



Datafox GmbH • Dermbacher Straße 12-14 • D-36419 Geisa • www.datafox.de

Softwareversion 04.02.03

Begleitheft

Flexible Datenerfassung mit Methode



© 2012 Datafox GmbH

Dieses Begleitheft dient nur als Ergänzung zu den bisherigen Handbüchern.
Es werden alle Neuerungen, die durch die neue Software zur Verfügung stehen, beschrieben.

Diese Abbildung zeigt Ihnen, für welche Datafox-Geräte der jeweils folgende Abschnitt gültig ist, sofern eine Funktion nicht für alle Geräte gilt.

Das jeweilige Gerät oder Geräte für die dieser Abschnitt gültig ist, sind mit einem ☒ gekennzeichnet.

										
☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Inhalt

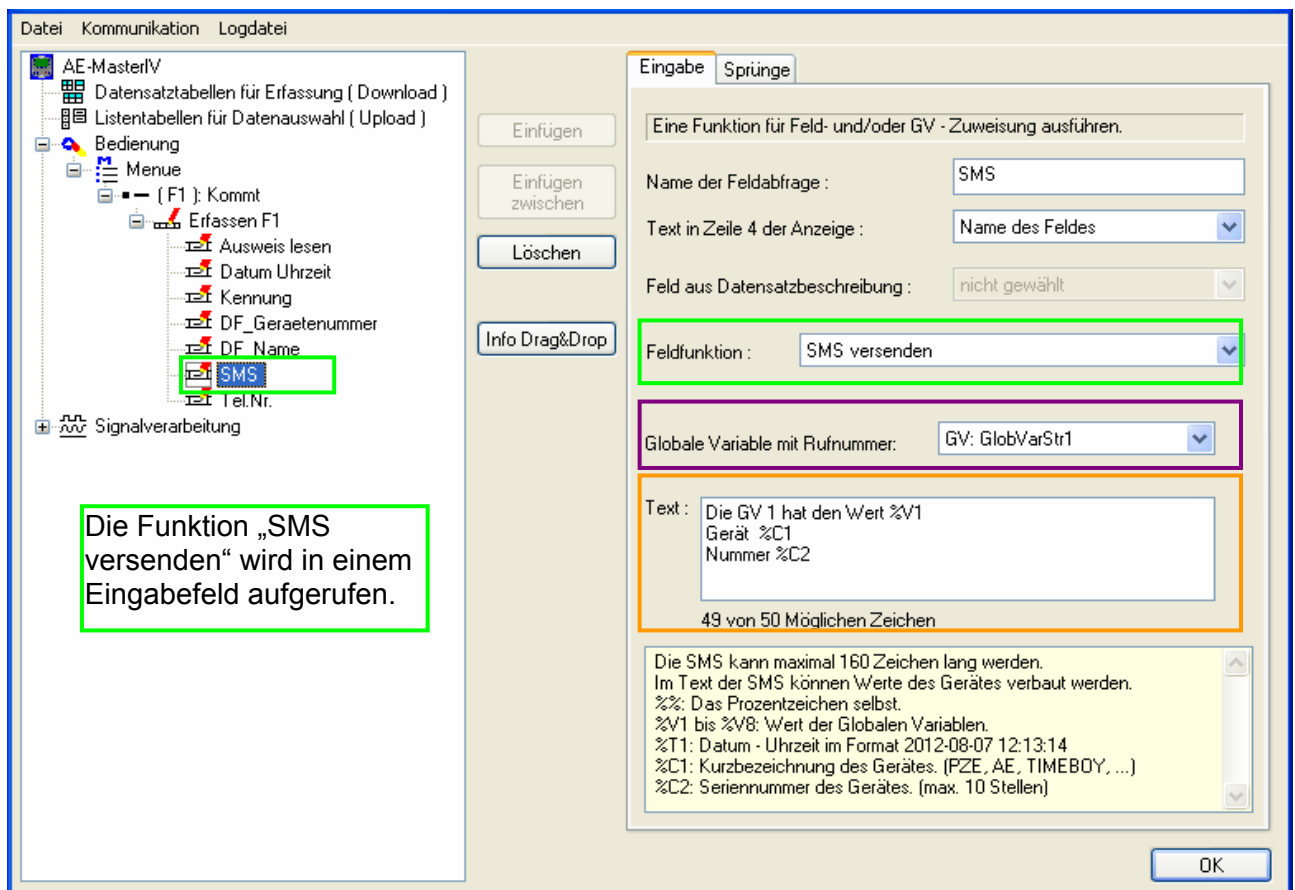
1.	SMS	1
1.1.	SMS versenden	1
1.2.	SMS empfangen	2
2.	Data on Card	4
2.1.	Allgemeine Informationen	4
2.2.	Einrichtung Data on Card	5
3.	Office Connect	9
3.1.	Allgemeine Informationen	9
3.2.	Bedienung.....	9
3.2.1.	Exportaufgaben erstellen.....	10
3.2.2.	Export starten	11
4.	Funktionserweiterung für die Zutrittskontrolle	12
4.1.	Allgemeine Informationen	12
4.2.	Beispiele	12
4.3.	Beschreibung der Tabelle „Action2“	16
5.	HTTP über LAN/WLAN mit DNS-Auflösung	17
6.	Neue RFID Reader (ISO14443 u. ISO15693) 13,56MHz	18
6.1.	ISO 14443A - Mifare Familie	19
6.1.1.	Mifare Mini	19
6.1.2.	Mifare Classic	19
6.1.3.	Mifare Plus.....	19
6.1.4.	Mifare Ultralight.....	20
6.1.5.	Mifare DESFire	21
6.2.	ISO 14443B – Calypso, CEPAS und Moneo	24
6.3.	ISO 14443-2 iClass, Picopass	24
6.4.	ISO 14443-3 SRX von ST Microelectronics.....	24
6.5.	ISO 15693 – iCode, Tag-it, MyD.....	24
6.5.1.	iCode	24
6.5.2.	Tag-it.....	24
6.5.3.	My-D Vicinity von Infineon	24
6.5.4.	24LR16 / 24LR64 von ST	25
6.5.5.	MB89R118 / MB89R119 von Fujitsu	25
6.5.6.	LRI 2k	25
6.6.	ISO 14443/15693 Seriennummer lesen	25
7.	Verschlüsselung der Kommunikation mit MasterIV Geräten	26
7.1.	Erstellung und Hinterlegen des Schlüssels im Gerät.....	26
7.2.	Hinterlegen des Passwortes im StudioIV.....	27
7.3.	Übergabe des Schlüssels in die DFComDLL.....	27
8.	Zusätzliche Erweiterungen	28
8.1.	Vorbelegung der Anzeige im Display bei Eingaben.....	28
8.2.	Signalisierung der Transponderbereitschaft	28

8.3.	Änderung der Schriftgröße	29
9.	TimeboyIV	30
9.1.	Infozeile	30
9.2.	WLAN für TimeboyIV	31
9.2.1.	Einstellen der WLAN Parameter	32
9.2.2.	Ad-hoc Mode	33

1. SMS

1.1. SMS versenden

Datafox MasterIV Geräte, die mit einem GPRS-Modem ausgestattet sind, sind nun in der Lage, eine SMS zu senden. Voraussetzung dafür ist, dass die Hauptkommunikation auf „GPRS“ eingestellt ist. Dazu wurde in der Parametriersoftware DatafoxStudioIV eine neue Feldfunktion „SMS versenden“ hinzugefügt. Siehe Bild:



Die SMS kann maximal 160 Zeichen lang werden.
Im Text der SMS können Werte des Gerätes verbaut werden.
%%: Das Prozentzeichen selbst.
%V1 bis %V8: Wert der Globalen Variablen.
%T1: Datum - Uhrzeit im Format 2012-08-07 12:13:14
%C1: Kurzbezeichnung des Gerätes. (PZE, AE, TIMEBOY, ...)
%C2: Seriennummer des Gerätes. (max. 10 Stellen) %1 für GV 1, %2 für GV2 usw..

Die Rufnummer, an die diese Nachricht gesendet werden soll, wird in einer GV (globalen Variablen) angegeben.



Achtung:

Geben Sie die Rufnummer immer mit einer Landesvorwahl an.
Bsp.: +49161458*****

Es werden bis zu 128 SMS im Gerät gespeichert. Kommt dann eine weitere hinzu, wird die älteste SMS gelöscht (Ringspeicher).

1.2. SMS empfangen

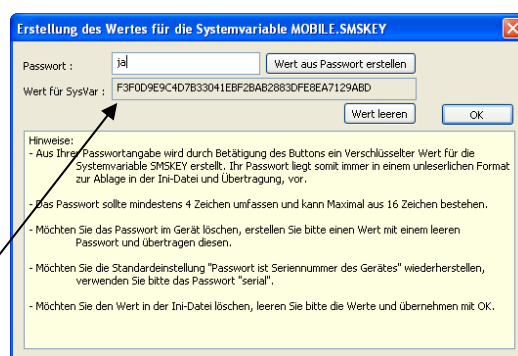
Datafox MasterIV Geräte, die mit einem GPRS-Modem ausgestattet sind, sind nun in der Lage eine SMS zu empfangen.

Folgende Funktionen können dadurch realisiert werden:

- ▶ Anzeige, einer an das Gerät gesendeten SMS auf dem Display. Wie es bereits durch DFCComSendMessage oder bei der HTTP-Rückantwort möglich ist.
- ▶ Aufforderung eine Serviceverbindung aufzubauen (Identisch zur http-Antwort)
- ▶ Eine Eingabekette in der Signalverarbeitung zu starten
- ▶ Einen Signalton ausgeben

Bedingung eine SMS zu empfangen ist, dass ein **KEY** in dem SMS-Text hinterlegt sein muss. Der Key für das Gerät, wird in der GPRS/HTTP .ini Datei hinterlegt.

Name	Wert
PHONE	*99***1#
GPRS	internet.eplus.de
USER	blau
PASSWORD	blau
HOST	www.datafox.de
PORT	80
HTTPSEND	GET /httpdemo/getdata.php?
ALIVE	0
HTTPTIMEOUT	10000
HTTPTYPE	1.1
SIMPIN	0
SIMPUK	0
ROAMING	1
RESETTRIGGER	32
ATTACH	32
ERRORLEVEL	0
HTTP	0
KEY	130.149.17.5
DNS1	130.149.17.5
SMSKEY	F3F0D9E9C4D7B33041EBF2B82883DFE8EA7129ABD



Textnachricht

Das Schlüsselwort welches in der SMS enthalten sein muss ist

message=Text1 ↵ Text Zeile2 ↵ Zeile3 usw.

&delay=10&key=ja

Hierbei bedeutet die **10**, dass die Nachricht für 10 Sekunden angezeigt wird.

Nach dem ↵ Zeichen wird jeweils automatisch ein Zeilenumbruch eingefügt.

Wurde noch kein **key** im Gerät hinterlegt, muss die Seriennummer des Gerätes als key verwendet werden. Wird der key im Gerät gelöscht (leeres Passwort), so wird jede SMS angenommen.

Serviceverbindung

Der Inhalt der SMS ist analog zu dem der http-Antwort vom WEB-Server.

Bisher werden 3 Schlüsselwörter unterstützt: **service**, **host** und **port**. Dem Schlüsselwort muss ein ‚=‘-Zeichen mit dem jeweiligen Wert folgen. Die einzelnen Felder wiederum werden mit dem ‚&‘-Zeichen getrennt.

Mit dem Schlüssel **service=1**, wird das Gerät veranlasst, eine Wartungsverbindung aufzubauen. Es wird versucht zu dem im Studio unter „Konfiguration->Systemvariablen Active-Mode“ eingestellten Server („Host“ und „Port“) eine Verbindung herzustellen. Optional ist es auch möglich, den Server direkt in der SMS anzugeben -> **host=**. Voreingestellt ist dann der Port 8000. Mit dem zusätzlichen Parameter **port=** kann auch dieser Wert in jeder SMS angepasst werden.

Beispiele:

- a) service=1
- b) service=1&host=www.datafox.de
- c) service=1&host=123.123.123.123
- d) service=1&host=www.datafox.de&port=4711

In Beispiel a) wird zu dem in der „Active-Mode“ hinterlegten Server eine Verbindung aufgebaut.

Bei b) und c) werden Verbindungen auf Port 8000 zum jeweils genannten Server aufgebaut.

Im letzten Beispiel wird versucht, eine Verbindung zum Datafox-Server an Port 4711 herzustellen.

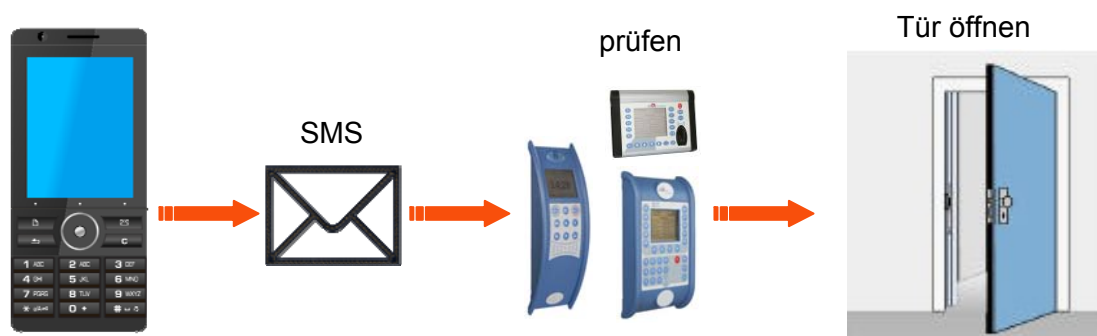
Eine Eingabekette in der Signalverarbeitung starten

Das Schlüsselwort, welches in der SMS enthalten sein muss, ist:
ek=Name (der Eingabekette).

Hierbei muss der **Name** der Eingabekette vollständig übereinstimmen, sonst wird diese nicht ausgeführt. Empfängt nun ein Gerät eine SMS mit diesem Text, so wird die Eingabekette ausgeführt.

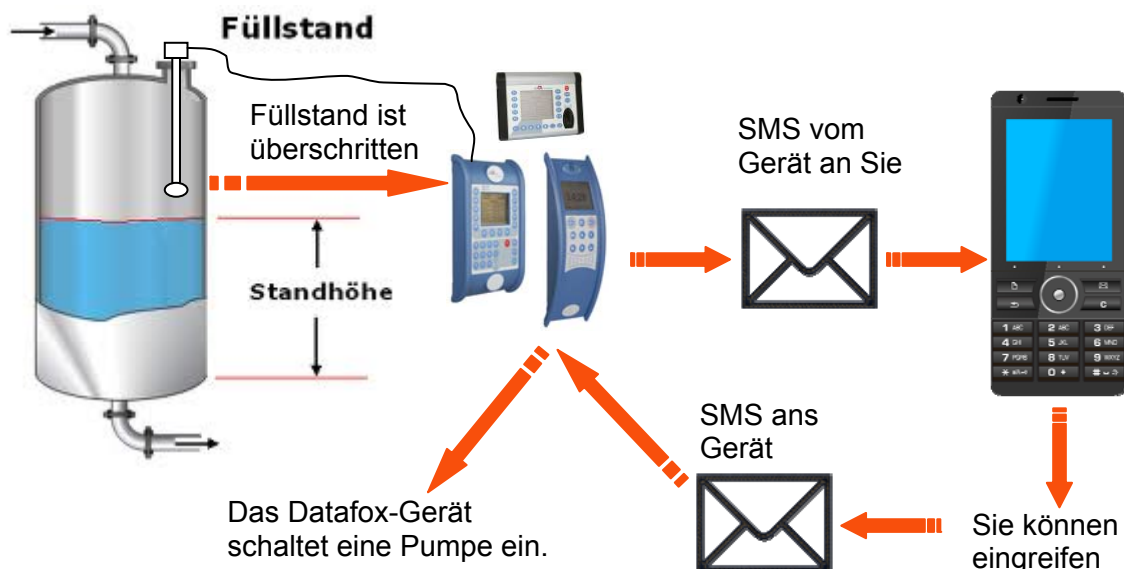
Die Möglichkeiten die sich dadurch ergeben sind sehr zahlreich.
 Beispiele:

Mit der SMS kann eine Türöffnung durchgeführt werden.



Überwachungsservice einer technischen Anlage bei Störung oä..

Sollte die Regelung des Füllstandes mal abweichen, kann dies durch eine SMS gemeldet werden. Das Datafox MasterIV soll hier nicht als Regler, sondern nur als Benachrichtigung bei einer Abweichung dienen. Bei Bedarf kann auch ein Eingriff erfolgen.



Achtung:

Dies ist nur ein Beispiel, die .welches die Möglichkeiten darstellen soll.
 Bedenken Sie hierbei, dass die Übertragung einer SMS keine 100% Sicherheit gibt.

2. Data on Card

2.1. Allgemeine Informationen

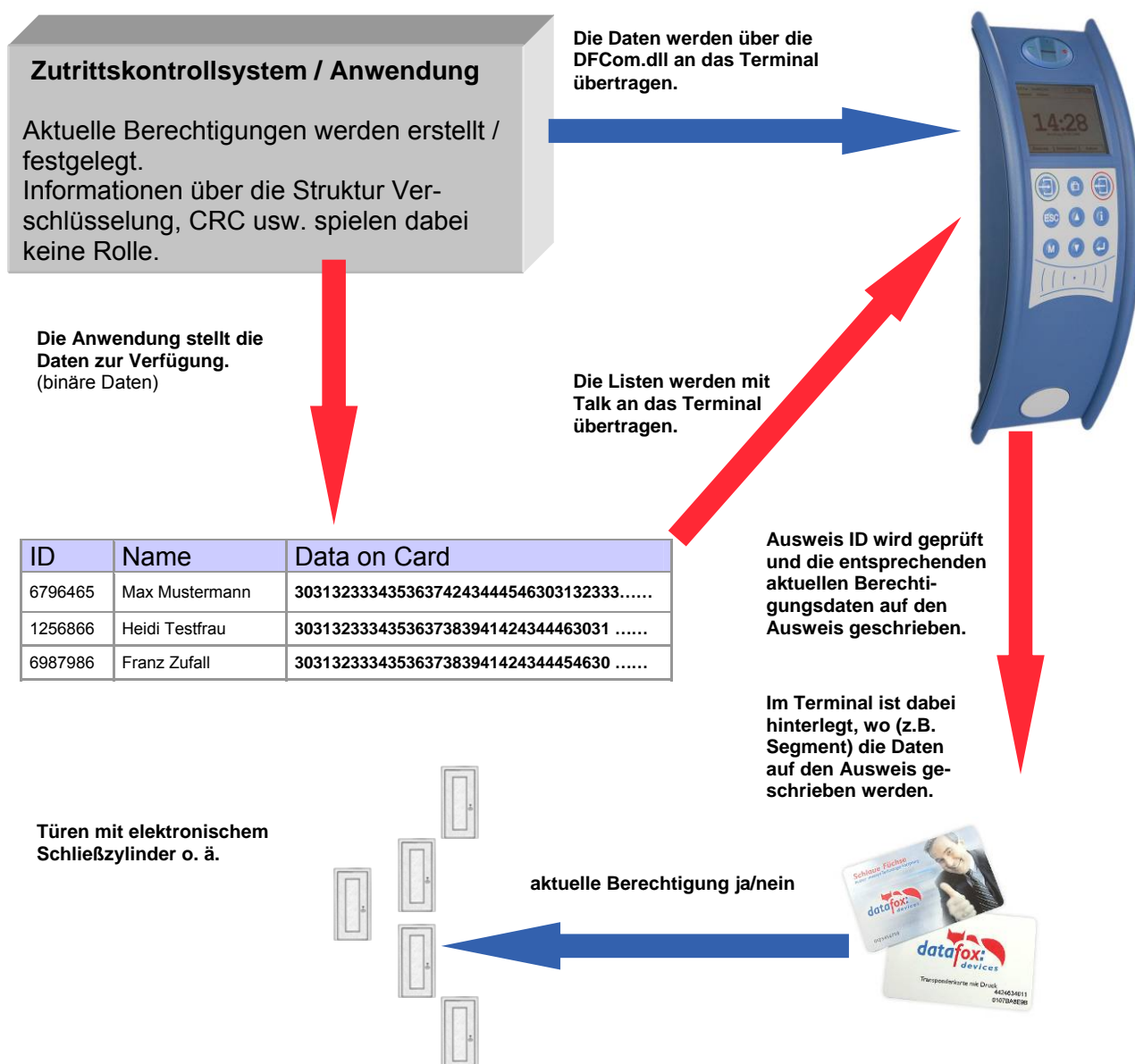
Mit der Funktion Data on Card ist es möglich, Daten mit einer individuellen Struktur auf einen Transponder zu schreiben.

Diese Daten werden in Form einer Liste von Ihrer Anwendung zur Verfügung gestellt.

Diese Liste wird dann in das Terminal geladen und beim Vorhalten eines Transponders werden die Daten dann auf diesen geschrieben.

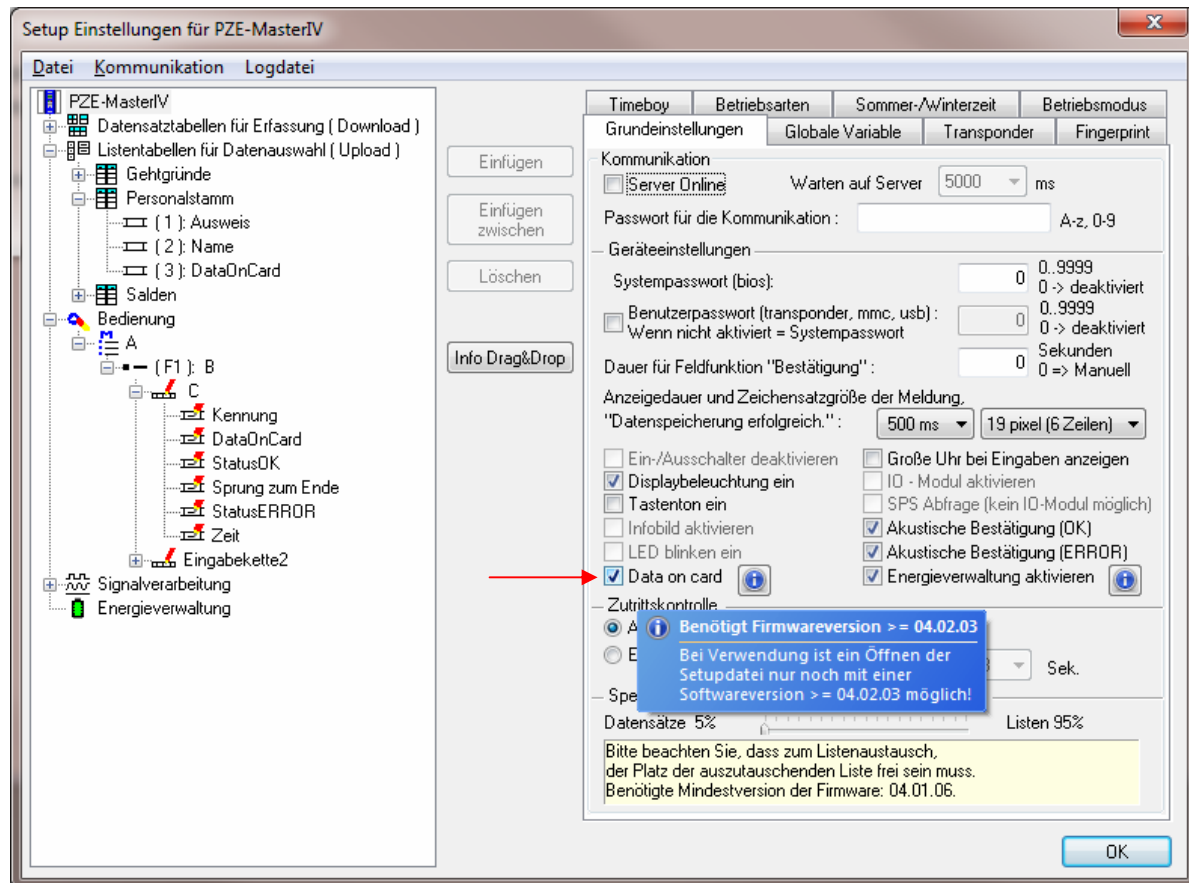
Folgendes Beispiel:

In Gebäuden mit „elektronischen“ Schließzylinder soll die aktuelle Tagesberechtigung für den Zutritt auf eine Transponderkarte geschrieben werden.



2.2. Einrichtung Data on Card

Data on Card ist eine Option des Gerätes bei der aus Listen Daten auf einen Transponder geschrieben werden können. Die Option muss bei der Bestellung mit angegeben werden. Bei Geräten die diese Option nicht haben, wird beim Ausführen eine Fehlermeldung angezeigt.



Data on Card arbeitet in **3 Schritten**:

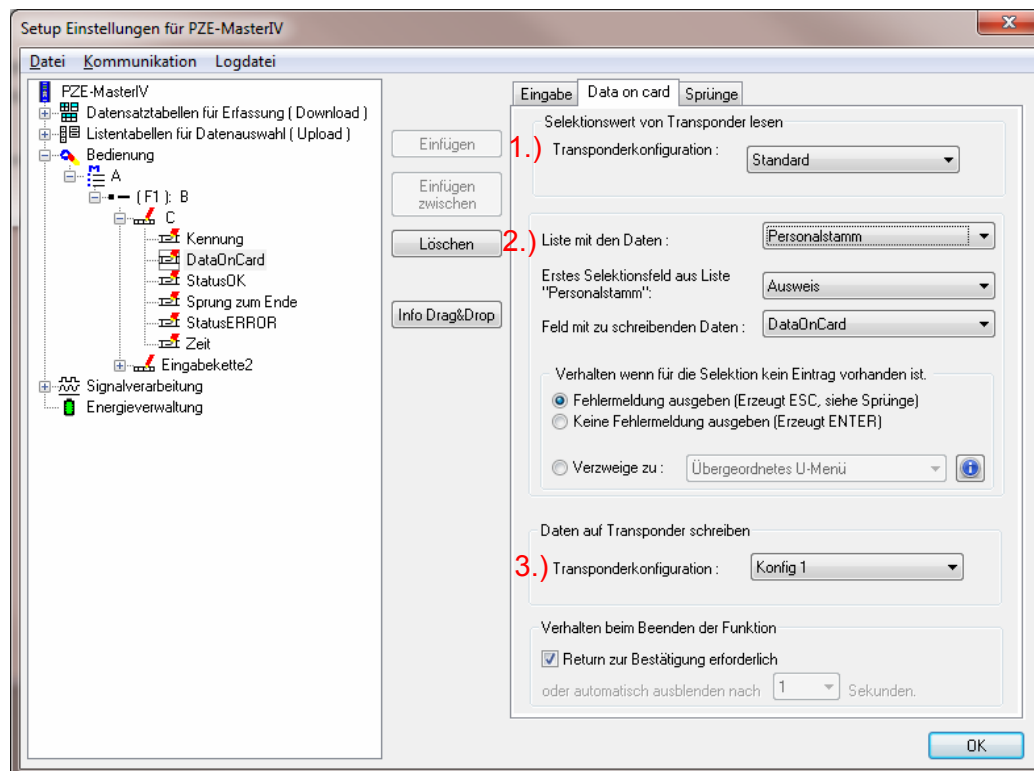
- Lesen eines Wertes vom Transponder, z.B. Seriennummer.
- Der Wert wird zum Selektieren einer Liste mit Binärfeld benutzt um die binären Daten zu lesen.
- Die binären Daten werden auf den Transponder geschrieben.

Der Rückgabewert der Funktion Data on Card für GV oder Datensatzfeld ist der Wert aus dem ersten Schritt „Lesen eines Wertes vom Transponder“. Bei Fehlern wie „der Wert wird nicht in der Liste gefunden“ oder das „Schreiben auf den Ausweis schlug fehl“ erzeugt die Funktion ein ESC. Über die Seite Sprünge kann dann entschieden werden, wie in der Eingabekette weiter gearbeitet wird.

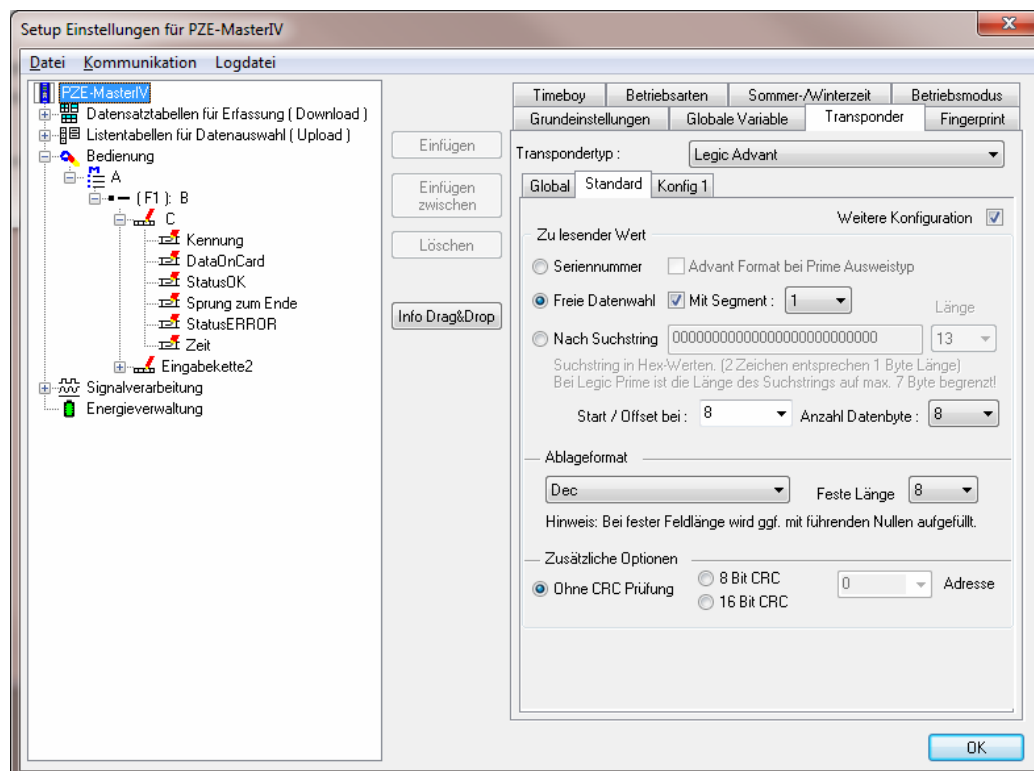
Die binären Felddaten innerhalb der Datei, die das DatafoxStudioIV importiert und überträgt, sind als Hexzeichenfolge anzugeben. Beim importieren über die DLL sind die Daten als Binärdaten zu übergeben.

Über die Bearbeitungsfunktionen von Listendaten DFCGetField, DFCSetField arbeiten Sie mit Zeichenfolgen, wobei die Firmware eine Konvertierung der Hexstrings in und zu den Binärdaten vornimmt.

Einstellungen bei Data on Card



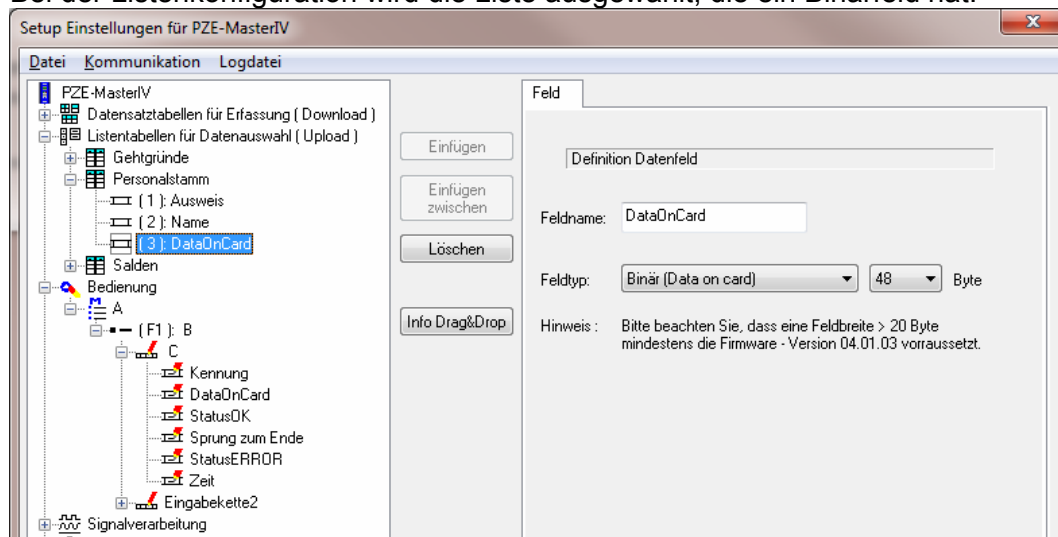
1.) Transponder Konfiguration Lesen



Die Transponderkonfiguration für das Lesen kann frei gewählt werden. Sie muss aber zuvor in den Tranpondergrundeinstellungen definiert worden sein.

2.) Listenkonfiguration

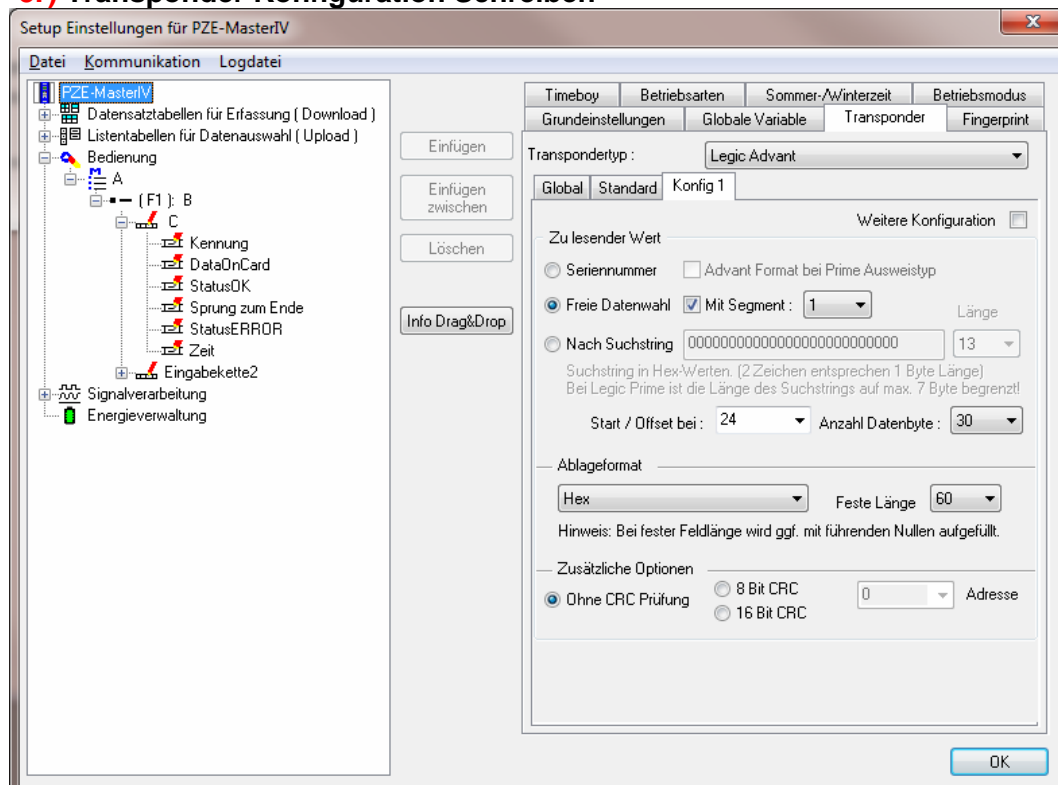
Bei der Listenkonfiguration wird die Liste ausgewählt, die ein Binärfeld hat.



In diesem Beispiel ist im Feld Ausweis der Wert vom Transponder Lesen, der in der Liste gesucht wird. Die zu schreibenden Daten sind im Feld Data on Card vom Typ Binär. Die max. Feldgröße darf 220 Byte nicht überschreiten.

Anschließend kann noch bei Listenfehlern die weitere Verfahrensweise festgelegt werden.

3.) Transponder Konfiguration Schreiben



Die Transponderkonfiguration für das Lesen kann frei gewählt werden, sie muss aber zuvor in den Tranpondergrundeinstellungen definiert worden sein.



Hinweis:

Zuerst die Transponderkonfiguration fertig stellen, dann die Liste mit dem Binärfeld anlegen und zum Schluss die Feldfunktion Data on Card parametrieren.

Beispiel für Data on Card:

Ausweis mit Seriennummer **1848989745**

Listeneintrag für **1848989745** in der Datei vor dem Übertragen in das Gerät

Feld ID Feld Data(Binärfeld) hier als Hex-Bytes

1848989745 30313233343536373839414243444546303132333435363738394142434445463031323334353637383941

Daten nach Konvertierung bzw. innerhalb des Gerätes

Feld ID Feld Data(Binärfeld) hier binär

1848989745 0123456789ABCDEF0123456789ABCDEF0123456789A

Auf den Ausweis werden folgende Daten geschrieben

0123456789ABCDEF0123456789ABCDEF0123456789A

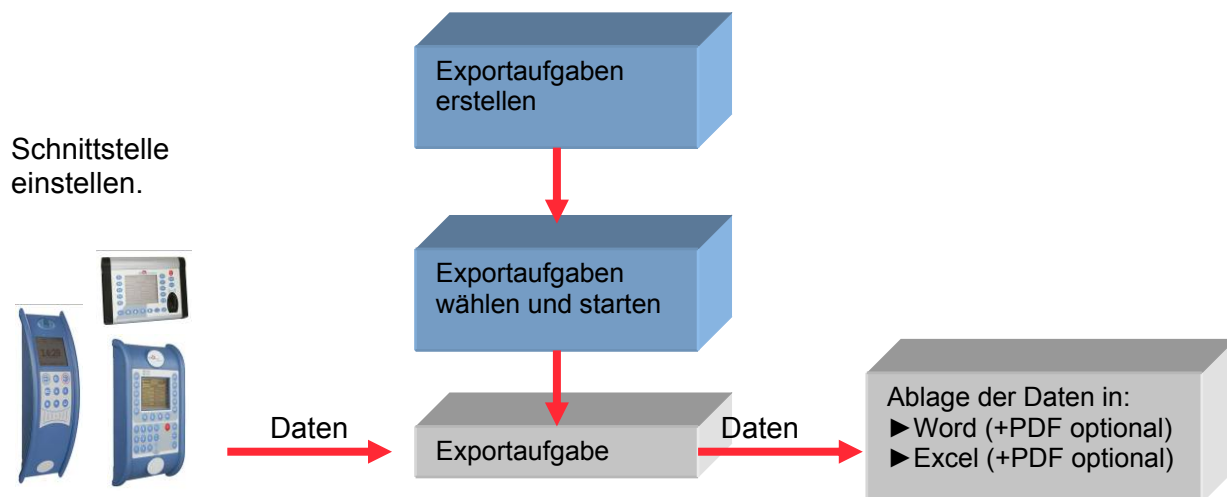
Binär sehen die Daten so aus:

0x30, 0x31, 0x32, 0x33, 0x34

3. Office Connect

3.1. Allgemeine Informationen


Office Connect stellt eine einfache Möglichkeit dar, die Daten aus Ihren Datafox MasterIV Geräten für die Einsichtnahme oder die Weiterverarbeitung bereitzustellen. Unterstützt werden die Ausgaben in die üblichen Office-Formate XLS und DOC. Zusätzlich kann eine Protokolldatei im PDF-Format zu jedem Export angelegt werden. Um die Einstellungen der Ausgaben zu speichern, legen Sie Exportaufgaben an. Sie stellen dann nur die Verbindungsparameter zu einem Gerät ein, wählen die Exportaufgabe und starten den Export. Diese legt die Daten aus dem eingestellten MasterIV Gerät in der zuvor gewählten Datei (Word, Excel, PDF) ab.

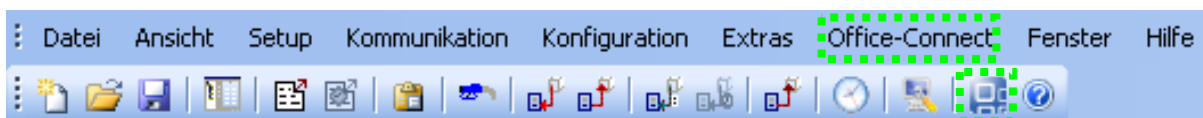


Achtung:

Die Einstellung der Schnittstelle zu dem jeweiligen Gerät muss vor dem Starten einer Exportaufgabe vorgenommen werden.
Die Exportaufgabe bezieht sich nur auf die Art der Ablage der Daten und nicht auf ein bestimmtes Gerät.

3.2. Bedienung

Um die Anwendung "Office Connect" zu starten, klicken Sie auf "Office-Connect" oder auf dieses Symbol .



Hinweis:

Für Office-Connect wird eine Mindestversion von Word / Excel 2003 vorausgesetzt.

3.2.1. Exportaufgaben erstellen

Eine Exportaufgabe enthält alle Einstellungen für einen Export der Daten von den Datafox MasterIV Geräten.

Das Erstellen und Ändern der Exportaufgaben erfolgt mit Hilfe eines Assistenten.

Die Einstellungen im Assistenten sind weitestgehend selbsterklärend.



Exportaufgabe Bearbeiten



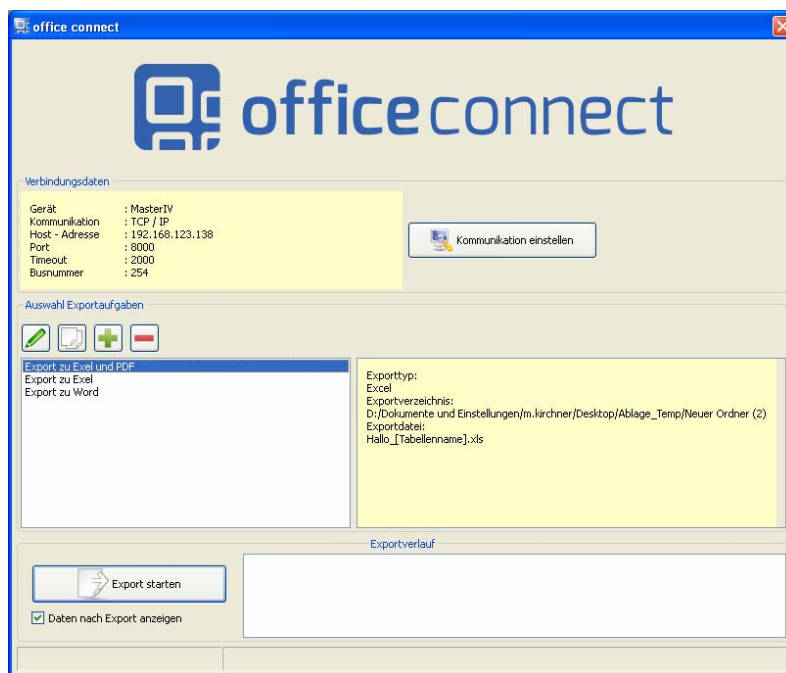
Exportaufgabe kopieren



Neue Exportaufgabe erstellen



Exportaufgabe löschen



Mit einem Klick auf den Button starten Sie den jeweiligen Assistenten.

Im Assistenten können Sie eine Exportvorlage heranziehen. Auf der Produkt-DVD finden Sie entsprechende Vorlagen.

Sie können nach dem ersten Export die Datei bearbeiten und Formatierungen ändern. Wenn dann ein erneuter Export (mit Option Daten anhängen) gestartet wird, werden diese Formatierungen beibehalten. (Spaltenbreite; Textformatierungen; Randeinstellungen usw.)



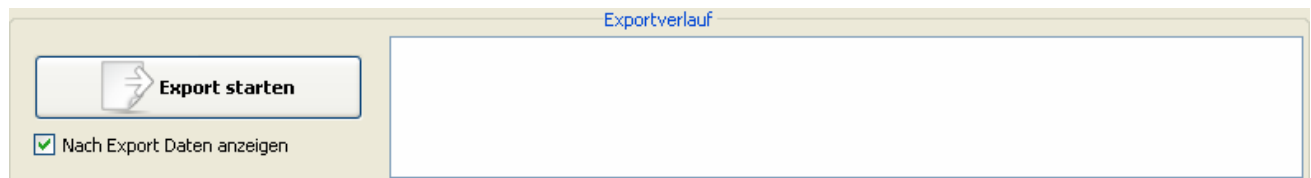
Hinweis:


Sie können in der Dokumentenvorlage bei Exporten vom Typ Word einen Textmarker mit der Bezeichnung „**insert**“ setzen, um zu bestimmen, an welcher Stelle die Daten in dem Dokument gespeichert werden sollen.

3.2.2. Export starten

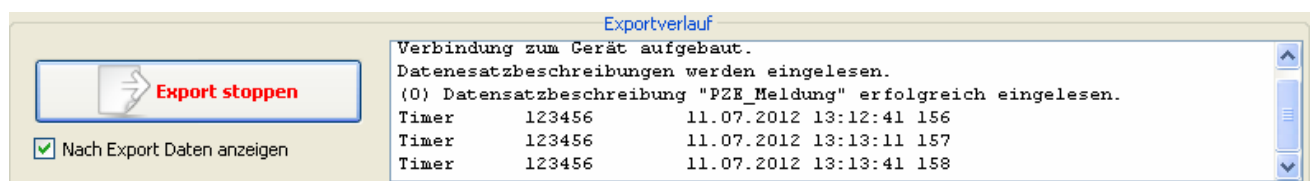
Um einen Export durchzuführen, müssen Sie zuerst die Verbindung zu einem Datafox Gerät herstellen. Sie kennen diesen Dialog aus dem Menü ->Kommunikation ->Einstellungen.

Mit der Schaltfläche „Export starten“ starten Sie eine Exportaufgabe, die Sie im folgendem Dialog aus der Liste auswählen.



Wählen Sie zusätzlich die Option  Nach Export Daten anzeigen wird die Exportdatei nach dem Export der Daten geöffnet.

Den Verlauf des Exports können Sie im Feld „Exportverlauf“ anschauen.



Sie können einen laufenden Export zu jeder Zeit stoppen mit der Schaltfläche „Export stoppen“. Alle Daten, die zu diesem Zeitpunkt bereits exportiert wurden, werden in der Exportdatei gespeichert und der Export wird beendet.

4. Funktionserweiterung für die Zutrittskontrolle

4.1. Allgemeine Informationen

Die Zutrittskontrolle wurde um einige Funktionalitäten erweitert. Dazu wurde die Tabelle „**Action2**“ eingeführt. Diese ersetzt die bisher bekannte „**Action**“-Tabelle. Eine Beschreibung zum Aufbau der [Tabelle „Action2“](#) finden Sie am Ende dieses Kapitels. Aufgrund der zusätzlichen Referenzen sind nun sehr viele Szenarien darstellbar.

Die nachfolgenden Beispiele geben einen kurzen Überblick dazu:

4.2. Beispiele

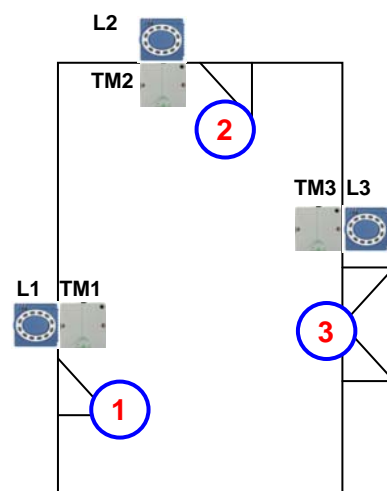
Beispiel Werkstatt

Der Hausmeister kommt am Morgen um 7.00 Uhr und nutzt dabei einen Eingang **1**.

- mit seinem Transponder wird der Eingang 1 für 5 Sekunden geöffnet.
- weiter wird das Tor **3** für das Öffnen mit einem Taster über einen Schließerkontakt bis 16.00 Uhr freigegeben.
- und der Eingang **2** bleibt bis 16.00 Uhr für das Personal geöffnet.

Die Schließung erfolgt über:

- 1 - einen Transponder der Gruppe 40
- 2 - durch ein langes Vorhalten eines berechtigten Transponders an der jeweiligen Tür
- 3 - Automatisch um 16.00 Uhr (muss im Zeitmodell hinterlegt werden siehe Nr.2 in Spalte „RefTime“)



Der Aufbau der Reader-, Location-, Action2- und Identification-Tabellen könnte wie folgt aussehen:

Tabelle Reader

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	320	0	0	0	Mastergerät
2	1	010	100	0	0	Türmodul an RS485 (TM1) Da dies nur ein Türmodul ist, muss hier keine Action ausgeführt werden.
3	1	011	100	1000	0	Leser über RS232 (L1) Wird an diesem Leser eine Buchung getätigt, werden alle Action mit der ID 1000 ausgeführt.
4	1	020	200	0	0	Türmodul an RS485 (TM2) Da dies nur ein Türmodul ist, muss hier keine Action ausgeführt werden.
5	1	021	200	2000	0	Leser über RS232 (L2) Wird an diesem Leser eine Buchung getätigt, werden alle Action mit der ID 2000 ausgeführt.
6	1	030	300	0	0	Türmodul an RS485 (TM3) Da dies nur ein Türmodul ist, muss hier keine Action ausgeführt werden.
7	1	031	300	3000	0	Leser über RS232 (L3) Wird an diesem Leser eine Buchung getätigt, werden alle Action mit der ID 3000 ausgeführt.

Tabelle Time

ID	Weekdays	TimeStart	TimeEnd	Beschreibung
1	1234567	00:01	23:59	24h Buchungen möglich
2	1234567	07:00	16:00	Zeit für Daueröffnung

Tabelle Action2

ID	RefGroup	RefTime	RefReader Relais	PortOut	Elapse	RefReader LED	RefTime Relais	Beschreibung
Buchungen am Leser 1								
1000	10	0	2	1	5	3	0	Normales Öffnen für 5s. Gruppen (10; 20; 30) haben Zugang. (immer)
1000	20	0	2	1	5	3	0	
1000	30	0	2	1	5	3	0	
1000	30	2	4	1	32400	5	0	Tür 2 wird für 9h geöffnet.
1000	30	2	6	1	32400	7	0	Tor 3 wird für 9h freigegeben.
1000	40	0	2	1	-1	3	0	Türöffnung wird zurückgenommen.
1000	40	0	4	1	-1	5	0	Torfreigabe wird zurückgenommen.
Buchungen am Leser 2								
2000	10	0	4	1	5	5	0	Normales Öffnen für 5s. Gruppen (10; 20; 30) haben (immer)
2000	20	0	4	1	5	5	0	
2000	30	0	4	1	5	5	0	
2000	30	2	4	1	32400	5	0	Tür 2 wird bis 16Uhr geöffnet.
2000	30	2	6	1	32400	7	0	Tor 3 wird für 16Uhr freigegeben.
2000	40	0	4	1	-1	5	0	Türöffnung wird zurückgenommen.
2000	40	0	6	1	-1	7	0	Torfreigabe wird zurückgenommen.
Buchungen am Tor (Leser 3)								
3000	0	0	6	1	5	0	0	Für alle Gruppen die in der Location für das Tor (L3) eingetragen sind, wird diese Action ausgeführt.

Tabelle Location

ID	refGroup	refTime	refTimeNoPin	Bemerkungen
100	10	1	0	Gruppe 10, 20, 30 und 40 haben Zutritt an diesem Leser.
100	20	1	0	
100	30	1	0	
100	40	1	0	
200	10	1	0	Gruppe 20 kann den Eingang L2 nicht benutzen.
200	30	1	0	
200	40	1	0	
300	10	1	0	Nur der Werkstattleiter und der Hausmeister können das Tor öffnen. Der Hausmeister ist aber nicht berechtigt, die Daueröffnung von hier aus zu aktivieren.
300	30	1	0	

Tabelle Identification

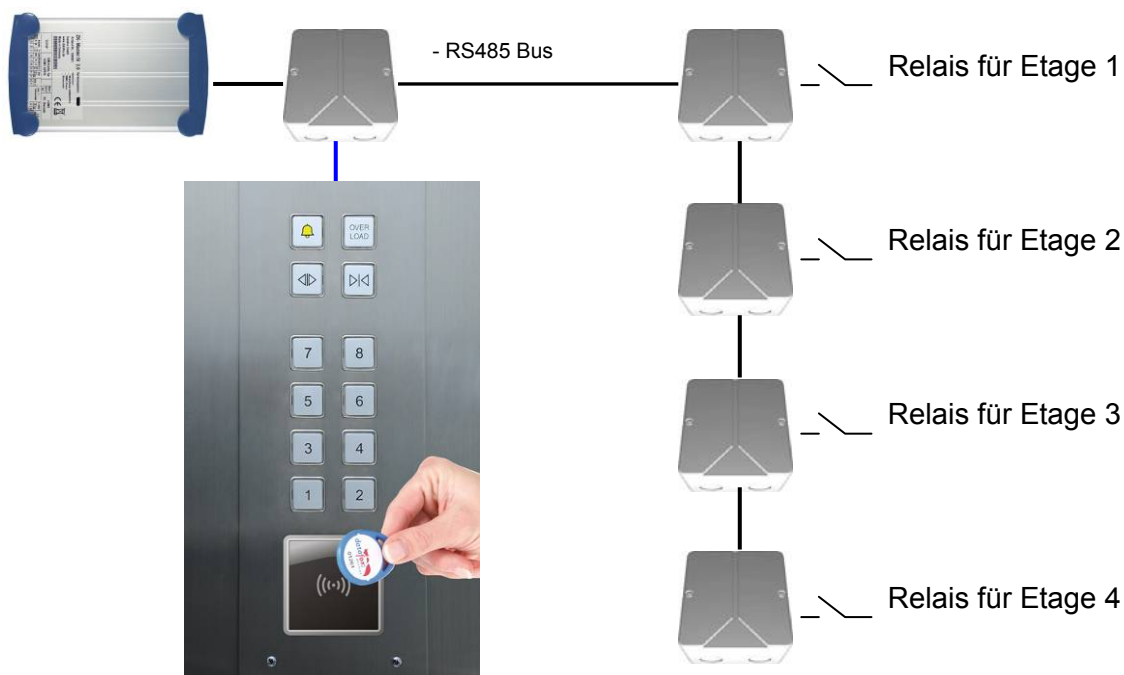
ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Beschreibung
1111	10	0	0	2005-01-01	2015-12-31	1	Werkstattleiter
2222	20	0	0	2005-01-01	2015-12-31	1	Angestellte
3333	30	0	0	2005-01-01	2015-12-31	1	Hausmeister
4444	40	0	0	2005-01-01	2015-12-31	1	Hausmeister 2, Transponder für Schließung

Beispiel Aufzugsteuerung

Ziel ist es, dass die jeweiligen Mieter nur in Ihre Etage fahren dürfen.

Hält der Mieter seinen Transponder vor, so wird der Taster am Bedienfeld im Fahrstuhl für die Etage, in der der Mieter wohnt, für 20 Sekunden freigegeben.

In der Aufzugskabine ist ein Transponderleser angebracht und die Steuerung befindet sich auf der Kabine. Der RFID-Leser ist dann in der Kabine angebracht.



Der Aufbau der Reader-, Location-, Action2- und Identification-Tabellen könnte folgendermaßen aussehen:

Tabelle Reader

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	100	0	0	Türmodul an RS485 mit Relais für die Etage 1
2	1	020	100	0	0	Türmodul an RS485 mit Relais für die Etage 2
3	1	030	100	0	0	Türmodul an RS485 mit Relais für die Etage 3
4	1	040	100	0	0	Türmodul an RS485 mit Relais für die Etage 4
5	1	320	0	0	0	Mastergerät
6	1	000	100	1000	0	Leser an RS485

Tabelle *Action2*

ID	RefGroup	RefTime	RefReader Relais	PortOut	Elapse	RefReader LED	RefTime Relais	Beschreibung
Buchungen am Leser in der Kabine								
1000	10	0	1	1	20	1	0	Gruppe 10 fährt nur in Etage 1.
1000	20	0	2	1	20	2	0	Gruppe 20 fährt nur in Etage 2.
1000	30	0	3	1	20	3	0	Gruppe 30 fährt nur in Etage 3.
1000	40	0	4	1	20	4	0	Gruppe 40 fährt nur in Etage 4.
1000	50	0	1	1	20	5	0	Gruppe 50 darf in die Etagen 1 und 2 fahren. Gruppe 60 darf in die Etagen 1,2,3 und 4 fahren.
1000	50	0	2	1	20	5	0	
1000	60	0	1	1	20	5	0	
1000	60	0	2	1	20	5	0	
1000	60	0	3	1	20	5	0	
1000	60	0	4	1	20	5	0	

Tabelle *Location*

ID	refGroup	refTime	refTimeNoPin	Bemerkungen
100	10	1	0	Die Gruppen 10, 20, 30, 40, 50 und 60 müssen am Leser zugelassen sein.
100	20	1	0	
100	30	1	0	
100	40	1	0	
100	50	1	0	
100	60	1	0	

Tabelle *Identification*

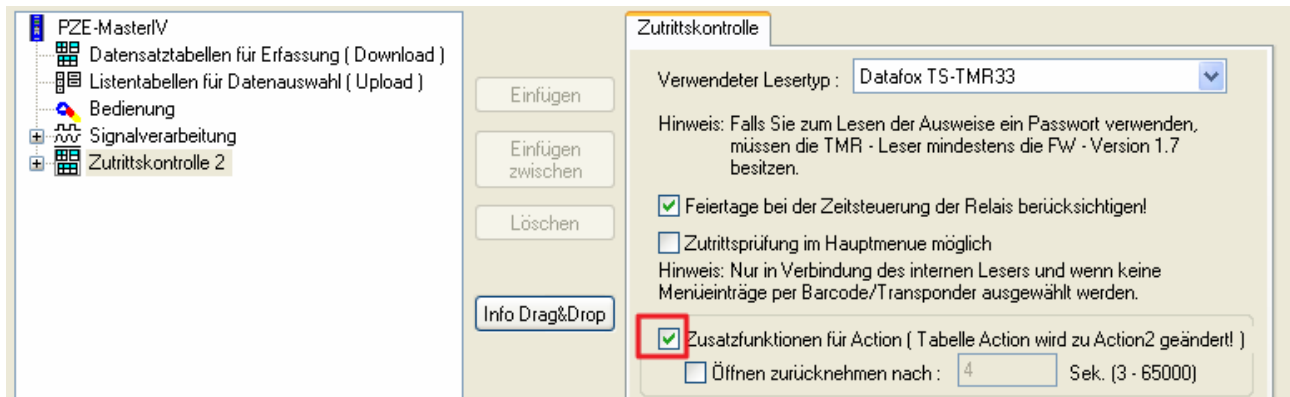
ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Beschreibung
1111	10	0	0	2005-01-01	2015-12-31	1	Mieter Wohnung 1. Etage
1112	10	0	0	2005-01-01	2015-12-31	1	
1113	10	0	0	2005-01-01	2015-12-31	1	
2222	20	0	0	2005-01-01	2015-12-31	1	Mieter Wohnung 2. Etage
3333	30	0	0	2005-01-01	2015-12-31	1	Mieter Wohnung 3. Etage
4444	40	0	0	2005-01-01	2015-12-31	1	Mieter Wohnung 4. Etage
5555	50	0	0	2005-01-01	2015-12-31	1	Mieter, der in Etage 1 und 2 fahren darf.
6666	60	0	0	2005-01-01	2015-12-31	1	Hausmeister darf in alle Etagen fahren.

Tabelle *Time*

ID	Weekdays	TimeStart	TimeEnd	Beschreibung
1	1234567	00:01	23:59	24h gültig an den in der ganzen Woche

4.3. Beschreibung der Tabelle „Action2“

Das Umschalten der Tabelle „Action“ in „Action2“ erfolgt im DatafoxStudioIV.



Bezeichner	Datentyp	Länge	Beschreibung
ID	Nummer (int)	4	Enthält eine eindeutige ID. Sind mehrere gleiche IDs vergeben, werden alle Aktionen mit ID ausgeführt.
RefGroup	Nummer (int)	4	Verweist auf die Gruppe für die diese Aktion durchgeführt werden darf. 0 = Alle Gruppen, die in der Location zugelassen sind, führen diese Action aus.
RefTime	Nummer (int)	4	Verweist auf den Zeitraum, an der die Aktion durchgeführt werden darf. (0 = immer gültig) ! Nicht mit Zeitangaben in RefTimeRelais vermischen!
RefReader Relais	Nummer (int)	4	Verweist auf die Reader Tabelle und gibt an, an welchem Türmodul das Relais geschaltet wird.
PortOut	Nummer (Byte)	1	Gibt an, welcher Relaisausgang geschaltet wird. Mögliche Angaben: 1 und 2
Elapse	Nummer (int)	6	Gibt die Zeit an, wie lange ein Relais geschaltet wird. ! Die Angabe erfolgt hier in Sekunden! Ist hier (-1) eingetragen, werden die Relaisschaltungen sofort zurückgenommen Ist hier (0) eingetragen, so werden die Relais für den unter RefTime angegebenen Zeitraum ab der Buchung geöffnet.
RefReaderLED	Nummer (int)	4	Verweist auf die Reader Tabelle und gibt an, an welchem Modul zusätzlich die grüne LED parallel zum Relais geschaltet wird.
RefTimeRelais (nur für Auto- matische Zeitsteuerung)	Nummer (int)	4	Das Zeitmodell gibt an, wann der Ausgang geschaltet wird. (0 = wird nicht verwendet). Wird ein Zeitmodell angegeben, so wird diese Aktion zur angegebenen Zeit durchgeführt. (Automatische Zeitsteuerung) ! Aktionen die hier ausgeführt werden, dürfen nicht mit Zutrittsaktionen gemischt werden!



Achtung:

Durch Übertragen der Tabelle „Action2“ an das Gerät, wird die Tabelle „Action“ ersetzt. Somit werden nur noch Einträge der Tabelle „Action2“ berücksichtigt.



Achtung:

Möchten Sie weiterhin nur mit der „Action“ Tabelle arbeiten, so darf die Tabelle „Action2“ nicht an das Gerät übertragen werden.
Wurde bereits eine Tabelle „Action2“ an das Gerät übertragen, muss diese durch das Einspielen eines Setups gelöscht werden.

5. HTTP über LAN/WLAN mit DNS-Auflösung



Ab der Firmware 04.02.02 wurde das Senden der Daten per HTTP über LAN/WLAN an einen Web-server ermöglicht.

Bisher musste die Adresse des Web - Servers in Punktnotation erfolgen (z.B.:192.185.123.456).

Nun ist es auch möglich, den Server mit dem Hostnamen aufzurufen (z.B.:www.datafox.de).

Dazu muss in der HTTP.ini die IP eines DNS-Servers hinterlegt werden, welcher dann die DNS-Auflösung übernimmt.

Die Angabe des Servers kann nun auch mit Namen erfolgen.

Angabe eines DNS-Servers für die Namensauflösung.

Werte der Variablen bearbeiten.

Durch einfaches Klicken auf den Wert oder Betätigung der F2 Taste, erhalten Sie die Möglichkeit, diesen zu verändern.
Um ggf. die Wertvorgabe wiederherzustellen, löschen Sie bitte den Wert aus dem Feld. Nach verlassen des Feldes wird die Vorgabe wiederhergestellt.

Name	Wert
PHONE	*99***1#
GPRS	internet.t-mobile
USER	
PASSWORD	
HOST	www.datafox.de
PORT	80
HTTPSEND	
ALIVE	0
HTTPTIMEOUT	20000
HTTPTYPE	1.1
SIMPIN	0
SIMPUK	0
ROAMING	1
RESETTRIGGER	32
ATTACH	32
ERRORLEVEL	0
HTTP	0
KEY	
DNS1	130.149.17.5

Information zum gewählten Eintrag

In diesem Bereich wird nach Selektion eines Listeneintrags, eine entsprechende Beschreibung und weitere Informationen zu diesem angezeigt.

Speichern unter ... Speichern



Hinweis:

In internen Netzwerken muss entweder ein DNS-Server vorhanden sein, oder über die Angabe eines Gateways, ein externer öffentlicher DNS-Server genutzt werden.

Links zu öffentlichen DNS-Servern:

<http://www.stanar.de/>

http://de.wikipedia.org/wiki/Domain_Name_System

6. Neue RFID Reader (ISO14443 u. ISO15693) 13,56MHz

Ab sofort stehen 2 neue RFID-Reader für 13,56MHz zur Verfügung. Siehe Preisliste:

1. Gerät mit 13,56 MHz

ISO 14443 für Mifare-Desfire
ISO 14443 Mifare-Plus, -Classic, -Ultralight

Dieser Leser (TWN3 Mifare NFC) ist aufgrund der Antennenbauart besonders für RFID - Karten geeignet.

2. Gerät mit 13,56 MHz

ISO 14443 für Mifare-Classic, -Plus, ...
ISO 15693 für ICode, My-D, Tag-it, ...

Dieser Leser (TWN3 Multi-ISO) ist aufgrund der Antennenbauart besonders für RFID - Schlüsselanhänger geeignet und bietet bei diesen die beste Lesereichweite.

Übersichtstabelle Leseverfahren

IEC/ISO	Beschreibung	read	write	read	write
14443A	Mifare Mini	X	X	X	X
	Mifare Classic 1k und 4k	X	X	X	X
	Mifare Plus S und X	X	X	X	X
	Mifare Ultralight/ Mifare Ultralight C	X	X	X	X
	Mifare DESFire	X	X	X	X
	LegicAdvant (ISO14443 Typ) nur Seriennummer *	X*	-	X*	-
	Andere ISO14443 Typen (SmartMX) nur Seriennummer*	X*	-	X*	-
14443B	Calypso, CEPAS, Moneo nur Seriennummer*	X*	-	X*	-
14443-2	iClass, Piccopass nur Seriennummer*	X*	-	X*	-
14443-3	SRX Transponder von ST Microelectronics, nur Seriennummer *	X*	#	X*	#
15693	iCode	X	X	-	-
	My-D Vicinity	X	#	-	-
	Tag-it nur Seriennummer*	X*	#	-	-
	LegicAdvant (ISO15693 Typ) nur Seriennummer*	X*	-	-	-
	24LR16 / 24LR64 von ST Microelectronics, nur Seriennummer *	X*	#	-	-
	MB89R118/MB89R119 von Fujitsu, nur Seriennummer *	X*	#	-	-
	LRI 2k / 64k von ST Microelectronics, nur Seriennummer*	X*	#	-	-
	Andere ISO15693 Typen nur Seriennummer*	X*	-	-	-

* lesen, nur Seriennummer.

schreiben, kann auf Anfrage umgesetzt werden.

6.1. ISO 14443A - Mifare Familie

6.1.1. Mifare Mini

Der Mifare Mini ist ein kompatibler Transponder zum Mifare Classic 1k, nur mit einer Speicherbegrenzung von 320 Byte. Er hat also nicht 16, sondern nur 5 Sektoren.



Hinweis:

Der Mifare Mini kann über die Mifare Plus Grundeinstellungen im DatafoxStudioIV konfiguriert werden.

6.1.2. Mifare Classic

Mifare ist in 16 Sektoren a 4 Blöcken zu je 16 Byte organisiert. Jeder 4. Block dient der Verschlüsselung der Daten auf dem Transponder und enthält, aufgeteilt in einen Key-A und einen Key-B, je 6 Byte lang ein Passwort für Schreib- und Leserechte, sowie die „Access Condition“, in der die Sektorformate definiert sind. Je nach Anwendung können alle Blöcke eines Sektors im Default-Format vorliegen (d.h., Key A ist der Lese- und Schreibschutzschlüssel) oder im Data bzw. Value-Format, wobei Key A das Lesekennwort und Key B der Masterschlüssel für Lesen und Schreiben ist. Die Datafoxgeräte bis Version 4.1.4.xx unterstützen derzeit nur das Defaultformat.



Achtung:

Das Value-Format wird nicht unterstützt.
Das Data-Format können wir mit KeyA nur lesen.
Das Default-Format können wir mit KeyA lesen und schreiben.



Hinweis:

Es ist auch möglich, über die MifarePlus Grundeinstellungen im DatafoxStudioIV den Mifare Classic zu konfigurieren. Das ist notwendig, wenn mehrere Mifaretypen zum Lesen verwendet werden müssen oder auch bei DataOnCard.

6.1.3. Mifare Plus

Mifare Plus ist von der Datenstruktur ähnlich wie Mifare Classic. Die ersten 16 Sektoren haben 4 Blöcke und die folgenden haben 16 Blöcke a 16 Byte. Der Unterschied zum Mifare Classic ist, dass man verschiedene Sicherheitsstufen (Security Level) hat, die sich in erster Linie auf die Kryptografie auswirken. Es gibt wie beim Mifare Classic einen KeyA und einen KeyB der, je nach Security Level, unterschiedliche Längen hat.

Sicherheitsstufe	Beschreibung
SL0	Auslieferungszustand, die Seriennummer kann gelesen werden, ein Zugriff auf die Datenbereiche ist nicht möglich. Mit dem Card Master Key und Level Switch Key kann die Sicherheitsstufe konfiguriert werden.
SL1	Kompatibilitätsmodus zum MifareClassic, der Mifare Plus ist 100% kompatibel zum Mifare Classic und benutzt auch den Crypto1 Algorhythmus mit 6Byte(48Bit) Keys.
SL2 Nur bei Plus X	Datenzugriff wie beim MifareClassic mit Cryptokey, aber die Authentifizierung erfolgt über 16 Byte AES-Keys. In SL2 gibt es als 2 Crypto1 Keys und 2 AES Keys.
SL3	Kommunikation über ISO1443-4 Protokoll und AES Authentifizierung und Pre-Shared Keys, sowie MACing. Es gibt 2 AES Keys. Weiterhin ist zum Schutz der Seriennummer optional Random UID möglich. Bei MifarePlus X erfolgt die Kommunikation über AES Verschlüsselung und beim MifarePlus S ist die Kommunikation unverschlüsselt.


Hinweis:

In SecurityLevel 1 können MifarePlus, Mifare Classic und Mifare Mini gelesen und geschrieben werden, soweit die eingestellten Sektoren auf dem Ausweis existieren.


Achtung:

Mifare Plus Karten können nur die Sicherheitsstufe nach oben wechseln. Rückwärts ist es nicht möglich.
Ein Ändern der Sicherheitsstufe über MasterIV Geräte ist nicht möglich.

6.1.4. Mifare Ultralight

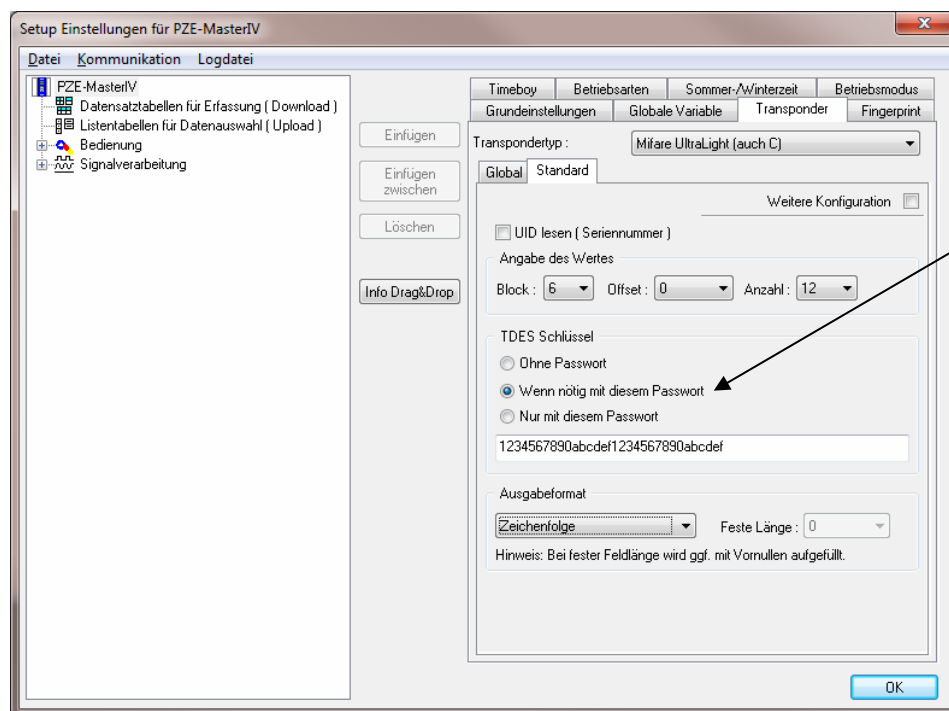
Mifare Ultralight benutzt im Gegensatz zu Mifare Classic und Plus keine Sektoren und Blöcke, sondern nur 16 Seiten mit 4 Byte, die man wie ein Segment bei Hitag Transpondern ansehen kann. Der einfache Ultralight hat keinen Zugriffsschutz bzw. nur einen Schreibschutz, der Ultralight C hingegen kann mit einer 3DES Authentifizierung geschützt werden. Im Auslieferungszustand ist dieser Schlüssel aber nicht gesetzt und der Ultralight verhält sich wie ein einfacher Ultralight. Der einfache Ultralight hat 16 Seiten mit 4 Byte, wobei nur 12 Seiten geschrieben werden können. Der Ultralight C hat 48 Seiten, von denen 40 geschrieben werden können.


Achtung:

Ein Mischbetrieb von Mifare Classic und Mifare Ultralight ist aufgrund der unterschiedlichen Datenstrukturen nicht möglich.


Hinweis:

Ein Mischbetrieb von Ultralight und Ultralight C ist möglich. Je nach Sicherheitsanforderungen ist die Schlüsselbenutzung auszuwählen.



Schlüsselbenutzung

6.1.5. Mifare DESFire

Der Mifare DESFire ist neben dem Mifare Plus X einer der sichersten und komplexesten Transponder. Im Gegensatz zum Mifare Plus oder Classic wird beim DESFire nicht auf feste Datenstrukturen mit Sektoren und Blöcken aufgebaut, sondern man benutzt beim DESFire ein Dateisystem wie beim PC.

Es gibt 2 Grundtypen beim DESFire: den alten DF40, auch als native Type bezeichnet und die Nachfolgeserie DF80, auch als EV1 bezeichnet.

Die Sicherheit beruht auf Verschlüsselungsverfahren, Authentifizierung mit Aushandlung von Sessionkeys und unterschiedlichen Kommunikationsmodi. Ebenso ist es möglich, die Seriennummer (UID) durch eine Random UID vor unberechtigtem Auslesen zu schützen.

	MF3IC40	MF3IC21-EV1	MF3IC41-EV1	MF3IC81-EV1
Speichergröße	4k	2k	4k	8k
Freier Speicher	4096 Bytes	2272 Bytes	4832 Bytes	7936Bytes
max. Anzahl Applikationen	28	28	28	28
max. Anzahl Dateien je Applikation	16	32	32	32
Verschlüsselung	DES, TDES (DF4)	DES, TDES, (DF4 und ISO) 3KTDES, AES	DES, TDES, (DF4 und ISO) 3KTDES, AES	DES, TDES, (DF4 und ISO) 3KTDES, AES
Anzahl Schlüssel je Applikation	14	14	14	14

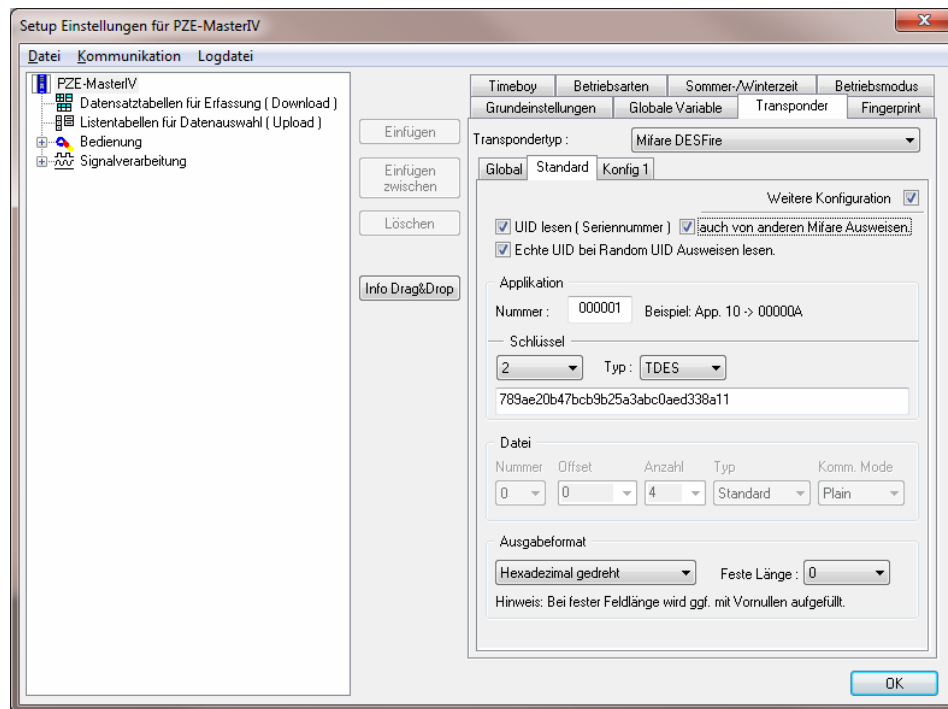
Die DF4 Verschlüsselung beruht auf dem DES-Algorithmus, jedoch mit besonderen NXP Abhandlungen. ISO Verschlüsselung beruht auf dem DES-Algorithmus entsprechend der ISO Norm.

Beide können DES mit 8 Byte Keys und TDES mit zwei 8 Byte Keys, also 16 Byte.

Bei Systemen, die nur einen 8Byte Key benutzen, muss der Key doppelt eingegeben werden. Der DESFire erkennt daran, ob DES oder TDES Verschlüsselung benutzt werden soll.

Kommunikationsmodi	Erklärung
Plain	Unverschlüsselt, die Daten zwischen Leser und RFID-Chip werden unverschlüsselt übertragen (nützlich für die Entwicklungsarbeit)
MACed	Unverschlüsselt mit verschlüsselter Prüfsumme (MAC), die Daten zwischen Leser und RFID-Chip werden unverschlüsselt übertragen, es wird aber eine Prüfsumme der Daten berechnet und diese wird verschlüsselt übertragen (alte Transpondermethode zur Validierung der Daten)
Enchiphered (Crypt)	Verschlüsselt, die Daten zwischen Leser und RFID-Chip werden verschlüsselt übertragen (Daten sind geschützt)

Lesen der Seriennummer



Für das Lesen der Seriennummer muss der Haken dafür gesetzt werden. Sollen zusätzlich zu DESFire Ausweisen auch noch andere Mifare Karten gelesen werden, so ist ein zusätzlicher Haken dafür zusetzen.

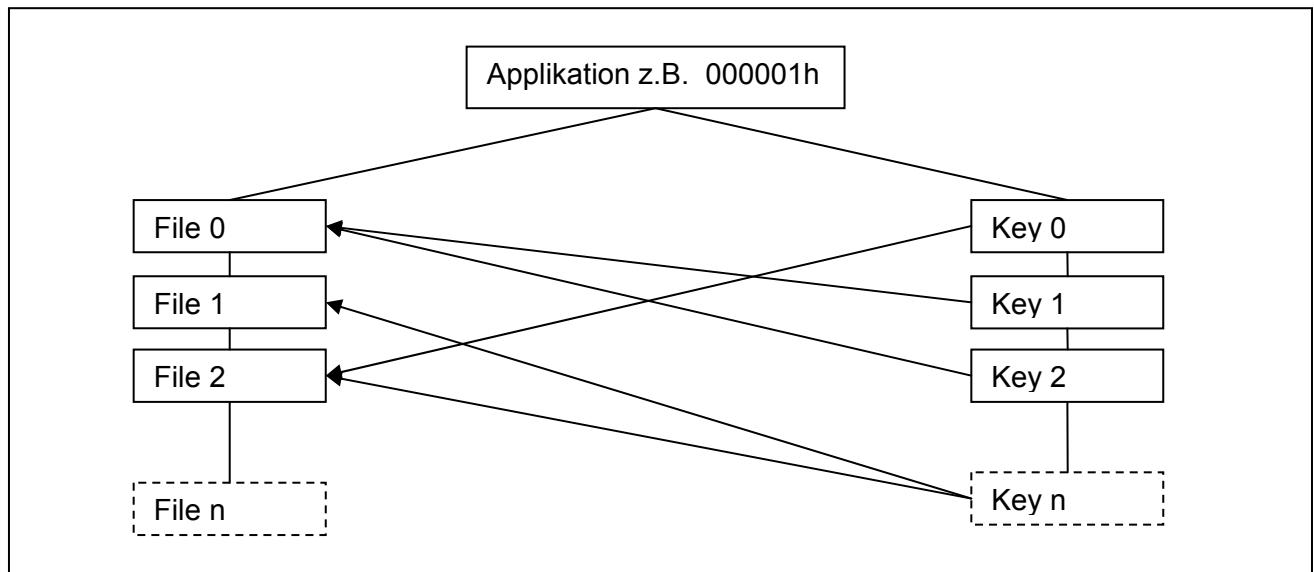
Sind DESFire Karten mit Random UID im Einsatz, so muss für das Ermitteln der echten Seriennummer eine Authentifizierung in eine Applikation erfolgen. Deshalb sind in diesem Fall noch die AID (Applikation Identifier) im Bereich von 000000 bis FFFFFFFF anzugeben, die Nummer von 0 bis 13 und der Typ des Schlüssels, sowie die Zeichenfolge des Schlüssels hexadezimal.

Lesen und Schreiben von Dateien

Typ	Beschreibung
Standard Data File	Datenfile
Backup Data File	Sicherheitskopie Datenfile
Value File	Zahlendatei (wird aktuell nicht unterstützt)
Linear Record File	Datenbanktabelle (wird aktuell nicht unterstützt)
Cyclic Record File	Datenbanktabelle, begrenzt, alte Daten werden überschrieben (wird aktuell nicht unterstützt)

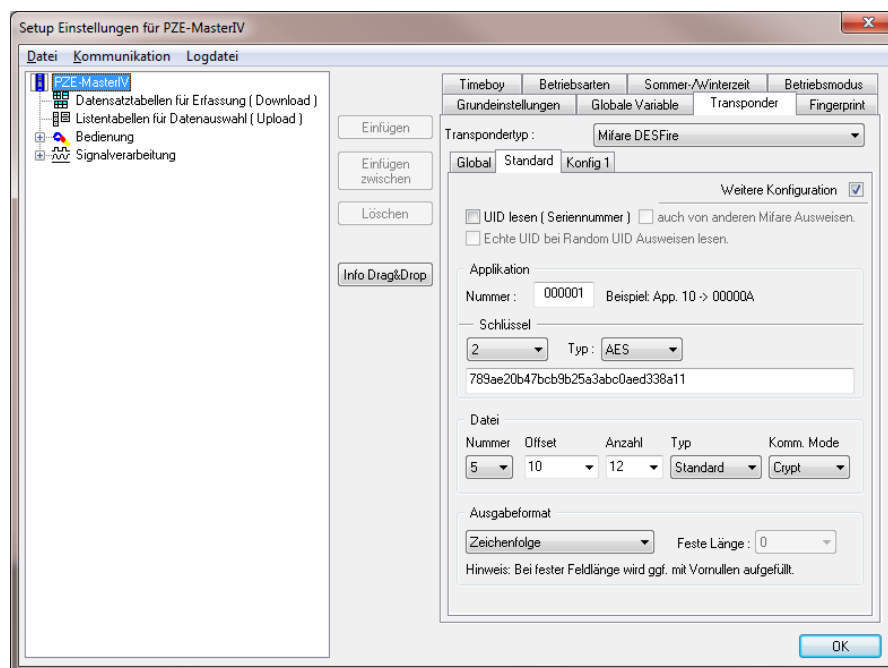
Tabelle Dateitypen

Der Zugriff auf die Daten erfolgt über das Auswählen einer Applikation mit anschließender Authentifizierung mittels eines Schlüssels. Der Schlüssel muss der Datei zugeordnet sein auf die der Zugriff erfolgen soll.



Achtung:

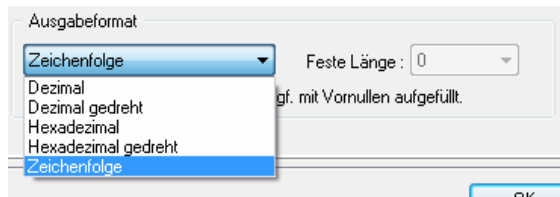
Dateien einer Applikation können verschiedene Schlüssel verwenden. Es ist wichtig, den richtigen Schlüssel für den Lese- oder Schreibzugriff auszuwählen.



Für den Zugriff auf eine Datei müssen folgende Einstellungen vorgenommen werden:

- Nummer der Applikation
- Nummer des Schlüssels in der Applikation
- Typ des Schlüssels (TDES, AES ...), DF4 Ausweise können nur DF4-Verschlüsselung
- Zeichenfolge des Schlüssels
- Nummer der Datei
- Offset, Startposition der Daten innerhalb der Datei
- Anzahl der zu lesenden Bytes
- Typ der Datei (Standard, Backup)
- Kommunikationsmodus (Plain, MACed, Crypt)

Ausgabeformat



Es gibt mehrere Ausgabeformate, wie die Daten im Datensatz und in der Anzeige aufbereitet werden. Wichtig ist hierbei die Betrachtungsweise, welches Byte das höherwertige ist. Dafür gibt es bei Dezimal und Hexadezimal auch die Variante gedreht, damit zum Schluss die richtigen Werte herauskommen. Die feste Länge dient dazu, eventuell zu kleine Zahlen auf eine definierte Länge durch Vornullen zu bringen.



Achtung:

Dezimale Zahlen basieren auf der Grundlage von 32Bit (4 Byte) Operationen. Es ist möglich, bis zu 64 Bit (8 Byte) zu verarbeiten, größere Daten führen zu Konvertierungsfehlern.

6.2. ISO 14443B – Calypso, CEPAS und Moneo

Bei diesen Transpondern kann nur die Seriennummer ermittelt werden. Ein Zugriff auf Datenbereiche ist nicht möglich. Diese Transponder können unter ISO Tags (13,56MHz) ausgewählt werden.

6.3. ISO 14443-2 iClass, Picopass

Bei diesen Transpondern kann nur die Seriennummer ermittelt werden. Ein Zugriff auf Datenbereiche ist nicht möglich. Diese Transponder können unter ISO Tags (13,56MHz) ausgewählt werden.

6.4. ISO 14443-3 SRX von ST Microelectronics

Bei diesen Transpondern kann nur die Seriennummer ermittelt werden. Ein Zugriff auf Datenbereiche ist auf Anfrage möglich. Diese Transponder können unter ISO Tags (13,56MHz) ausgewählt werden.

6.5. ISO 15693 – iCode, Tag-it, MyD

6.5.1. iCode

I-Code gibt es in verschiedenen Speichergrößen bis zu 64 Blöcken a 4 Byte. Die Datenbereiche können gelesen und geschrieben werden, außer der 8 Byte Seriennummer. Datenbereiche können mit einem Schreibschutz versehen werden.

6.5.2. Tag-it

Bei diesen Transpondern kann nur die Seriennummer ermittelt werden. Ein Zugriff auf Datenbereiche ist nicht möglich. Diese Transponder können unter ISO Tags (13,56MHz) ausgewählt werden.

6.5.3. My-D Vicinity von Infineon

My-D Vicinity gibt es in verschiedenen Speichergrößen bis zu 1024 Byte. Diese Transponder haben je nach Größe bis zu 128 Seiten a 8 Byte oder 256 Seiten a 4 Byte. Aktuell kann nur unverschlüsselt kommuniziert werden. Bei Ausweisen die mit einem Key belegt sind, kann nur die Seriennummer ermittelt werden.

6.5.4. 24LR16 / 24LR64 von ST

Bei diesen Transpondern kann nur die Seriennummer ermittelt werden. Ein Zugriff auf Datenbereiche ist nicht möglich. Diese Transponder können unter ISO Tags (13,56MHz) ausgewählt werden.

6.5.5. MB89R118 / MB89R119 von Fujitsu

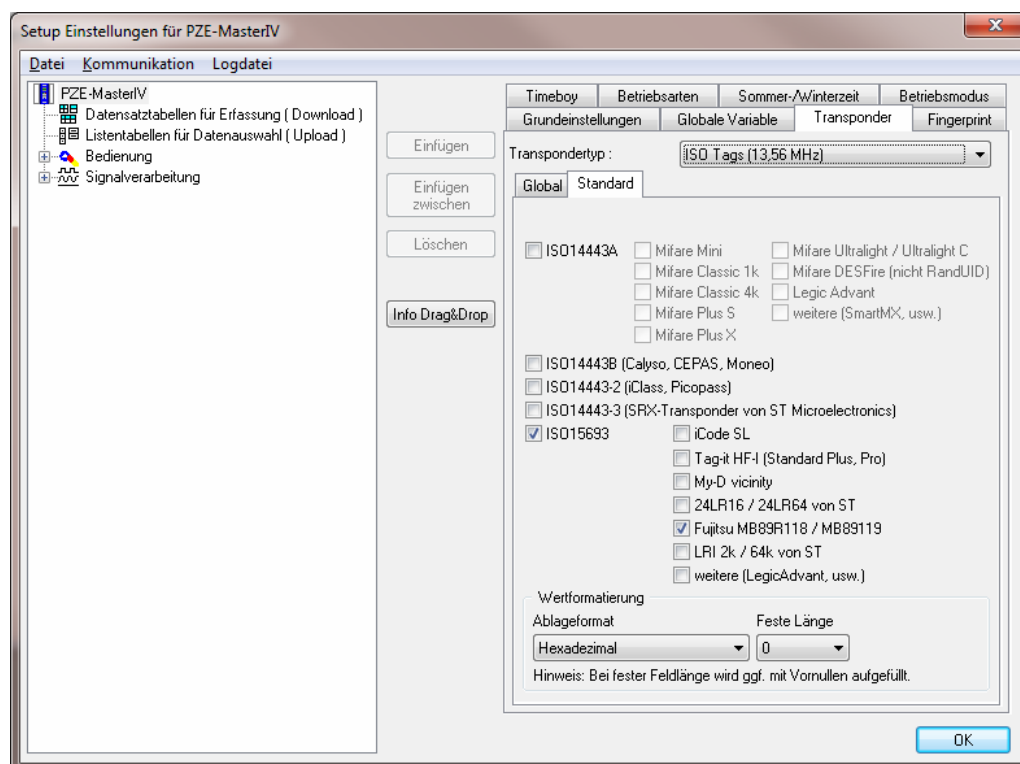
Bei diesen Transpondern kann nur die Seriennummer ermittelt werden. Ein Zugriff auf Datenbereiche ist nicht möglich. Diese Transponder können unter ISO Tags (13,56MHz) ausgewählt werden.

6.5.6. LRI 2k

Bei diesen Transpondern kann nur die Seriennummer ermittelt werden. Ein Zugriff auf Datenbereiche ist nicht möglich. Diese Transponder können unter ISO Tags (13,56MHz) ausgewählt werden.

6.6. ISO 14443/15693 Seriennummer lesen

Mit dem TWN3 Multi ISO Reader ist es möglich, bei allen 13,56 MHz Transpondern von ISO14443 und ISO15693 die Seriennummer zu lesen. Damit man bei verschiedenen Verfahren wählen kann, welche Transpondertypen man tatsächlich möchte und welche nicht, kann man beim Transpondertyp **ISO Tags (13,56MHz)** die jeweils gewünschten auswählen.



Hinweis:

Oft ist es besser bei den Seriennummern mit dem Hexadezimalformat zu arbeiten, weil man die Seriennummer ab 7 Byte auch die Herstellerangaben enthält.

7. Verschlüsselung der Kommunikation mit MasterIV Geräten

Datafox Geräte sind nun in der Lage, die Kommunikation per AES zu verschlüsseln.

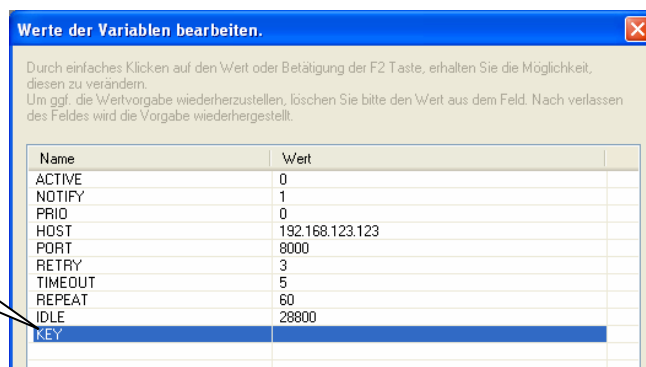
Es gibt damit nur 3 Arten der Kommunikation:

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

7.1. Erstellung und Hinterlegen des Schlüssels im Gerät

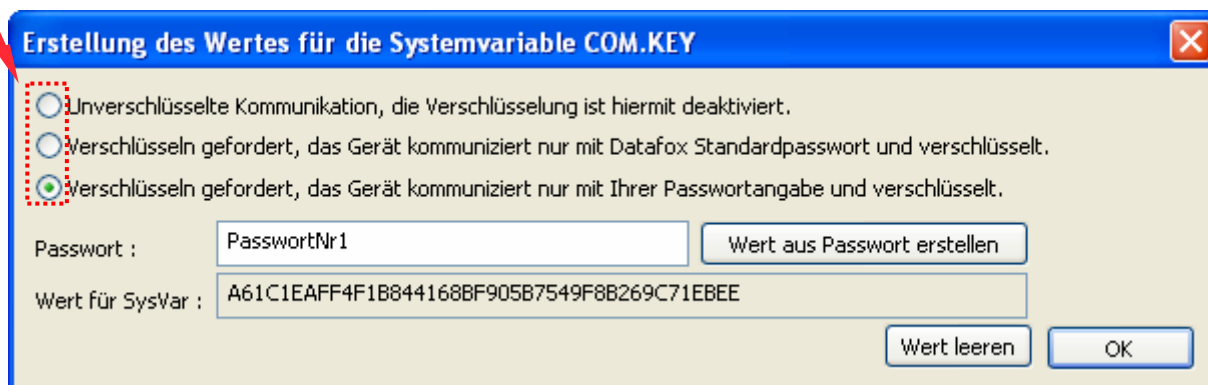
Unter dem Menüpunkt Konfiguration „Systemvariablen Aktive Verbindung“ öffnen Sie bitte die Konfigurationsdatei (z.B.: active.ini) zum Bearbeiten.

Durch einen Mausklick auf der Zeile KEY, öffnet sich das Fenster für die Erstellung des Schlüssels.



Name	Wert
ACTIVE	0
NOTIFY	1
PRI0	0
HOST	192.168.123.123
PORT	8000
RETRY	3
TIMEOUT	5
REPEAT	60
IDLE	28800
KEY	

Hier können Sie zwischen den Kommunikationsvarianten wählen



Erstellung des Wertes für die Systemvariable COM.KEY

☐ Unverschlüsselte Kommunikation, die Verschlüsselung ist hiermit deaktiviert.
☐ Verschlüsseln gefordert, das Gerät kommuniziert nur mit Datafox Standardpasswort und verschlüsselt.
☒ Verschlüsseln gefordert, das Gerät kommuniziert nur mit Ihrer Passwortangabe und verschlüsselt.

Passwort :

Wert für SysVar :

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.

7.2. Hinterlegen des Passwortes im StudioIV

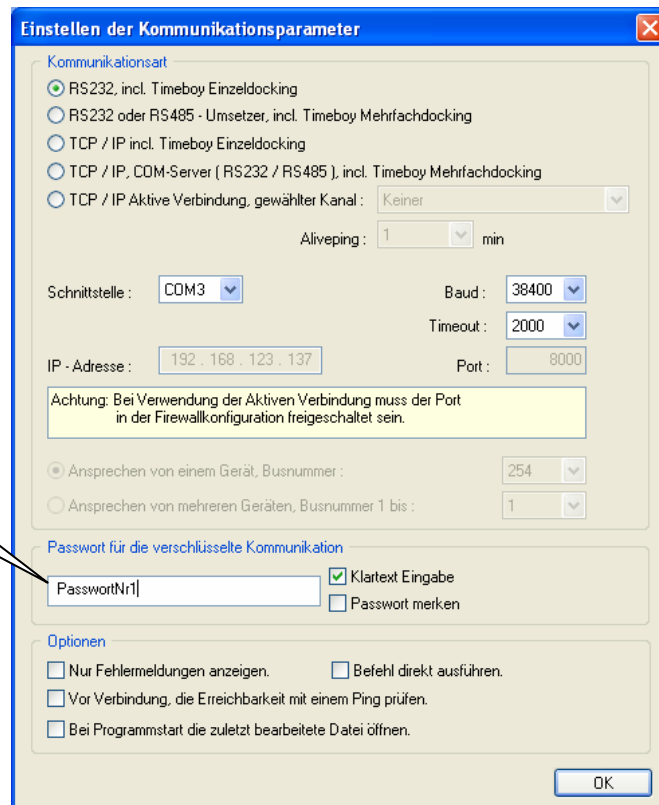
Ist bei einem Gerät ein Kommunikationsschlüssel hinterlegt, so muss das Passwort im StudioIV auch angegeben werden, da sonst keine Kommunikation mit dem Datafox Gerät möglich ist.

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

Das Passwort gilt für alle Kommunikationsarten.

Geben Sie hier Ihr Passwort ein.

Klartext Eingabe funktioniert nur bei der ersten Eingabe. Wird dieses Fenster erneut geöffnet, ist der Klartext nicht mehr darstellbar.



7.3. Übergabe des Schlüssels in die DFComDLL

Der Schlüssel wird über die DLL-Routine DFComSetCommunicationPassword gesetzt. Hierbei handelt es sich um den „echten“ Schlüssel (private Key), nicht der, der über das DatafoxStudioIV generiert wurde. Der Schlüssel wird im Klartext übergeben.

Mehr dazu finden Sie in der Dokumentation für die DFComDLL.





8. Zusätzliche Erweiterungen

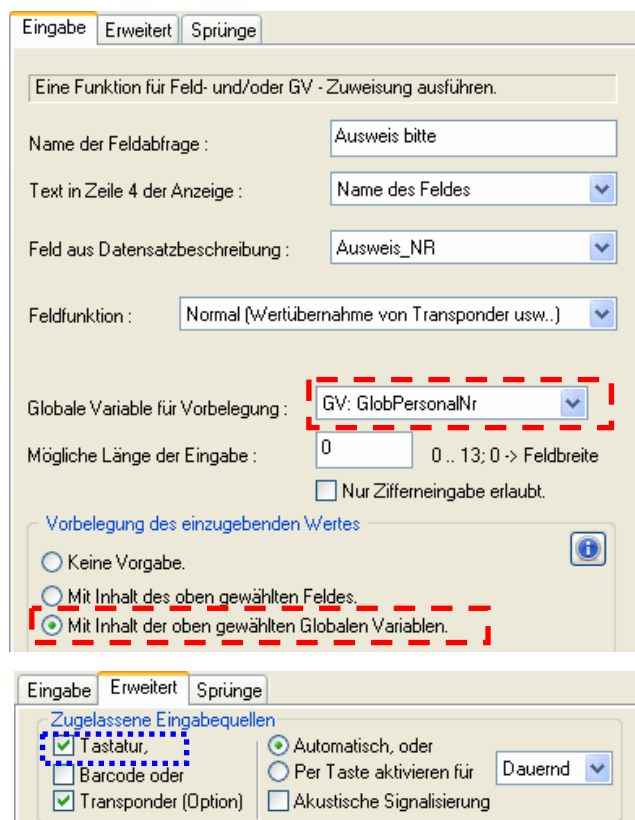
8.1. Vorbelegung der Anzeige im Display bei Eingaben

Mit dieser Funktion besteht die Möglichkeit, bei der Eingabe einem „Wert“ vorzugeben. Hierbei kann gewählt werden, ob der Wert aus dem Datenfeld oder aus einer GV genommen wird. Diese Funktion ist besonders hilfreich, wenn man GVs prüfen und gegebenenfalls ändern möchte.

Hier wird der Wert aus der **GV** im Display angezeigt, bevor dieser Inhalt über Eingabe geändert wird.

Anzeigebeispiel am TimeboyIV, ändern des Inhaltes in einer GV:

15.08.11 11:28:08				
Timeboy IV				
Demo Setup 3				
123456 Test_				



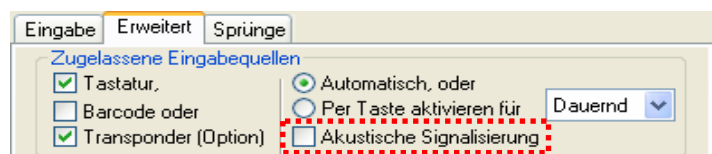
Beim Lesen eines Transponders wird der Wert überschrieben.

Bei Eingaben über die **Tastatur** kann z.B. bei einem Datafox TimeboyIV oder AE-MasterIV dieser Vorgabewert geändert werden.

Gleiches gilt, wenn die Vorbelegung aus dem Datenfeld stammt. Damit könnte nachträglich der Datensatz schrittweise auf korrekte Eingaben geprüft werden.

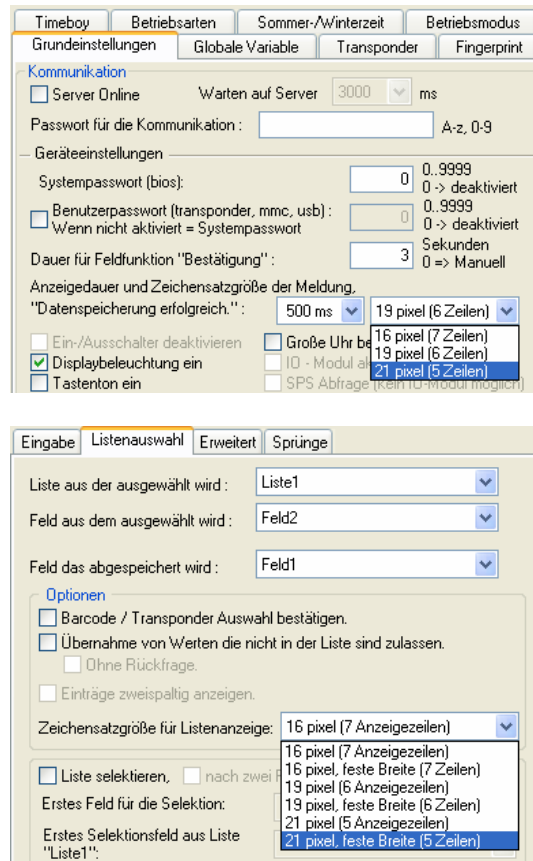
8.2. Signalisierung der Transponderbereitschaft

Unter der Registerkarte „Erweitert“ haben Sie die Möglichkeit, eine akustische Signalisierung zu geben, wenn ein Wert eingelesen werden soll. Dabei können Sie wählen, wie lange die Signalisierung aktiv sein soll.



8.3. Änderung der Schriftgröße

Bisher wurden bei der Meldung „Datenspeicherung erfolgreich“ und bei der Anzeige von Listen drei Schriftgrößen angeboten.



Die Änderung bezieht sich auf die Schriftgröße 21 Pixel. Diese wurde auf 23 Pixel erhöht.

Damit sind die Zeilen auch von weitem zu lesen.

Die Schriftgrößenbezeichnung wurde angepasst in:



Die Änderung der Schriftgröße „Groß“ von 21 auf 23 Pixel ist vergleichbar mit einer Wordschriftgröße von 12 auf 14.

Mit der Schriftgröße „Groß“, werden auch die Kopfzeilen angezeigt. Somit sind diese auch deutlich besser lesbar.

9. TimeboyIV



9.1. Infozeile







Ab sofort werden zusätzliche Informationen auch im TimeboyIV in einer Informationszeile angezeigt, welche unten im Display angezeigt wird.

Diese Informationszeile kennen Sie auch aus dem PZE-MasterIV.





Das Display baut sich nun wie folgt auf:

Die Infozeile ändert sich je nach Eingabeaufforderung und gibt Hinweise für die Bedienung.



15.08.11 11:28:08					
Timeboy IV					
Demo Setup 3					
F1	Projektzeit				
F2	Materialverb.				
F3	Telefonliste				
F4	Text				
ESC	Abbruch			Seite	Exp Taste

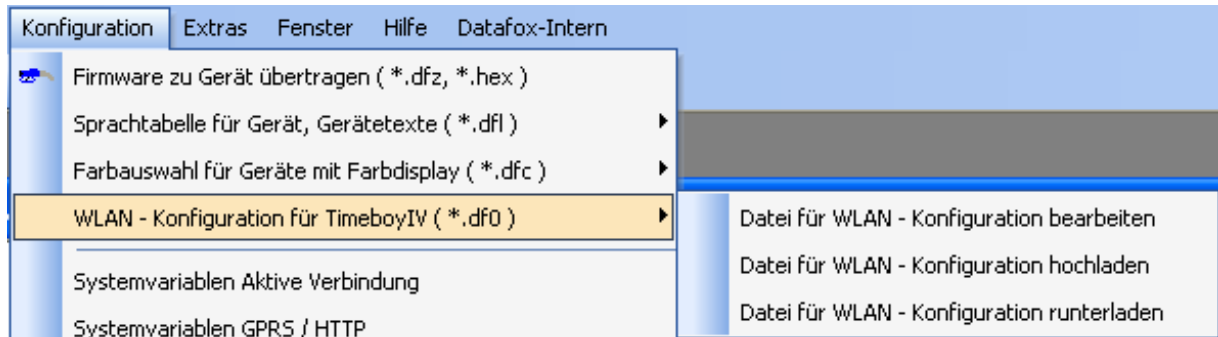
Neu eingeführt wurde auch das Icon für die Kommunikation über WLAN.

- WLAN Kommunikation
 -  WLAN als Hauptkommunikation aktiviert
 -  WLAN verbunden
 -  WLAN Kommunikation gerade aktiv
 -  Signalstärke des nächsten Signals (AP)

9.2. WLAN für TimeboyIV

Ab sofort kann der TimeboyIV auch mit einem WLAN-Modul ausgerüstet werden.

Die Einstellung der WLAN Parameter erfolgt nicht mehr, wie bei anderen MasterIV Geräten gewohnt, über das Bios-Menü, sondern über „Konfiguration->WLAN – Konfiguration für TimeboyIV“.



Die WLAN Konfigurationen werden in einer Datei mit der Endung „.df0“ abgelegt.

Hier haben Sie nun die Möglichkeit die Datei zu bearbeiten, in den TimeboyIV zu laden (hochladen) oder aus dem TimeboyIV zu lesen (runterladen).

Beim Lesen der WLAN Einstellung aus dem TimeboyIV wird die aktuell angegebene Datei überschrieben.

Im Bearbeitungsmodus können bis 8 Konfigurationen hinterlegt werden. Dies bietet sich besonders da an, wenn das Gerät an mehreren Standorten eingesetzt werden soll.

Wählen Sie hier die bevorzugte Konfiguration.

Vergeben Sie hier die Namen für die Konfigurationen.



Die gesamte Datei, mit allen Einstellungen wird in den TimeboyIV übertragen.

Im Bios-Menü -> Kommunikation -> WLAN kann der Standort gewählt werden. Je Standort wird eine eigene Konfiguration für die WLAN – Anbindung hinterlegt. Der User hat somit keinen Einblick auf die Einwahlparameter an den verschiedenen Standorten.



Hinweis:

Bei automatischer Wahl der Konfiguration / Standort, wird immer zuerst versucht, die Verbindung mit dem Default-Schema aufzubauen.



Achtung:

Verwenden Sie mehrere Standorte und eine Automatische Wahl der Konfiguration, benötigt der Scan nach APs recht viel Energie. Begrenzen Sie daher die Scans nach neuen APs.

9.2.1. Einstellen der WLAN Parameter

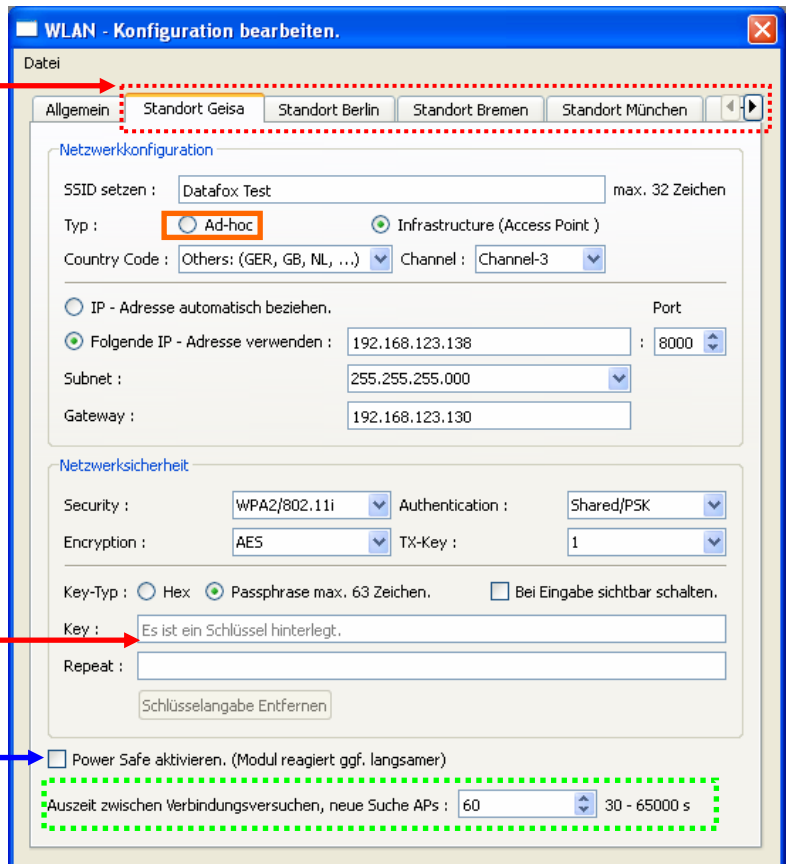
Wählen Sie hier die Konfiguration bzw. den Standort, für den Sie die WLAN Parameter einstellen möchten.

Hier können alle Einstellungen vorgenommen werden, die für ein AP notwendig sind.

Mit dem **Ad-hoc**-Mode können Sie eine direkte Verbindung zum PC herstellen.

Ist ein Key hinterlegt, so wird Ihnen dies so angezeigt

Setzen Sie diesen Haken, so erhöht sich die Akkulaufzeit deutlich.



Ein Scan (Suche) nach APs, wird nach einem Verbindungsabbruch erst nach dieser eingestellten Zeit durchgeführt. Beachten Sie dazu die nachfolgende Achtung Box!

Achtung:



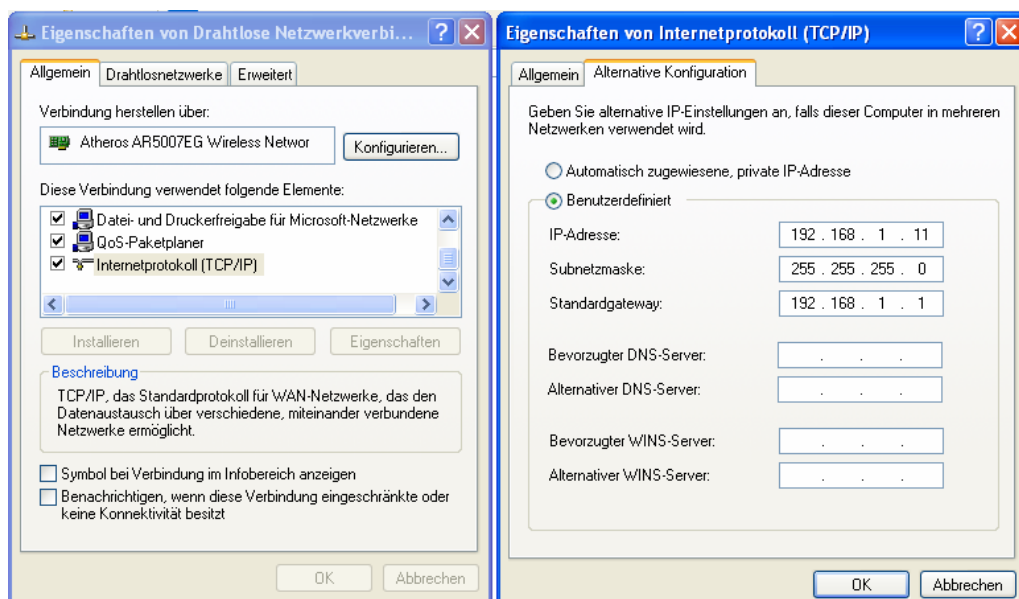
Eine Suche nach einem neuen AP, benötigt sehr viel Energie und entleert den Akku dadurch. Vermeiden Sie eine dauernde Suche nach einem AP, wenn das Gerät im Grenzbereich arbeitet, in dem Sie die Pause zwischen den Scans nach neuen APs großzügig wählen (80-120s).

An den meisten AP gibt es die Möglichkeit das „Bacon Interval“ einzustellen. Je höher dies eingestellt ist, um so weniger Strom benötigt der TimeboyIV. Empfehlung: Bacon Interval >300.

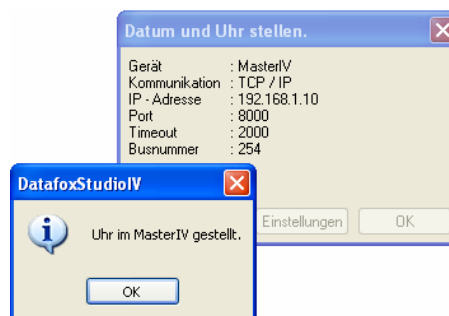
9.2.2. Ad-hoc Mode

Mit dem Ad-hoc Mode ist es möglich, eine direkte Verbindung zwischen einem PC und dem Time-boyIV aufzubauen. Folgende Einstellungen sind dafür notwendig:

- ▶ Wählen Sie im Bios Menü -> Kommunikation -> WLANRS9110 -> Standardeinst. laden.
- ▶ Stellen Sie die Kommunikation auf WLAN um.
- ▶ Scannen Sie nach Drahtlosnetzwerken (Das Gerät meldet sich mit Datafox-MasterIV).
- ▶ Klicken Sie das Netzwerk an und anschließend auf verbinden.
- ▶ Geben Sie den Schlüssel „Datafox-Geisa“ ein.
- ▶ Die IP-Adresse, die im Gerät als Standard (default) hinterlegt wird ist: 192.168.1.10
- ▶ Konfigurieren Sie Ihr Netzwerk so, dass der IP-Adressbereich zueinander passt.
- ▶ Klicken Sie dazu auf:



- ▶ Nun können Sie das Gerät unter der IP-Adresse 192.168.1.10 erreichen.



Achtung:
Im Ad-hoc Mode gibt es keine Möglichkeit der Energiesparoptionen. Verwenden sie diesen möglichst nur zum Einrichten des Gerätes.

Achtung:
Das WLAN-Modul ist nur an, wenn die Kommunikation auch auf diese eingestellt ist. Der Stromverbrauch des Moduls bei anderen Kommunikationsarten ist null.