameterangaben bei der Antwort ... 27
7.1.3. Verschlüsselung ... 29
7.1.3.1. Veranschaulichung der GET-Anfrage ... 32
7.1.3.2. Erkennung einer Verschlüsselung ... 33
7.2. https Kommunikation ... 33
7.2.1. Voraussetzungen ... 33
7.2.2. Elemente der https Infrastruktur ... 33
7.2.3. Nutzung der Verschlüsslung / Zertifikate ... 33
8. Datafox Connect ... 34
8.1. Connect im Remote-Modus ... 34
8.2. Connect im Transparent Mode ... 35
8.3. Connect im Parallel-Modus ... 36
9. Anhang ... 37
9.1. Alle wichtigen Links ... 37
9.1.1. Geräte Handbücher ... 37
9.1.2. Software und SDK (Schnittstellenbeschreibungen) ... 37
9.1.3. Sonstige wichtige Links ... 37
9.1.4. Alle Neuerungen kompakt ... 38
9.1.5. Softwareversionslisten ... 38
9.2. Info zu HTTPS ... 39

Änderungen in diesem Dokumen t

Datum	Kapitel	Beschreibung
07.08.2013	Alle	Neuauflage der Dokumentation
08.09.2013	Alle	Ausdruckkorrektur
14.05.2014	4.3 4.4	Hinweis Unterschiede Active-Mode -> Passive Mode Onlinefunktion ZK über HTTP
10.05.2015	4.3.4 und 4.4.5	Verschlüsselung ergänzt
30.03.2016		Links aktualisiert
09.08.2016	4.2	Übersicht / online offline Funktionen der ZK ergänzt
07.11.2016	2.2 2.3 4.3.4	Sprache Zeichensätze Beschreibung der DLL Verschlüsselung
21.12.2016	2.4	Displaydesigner
28.12.2017	5.6	http Level 1
28.12.2017	5.7	https
23.01.2018	4.2	WLAN Security
17.12.2019	5.6	Weitere Möglichkeiten im http Level 1
28.07.2020	Anhang Struktur der Kapitel	Informationen zu HTTPS Hauptstruktur des Dokuments geändert
11.12.2023	Alle notwendigen	Links an die neue Homepage angepasst http Level 0 gekürzt, da nicht mehr relevant. Neue Seite mit allen wichtigen Downloads hinzugefügt.
12.11.2025	Talk Entfernt Datafox Connect hinzugefügt	Datafox Connect - Remote Modus - Transparent Modus - Parallel Modus
05.03.2026	Connect	Schaubilder angepasst

1. Einleitung

Dieses Dokument ist ein Leitfaden zur Einarbeitung in die Themen:

a.) Parametrierung und
b.) Einbindung der Kommunikation

Der Leitfaden gilt für alle Mikrocontroller-Geräte der MasterIV-Serie und EVO-Serie, als auch für die in den Industrie-PCs integrierten Embedded-Baugruppen.
(Hinweis: Die in den Industrie-PCs integrierten Embedded-Baugruppen können alternativ auch im HID-Modus betrieben werden.)

Das Dokument hilft Ihnen, den Integrationsaufwand abschätzen zu können.
Es werden Ihnen Links und Hinweise gegeben, wo Sie Information zum jeweiligen Thema finden.

Die **Parametrierung der Geräte** erfolgt über Datafox-Studio. ***Dieses Programm ermöglicht Ihnen die gewünschten Erfassungs- und Prüf-Funktionen schnell, einfach und ganz ohne Programmierkenntnisse zu erstellen oder wie wir sagen zu parametrieren.***
Das kosten-/lizenzfreie Programm finden Sie auf unserer Internetseite.

Bei der **Einbindung der Kommunikation** geben wir Ihnen einen Überblick über die möglichen Kommunikationswege mit Datafox-Terminals. Hierbei werden die einzelnen Wege aufgezeigt und deren Vor- und Nachteile beschrieben. ***Auf der Internetseite finden Sie Programmbeispiele für die Einbindung der DLL in den gängigen Programmiersprachen zu Ihrer freien Verwendung.***

2. Systemaufbau

Folgende Komponenten sind in den nachfolgenden Kapiteln erklärt:

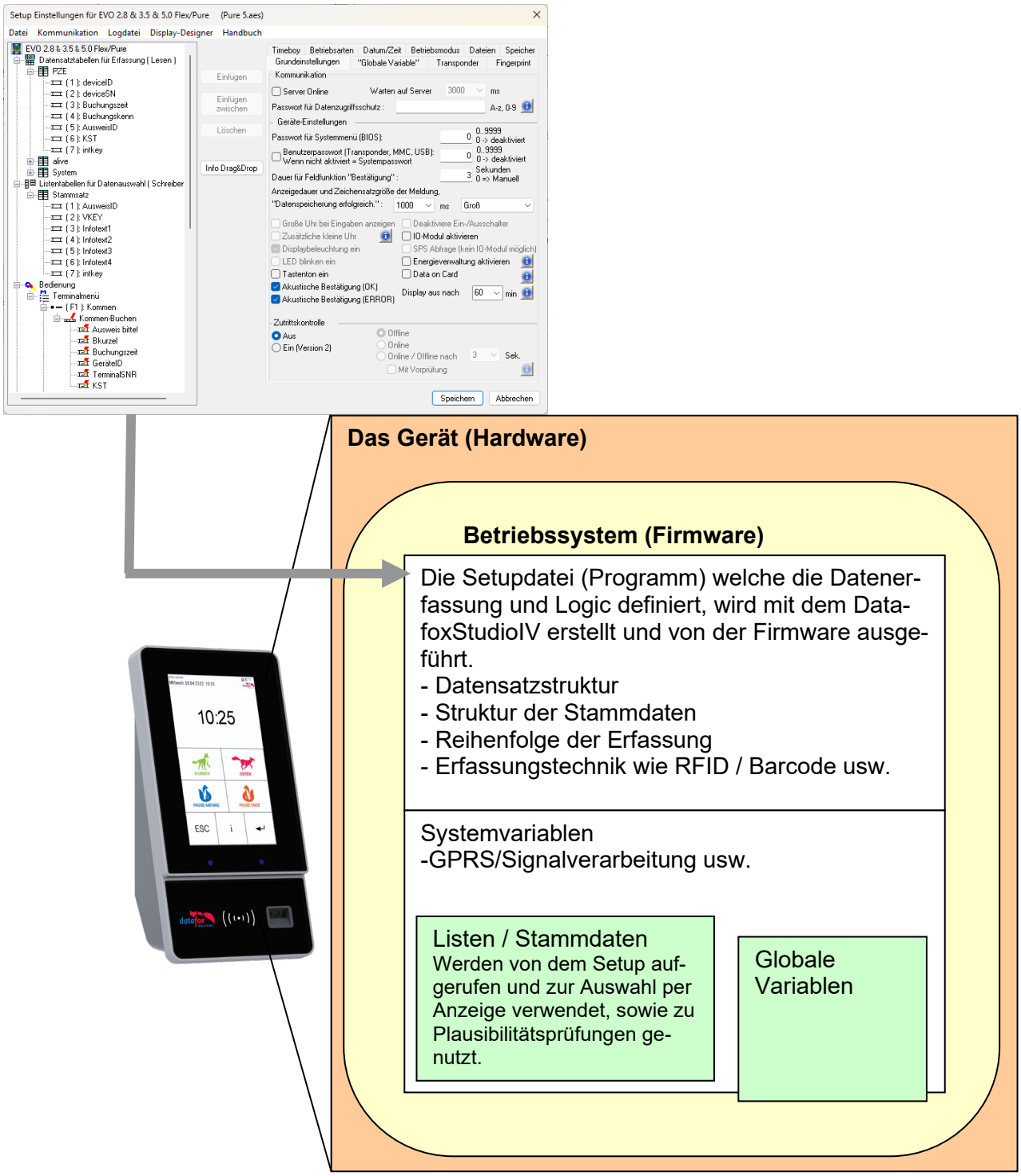
Aufbau der Hardware / Gerät und Firmware (Link)

Erstellung eines Setups (Link)

Kommunikationstechniken mit Datafox- Geräten (Link)

2.1. Aufbau der Hardware / Gerät und Firmware

Diese Grafik zeigt Ihnen den Aufbau der Datenerfassungsgeräte im Zusammenhang.
Zu Grunde liegt die Hardware mit der gewünschten Ausstattung.
Darauf befindet sich die Firmware, die das Betriebssystem darstellt.
Das Programm, wir nennen dies Setup-Datei, wird von der Firmware ausgeführt.



Dieser Zusammenhang ist wichtig, da Sie nicht mit jeder Kommunikationstechnik Zugriff auf die einzelnen Bereiche des Systems haben.

2.2. Unterstützte Zeichensätze

Zu Ihrer Information haben wir nachfolgend eine Erläuterung zu den Zeichen im Standard-Lieferumfang zusammengestellt.
Diese Information finden Sie auch in den Handbüchern.
Die Datafox Geräte unterstützen im Standard einen Teil der Zeichenkodierung Latin-1 (ISO-8859-1) für die Zeichenausgabe am Display und die Daten.

ISO 8859-1, genauer **ISO/IEC 8859-1**, auch bekannt als **Latin-1**, ist ein von der ISO zuletzt 1998 aktualisierter Standard für die Informationstechnik zur Zeichenkodierung mit acht Bit und der erste Teil der Normenfamilie **ISO/IEC 8859**.

Zeichentabelle Latin-1:

Code	…0	…1	…2	…3	…4	…5	…6	…7	…8	…9	…A	…B	…C	…D	…E	…F
0…	nicht belegbar															
1…																
2…	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3…	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4…	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5…	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6…	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7…	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
8…	nicht belegbar															
9…																
A…	NBSP	¡	¢	£	¤	¥	¦	§	¨	©	ª	«	¬	SHY	®	¯
B…	°	±	²	³	´	µ	¶	·	¸	¹	º	»	¼	½	¾	¿
C…	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï
D…	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
E…	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î	ï
F…	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	ÿ

SP = Leerzeichen, NBSP = feste Leerzeichen, SHY = bedingter Trennstrich

	Steuerzeichen nach ISO-Norm nicht belegbar
	von Datafox festgelegt als nicht nutzbare Zeichen
	nutzbare Zeichen von Firmware-Version 04.01.xx.xx bis Firmware-Version 04.03.02.xx
	Zeichenerweiterung ab Firmware-Version 04.03.03.xx ***(nur bei Hardware V4)***
	Zeichenerweiterung ab Firmware-Version 04.03.04 bei Verwendung Zeichentabelle Latin-1 ***(nur bei Hardware V4)***

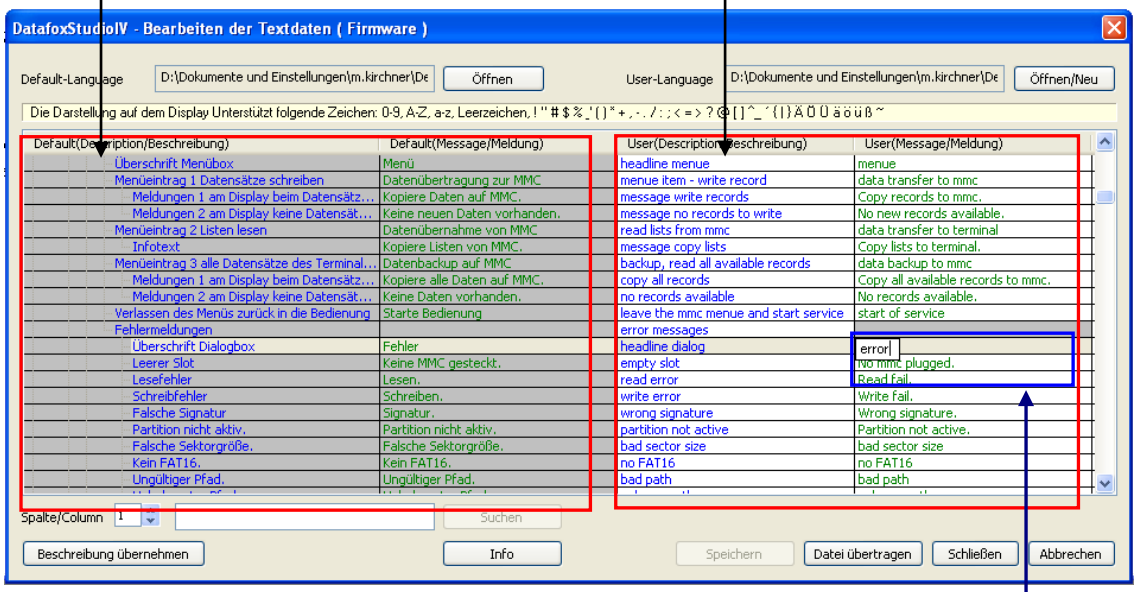
Andere Zeichentabellen sind grundsätzlich möglich und wir bitten ggf. um Anfrage.

2.3. Mehrsprachenfähigkeit

Um eine Sprachkompatibilität zu bieten, haben Sie die Möglichkeit, die von der Firmware angezeigten Texte und Meldungen zu bearbeiten.
Öffnen Sie den Bearbeitungsdialog über das Menü
„Konfiguration – Sprachtabelle für Gerät, Gerätetexte(*.dfl) – Datei für Sprachtabelle bearbeiten“.

Öffnen Sie nun ein Gerätedateiarchiv (Firmware)*.dfz. Es werden die Default-Texte der Firmware mit einer Beschreibung und der zugehörigen Meldung angezeigt.

Öffnen bzw. erstellen Sie nun eine neue Sprachdatei für die Firmware mit der Endung *.dfl. Wenn Sie eine neue Datei erzeugt haben, ist die rechte Seite der Liste leer.



Innerhalb der Liste arbeiten Sie nur mit einfachen Mausklicks. KEINE Doppelklicks! Selektieren Sie mit einem einfachen Klick eine Zeile aus der Liste.
Mit einem weiteren einfachen Klick in die Spalte User(.../Beschreibung) oder User(.../Meldung) setzen Sie den Cursor in dieses Feld.

Nun können Sie einen Text ihrer Wahl eingeben bzw. bearbeiten.
Wenn Sie die Eingabe abschließen, wird die Beschreibung aus der Spalte Default(.../Beschreibung) übernommen und können diesen ebenfalls bearbeiten.

Hinweis:
Kyrillische und Chinesische Zeichen können nicht abgebildet werden.

Auf unserer Homepage finden Sie Sprachdateien (.dfl) für die Sprachen:
- Englisch, Niederländisch, Französisch
- Deutsch ist als Grundeinstellung immer in der Firmware enthalten und entspricht der Grundeinstellung.

https://www.datafox.de/d67/unternehmen/downloads/software/master4-v4/Datafox_Softwarepaket_MasterIV.zip

2.4. Displaydesigner

Anwendungsbereich:

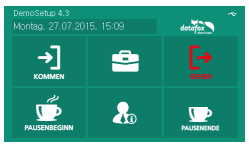
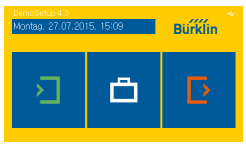
		4.3/ 7.0 Flex	2.8/3.5	EVO 5.0 Flex, Pure	Uni- versal	Agera ZK	Inloc	Mobil Box	IO-Box	Oneloc	EVO- PC
☒	☒	☒	☒	☒	☒	☒					

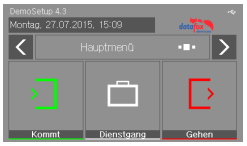
Bei AE-MasterIV V4, Basic V4 ist der Designer nur für Farbdisplay anwendbar.

Mit dem Display-Designer bietet Datafox die Möglichkeit für Partner und Anwender die Darstellung den Wünschen entsprechend anzupassen. Aber Achtung, aufgrund der notwendigen Bedienfolgen kann das keine komplett freie Gestaltung sein, sondern es müssen schon Dinge wie Kopfzeilen, Menüstrukturen und Fußzeilen gewährleistet sein. Ziel des Display-Designers ist es, mit minimalem Aufwand die machbaren Einstellungen zu ermöglichen.

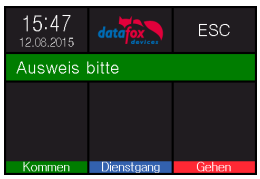
Wir freuen uns auf viele Anwender und empfehlen:
Erstellen Sie sich Ihr firmeneigenes Display-Design:

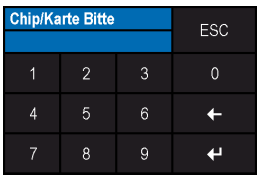
Beispielbilder für EVO 4.3 Flex

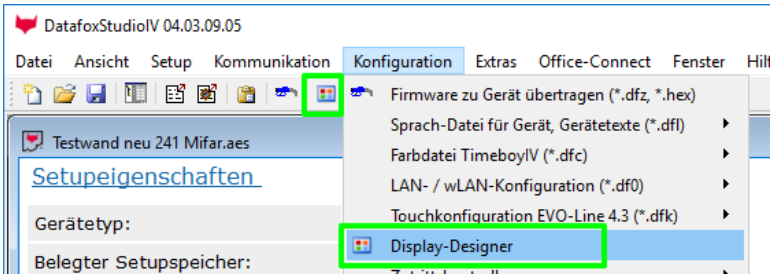


Beispielbilder für EVO 2.8 / 3.5 Pure

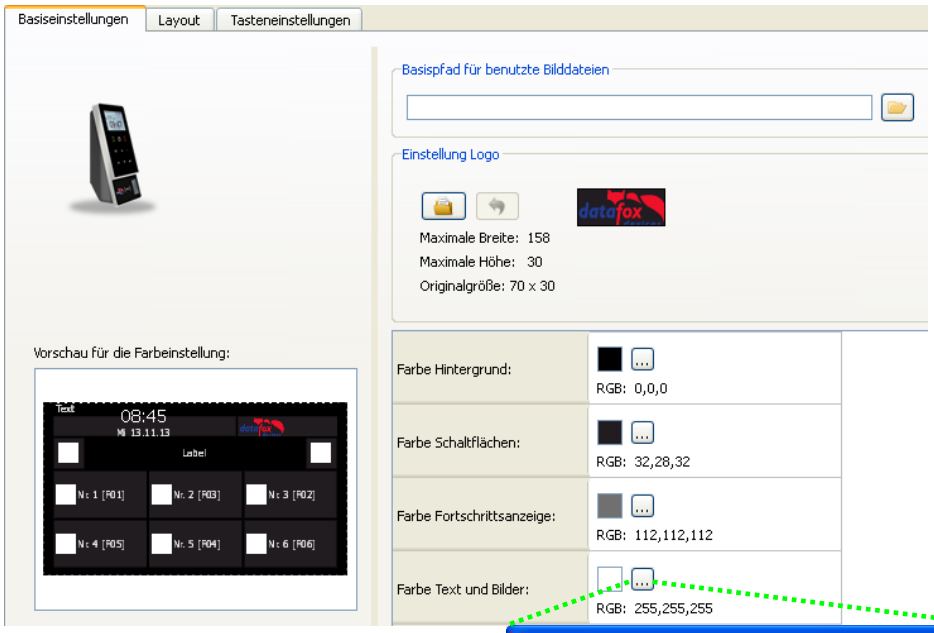


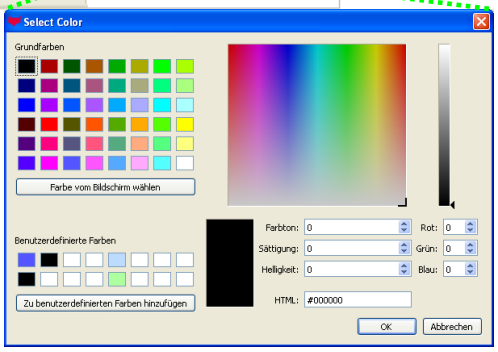


Der Aufruf des Display-Designers erfolgt über das Menü Konfiguration oder direkt aus der Setup-Editier-Maske heraus.

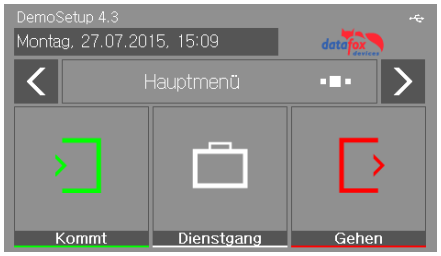


2.4.1. Farbeinstellung für die Anzeigen im EVO 4.3 Multifunktionsterminal / 2.8 und 3.5 Pure





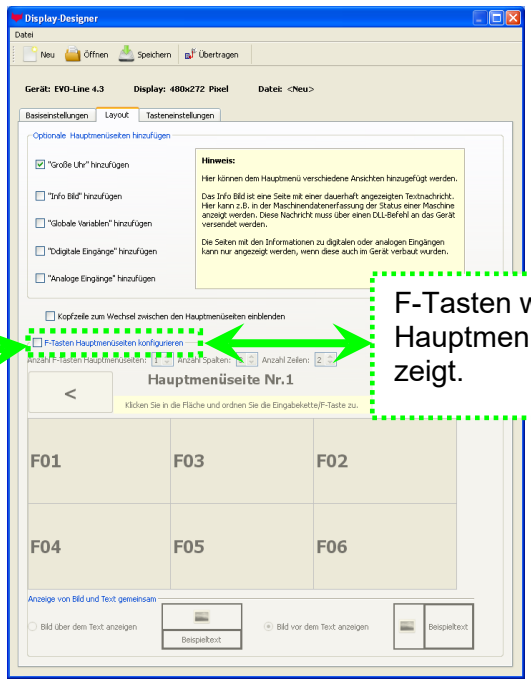
Beispielbild:



2.4.2. Standardeinstellungen

Die Geräte werden im Standard „PZE“ Design ausgeliefert.

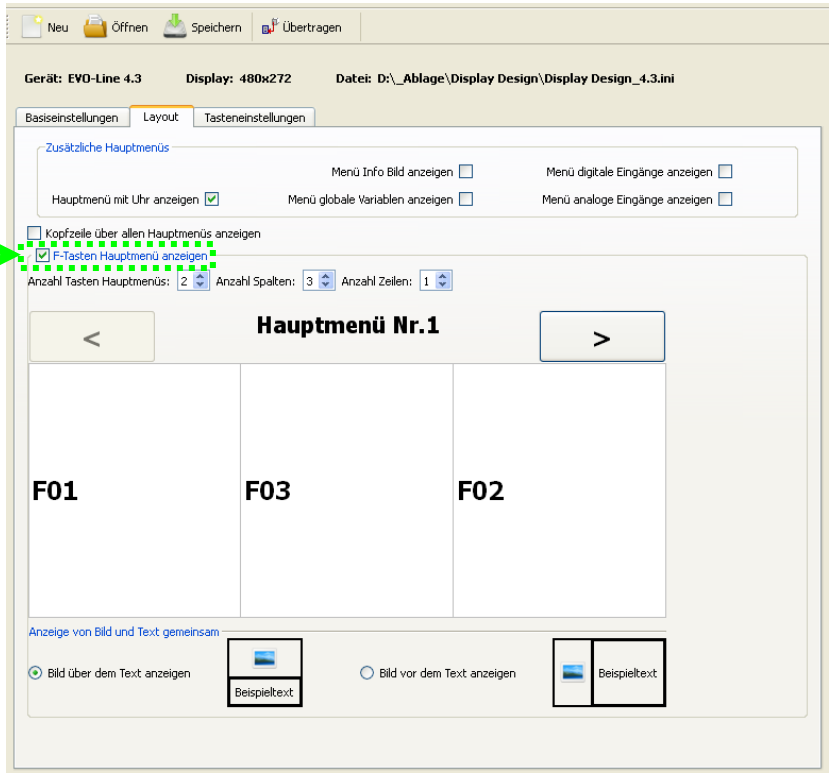
Dieses Design ist auch als Standard beim ersten Erstellen eines neuen Designs im Display-Designer voreingestellt.



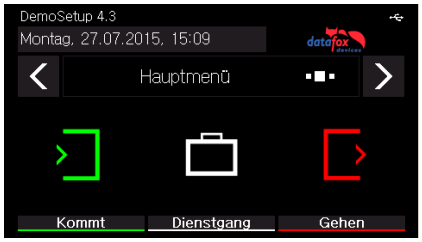
F-Tasten werden im Hauptmenü **nicht** angezeigt.

2.4.3. Funktionstasten im Display des EVO 4.3 Flex / 2.8 und 3.5 Pure anzeigen

Durch das Einblenden der Funktionstasten aus dem Setup, kann nun die Anzahl der im Display angezeigten Tasten angepasst werden.

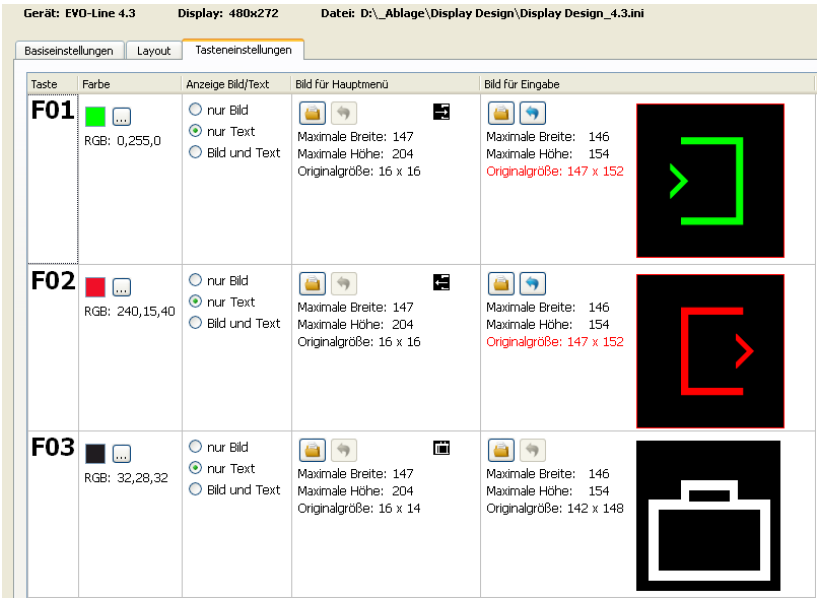


Beispiel:



2.4.4. Bilder für Funktionstasten des EVO 4.3 Flex / 2.8 / 3.5 Pure hochladen

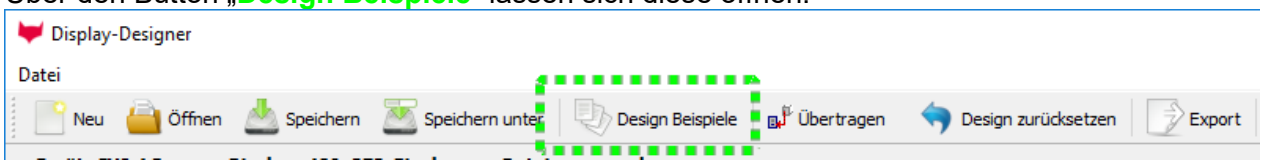
Unter diesem Menüpunkt „Tasteneinstellungen“ können Sie die Bilddatei für jede Funktionstaste importieren.



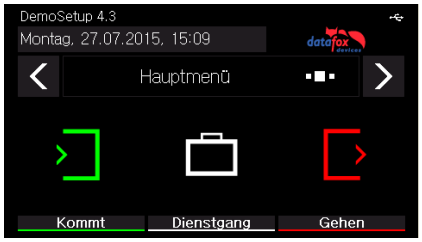
Beispielbild für die Tastenbilder:

2.4.5. Designbeispiele im Designer

Mit der Installation des Datafox StudioIV erhalten Sie verschiedene Designbeispiele für die Geräte. Über den Button „**Design Beispiele**“ lassen sich diese öffnen.



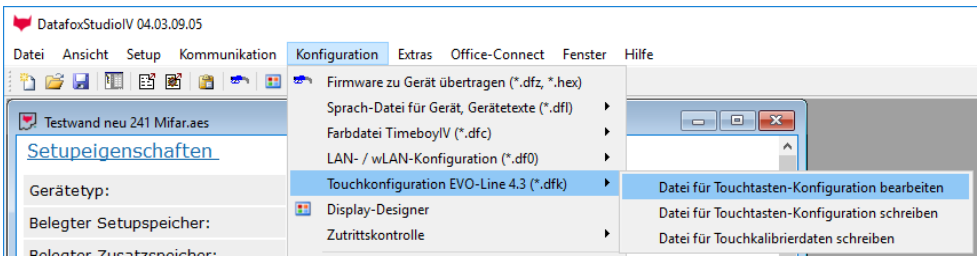
Die Beispiele werden von Datafox nach und nach erweitert.
Sollten Sie hierzu Anregungen und Wünsche haben, dann teilen Sie uns diese gerne mit.



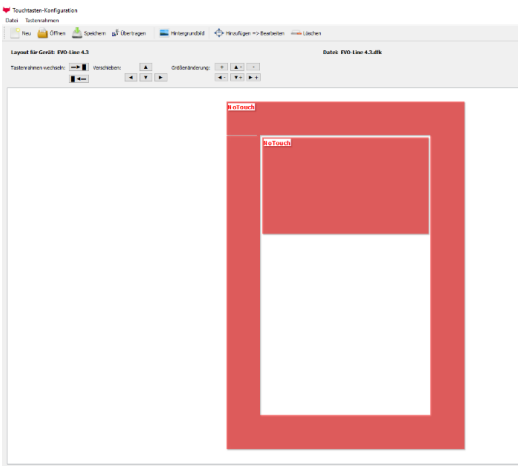
2.5. Individuelle Touch-Layouts für EVO 5.0 Pure/Flex und EVO 7.0 Flex

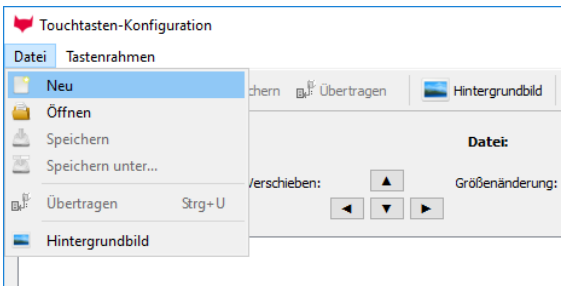
In den Geräten EVO 5.0 Pure/Fles und EVO 7.0 Flex, kann man die Touchflächen individuell gestalten.
Hierzu wird ein Bild für die Tastatur auf dem Gerät hinterlegt und angezeigt.
Mit dem Datafox StudioIV kann man dann die gewünschten Tasten auf das Bild legen.

In das Menü gelangen Sie über:



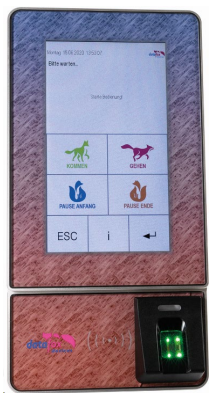
Über „Datei Neu“, können Sie eine neue Touchkonfiguration anlegen.

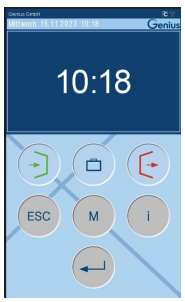




Eine detaillierte Anleitung finden Sie Im Handbuch.

So könnte Ihr Display aussehen.





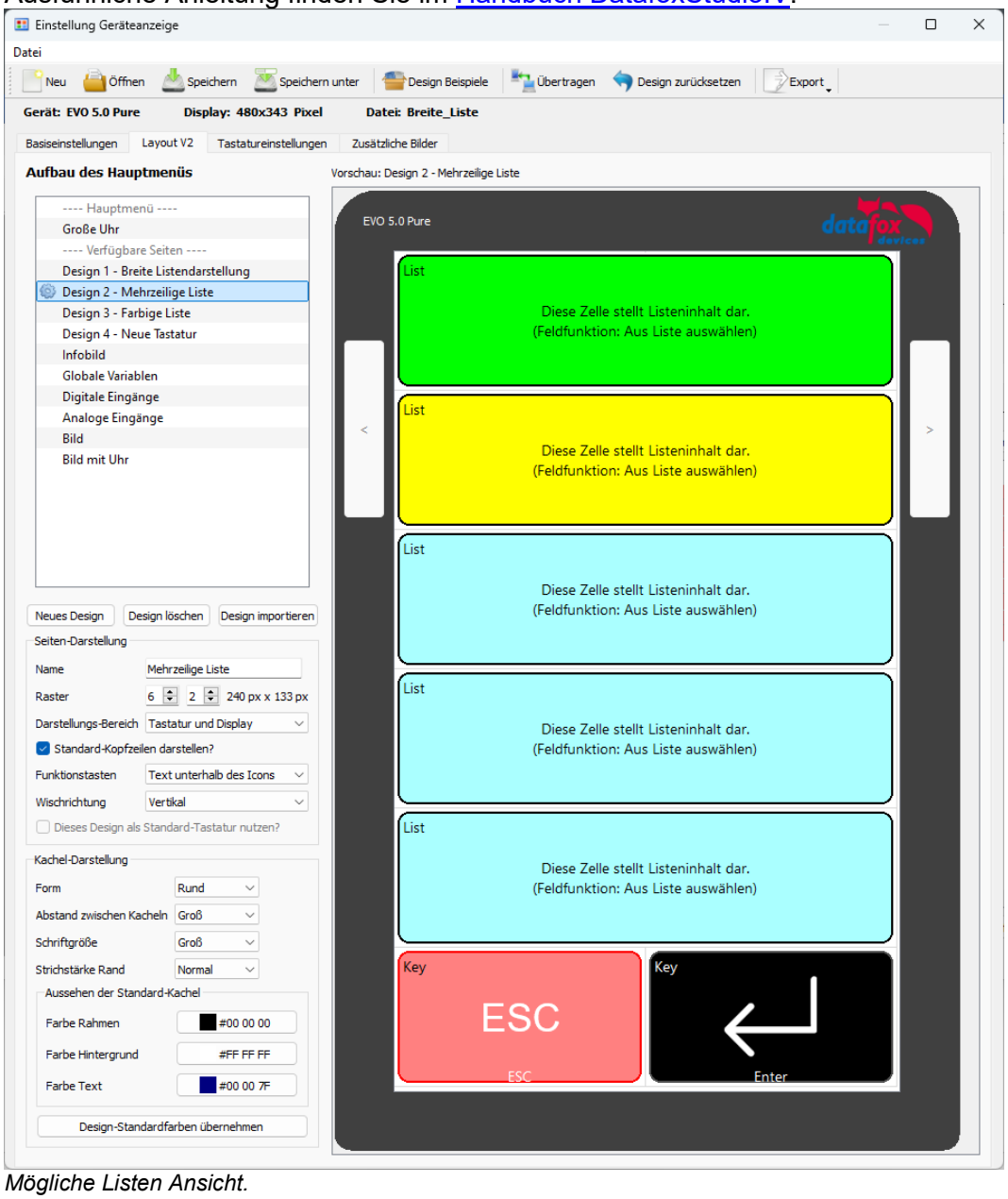
2.6. Individuelle Display-Layouts V2 für EVO 5.0 Pure/Flex und EVO 7.0 Flex

Ab der Firmware 04.03.23 können die Displays von den Geräten:

- EVO 5.0 Pure
- EVO 5.0 Flex
- EVO 7.0 Flex

Komplett frei gestaltet werden.

Hier ein paar Beispiele: Ansicht aus der Software DatafoxStudioIV
Ausführliche Anleitung finden Sie im Handbuch DatafoxStudioIV.

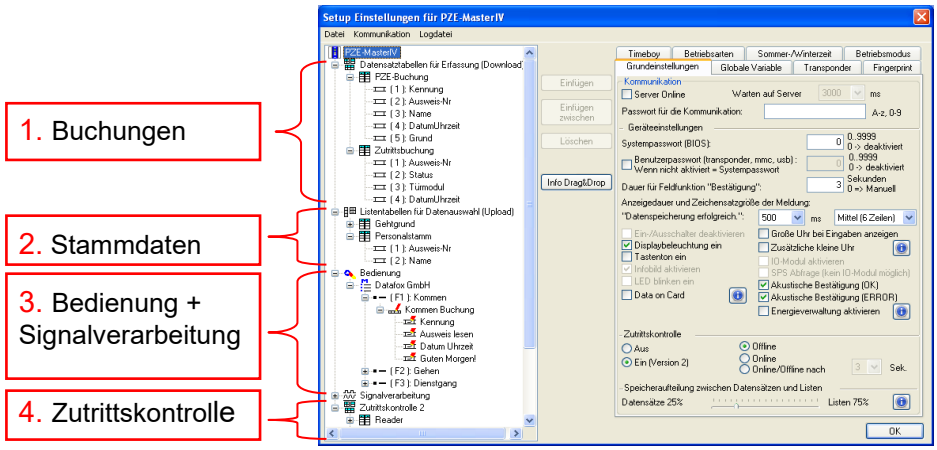


Mögliche Listen Ansicht.

Weitere Besipiele:

3. Erstellung eines Setups (Programm)

Die Erstellung des Setups erfolgt mit dem kostenlosen Tool „DatafoxStudioIV“.
Der Aufbau der Tabellen für Stammdaten und Buchungen, sowie die Bedienabläufe sind frei definierbar. ***Es sind keine Programmierkenntnisse notwendig.***



1. Legen Sie die Datenstruktur der Tabellen für die Buchungen individuell fest.

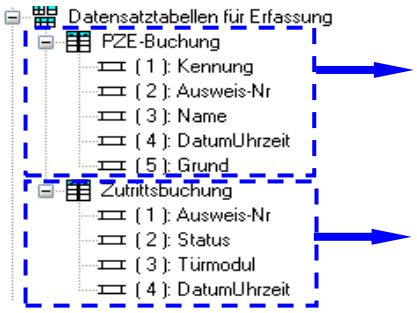


Tabelle: PZE - Buchungen (Datensatzbeschreibung)

Kennung	Ausweis-Nr	Name	Datum/Zeit	Grund
K	656556	M. Musterman	21.02.2013 12:31:15	0
K	656556	F. Muster	21.02.2013 12:32:45	0

Tabelle: Zutrittsbuchung (Datensatzbeschreibung)

Ausweis-Nr	Status	Türmodul	Datum/Zeit
056623665436366	20	M. Mustermann	21.02.2013 12:31:15
000001558996655	42		21.02.2013 12:32:45
1566959651001565	21	J. Müller	21.02.2013 14:12:05
0000489722102451	20	L. Klaus	21.02.2013 16:55:14

2. Legen Sie die Struktur der Tabellen für die Stammdaten fest.

Es können: 20 Datensatztabellen und 20 Listentabellen mit je 25 Feldern definiert werden

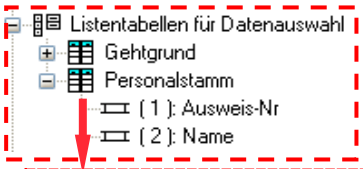
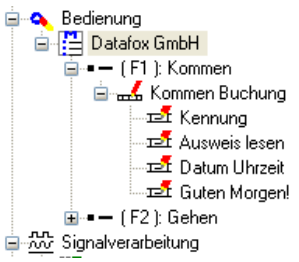


Tabelle: Stammdaten (Beschreibung)

Ausweis-Nr	Name
00799611485215	M. Mustermann
05597861113494	M. Musterfrau

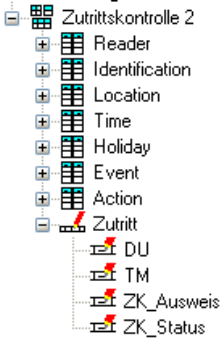
Listen sind z.B. Stamm- oder Auftragsdaten, die bereits existieren und in einer definierten Form (Listenbeschreibung) in das Gerät übertragen werden. Z.B. Personalstamm, Kostenstellen, Fertigungsaufträge, etc..
Diese Daten unterstützen die Datenerfassung durch die Möglichkeit eine Auswahl aus einer Liste durchzuführen oder Daten mit einer Liste zu vergleichen (Plausibilitätsprüfung).

3. Legen Sie die Bedienung und Signalverarbeitung fest.



- Menüs
- Textanzeigen
- Listenanzeigen
- Untermenüs
- RFID-Verfahren
- Art der Eingaben

4. Legen Sie die Zutrittskontrolle an



- Erfassungsreihenfolge
- Status
- online / offline

5. Übertragen Sie das Setup auf das Terminal.

6. Erfassen Sie Daten

4. Geräteschlüssel und Sicherheit

Es gibt bei den Datafox Geräte verschiedene Techniken das Gerät vor unqualifiziertem Zugriff zu schützen.

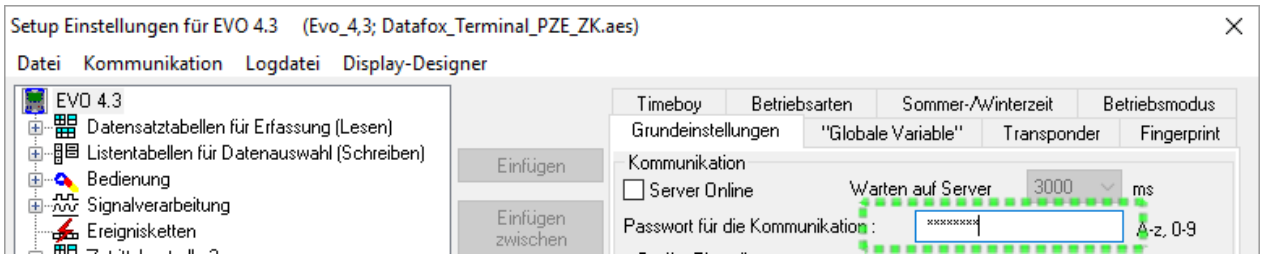
4.1. Gerätepasswörter

Die Gerätepasswörter dienen dazu, dass Geräte von Usern nicht ungewollt /versehentlich oder absichtlich in den Einstellungen für die Kommunikation oder Daten gelesen oder anderweitig manipuliert / Verstellt werden können.

Diese Einstellungen dienen nur zur Betriebssicherheit der Geräte und sollten unbedingt zum Standard gehören.
Diese Einstellungen haben nichts mit den Verschlüsslungspasswörtern zu tun.
Hierzu schauen Sie bitte in die Kapitel Verschlüsselung per http und DLL.

4.1.1. Kommunikationspasswort

Unsere Software „Datafox StudioIV“ ist auf der Homepage frei verfügbar.
Hiermit werden die Geräte von unseren Partnern konfiguriert.
Um einem Missbrauch oder einer Manipulation durch Nutzer zu verhindern, kann im Gerät ein Kommunikationspasswort hinterlegt werden. Nur wer dieses kennt, kann die Konfiguration des Gerätes ändern.
Das **Passwort** wird mit der Konfiguration (Setupdatei) an das Gerät übergeben.

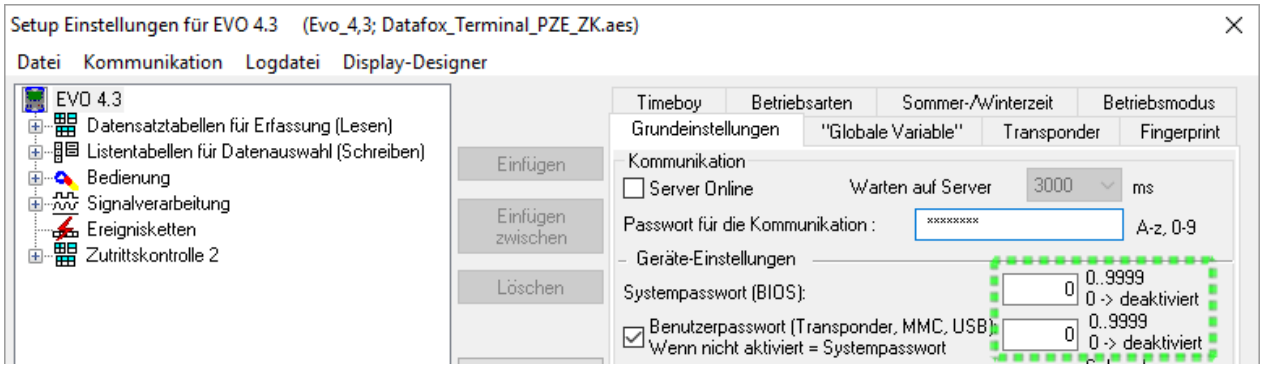


4.1.2. Bios Menü Passwort

Alle Geräte mit Display verfügen über ein Bios Menü, in dem Einstellungen vorgenommen werden können wie:

- IP-Adresse
- Kommunikationsart (GPRS, USB, TCP/IP) usw.
- Displayhelligkeit uvm.

Damit nicht jeder Zugang zu dem Bios-Menü hat, kann hier eine Passwortabfrage hinterlegt werden. Dieses Passwort wird dann mit der Konfiguration (Setup) an das Gerät übertragen.



4.2. WLAN Sicherheit

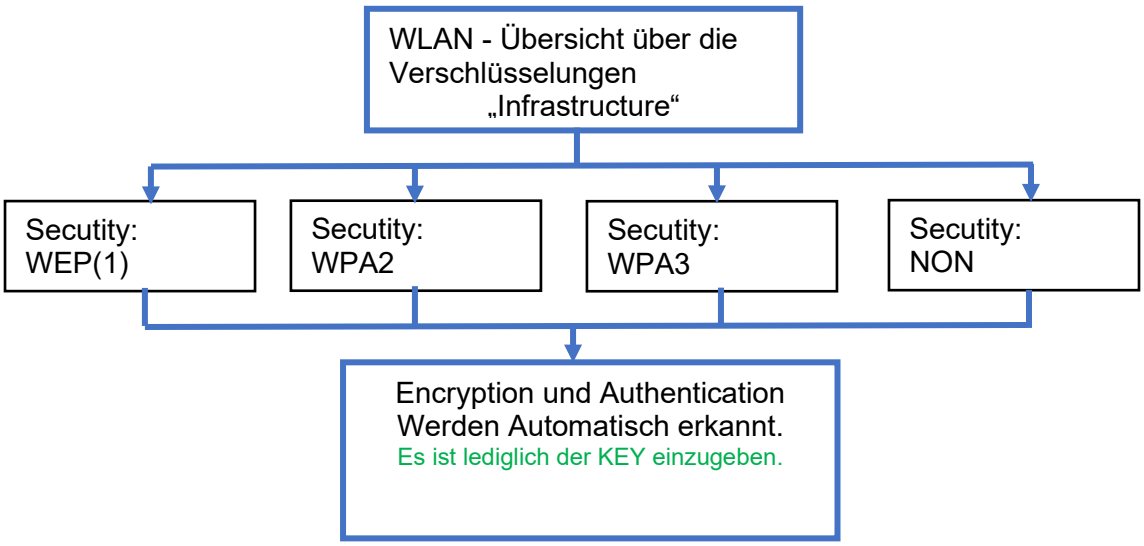
4.2.1. M111_WLAN ESP32-c3 ML01 (WLAN-Modul DF-WL03)

Diese Übersicht zeigt Ihnen, welche WLAN Verfahren unterstützt werden.

Das WLAN 3 Modul erkennt automatisch die Verschlüsselung des AP. Daher muss nur der Security Parameter Eingestellt werden. Die Anderen Parameter (Encryption und Authentication) werden automatisch erkannt.

Router die WPA3/WPA2 im Mixed Modus betreiben können bereits jetzt genutzt werden.

Unterstützt wird hier das 2.4Ghz Band.



Achtung:
Wir können nicht jeden auf dem Markt befindlichen Access-Point testen.
Daher ist es uns nicht möglich, einen Verbindungsaufbau zu jedem AP zu garantieren.

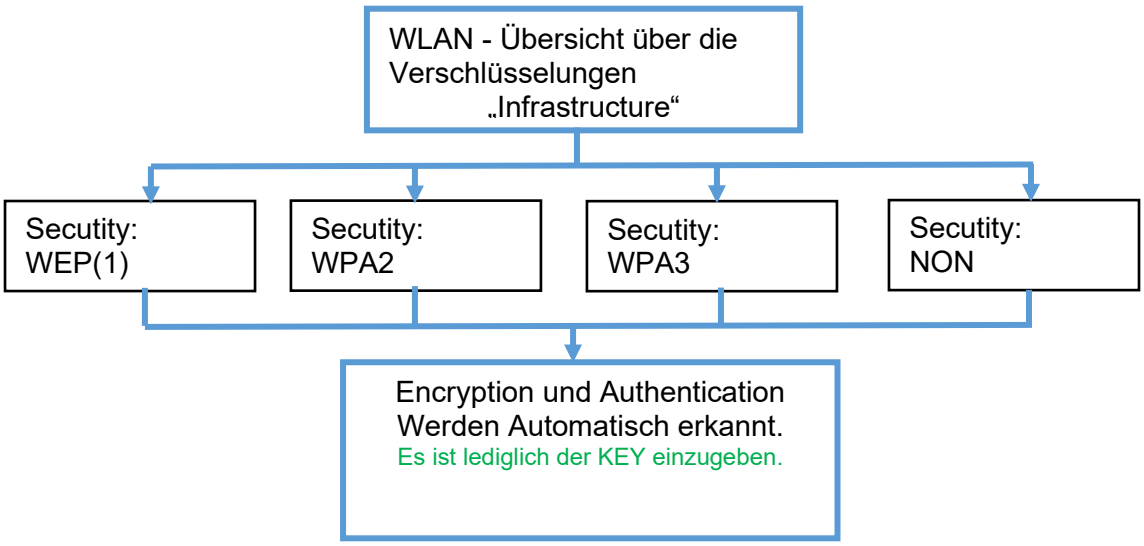
4.2.2. Texas Instruments TI-CC3135 (Generation 2)

Diese Übersicht zeigt Ihnen, welche WLAN Verfahren unterstützt werden.

Das TI-CC3135 Modul erkennt automatisch die Verschlüsselung des AP. Daher muss nur der Security Parameter Eingestellt werden. Die Anderen Parameter (Encryption und Authentication) werden automatisch erkannt.

Router die WPA3/WPA2 im Mixed Modus betreiben können bereits jetzt genutzt werden.

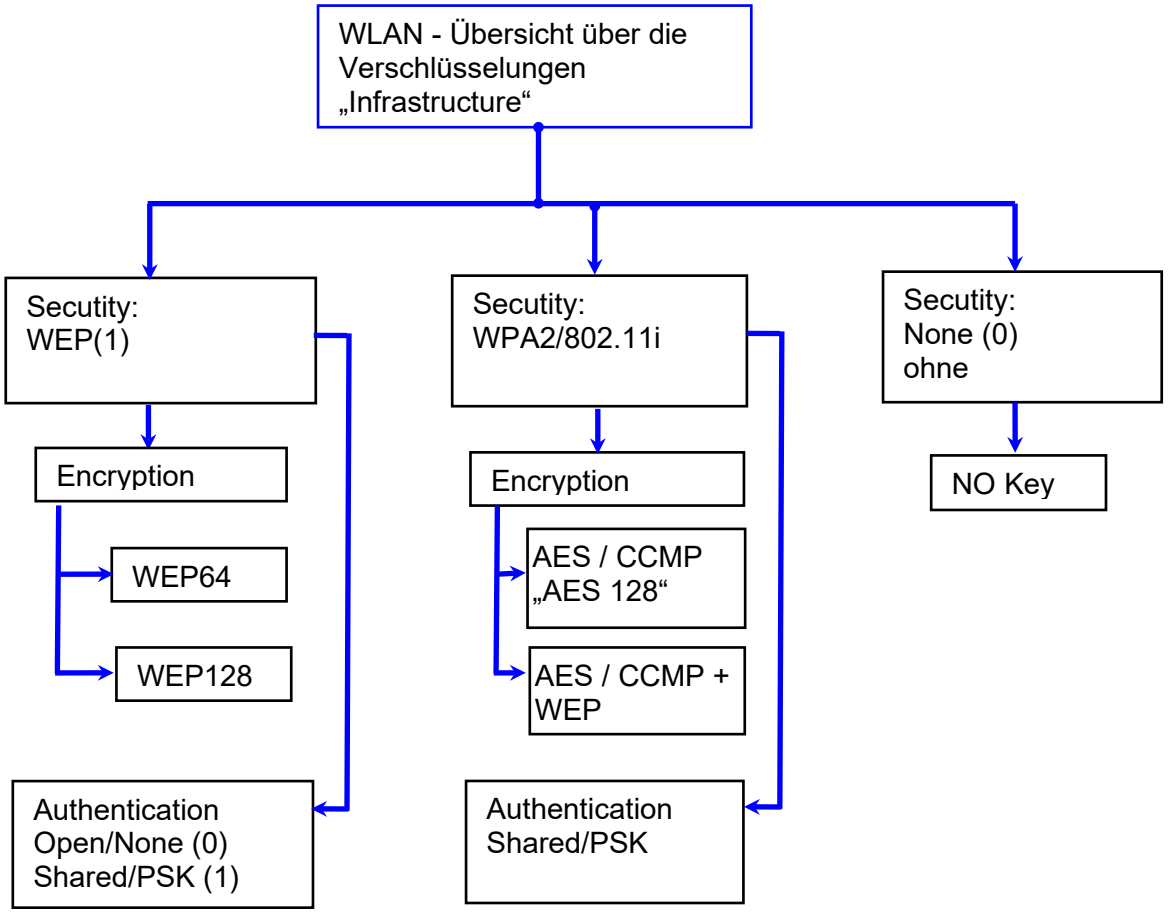
Im Fall, dass die Netze im 5Ghz und 2.4Ghz Band denselben Namen haben wird das Netz mit der besseren Empfangsqualität gewählt. Dies ist meistens das Netz im 2.4Ghz Band.



Achtung:
Wir können nicht jeden auf dem Markt befindlichen Access-Point testen.
Daher ist es uns nicht möglich, einen Verbindungsaufbau zu jedem AP zu garantieren.

4.2.3. Redpine (Generation 1)

Diese Übersicht zeigt Ihnen, welche WLAN Verfahren unterstützt werden.
Nicht Unterstützt wird WPA (Vorgänger vom WPA2).
Nicht Unterstützt wird multiple-input multiple-output (MIMO)
Nicht Unterstützt werden 5 GHz Verbindungen und auch keine Mischbetrieb 2,4GHz / 5 GHz.
Nicht Unterstützt wird die Authentifizierung via WPA2 Enterprise nach IEEE 802.1x



Unseren FAQ zu WLAN: https://www.datafox.de/support/faq

Achtung:
Wir können nicht jeden auf dem Markt befindlichen Access-Point testen.
Daher ist es uns nicht möglich, einen Verbindungsaufbau zu jedem AP zu garantieren.

Achtung:
multiple-input multiple-output (MIMO) wird nicht unterstützt. Wenn Sie den AP von b/g/n zu b/g umschalten, wird automatisch nur SISO verwendet.
https://en.wikipedia.org/wiki/Single-input_single-output_system

Bei der Einstellung der Verschlüsselung AES oder WEP wird immer nur eine Art verwendet.
Die Einstellung AES+WEP bedeutet bei machen APs, dass erst eine AES Verschlüsslung durchgeführt wird und danach noch zusätzlich mit WEP verschlüsselt wird.
Stellen Sie für diesen Fall nur AES ein.

5. Beschreibung der einzelnen Kommunikationstechniken

5.1. Übersicht über die Kommunikationstechniken

Diese Übersicht gilt für alle Mikrocontroller-Geräte der MasterIV-Serie und EVO-Serie, sowie für die in den Industrie-PCs integrierten Embedded-Baugruppen.
(Hinweis: Die in den Industrie-PCs integrierten Embedded-Baugruppen können alternativ auch im HID-Modus betrieben werden.)

Direkte Einbindungsmöglichkeiten in Ihre Software über:

DLL Einbindung
DFCom API
„Passiv-Mode“
= Polling
(kostenfrei)

DLL Einbindung
DFCom API
„Activ-Mode“
Daueraktive Verbindung zum Terminal
(kostenfrei)

„http(s)“
Level 1
Automatisches Senden der Daten an einen Webserver und Stammdaten Übertragung
(kostenfrei)

Anbindung über unser SW Datafox Connect (Gerätemanagement SW)
Zur Kommunikation zwischen Datafox Geräten und einer Management-Software stehen drei Möglichkeiten zur Verfügung:

Datafox Connect Remote-Modus
Datenaustausch über Dateiablage oder Datenbank.
(Lizenz erforderlich)

Datafox Connect Transparent-Modus
Datenaustausch über eine bereits integrierte SW.
(Lizenz erforderlich)

Datafox Connect Parallel-Modus
(Lizenz erforderlich)

5.2. Funktionsübersicht der Kommunikationstechniken

Zugriff auf: / Beschreibung		DLL Einbindung Polling	DLL active-Mode	http Level 1	Connect		
					Remote	Transpa-rent	Parallel
Datensätze	Erzeugte Daten aus der Er-fassung	✓	✓	✓	✓	✓	✗
Stammda-ten übertragen	Personallisten Artikelstamm -Aufträge	✓	✓	✓	✓	✓	✓
System	-Firmware -Sprache -Farbe/Anzeige	✓	✓	✓	✓	✓	✓
System	- Setup	✓	✓	✓	✓	✓	✓
GV globale Variablen	8 x freie Verwendung	✓	✓	✓	✓	✓	✓
System-variablen	http COM I/O	✓	✓	✓	✓	✓	✓
Message an das Gerät	Direkte Anzeige des Textes auf dem Display	✓	✓	✓	✓	✓	✓
Online Modus		✓	✓	✓	✓	✓	✗
Zutritt nur Online	Alle Zutrittsberechti-gungen werden direkt vom Server entschieden	✓	✓	✓	✓	✓	✗
Zutritt im Wechsel-online off-line	„Server offline“ = automatischer Wechsel in Ofline-Mode	✓	✓	✓	✓	✓	✗
Zutritt offline	Das Gerät greift auf eigene ZK-Listen zu	✓	✓	✓	✓	✓	✓
Zutritt Online mit Vorprüfung	Das Gerät greift auf eigene ZK-Listen zu und meldet die Ent-scheidung zum Server. Dieser kann dann noch anders entscheiden.	✓	✓	✓	✓	✓	✗
Aktualität der Daten ca. in Sekun-den	Wie schnell stehen die erzeugten Daten zur Verfügung	Abhängig, wie oft die Daten abgeholt werden	Meldung „Datensätze vorhanden“ < 1s	< 1s HTTP über Lan 1-2s über GPRS	Aktive, https <1s Bzw. abhängig von der Ein-stellung im Connect		Nicht rele-vant.
Download Hinweise Zusatzinfo		Downlaod: Windows Linux	Downlaod: Windows Linux	Download Hinweise/Info			

✗ Kontrolle über Connect nicht möglich.

✓ nicht möglich bei Ablage der Daten über Dateiebene!

6. Kommunikation per DFCom API (DLL)

6.1. Programmbibliothek [Dynamic Link Library (DLL)] – Allgemeines

6.1.1. Was ist eine Programmbibliothek?

„Eine Programmbibliothek bezeichnet in der Programmierung eine Sammlung von Unterprogrammen, die Lösungswege für thematisch zusammengehörende Problemstellungen anbieten. Bibliotheken sind im Unterschied zu Programmen keine eigenständig lauffähigen Einheiten, sondern Hilfsmodule, die von Programmen angefordert bzw. aufgerufen werden.“

Wikipedia zu Programmbibliothek

Um die Funktionen (Unterprogramme) der Programmbibliothek ansprechen zu können, muss sie in Ihre Softwarelösung eingebunden werden. Hierbei ist je nach Entwicklungsumgebung eine gewisse Vorgehensweise notwendig. Prinzipiell ist allen eines gemeinsam: die benötigten Funktionen müssen Ihrer Softwarelösung bekannt gegeben werden (sie sind zu Deklarieren).

6.1.2. Vorteile einer Programmbibliothek in DLL- oder so-Form.

Hier spez. für die Datafox-DLL.

- Die Einbindung über eine DLL ist einfacher und schneller als die direkte Einbindung eines Protokolls.
- Kann von der Programmiersprache unabhängig verwendet werden.
- Einheitliche Programmschnittstelle (API) zu den unterschiedlichen Datafox-Geräten.
- Die DLL gibt definierte Fehlermeldungen aus, wenn Funktionen nicht korrekt ausgeführt werden können.
- Die DLL schreibt automatisch Logfiles für das Debugging.
- Aktualisierbar ohne Neuerstellung Ihrer Softwarelösung. Abwärtskompatibel.

6.1.3. Die Kommunikations-Bibliothek ist für folgende Systeme verfügbar:

- Als DLL für Windows 32bit, DFComDLL.dll; 64bit, DFCom_x64.dll
- Als Shared Library oder Static Library für Linux 32/64bit libDFCom.so (Makefile)

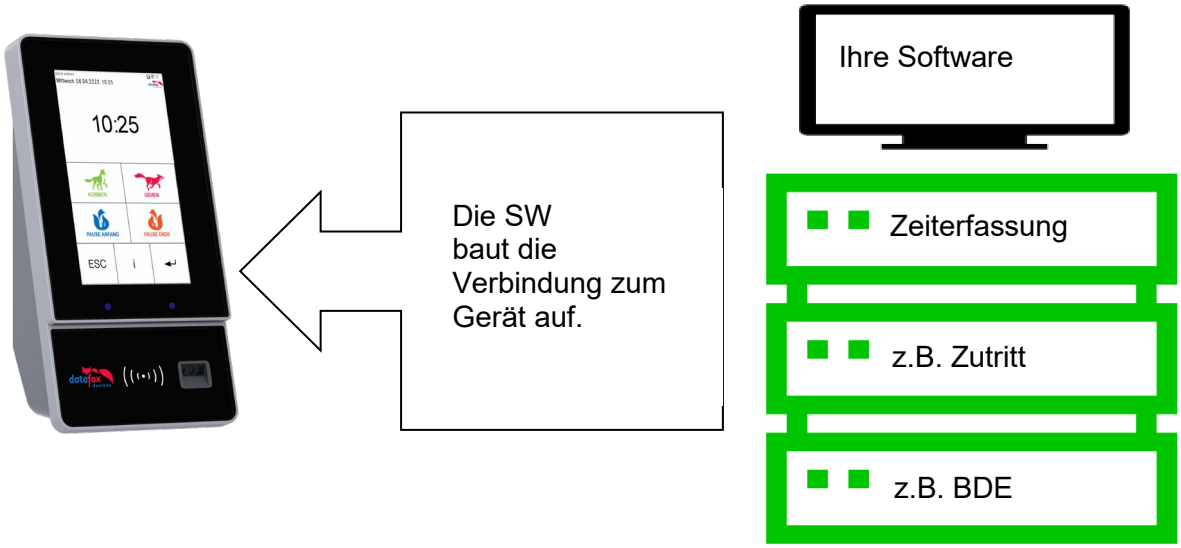
Hier die Download Links:

https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.23-Dokumentation.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.23-Source.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.23-x64.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.23-x86.zip

6.1.4. Programmbibliothek (DLL) - Einbindung Passiv-Mode (Polling)

Im Passiv-Mode wird die Kommunikationsverbindung von der Programmbibliothek ausgehend zu den Geräten hergestellt. Hierfür benötigten Sie eine einzelne Funktion zum Verbindungsaufbau und eine weitere zum Verbindungsabbau.

Funktionsprinzip beim Übertragen der Buchungen:
Die Anwendung fragt die Geräte über die DLL regelmäßig an, um die Daten abzuholen.



Folgende Verbindungstypen werden durch den Passiv-Mode unterstützt:
- USB (über virtuellen COM-Port)
- TCP / IP (LAN / WAN / WLAN)

Exemplarischer Abruf einer Geräteseriennummer bei einem über TCP / IP eingerichteten Gerät mittels Programmiersprache C:

```
int err, serial;
DFCComOpenIV( 5, 0, 3, "192.168.0.3", 8000, 3000 );
DFCGetSeriennummer( 5, 254, &err, &serial );
DFCComClose( 5 );
```

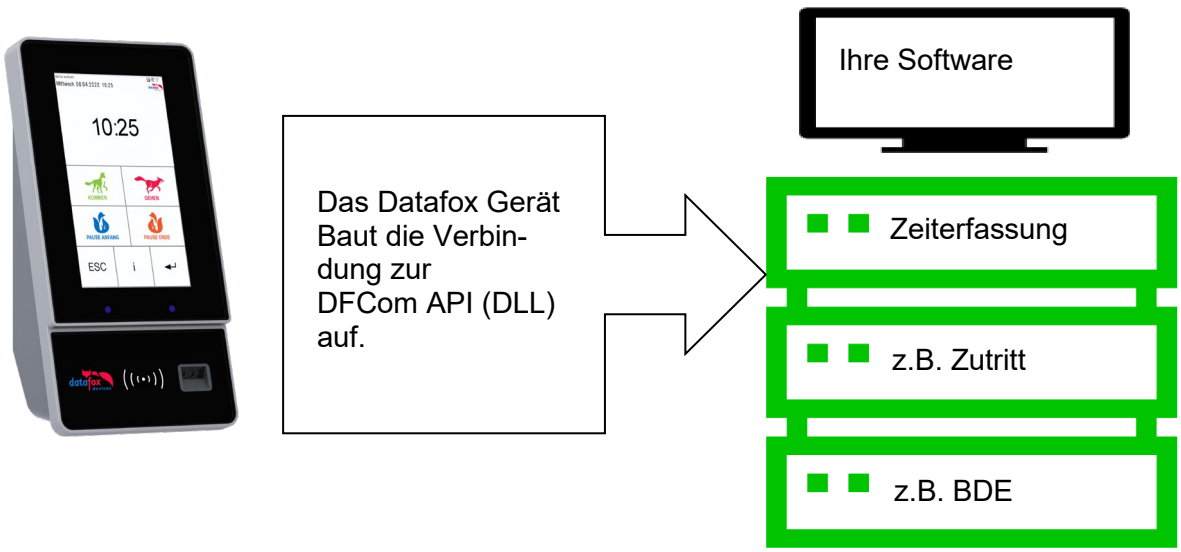
Vorteil:
- Alle Verbindungstypen und Gerätearten werden unterstützt.
- Alle Funktionen der Programmbibliothek stehen Ihnen uneingeschränkt zur Verfügung.

Nachteile:
- Möchte man die generierten Datensätze sofort nach Erstellung erhalten ist eine ständige Kommunikation mit dem Gerät notwendig (Polling). In TCP / IP Netzwerken kann dieses, je nach Geräteanzahl, eine unerwünschte Einbuße von Bandbreite bedeuten.
- Nicht zu empfehlen beim Mobilfunkübertragungen, weil dann hohe Kosten entstehen können.

6.2. Programmbibliothek (DLL) - Einbindung Active-Mode (Aktive Verbindung)

Im Active-Mode wird die Kommunikationsverbindung von den Geräten zur Programmbibliothek hin hergestellt. Zuvor muss den Geräten über die Einrichtung mitgeteilt werden wohin sie sich verbinden sollen. Bei der Programmbibliothek benötigten Sie eine einzelne Funktion zum Start des Active-Mode und eine weitere zum Beenden des Active-Mode.
Die Funktion „DFCStartActiveConnection“ ersetzt hierbei die Funktion „DFComOpenIV“ beim Passiv-Mode.
Nach Aktivierung des Active-Mode in der Programmbibliothek wartet diese auf eingehende Verbindungen und stellt diese dann für weitere Bearbeitungen Ihrer Anwendung zur Verfügung.

Funktionsprinzip beim Übertragen der Buchungen:
Die Geräte melden sich bei der DLL an. Diese schreibt eine Liste der angemeldeten Geräte. Hat ein Gerät eine Buchung sendet dieses einen Trigger an die DLL. Die Anwendung reagiert auf die Trigger und holt die Buchung. Die dafür notwendigen Verbindungsdaten stehen in der Anmeldeliste. Das Abholen der Buchung erfolgt mit den gleichen Funktionen wie beim Pollen. Dadurch unterscheiden sich Pollen und aktive Verbindung beim Abholen der Daten nur wenig.



Folgende Verbindungstypen werden durch den Active-Mode unterstützt:
- TCP / IP (LAN, WAN, WLAN, Mobilfunk G2, G3, G4, LTE)

Vorteile:
- Die Geräte melden sich selbstständig an und melden auch vorliegende Datensätze.
- Die Anwendung muss keine Geräteliste führen, weil sich die Geräte automatisch bei der DLL anmelden und die DLL eine Liste der aktiven Geräte zur Verfügung stellt.
- Alle Funktionen der Programmbibliothek stehen Ihnen uneingeschränkt zur Verfügung.

Nachteil:
- Da hier das Multimaster-Prinzip notwendig ist, wird diese Verbindungsart nur vom Verbindungstyp TCP/IP unterstützt.

Mehr Informationen und Unterlagen finden Sie hier:
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.23-Dokumentation.zip

6.3. Verschlüsselung der Daten bei der Verwendung der DFCom.dll

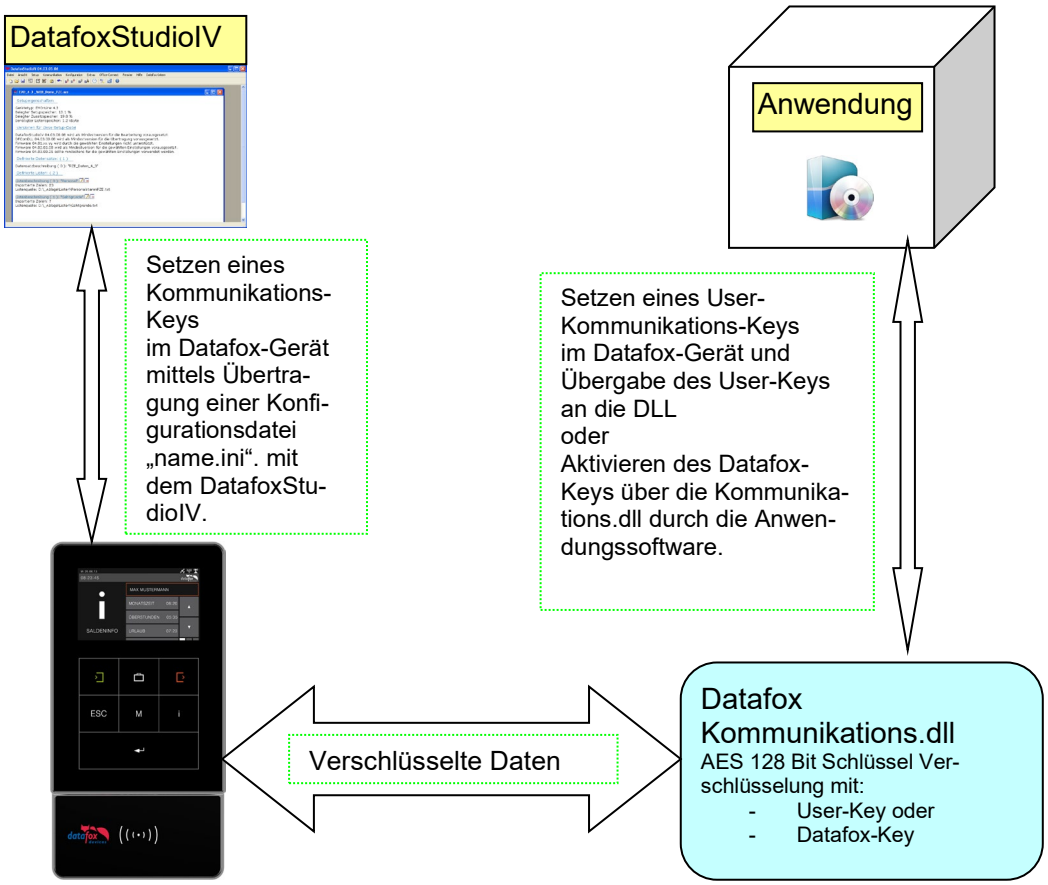
Bei der Verwendung der Datafox Kommunikations- DLL können alle Daten die von Gerät kommen oder zum Gerät gesendet werden, mit einer AES 128 Bit Verschlüsselung übertragen werden.

Es gibt damit nun 3 Arten der Kommunikation:

1. Unverschlüsselte Kommunikation
2. Verschlüsseln mit Datafox-Key
3. Verschlüsseln mit User-Key

Bei der Integration der Datafox DFCom.dll muss von der Seite der Anwendung nur ein User-Kommunikationsschlüssel an die .dll übergeben werden. Der Aufwand der Einbindung einer Verschlüsselung ist somit sehr gering.

Übersicht über die Verschlüsselung, schematische Darstellung.

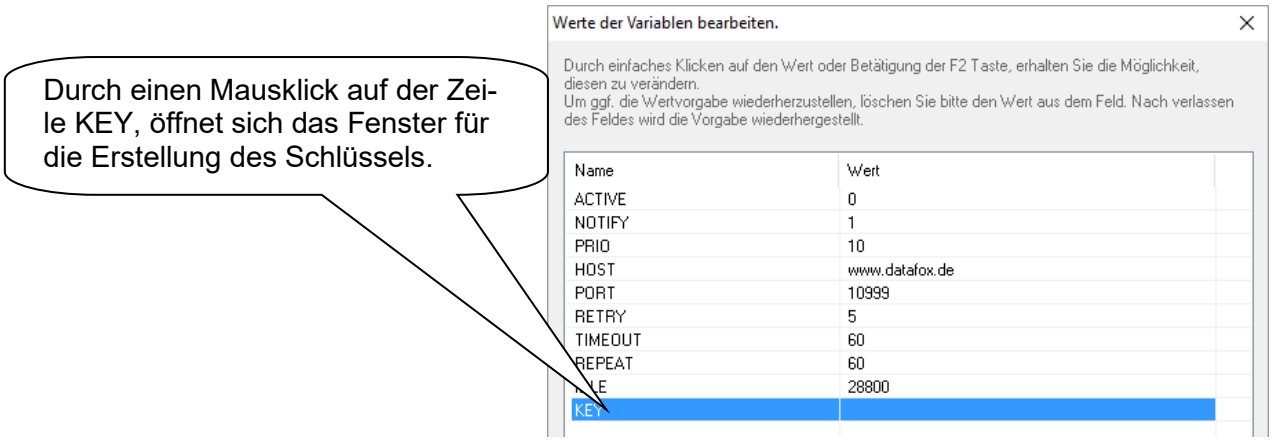


Eine detaillierte Beschreibung, wie die Übergabe des Schlüssels erfolgt, finden Sie:

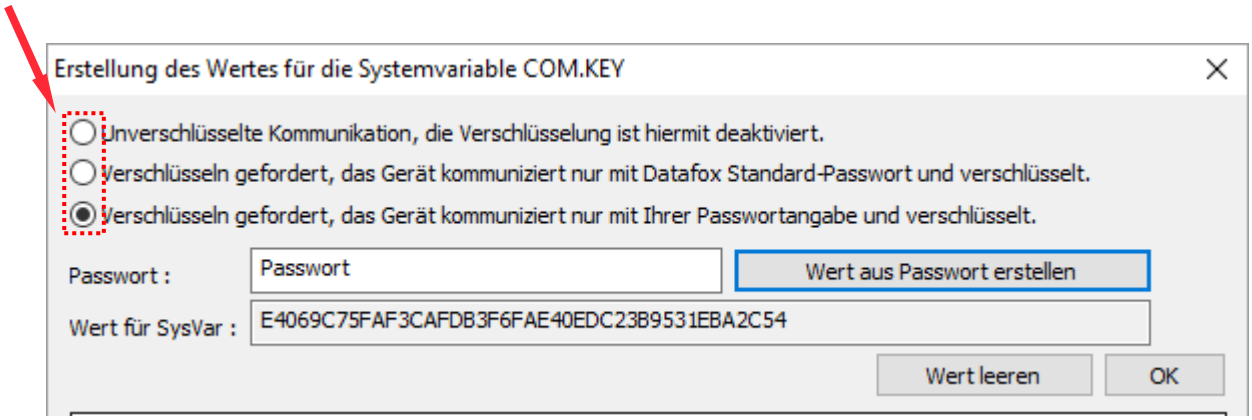
- für das Datafox StudioIV im Handbuch unter dem Kapitel „Verschlüsselung der Kommunikation mit MasterIV Geräten“
- und für die DLL in der DLL-Dokumentation

6.3.1. Erstellung und Hinterlegen des Schlüssels im Gerät

Unter dem Menüpunkt Konfiguration „Systemvariablen Aktive Verbindung“ öffnen Sie bitte die Konfigurationsdatei (z.B.: active.ini) zum Bearbeiten.



Hier können Sie zwischen den Kommunikationsvarianten wählen



Möchten Sie, dass die Kommunikation mit einem eigenen hinterlegten Passwort verschlüsselt wird, geben Sie ein Passwort ein und klicken auf den Button „Wert aus Passwort erstellen“.

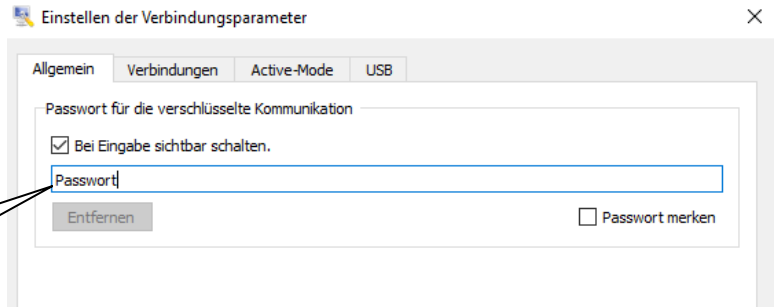
Es wird nun ein Kommunikationsschlüssel erstellt. Schließen Sie die Eingabe mit „OK“ ab.
Nach der Erstellung eines Schlüssels und Übertragung der Datei active.ini, wird nur noch unter Angabe des Passwortes eine Kommunikation zum Gerät zugelassen.

6.3.2. Hinterlegen des Passwortes im Datafox StudioIV

Ist bei einem Gerät ein Kommunikationsschlüssel hinterlegt, so muss das Passwort im Datafox StudioIV auch angegeben werden, da sonst keine Kommunikation mit dem Datafox Gerät möglich ist.

Unter dem Menüpunkt „Kommunikation-> Einstellungen“ auf dem Reiter „Allgemein“ kann das Passwort hinterlegt werden.

Das Passwort gilt für alle Kommunikationsarten.



Geben Sie hier Ihr Passwort ein.

Das Passwort kann durch die Option „Bei Eingabe sichtbar schalten“ in Klartext angezeigt werden.

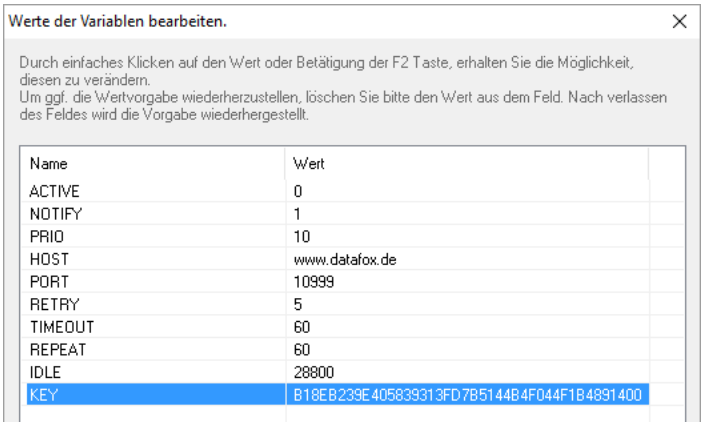
6.3.3. Übergabe des Schlüssels in die DFComDLL

Der Schlüssel wird über die DLL-Routine DFCSetCommunicatonPassword gesetzt. Hierbei handelt es sich um den „echten“ Schlüssel (private Key), nicht der, der über das Datafox StudioIV generiert wurde. Der Schlüssel wird im Klartext übergeben.
Mehr dazu finden Sie in der Dokumentation für die DFComDLL.

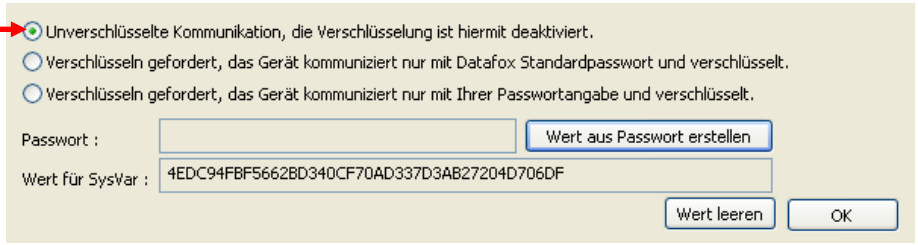
6.3.4. Löschen des Kommunikationsschlüssels

Ist ein Kommunikationsschlüssel hinterlegt, wird dieser wie folgt gelöscht.

Klicken Sie auf KEY, um diesen zu bearbeiten.

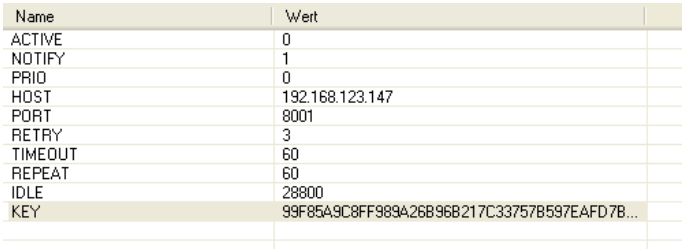


Schalten Sie auf



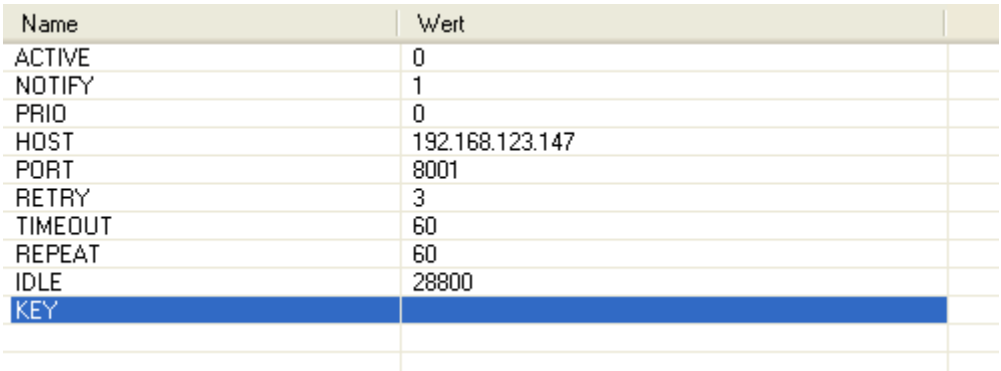
Klicken Sie anschließend auf „Wert leeren“.
Danach klicken Sie auf „Wert aus Passwort erstellen“. Dieser „leere Wert“ ist notwendig, um das Passwort im Gerät zu löschen.

Speichern Sie die Datei und übertragen diese an das Gerät.



Name	Wert
ACTIVE	0
NOTIFY	1
PRIO	0
HOST	192.168.123.147
PORT	8001
RETRY	3
TIMEOUT	60
REPEAT	60
IDLE	28800
KEY	99F85A9C8FF989A26B96B217C33757B597EAFD7B...

Anschließend können Sie auch den „KEY“ ganz aus der .ini-Datei löschen.



Name	Wert
ACTIVE	0
NOTIFY	1
PRIO	0
HOST	192.168.123.147
PORT	8001
RETRY	3
TIMEOUT	60
REPEAT	60
IDLE	28800
KEY	

7. http Level 1

7.1. Voraussetzungen

Voraussetzung für die Übertragung der Daten via http Level 1:

Hardware V4:

- Gerät mit TCP/IP (LAN / WLAN) oder Mobilfunk
- Mindestfirmware 04.03.19.XX

Software:

- Server muss einen http-Request entgegennehmen und eine aktive Antwort geben
- Server muss Stammdaten wie Personallisten oder Auftragslisten zum Download bereitstellen

Hinweis:
Sollten Sie noch Geräte älterer Bauart haben, können diese umgerüstet werden.

http Level 0 finden Sie noch in der SDK http(s)

Eine Detaillierte Beschreibung für Ihre Entwicklung finden Sie hier:
Link: https://www.datafox.de/download/Datafox%20Datenprotokoll%20zur%20HTTP(S)-Kommunikation.pdf

7.1.1. Request

Anfrage des Client an den Server.

7.1.1.1. Methode: GET

Für die Kommunikation via http Level 1, hat Datafox einen spezifischen Kontext entwickelt der nur für Datafox Geräte gilt.
Zur http-Kommunikation wird die Methode GET verwendet.
Über den Kontext werden nun umfangreiche Möglichkeiten geboten, um mit den Datafox Geräten Daten komfortabel und schnell auszutauschen.

Funktionsübersicht über GET:

Parametername	Bedeutung
df_table	Name der Datensatzbeschreibung
df_record_state	online / offline Kennung des Datensatzes
df_col_{Feldname}	Der Name des Daten-Feldes und Wert. Entsprechend der Gerätekonfiguration „Setup“.

7.1.2. Response

Antwort des Servers an den Client.
Jeder Datensatz von einem Datafox Gerät muss vom Server quittiert werden.
Die Quittierung erfolgt mit:
df_api=1 und HTTP–Result „200 OK“

7.1.2.1. Optionale Parameterangaben bei der Antwort

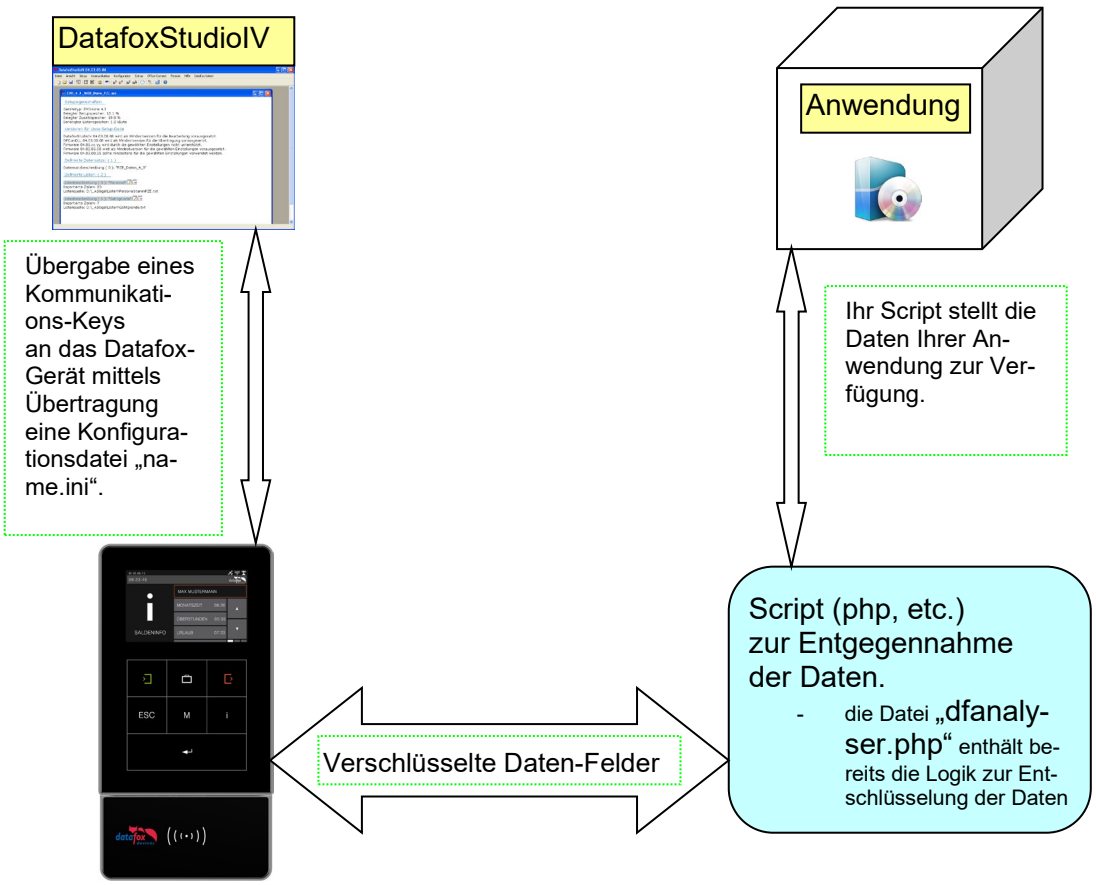
Parametername	Bedeutung
df_time=2016-11-17T12:13:14	Datum Uhrzeit am Gerät stellen.
df_beep=1 (1-11)	OK-Signal / Beep am Gerät erzeugen
df_service=1,www.datafox.de,10047	Verbindung zur DLL herstellen. Auch zum Datafox StudioIV möglich. Angabe von IP/URL und Port möglich.
df_var=setup.1,wert	Wert einer GV im Setup ändern.
df_ek=name	Eine Aktion im Gerät auslösen. Starten eine Ereigniskette in der Signalverarbeitung.
df_msg=Dieses\rist\reine\rNachricht,5,1,0	Textnachricht auf das Display senden.
df_msg_icon=2	Stelle folgende Nachrichten auf dem Display mit dem Icon einer F-Kette (hier F2) dar.
df_backlight=0,5,255,255,0,192	Stellt ein Geräte-Backlight für eine gewisse Zeit, auf eine bestimmt Farbe (RGBW) ein.
df_info_msg=Info\rNachricht,0	Stellt die Info-Nachricht des Geräts ein.
df_ac2=010,1,10,20,5	AC = access control. Aktionen in der Zutrittskontrolle auslösen.
df_custom_msg_ac2=010,1,1,0,Hallo%20Welt	Sendet eine Nachricht an einen Bus-Teilnehmer in einer Zutrittskontroll-Installation
df_ao_ac2=0,1234	Quittiert eine Aktion der Zutrittskontrolle mit Vorprüfung
df_trigger_ac2=1,011,6543210,0	Simuliert den Eingang einer Buchung von einem Leser am ZK-Controller
df_kvp=var,ID	Fordert einen Wert vom Gerät an. Dieser wird dann als Key-Value-Paar an den Server übermittelt.
df_set_relay=2,close,5	Setzt den Zustand eines nicht von der Zutrittskontrolle verwendeten Relais
df_toggle_relay=2,5	Ändert den Zustand eines nicht von der Zutrittskontrolle verwendeten Relais
df_load_file=/path/on/server	Veranlasst das Herunterladen einer Datei vom Server
df_send_file=/logs/,syslog,0	Veranlasst das Übermitteln einer Datei an den Server

Parametername	Bedeutung
df_remove_file=root:datafox.cert	Veranlasst das Löschen einer Datei durch das Gerät
df_remove_finger=1980,all	Löschen von Fingern aus dem Fingerprint-Sensor
df_setup_list=Personal,/Pfad/zur/liste.txt	Dem Gerät eine neue Liste z.B. Personal geben
df_ac2_list=Identification,/pfad/zur/liste.txt	Dem Gerät eine neue Liste ZK-Liste geben
df_table_count=list.PID	Liefert die Anzahl der Einträge in einer Liste
df_table_select=list.PID,/upload/form,Abteilung=Entwicklung,PID=5	Wählt einen oder mehrere Datensätze aus einer Liste zum Upload aus
df_table_append=list.PID,9999,,Besucher,	Fügt einen Datensatz an eine Liste an
df_table_update=list.PID,,,Abteilung=	Ändert Werte in einer Liste
df_table_delete=list.PID,Abteilung=Entwicklung	Löscht Zeilen aus einer Liste

7.1.3. Verschlüsselung

Werden Datensätze über HTTP versendet, können die Feldinhalte verschlüsselt übertragen werden. Die Datenfelder des Datensatzes werden dann mittels einer RC4-Verschlüsselung chiffriert. Die so verschlüsselten Zeichen werden in Hexadezimaldarstellung als Feldinhalt übertragen.

Übersicht über die Verschlüsselung bei HTTP; schematische Darstellung:



Eine detaillierte Beschreibung wie die Übergabe des Schlüssels erfolgt, finden Sie:

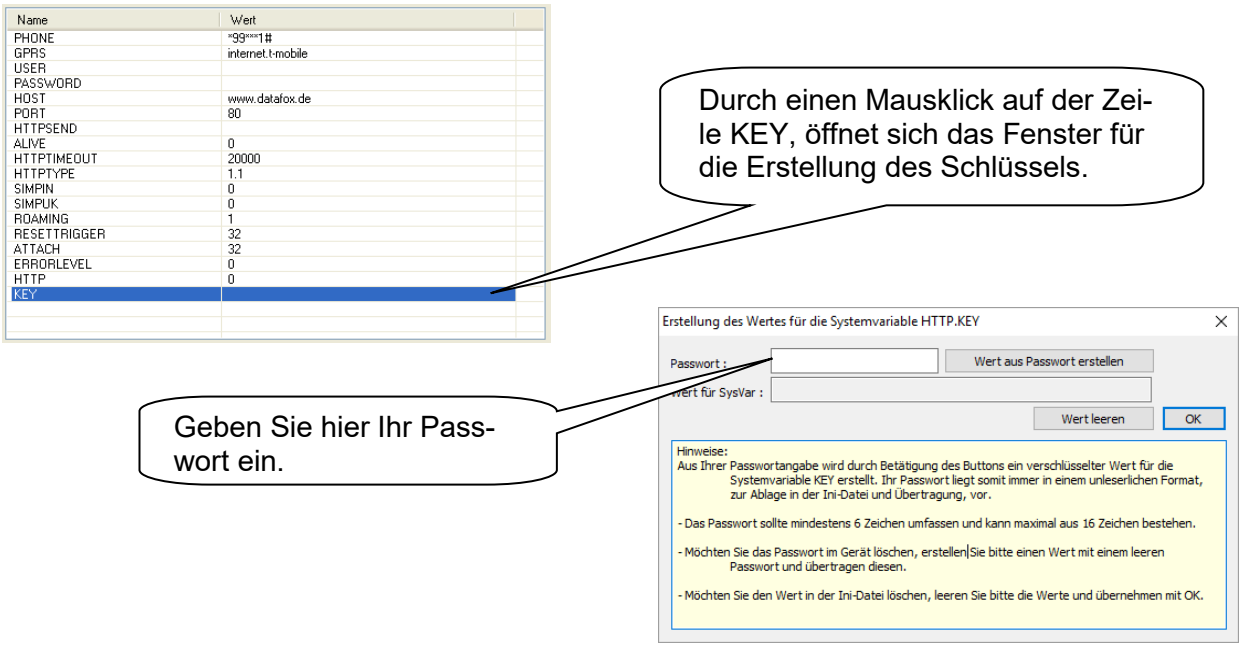
- für das Datafox StudioIV im Handbuch unter dem Kapitel „Verschlüsselung der Datenfelder beim Versand per HTTP“
- und die Datei „dfanalyser.php“ finden Sie im Download Software für Windows

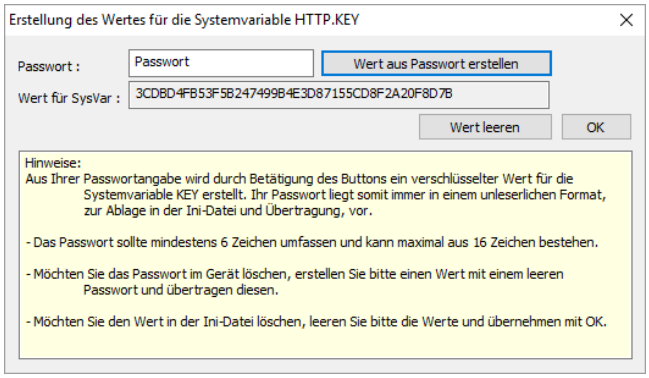
Hinweis:
Verwenden Sie die Verschlüsselung für mehrere Mandanten, so müssen Sie eine Man-danten-Kennung im Klartext übergeben.
So sind Sie in der Lage pro Mandant einen unterschiedlichen zu verwenden.

PORT	80
HTTPSEND	GET /getdata.php?Mandant=1024&
ALIVE	60

Aktivierung der Verschlüsselung über das Datafox StudioIV

Unter dem Menüpunkt Konfiguration „GPRS / HTTP – Konfiguration“ öffnen Sie bitte die Konfigurationsdatei (z.B.: GPRS.ini) zum Bearbeiten.





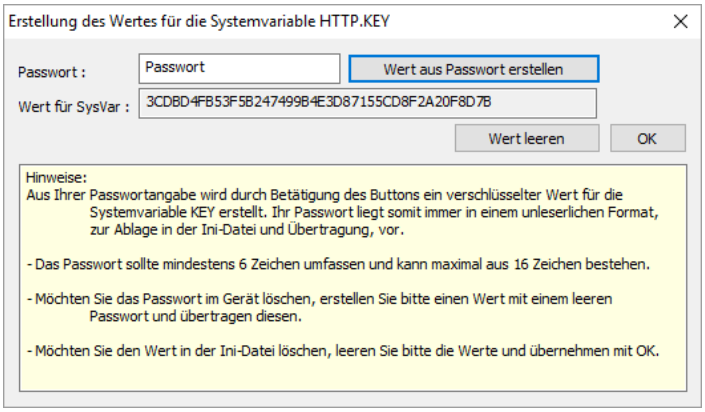
Mit dem Button „Wert aus Passwort erstellen“, wird ein Schlüssel für die Übertragung generiert.

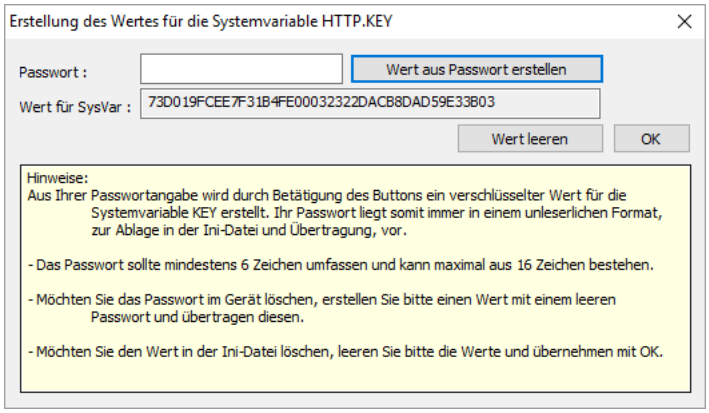
Klicken Sie auf „OK“, um den Schlüssel zu übernehmen.
Anschließend können Sie die Einstellung speichern und an das Datafox Gerät übertragen.

Verschlüsselung deaktivieren

Um den an das Gerät übertragenen Schlüssel wieder zu deaktivieren, ist es notwendig ein leeres Passwortfeld mit dem Button „Wert leeren“ zu erstellen und diesen leeren Schlüssel an das Gerät zu übertragen.

Klicken Sie auf „Wert leeren“

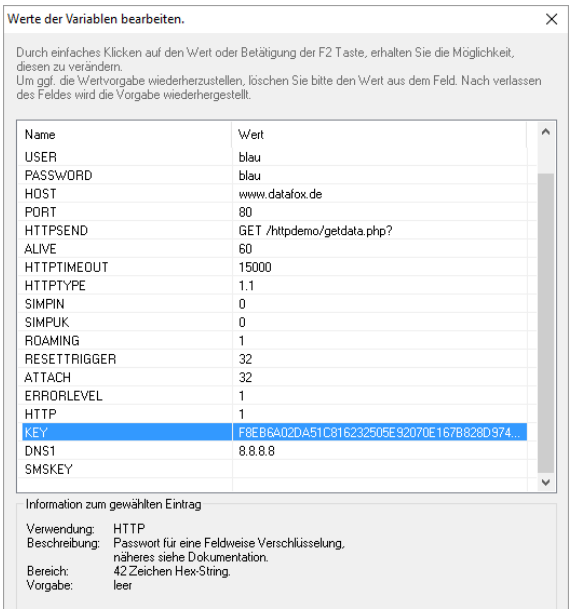




Klicken Sie auf „Wert aus Passwort erstellen“
Nun wird ein Schlüssel aus einem „leeren“ Wert erstellt.

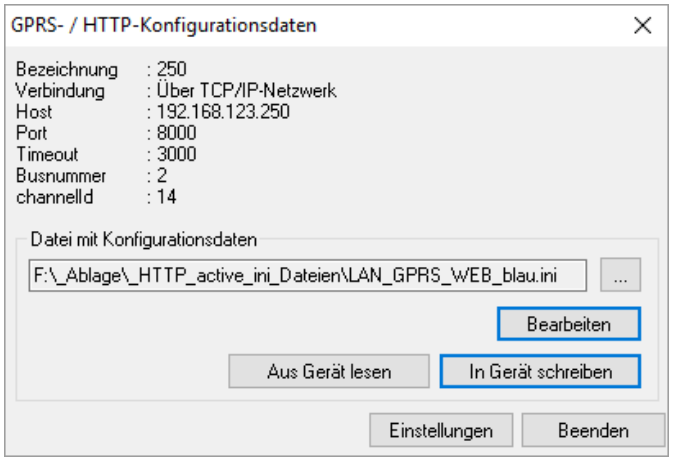
Dann klicken Sie auf „OK“

Speichern Sie die Datei mit dem neu generierten Schlüssel.



Klicken Sie auf „In Gerät Schreiben“.

Nun wird der Schlüssel im Gerät gelöscht.



Die Datensätze werden dann wieder unverschlüsselt gesendet.
Danach können Sie den gespeicherten Key aus der .ini - Datei löschen.

Die Datenfelder des Datensatzes können mittels eines Streamchiffre RC4 verschlüsselt werden. Dabei werden die Feldinhalte dann in ihrer Hexadezimaldarstellung übertragen.

Parametername	**Bedeutung**
df_cb	Der Parameter gibt an, dass alle folgenden Felder bis einschließlich *df_ce* verschlüsselte Feldinhalte haben. Der Wert von *df_cb* enthält den vierstelligen (1000-9999) Public-Key des anzuwendenden Passwortes für den Streamchiffre.
df_ce	Der Parameter gibt an, dass alle folgenden Felder keine verschlüsselten Feldinhalte mehr haben. Wird der Wert korrekt entschlüsselt muss er mit dem Wert von *df_cb* übereinstimmen.

7.1.3.1. Veranschaulichung der GET-Anfrage

Im Klartext (unverschlüsselt) und verschlüsselt:

Klartext Anfrage
df_api=1&df_record_state=1&df_table=Booking&df_col_sn=2042&df_col_recordtype=1&df_col_badge=3974679390&df_col_timestamp=2017-11-22T08:23:39&df_col_status=online
Klartext Antwort
df_api=1&df_time=2017-11-22T08:24:00
Verschlüsselte Anfrage
df_api=1&df_cb=6102&df_record_state=CC&df_table=66E9B37516AA8C&df_col_sn=0BDC8F79&df_col_recordtype=AB&df_col_badge=AF9B3A929994A5BD7D88&df_col_timestamp=B237B8CA4FA80FD563359C3EE70FE7FC99AF60&df_col_status=9BACFC1E5E0B&df_ce=A344D33B
verschlüsselte Antwort
df_api=1&df_cb=6102&df_time=e1ba6575855619c4d634f7865c01c4b2bc2ec138670ac2&df_ce=a414ebd6

7.1.3.2. Erkennung einer Verschlüsselung

Um zu erkennen, ob die Datenfelder verschlüsselt versendet werden, wird der Anfang der Verschlüsselung mit ‚df_cb' (Datafox Crypt Begin) gekennzeichnet und mit ‚df_ce' (Datafox crypt end) das Ende gekennzeichnet. ‚df_cb' stellt das erste Feld im Request und ‚df_ce' das letzte Feld im Request dar.

Der Wert des Feldes ‚df_cb' selbst wird im Klartext übertragen und ist der ‚public key'. Er ist eine Zufallszahl zwischen 1000 und 9999. Der Wert muss in Verbindung mit dem Benutzerpasswort für die Ver- und Entschlüsselung herangezogen werden.
Die Chiffrierung der Daten erfolgt somit durch „private key + public key" als Passwortschlüssel.

7.2. https Kommunikation

7.2.1. Voraussetzungen

Voraussetzung für Nutzung eines SSL Zertifikates (https):

Hardware V4:

- Gerät mit TCP/IP (LAN / WLAN) oder Mobilfunk
- Mindestfirmware 04.03.11.XX (aktuell als Prototyp Firmware nutzbar)

Software:

- Server muss einen https-Request entgegennehmen und eine aktive Antwort geben

Eine Detaillierte Beschreibung für Ihre Entwicklung finden Sie hier:
Link:
https://www.datafox.de/download/Datafox%20Datenprotokoll%20zur%20HTTP(S)-Kommunikation.pdf

7.2.2. Elemente der https Infrastruktur

Wie auch http ist https ein Client-Server-Protokoll. Der Client baut eine Verbindung zum Port des https-Servers über TCP/IP auf, der Datenstrom wird zur Absicherung gegen Mithörer verschlüsselt.

Zum Einsatz kommen hierbei sowohl asymmetrische Verschlüsselung (Aushandlung der Verbindung) in Form des Server-Zertifikats wie auch symmetrische Verschlüsselung für den (späteren) Datenaustausch.

7.2.3. Nutzung der Verschlüsslung / Zertifikate

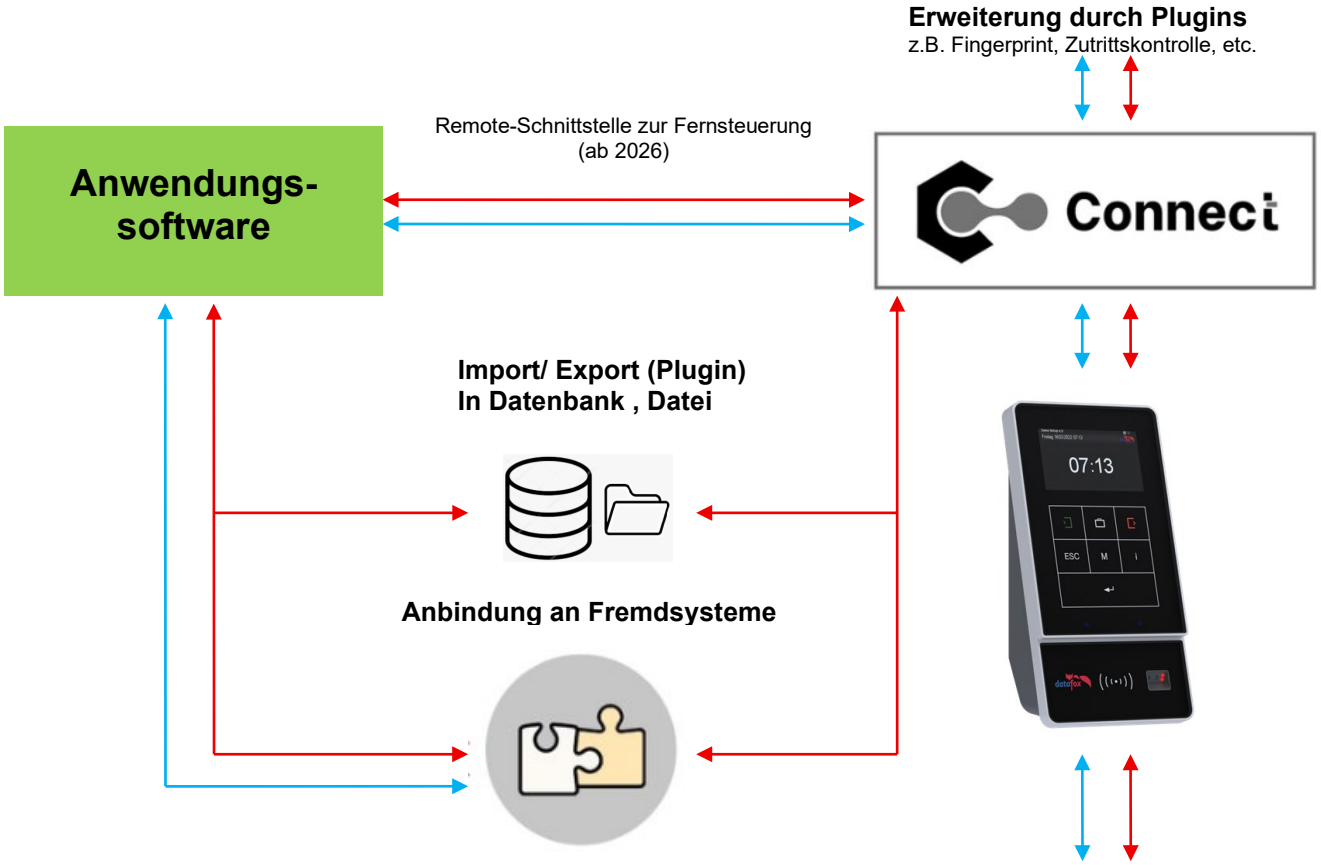
Es können mehrere Zertifikate für die Kommunikation in den Datafox Geräten hinterlegt werden. Sie können von Datafox signiertes Zertifikat verwenden oder ein Eigenes.

Die Firmware lehnt die Nutzung der als nicht mehr zeitgemäß (da unsicher) eingestuften Verschlüsselungsverfahren nach Spezifikation TLS 1.0 ab. Es werden lediglich Verfahren akzeptiert, die ab TLS 1.1 eingeführt wurden.

Die Übertagung der Zertifikate erfolgt mit dem Datafox StudioIV
Der Menüpunkt steht ab der StudioIV Version 04.03.11.XX zur Verfügung.
Sie finden diese unter: „Konfiguration>Zertifikate übertagen".

8. Datafox Connect

8.1. Connect im Remote-Modus



Ideal für:

- Projekte ohne eigene Geräteschnittstelle.
- Kunden, die eine einfache, zentrale Lösung ohne tiefgehende Integration suchen.
- Zukünftig auch für Systeme mit direkter Fernsteuerung via Remote-API (geplant ab 2026).

Im Remote-Modus übernimmt Connect vollständig die Kommunikation mit den Geräten. Anwendungssoftware greift lediglich auf die bereitgestellten Daten zu – dafür ist das Import/Export Plugin erforderlich. Die Gerätesteuerung wird komplett von Connect übernommen.

Warum dieser Modus?

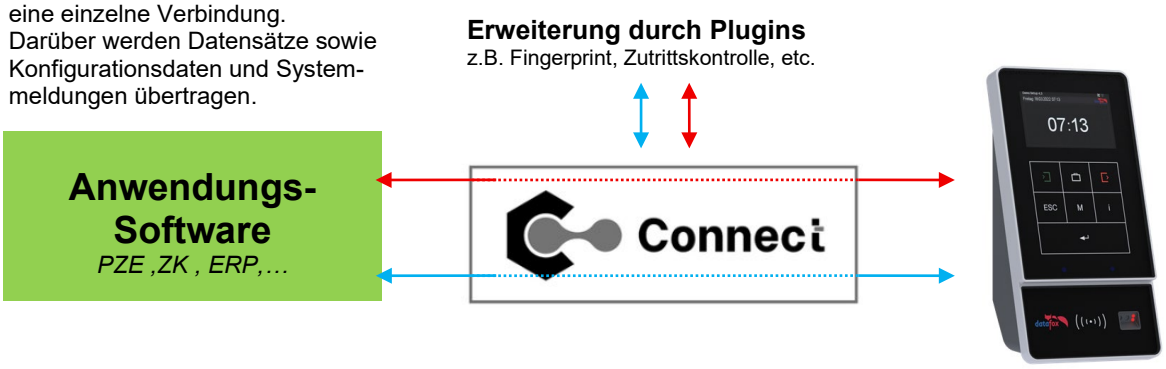
Er eignet sich besonders für Projekte, bei denen keine direkte Verbindung zwischen Anwendung und Geräten besteht – z. B. bei einfacher Datenübernahme über Datei/DB. So entfällt der Integrationsaufwand auf Anwendungsseite.

Vorteile:

- Einfacher Datenaustausch über Dateiablage oder Datenbank
- Automatisches Abholen der Daten über Dienste
- Integrierter Webserver, um Daten per HTTP entgegen zu nehmen
- Kein Programmieraufwand
- Einfache Aktualisierung der Stammdaten

8.2. Connect im Transparent Mode

Die Geräteverbindung erfolgt über eine einzelne Verbindung.
Darüber werden Datensätze sowie Konfigurationsdaten und Systemmeldungen übertragen.



TRANSPARENZ-MODUS

Integration von Datafox Connect ohne Veränderung der Anwendungssoftware, da die Gerätekommunikation transparent durchgereicht wird.

Die Verbindung zwischen Anwendungssoftware und Datafox Connect ist rein Dateibasiert.

↔ Konfigurationsdaten und Systemmeldungen

↔ Datensätze

Ideal für:

- Kunden, die Datafox Geräte bereits angebunden haben.
- Projekte, bei denen bestehende Systeme nicht angepasst werden sollen oder dürfen.
- Partner, die Connect als Mehrwert ohne Eingriff in die Datennutzung integrieren möchten.

Im Transparenzmodus fungiert Connect als unsichtbare Zwischeninstanz: Die Kommunikation zwischen Software und Gerät läuft weiterhin wie gewohnt – Connect reicht sämtliche Daten 1:1 durch, ergänzt aber gleichzeitig die Infrastruktur um Verwaltungs- und Erweiterungsfunktionen.

Warum dieser Modus?

Er erlaubt die Einführung von Datafox Connect ohne Anpassung der bestehenden Software – und bringt trotzdem alle Vorteile: zentrale Geräteverwaltung, einfache Erweiterung per Plugin, Supportfunktionen etc.

Vorteile:

- Die Daten fließen wie bei der bereits integrierten DFCom.dll weiterhin wie gewohnt in Ihre Anwendung
- Zusatzfunktionen z.B.,
  - wie Fingertemplates Verteilung
  - ZK Verwaltung (geplant)
  - Geräteupdates
  - Logdaten

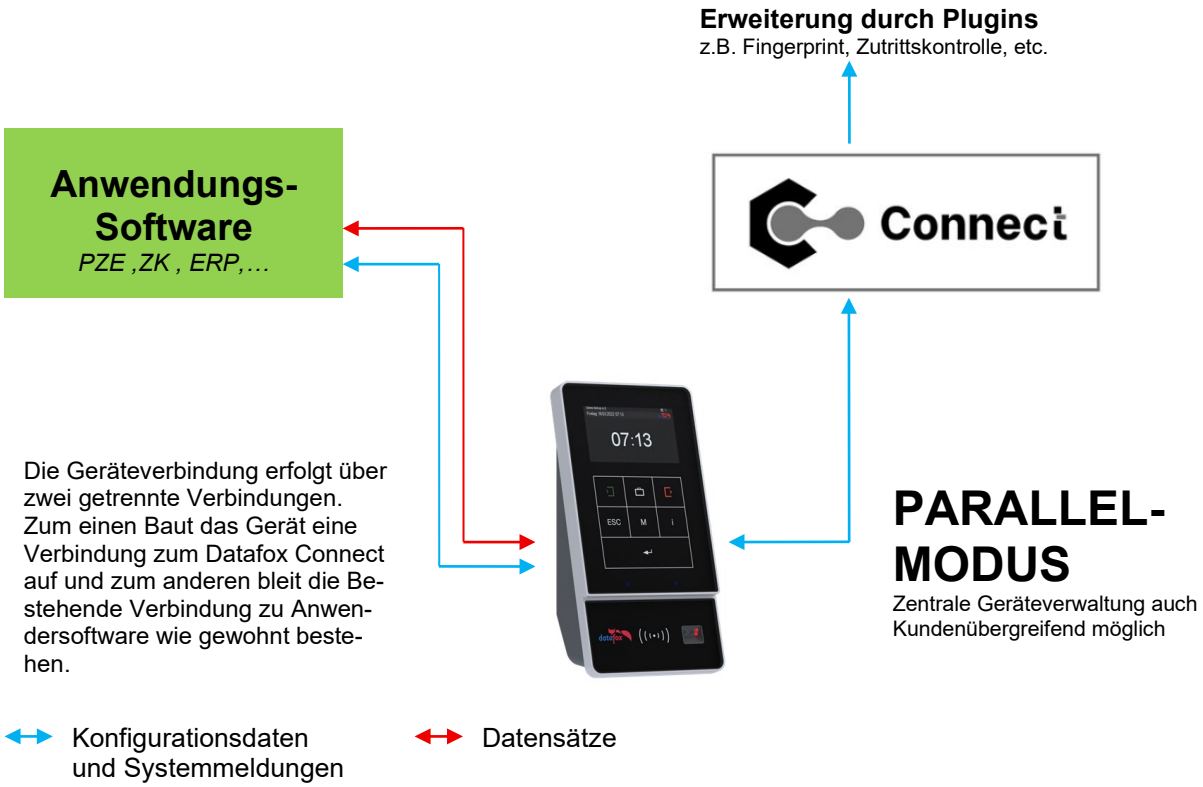
  Werden im Connect verwaltet bzw. zu Verfügung gestellt.

Nachteile:

- Eine bereits bestehende Geräteanbindung in der Anwendungssoftware notwendig

8.3. Connect im Parallel-Modus

Der Parallel-Modus ist ab der Firmware 04.03.24.01 verfügbar.



Ideal für:

- Partner und Kunden, deren Software bereits direkt mit Datafox Geräten kommuniziert.
- Projekte, bei denen Geräteverwaltung ausgelagert, aber Datenströme unangetastet bleiben sollen.

Im Parallelmodus bleibt die direkte Verbindung zwischen Datafox Hardware und Anwendungssoftware bestehen – Connect arbeitet unabhängig davon im Hintergrund. Es erhält keine Nutzdaten, sondern übernimmt ausschließlich Aufgaben rund um Konfiguration, Verwaltung und Support der Geräte.

Warum dieser Modus?

Er ermöglicht die Nutzung der Vorteile von Datafox Connect (zentrale Geräteverwaltung, Fernwartung, Plugin-Erweiterung), ohne bestehende Softwareprozesse zu verändern oder sensible Daten zu berühren.

Das Datafox Connect kann hier eigenständig neben der bereits bestehenden Anbindung der Datafox-Geräte installiert werden.
Das Gerät verbindet sich mit beiden Anwendungen.

9. Anhang

9.1. Alle wichtigen Links

9.1.1. Geräte Handbücher

https://www.datafox.de/download/Datafox EVO 2.8 Pure-DE.pdf
https://www.datafox.de/download/Datafox EVO 2.8 Pure-EN.pdf
https://www.datafox.de/download/Datafox EVO 3.5 Pure-DE.pdf
https://www.datafox.de/download/Datafox EVO 3.5 Pure-EN.pdf
https://www.datafox.de/download/Datafox EVO 3.5 Universal-DE.pdf
https://www.datafox.de/download/Datafox EVO 3.5 Universal-EN.pdf
https://www.datafox.de/download/Datafox EVO 3.5 Universal Handbuch.pdf
https://www.datafox.de/download/Datafox EVO 3.5 Universal Manual.pdf
https://www.datafox.de/download/Datafox EVO 4.3-DE.pdf
https://www.datafox.de/download/Datafox EVO 4.3-EN.pdf
https://www.datafox.de/download/Datafox EVO 7.0 Flex-DE.pdf
https://www.datafox.de/download/Datafox EVO 7.0 Flex-EN.pdf
https://www.datafox.de/download/Datafox EVO 5.0 Pure-DE.pdf
https://www.datafox.de/download/Datafox EVO-PC-DE.pdf
https://www.datafox.de/download/Datafox IO-Box V4-DE.pdf
https://www.datafox.de/download/Datafox KYO Cenloc V4-DE.pdf
https://www.datafox.de/download/Datafox KYO Cenloc V4-EN.pdf
https://www.datafox.de/download/Datafox KYO Fourloc V4-DE.pdf
https://www.datafox.de/download/Datafox KYO Fourloc V4-EN.pdf
https://www.datafox.de/download/Datafox KYO Inloc V4-DE.pdf
https://www.datafox.de/download/Datafox KYO Inloc V4-EN.pdf
https://www.datafox.de/download/Datafox KYO Oneloc-DE.pdf
https://www.datafox.de/download/Datafox KYO Oneloc-EN.pdf
https://www.datafox.de/download/Datafox MDE-BoxIV-DE.pdf
https://www.datafox.de/download/Datafox Mobil-Box V4-DE.pdf
https://www.datafox.de/download/Datafox AE-MasterIV V4-DE.pdf
https://www.datafox.de/download/Datafox Fahrzeugdatenlogger V2-DE.pdf

https://www.datafox.de/download/Datafox IPC Vario-DE.pdf

9.1.2. Software und SDK (Schnittstellenbeschreibungen)

https://www.datafox.de/download/Datafox StudioIV Handbuch.pdf
https://www.datafox.de/download/Datafox StudioIV Manual.pdf

https://www.datafox.de/download/Datafox data protocol HTTP(S)-communication.pdf
https://www.datafox.de/download/Datafox Datenprotokoll zur HTTP(S)-Kommunikation.pdf
DFCom-DLL
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.23-Dokumentation.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.23-Source.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.23-x64.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.23-x86.zip

9.1.3. Sonstige wichtige Links

https://www.datafox.de/download/Datafox-Infoblatt Ausweis im Kartenhalter.pdf
https://www.datafox.de/download/Datafox-Infoblatt KYO Oneloc neue CPU.pdf
https://www.datafox.de/download/Datafox-Infoblatt phg_crypt Umsetzung (Intera II, Agera).pdf

https://www.datafox.de/download/Datafox-Infoblatt Zutrittskontrolle-Access Control.pdf
https://www.datafox.de/download/Datafox Beschreibung Fingerscanner mit Flächensensor Saturn Template Austausch.pdf
https://www.datafox.de/download/Datafox Studio-Enhancements Firmwareupdate 04.03.15.06.pdf
https://www.datafox.de/download/Datafox Studio-Erweiterungen Firmwareupdate 04.03.15.06.pdf
https://www.datafox.de/download/Fingerprint module-firmware update-info-ENG.pdf
https://www.datafox.de/download/Fingerprint Modul-Firmware Update-Info.pdf

9.1.4. Alle Neuerungen kompakt

Jede neue Softwaregeneration wird mit einem Begleitheft vorgestellt.
Hier sehen Sie genau, ab wann die Neuerungen Verfügbar waren.

https://www.datafox.de/download/Datafox Begleitheft für Softwareversion 04.03.12.pdf
https://www.datafox.de/download/Datafox Begleitheft für Softwareversion 04.03.13.pdf
https://www.datafox.de/download/Datafox Begleitheft für Softwareversion 04.03.14.pdf
https://www.datafox.de/download/Datafox Begleitheft für Softwareversion 04.03.15.pdf
https://www.datafox.de/download/Datafox Begleitheft für Softwareversion 04.03.16.pdf
https://www.datafox.de/download/Datafox Begleitheft für Softwareversion 04.03.18.pdf
https://www.datafox.de/download/Datafox Begleitheft für Softwareversion 04.03.20.pdf
https://www.datafox.de/download/Datafox Begleitheft für Softwareversion 04.03.21.pdf
https://www.datafox.de/download/Datafox Companion Software Version 04.03.12.pdf
https://www.datafox.de/download/Datafox Companion Software Version 04.03.13.pdf
https://www.datafox.de/download/Datafox Companion Software Version 04.03.14.pdf
https://www.datafox.de/download/Datafox Companion Software Version 04.03.15.pdf
https://www.datafox.de/download/Datafox Companion Software Version 04.03.16.pdf
https://www.datafox.de/download/Datafox Companion Software Version 04.03.18.pdf
https://www.datafox.de/download/Datafox Companion Software Version 04.03.20.pdf
https://www.datafox.de/download/Datafox Companion Software Version 04.03.21.pdf

9.1.5. Softwareversionslisten

Hier werden alle Änderungen und Bugfixes beschrieben.

https://www.datafox.de/download/MasterIV%20Software-Versionsliste%2004.02,%2004.03.pdf
https://www.datafox.de/download/MasterIV%20Software-Versionsliste%2004.02,%2004.03-EN.pdf

9.2. Info zu HTTPS

https://pixabay.com/illustrations/cyber-security-technology-network-3374252/

HTTPS dient zum verschlüsselten Verbindungsaufbau und zur verschlüsselten Übertragung von Daten über LAN, WLAN oder Mobilfunk.
Dieses Dokument beschreibt die prinzipielle Funktionsweise, gibt Tipps zur Implementierung und Hintergrundinformationen zu den eingesetzten Technologien

Die in Datafox Geräten eingesetzte TLS-Implementierung (TLS bedeutet „Transport Layer Security“, zu Deutsch etwa: „sichere Transport-Schicht für Daten“) für die HTTPS-Kommunikation setzt auf mbed-TLS auf. Mit Hilfe dieser Bibliothek werden die Verschlüsselungsstandards TLS 1.1 und TLS 1.2 erfüllt, TLS 1.3 ist aktuell (Mai 2020) nicht verfügbar.
Dieses Dokument bewertet nicht, ob die übertragenen Daten den Aufwand für das „Knacken“ einer HTTPS-Verschlüsselung rechtfertigen. Diese Bewertung bleibt dem Leser vorbehalten. Übermittelte Stempelzeiten sind fraglos personenbezogene Daten, die nach DSGVO geschützt werden müssen – unterliegen aber oft keinen Geheimhaltungsanforderungen.

Aufbau einer HTTPS-Kommunikation
Die HTTPS-Kommunikation findet in zwei Phasen statt:
- Im Rahmen des TLS-Handshakes überprüfen Client und ggf. Server die Authentizität des Kommunikationspartners. Dazu wird der Diffie-Hellmann-Algorithmus eingesetzt. Nach dem Prüfen der gegenseitigen Authentizität wird ein Schlüssel für die nachfolgende Datenkommunikation ausgehandelt. Da die Aushandlung am Beginn jeder Kommunikation steht, erfolgt diese für jede Verbindung erneut.
- Im Rahmen der Datenkommunikation werden, unter Nutzung des zuvor ausgehandelten Schlüssels, die Daten ausgetauscht.

Im Rahmen des TLS-Handshakes werden asymmetrische Verschlüsselungsverfahren, im Rahmen der Datenkommunikation werden symmetrische Verschlüsselungsverfahren eingesetzt. Die klassischen Vertreter sind RSA (benannt nach den Erfindern Rivest, Shamir und Adleman) und ECC (Elliptic Curve Cryptography) für den TLS-Handshake und AES (Advanced Encryption Standard) für die symmetrische Kanalverschlüsselung. Man spricht hier davon, dass HTTPS „eine hybride Verschlüsselung“ nutzt.

Asymmetrisch vs. Symmetrische Verschlüsselung
Bei asymmetrischen Verschlüsselungsverfahren werden von den Kommunikationspartnern unterschiedliche Schlüssel eingesetzt, bei symmetrischen Verfahren nutzen beide denselben Schlüssel. Die Nutzung unterschiedlicher Schlüssel bei asymmetrischer Verschlüsselung erlaubt die Unterscheidung von „öffentlichem“ und „privatem“ Teil-Schlüssel – wie bei einer „Public Key Infrastructure“ (PKI) erforderlich. Diese Schlüssel-Teilung wird mit höherem Ressourcen-Aufwand (sowohl Rechenzeit als auch Speicher) erkauft, als bei einer vergleichbar sicheren symmetrischen Verschlüsselung erforderlich ist.

Einflussgrößen auf die Sicherheit der Verschlüsselung
Die Sicherheit einer Verschlüsselung hängt von verschiedenen Faktoren ab:
- Sicherheit des Algorithmus,
- Länge des Schlüssels,
- Sicherheit der Systeme, zwischen denen verschlüsselt wird und
- Sicherheit der Infrastruktur, über die Daten getauscht werden

Typischerweise sind nicht alle diese Aspekte durch den Nutzer der Verschlüsselung beeinflussbar. Der Algorithmus ist in Soft-/Hardware implementiert, die Sicherheit des Server-Systems mag kontrollierbar sein, die des Client normalerweise nicht und auch die Infrastruktur kann – sofern die Kommunikation nicht nur über eigene Netzwerk-Infrastruktur erfolgt – normalerweise nicht beeinflusst werden. Damit bleibt die Schlüssellänge der am einfachsten austauschbare Parameter.

Bewertung der Algorithmen

Es ist ferner noch zu bemerken, dass nicht alle Verschlüsselungsverfahren die gleiche Sicherheit bieten. Um Algorithmen vergleichbar zu machen, werden diese auf einen idealen Blockchiffre abgebildet und dessen Schlüssellänge (engl. Security Bits) verglichen. Da in TLS sowohl asymmetrische als auch symmetrische Verschlüsselung eingesetzt wird, ist das Minimum der Security-Bits beider Verfahren ein Maß für die Sicherheit des hybriden Verfahrens.

Microchip [2] nennt unter Berufung auf die NSA folgende Schlüssellängen zum Vergleich der AES-, RSA- und ECC-Algorithmen:

Schlüssellänge | Security Bits	Symmetrisch Verschlüsselung | Symmetric cipher	Asymmetrisch Verschlüsselung | Asymmetric cipher
112	3DES	RSA-2048
128	AES-128	RSA-3072, ECC-256 (prime256v1)
192	AES-192	RSA-7680, ECC-384 (secp384r1)
256	AES-256	RSA-15360, ECC-521 (secp521r1)

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) gibt eine Empfehlung für Schlüssellängen:
- Bis Ende 2022 sollen Schlüsselverfahren mit 100 Security Bits genügen,
- ab 2023 voraussichtlich 120 Security Bits (BSI TR-02102-1 vom 24.03.2020, S. 14, vgl. [1]).

Einsatz unterschiedlicher Schlüssel auf einem HTTPS Server
Ist es erforderlich, unterschiedliche Schlüssel auf einem physikalischen Server-Host (Hardware) einzusetzen und diese über einen gemeinsamen Netzwerk-Port anzusprechen, so gibt es in Verbindung mit **SNI** ein mit den virtuellen Hosts im HTTP Protokoll vergleichbares Verfahren. Hierbei wird die sog. Server Name Indication (SNI, vgl. [7] und [9]) im TLS-Handshake aktiviert, die auch von Datafox Geräten unterstützt wird. Mit SNI findet die Auswahl des korrekten HTTPS-Server-Prozesses (Software) bereits im Rahmen des Handshakes statt.

Die Einrichtung von SNI unterscheidet sich zwischen Webservern. Einen Leitfaden, wie dieses auf einem Mircosoft IIS erfolgen kann, ist unter [8] dokumentiert. Setzt Ihre Installation einen Reverse-Proxy oder Load-Balancer ein, so muss dieser mit **SNI** umgehen können – dieses aufzuarbeiten ist weit jenseits des Anspruchs dieses Dokuments. Bitte konsultieren Sie bei Bedarf Ihre Netzwerk-Administratoren.

SNI als Verfahren kann genutzt werden, um z.B. einem ERP-System einen anderen TLS-Schlüssel zuzuordnen als den Datafox-Geräten, die Daten an denselben Server liefern. Somit können Sie Datafox-Geräten einen 2048-Bit oder 3072-Bit RSA-Schlüssel zuordnen und trotzdem ein ERP-System mit Schlüsseln der Länge 4096 Bit betreiben, sofern Sie dieses Schutzniveau benötigen.

Fazit
Wir empfehlen, bei Datafox Geräten ein ECC-basiertes Zertifikat mit einer Schlüssellänge von 256 Bit einzusetzen. Das entspricht der BSI-Empfehlung ab 2023. Gegenüber vergleichbaren RSA-Zertifikaten sparen Sie Speicher im Gerät sowie Rechenzeit.

Informationen zur Erstellung und Nutzung von RSA- und ECC-basierten Zertifikaten finden Sie unter [9].

Detailliertere Betrachtungen zu symmetrischer und asymmetrischer Verschlüsselung finden Sie im Anhang.

Sollten Sie längere Zertifikate für einzelne Ihrer Services benötigen, so können Sie diese mit unterschiedlich langen Zertifikaten ausstatten. Hier steht mit SNI ein standardisiertes Verfahren bereit, das in vielen Cloud-Plattformen eingesetzt wird.

Anhang

Eingesetzte Standards

Die Verschlüsselungsstandards TLS 1.1 und TLS 1.2 sind Mengen von Verschlüsselungs- und Signaturalgorithmen. Diese Algorithmen unterliegen der „Alterung durch Krypto-Analyse“. Verfahren, die vor 10 Jahren noch sicher waren, sind das möglicherweise jetzt nicht mehr, da die Zunahme von Rechenleistung oder algorithmische Schwächen sie angreifbar gemacht haben. Daher unterstützt unsere TLS-Implementierung bewusst TLS 1.0 und die noch älteren Standards SSLv2 und SSLv3 nicht mehr.

Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung wird im Rahmen der Überprüfung der Identität des Servers und ggf. des Clients eingesetzt. Die Schlüsselteile (öffentlich und privat) werden dazu als X509.3-Zertifikate repräsentiert. Vereinfacht gesagt werden beide Schlüsselteile benötigt, um eine Nachricht zu ver- und entschlüsseln. Ist mindestens einer der Schlüssel nicht bekannt, ist der Rechenaufwand zur Entschlüsselung erheblich höher. Das Verfahren ist ferner meist nicht eindeutig umkehrbar.

Der private Schlüssel ist hierbei die schützenswerte Information. Alle Geräte, die auf den privaten Schlüssel Zugriff haben, können sich dem Client gegenüber ausweisen – sind also vom Client im Rahmen der Verschlüsselung nicht zu unterscheiden.

Die Anfälligkeit des Verfahrens gegenüber der Geheimhaltung der Schlüssel wird im Rahmen der X509.3 Zertifikate durch eingeschränkte Gültigkeitsdauer, Hierarchie von Zertifikaten („Zertifikatskette“) und Revocation-Lists unterstützt. In diesem Zusammenhang sei darauf verwiesen, dass die Zertifikate am oberen Ende einer Zertifikatskette häufig eine sehr lange Gültigkeitsdauer ausweisen, häufig 10 Jahre oder länger, das eigentliche Server-Zertifikat aber häufig nur eine Gültigkeitsdauer von 90 Tagen bis 2 Jahren hat. Dieses liegt daran, dass der Stelle, die Zertifikate verwaltet („Certificate Authority“, CA), eine sicherere Verwahrung der Schlüssel zugetraut wird als uns, die wir die Zertifikate nutzen.

Die Überprüfung der Authentizität in TLS ist so ausgelegt, dass nicht alle öffentlichen Schlüssel für die Prüfung erforderlich sind. Das Zertifikat der CA genügt. Damit ist die Auswirkung der Gültigkeitsdauer des Serverzertifikats für die Client-Seite deutlich unproblematischer, da CA-Zertifikate (s.o.) eine vergleichsweise lange Gültigkeitsdauer aufweisen.

Analog zur Prüfung der Identität des Servers durch den Client während des Handshakes, kann der Server die Identität des Clients prüfen. Dazu wird dann ein sog. Client-Zertifikat eingesetzt.

Ist die Identitätsprüfung abgeschlossen, werden symmetrische Verschlüsselungsverfahren für die Kommunikation abgestimmt und der dazu notwendige Schlüssel ausgehandelt. Details zum Auflauf des Diffie-Hellmann-Algorithmus sind im Netz an vielen Stellen dokumentiert, die Darstellung unter [5] ist eine gute Einstiegsbasis.

Symmetrische Verschlüsselung

Als symmetrisches Verschlüsselungsverfahren wird häufig der AES Algorithmus verwendet. Dieser setzt einen Schlüssel der Länge 128, 192 oder 256 Bit ein, der verglichen mit den Schlüssellängen des RSA-Verfahrens recht kurz wirkt. Entsprechend ist auch der AES Algorithmus inzwischen gut untersucht, was einige algorithmische, nicht-dramatische Schwächen zu Tage gefördert hat.

Die Schätzung für den Aufwand des Knackens eines 128 Bit Schlüssels belaufen sich auf

- 30 Jahre auf einem Quantencomputer (etwa 10 Sekunden bei 100 Bit)
- 2,15 * 1012 Jahre auf einem aktuell verfügbaren Rechner (etwa 6.000 Jahre bei 100 Bit)

Die Rest-Lebensdauer unserer Sonne wird aktuell mit etwa 5 * 109 Jahren angenommen.
Hinzu kommt, dass die symmetrische Verschlüsselung bei jedem Handshake neu aufgebaut wird. Der Abbau einer HTTPS-Verbindung erfolgt nach etwa 30 Sekunden Inaktivität. Versucht man folglich, den symmetrischen Kanal zu knacken, so wird der Rechenaufwand dafür nach jeder Verbindungsaushandlung erneut erforderlich.

Angriffsszenarien
Da kein praktikabler Angriff auf einen bestehenden, AES-verschlüsselten Kanal mit aktueller Hardware bekannt ist, konzentrieren sich Angriffe auf TLS eher auf Handshake, Algorithmen und deren Implementierungen. Einige Angriffe haben es in den letzten Jahren zu „Weltruhm“ gebracht:

- Heartbleed (OpenSSL < 1.0.1g: Der Client konnte Daten eines Server auslesen, u.U. auch dessen geheimen Schlüssel)
- FREAK (Problem in der Implementierung der USA Exportbeschränkungen, konnte zur Verwendung von kurzen Schlüssel bei asymmetrischer Verschlüsselung führen)
- BEAST (TLS < 1.1: Algorithmisches Problem bei Initialisierung der symmetrischen Verschlüsselung)

Besonders interessant sind hier Verfahren, die über das Netzwerk genutzt werden können, so dass der Angegriffene diese nicht bemerkt.

Angriff auf den Handshake
Bei Angriffen auf den Handshake geht es entweder darum, die Aushandlung zu beeinflussen, so dass wenig sichere Verfahren eingesetzt werden oder darum, einen Schlüsselteil (und das Verfahren) direkt abzugreifen.

Kompromittieren von Client oder Server
Ein Angreifer, der Kontrolle über Client oder Server einer Kommunikation hat, ist dazu in der Lage, Schlüssel auszulesen und u.U. zu modifizieren.

Cipher-Suite Downgrade
Downgrade-Attacken können eingesetzt werden, wenn ein Angreifer entweder Client oder Server unter Kontrolle bekommt. Bei diesem Angriff behauptet einer der Kommunikationsteilnehmer, dass er nur weniger sichere Verfahren einsetzen kann. Wenn sich der andere Teilnehmer darauf einlässt, wird eine nicht optimal abgesicherte Verbindung hergestellt, und die Daten sind u.U. auch zwischendurch entschlüsselbar. Der Nutzen des Zwischendurch-Entschlüsselns ist natürlich begrenzt, wenn der Angreifer ohnehin Zugang zu einem der Systeme hat.

Random Number Generator Attack
Viele Verschlüsselungs- und Signatur-Algorithmen nutzen „Entropie“, um es einem Angreifer schwieriger zu machen, die ausgetauschten Daten zu interpretieren. Diese Entropie ist häufig Bestandteil der Schlüssel. Produziert ein System hier keine „guten“ Zufallszahlen, so kann das Wissen darüber das Ermitteln der eingesetzten Schlüssel erheblich einfacher gestalten.

Timing-Angriffe
Zeitliche Unterschiede zwischen erfolgreicher und nicht erfolgreicher Schlüsselprüfung können u.U. Rückschlüsse zulassen, wir dicht ein Test-Schlüssel am tatsächlichen Schlüssel ist. Die Dauer der Prüfung kann i.d.R. extern beobachtet werden.

Angriff auf den verschlüsselten Kanal
Angriffe auf einen bereits verschlüsselten Kanal sind schwierig, wenn der Angreifer keine der beiden Seiten der Kommunikation beeinflussen kann. Der Schlüsselraum, der heute eingesetzten Verfahren, ist zu groß, um diese durch Ausprobieren („Brute Force“) alle zu bewerten. Ferner muss nach dem durchprobieren der Schlüssel ja noch derjenige Datensatz ermittelt werden, der tatsächlich verschlüsselt wurde.

Padding oracle Angriffe
Viele symmetrische Verschlüsselungsalgorithmen basieren auf einer festen Blocklänge. Diese erfordert, dass eine Nachricht, deren Länge nicht durch die Blocklänge teilbar ist, bis zur Länge des Blocks aufgefüllt und dann verschlüsselt wird. Einige Implementierungen haben hier Schwächen, die Padding-Oracle-Angriffe ausnutzen um selbst Nachrichten durch den Server verschlüsseln zu lassen.

Algorithmische Schwächen des eingesetzten Verschlüsselungsverfahrens
Weist ein Algorithmus selbst Schwächen auf, so können diese bei der Entschlüsselung helfen. Im Falle von AES-128 verkleinert sich damit der Schlüsselraum auf etwa ein Milliardstel des ursprünglichen Schlüsselraums – was eine erheblich Zeitersparnis beim Ausprobieren der Schlüssel ermöglicht.

Weist ein Algorithmus keine weiteren Schwächen auf, die etwa das Ermitteln von wesentlichen Teilen des Schlüssels aus dem verschlüsselten Datenstrom ermöglichen, so kann er dennoch eingesetzt werden. Im Falle von AES-128 bleiben immerhin noch etwa 1030 Schlüssel übrig.

Brute-Force Ermittlung des Schlüssels
Brute-Force Angriff sind i.d.R. nicht praktikabel – jedenfalls nicht für gegenwärtige Algorithmen.

Am Beispiel des DES-Algorithmus mit 56 Bit Schlüssellänge gibt es unter [6] eine Chronologie der Ereignisse, die letztendlich dazu geführt haben, dass DES als unsicherer Algorithmus bewertet wurde. Ein wesentlicher Anteil dürfte hier der Anstieg der Rechenleistung seit 1975 sein, der Brute-Force-Angriffe über verteiltes Rechnen ermöglicht.
Vermutlich werden viele der aktuell eingesetzten Algorithmen ähnlich geschwächt, sobald Quantencomputer verfügbar werden.

Betrachtung der Schlüssellängen der PKI
Neben den oben beschrieben Aspekten, die beim Absichern der Kommunikationsteilnehmer berücksichtigt werden müssen, bleibt die Länge der Schlüssel in der PKI als Einflussparameter für die Sicherheit des Gesamtverfahrens.
Aktuell werden hier typischer Weise RSA- oder ECC-Algorithmen eingesetzt.

RSA
Für den RSA Algorithmus gibt es u.a. seitens des BSI die Empfehlung, dass ein Schlüssel mit mindestens 2000 Bit eingesetzt werden soll und dieser dann auch für das ganze Jahr 2022 noch eingesetzt werden kann (BSI TR-02102-1 vom 24.03.2020, S. 14, vgl. [1]).

RSA, wie auch das eingesetzte symmetrische Verfahren, werden hierbei auf eine Schlüssellänge bezüglich eines idealen Blockchiffres (engl. Security Bits) reduziert. Das BSI fordert aktuell 100 Bits (etwa 1900 Bit RSA), ab 2023 soll diese Länge auf 120 Bits (etwa 2800 Bit RSA) angehoben werden.

Auch Microchip nutzt in seinen Empfehlungen unter [2] Security Bits und kommt zu einer ähnlichen Einschätzung wie das BSI.
Anhand der Microchip-Tabelle ist ersichtlich, wie wenig mehr Sicherheit RSA bietet, wenn der Schlüssel verlängert wird. Um ein zum AES-256-Algorithmus äquivalentes Schutzniveau zu bieten, müsste der RSA-Schlüssel eine Länge von 15360 Bit erreichen.

Hinsichtlich der Rechenzeit gibt es im Netz sehr unterschiedliche Aufwandsschätzungen zum Faktorisieren („Knacken“) eines 2048 Bit RSA Schlüssels, vgl. [3] und [4].
Alle diese Schätzungen deuten darauf hin, dass ein 2048 Bit Zertifikat noch genügend Sicherheit bietet, um nicht mit realistischem Aufwand angreifbar zu sein. Allerdings sieht das BSI RSA als Übergangstechnologie und empfiehlt den Einsatz von ECC-basierten Verfahren.

ECC
ECC Verfahren erreichen bei deutlich kürzeren Schlüsseln ein mit RSA-Verfahren vergleichbares Sicherheitsniveau (vgl. [2]). Wir haben im Labor den Speicherbedarf von RSA-2048-, RSA-3072- und ECC-256-basiertem TLS-Handshake nachvollzogen und festgestellt, dass ECC-256 während des TLS-Handshakes

- 6 % weniger Speicher als das RSA-2048-Verfahren und
- 22% weniger Speicher als das RSA-3072-Verfahren benötigt.

Damit ist ECC-basierte Verschlüsselung erheblich effizienter einsetzbar als RSA-basierte Verschlüsselung, auch wenn RSA als Industrie-Standard betrachtet wird. Wir empfehlen daher den Einsatz von ECC.

Quellen

Sources

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html

BSI TR-02102-1 vom 24.03.2020

Germany federal agency for IT safety, Technical Report on Data Security and Safety, TR-02102-1 issued March 24th 2020

[2] http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-8951-CryptoAuth-RSA-ECC-Comparison-Embedded-Systems-WhitePaper.pdf

Vergleich von RSA und ECC für eingebettete Systeme, Whitepaper

RSA vs ECC Comparison for Embedded Systems, Whitepaper

[3] https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/

Schätzungen zum Knacken eines RSA Schlüssels

Estimates of breaking RSA encryption

[4] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Beschreibung des RSA Algorithmus

Description of the RSA algorithm

[5] https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/

Beschreibung der TLS Verbindungsaushandlung

Description of the TLS handshake

[6] https://de.wikipedia.org/wiki/Data_Encryption_Standard

Beschreibung des Data Encryption Standards (DES) aus 1975

Description of the Data Encryption Standard (DES) from 1975

[7] https://de.wikipedia.org/wiki/Server_Name_Indication

Beschreibung der TLS-Erweiterung SNI

Description of the TLS-Extension SNI

[8] https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-8/iis-80-server-name-indication-sni-ssl-scalability

Erläuterung zur Nutzung von SNI mit dem Microsoft IIS

Explanation for using SNI with a Microsoft IIS

[9] https://www.datafox.de/download/Datafox%20Datenprotokoll%20zur%20HTTP(S)-Kommunikation.pdf

https://www.datafox.de/download/Datafox%20data%20protocol%20HTTP(S)-communication.pdf

Datafox http/https Protokoll Dokumentation

Datafox http/https protocol documentation