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

Guide to

Parameterization and integration of microcontroller devices

Flexible data collection with method

Content

Changes within this document

Date	Chapter	Description
07.08.2013	Alle	New edition of the documentation
08.09.2013	Alle	Expression correction
14.05.2014	4.3 4.4	Note Differences active mode -> passive mode Online function Access control via HTTP
11.05.2015	4.3.4 und 4.4.5	Encryption added
09.08.2016	4.2	Overview / online offline access control functions added
07.11.2016	2.2 2.3 4.3.4.1-4	Language Characters / Encryption method in detail
22.12.2016	4.2	Display Designer
28.12.2017	5.6	http Level 1
28.12.2017	5.7	https
23.01.2018	4.2	wireless security
17.12.2019	5.6	More options for the http Level 1
28.07.2020	Appendix Structure of the Chapter	Information for HTTPS Main structure of the document changed
30.09.2022	All	update the links
21.12.2023	All	Updating all links for the new Homepage http Level 0 deleted. Not relevant for new integrators new side with all important download-links

1. Introduction

This document is a guide to training in the topics:

a) Configuration and

b.) integration of communication

The guideline applies to all microcontroller devices MasterIV series and EVO series, as well as integrated embedded modules in the industrial PC .
(Note: The built-in Industrial PC embedded modules can also be operated in HID mode.)

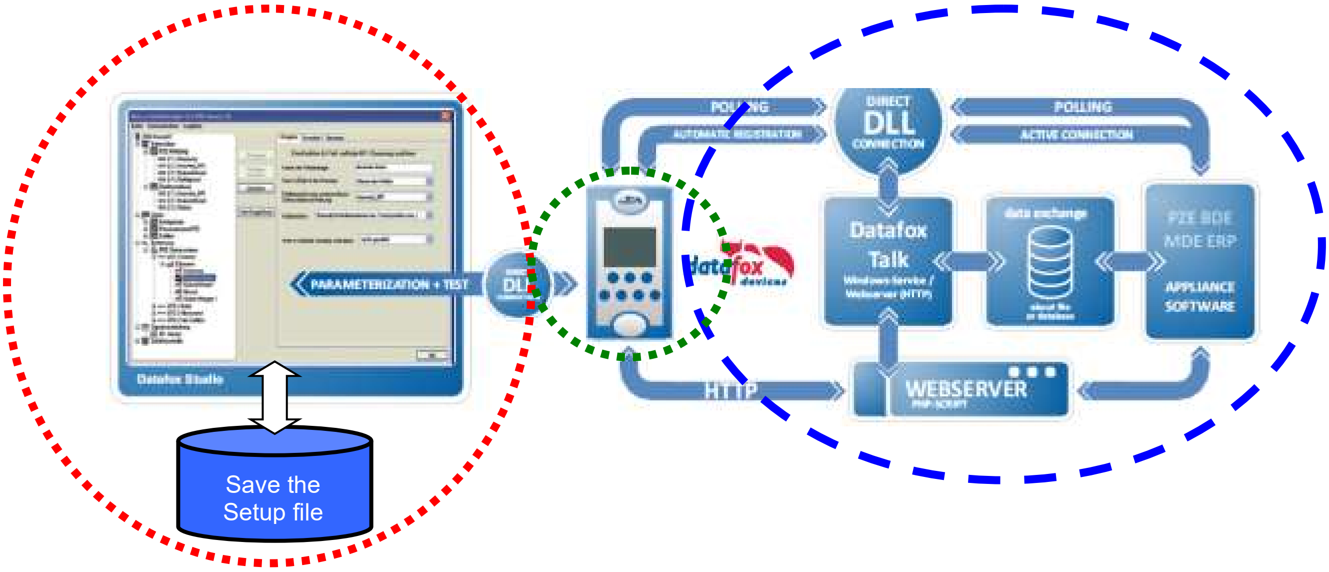
This document will help you to estimate the integration effort.
There you will be given links and notes, where you will find information on each topic.

The **Parameterization of the devices** is done via Datafox studio. ***This program allows you to create the desired acquisition and testing functions quickly, easily and without any programming knowledge or, as we say, to parameterize.*** The free of charge/licence free program can be found on our website.

When **integrating communication**, we give you an overview of the possible communication channels with Datafox terminals. The individual channels are shown and described with their advantages and disadvantages. ***On our website you will find sample programs for the integrati-on of the DLL in the current programming languages for your use.***

2. System Structure

This overview shows the basic structure of the complete data acquisition system and its areas:



<u>The following components are explained in the following chapters:</u>

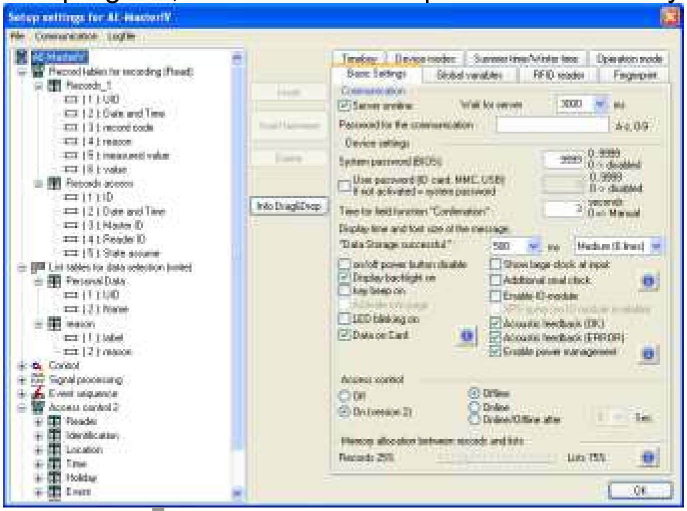
Structure of the hardware / device and firmware <u>(Link)</u>

Creating a setup <u>(Link)</u>

Communication techniques with Datafox devices <u>(Link)</u>

2.1. Structure of the hardware / device and firmware

This graphic shows the structure of data acquisition devices in context.
Underlying hardware is fitted out as desired.
Then there is the firmware, which is the operating system.
The program, which we call setup file is executed by the firmware.



Setup settings for AE-MasterIV

File Communication Logfile

- AE-MasterIV
  - Record tables for recording (Fixed)
    - Records_1
      - [1] UID
      - [2] Date and Time
      - [3] record code
      - [4] reason
      - [5] measured value
      - [6] value
    - Records access
      - [1] ID
      - [2] Date and Time
      - [3] Master ID
      - [4] Reader ID
      - [5] State access
  - List tables for data selection (voted)
    - Personal Data
      - [1] UID
      - [2] Name
    - reason
      - [1] label
      - [2] reason
  - Control
  - Signal processing
  - Event sequence
  - Access control 2
    - Reader
    - Identification
    - Location
    - Time
    - Holiday
    - Event

Info Drag&Drop

Timebox | Device modes | Summer time/Winter time | Operation mode
Basic Settings | Global variables | RFID reader | Fingerprint

Communication

☑ Server online — Wait for server 3000 ms

Password for the communication: — A-z, 0-9

Device settings

System password (BIOS): 9999 — 0..9999, 0 = disabled

□ User password (ID card, MMC, USB) If not activated = system password — 0..9999, 0 = disabled

Time for field function "Confirmation": 2 — seconds, 0 => Manual

Display time and font size of the message "Data Storage successful": 500 ms — Medium (3 lines)

□ on/off power button disable
☑ Display backlight on
□ key beep on
□ LED blinking on
☑ Data on Card

□ Show large clock at input
□ Additional mail clock
□ Enable ID-module
☑ Acoustic feedback (OK)
☑ Acoustic feedback (ERROR)
☑ Enable power management

Access control

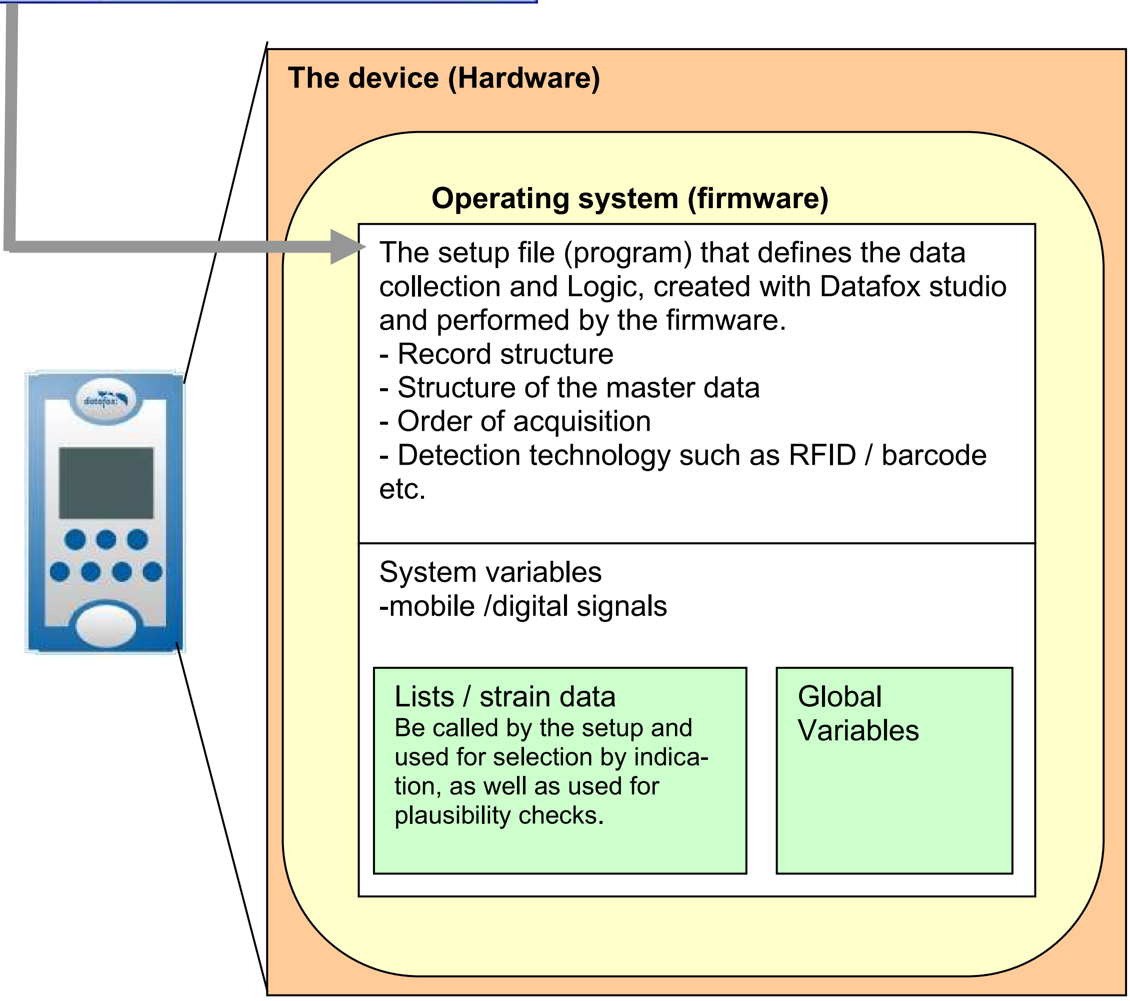
○ Off
● On (version 2)

● Offline
○ Online
○ Online/Offline after — Sec.

Memory allocation between records and lists

Records 25% — Lists 75%

OK



The device (Hardware)

Operating system (firmware)

The setup file (program) that defines the data collection and Logic, created with Datafox studio and performed by the firmware.
- Record structure
- Structure of the master data
- Order of acquisition
- Detection technology such as RFID / barcode etc.

System variables
-mobile /digital signals

Lists / strain data
Be called by the setup and used for selection by indication, as well as used for plausibility checks.

Global Variables

This connection is important because you do not have access to the individual areas of the system with every communication technology.

2.2. Usable Characters

For your information, we have put together an explanation of the characters in the standard scope of delivery.
This information can also be found in the manuals.
The Datafox devices support a part of the character encoding Latin-1 (ISO-8859-1) for the character output on the display and the data.

ISO 8859-1, more accurate **ISO/IEC 8859-1**, also known as **Latin-1**, is a standard for information technology on eight-bit character encoding, updated by the ISO last 1998, and the first part of the standards family **ISO/IEC 8859**.

Character Table - Latin-1:

Code	…0	…1	…2	…3	…4	…5	…6	…7	…8	…9	…A	…B	…C	…D	…E	…F
0…	not usable															
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…	not usable															
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 = space, NBSP = hard coded space, SHY = conditional separator

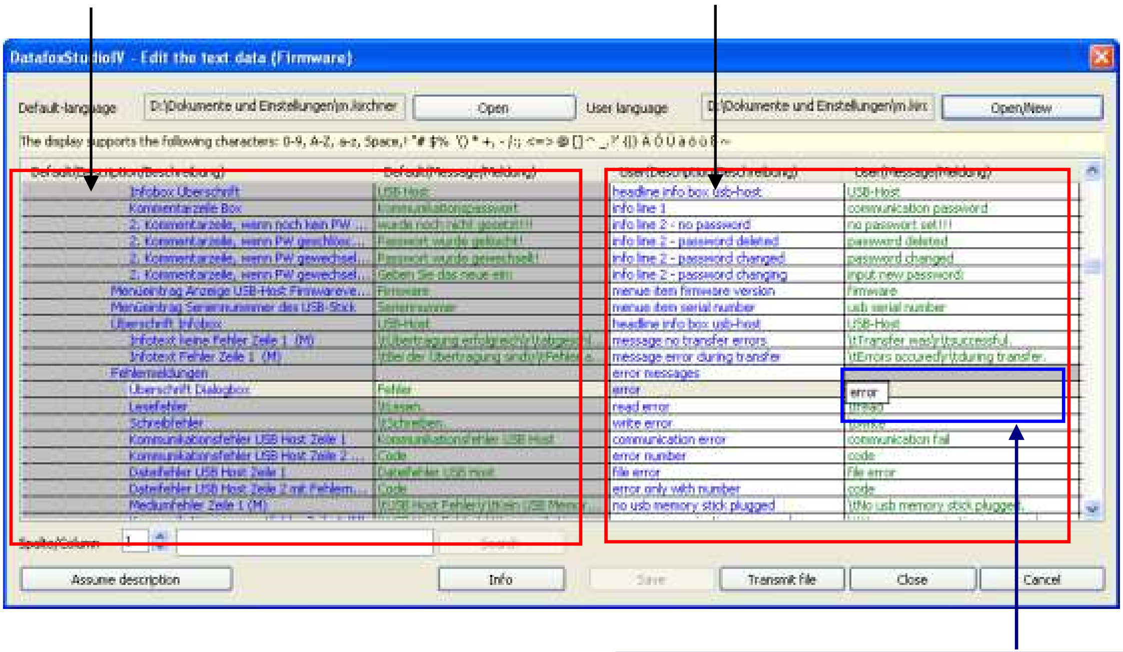
⬛	Control characters according to ISO standard can not be used
🟥	characters can not be used
🟩	Usable characters of Firmware-Version 04.01.xx.xx to Firmware-Version 04.03.02.xx
🟦	Character extension Firmware-Version 04.03.03.xx ***(only Hardware V4)***
🟨	character extension Firmware-Version 04.03.04 when using character table Latin-1 ***(only Hardware V4)***

2.3. Language / Table

In order to ensure language compatibility, it is possible to edit the texts and messages displayed by the firmware.
Open the editing dialog via the menu
"Configuration – Language file for device (*.dfl) – Edit file for language table".

Open a device file archive (firmware)*.dfz. The default texts of the firmware with a description and the corresponding message are displayed.

Open or create a new language file for the firmware with the extension *.dfl. If you have created a new file, the right column of the list is empty.



Default-language D:\Dokumente und Einstellungen\m.kirchner

User language D:\Dokumente und Einstellungen\m.kirc

The display supports the following characters: 0-9, A-Z, a-z, Space,! "# $% '()* +, -/:; <=> @ []^_´{|} Ä Ö Ü ä ö ü ß ~

Spalte/Column 1

Default(Description/Beschreibung)	Default(Message/Meldung)	User(Description/Beschreibung)	User(Message/Meldung)
Infobox Überschrift	USB-Host	headline info box usb-host	USB-Host
Kommentarzeile Box	Kommunikationspasswort	info line 1	communication password
2. Kommentarzeile, wenn noch kein PW ...	wurde noch nicht gesetzt!!!	info line 2 - no password	no passwort set!!!
2. Kommentarzeile, wenn PW geschlos...	Passwort wurde gelöscht!	info line 2 - password deleted	password deleted
2. Kommentarzeile, wenn PW gewechsel...	Passwort wurde gewechselt!	info line 2 - password changed	password changed
2. Kommentarzeile, wenn PW gewechsel...	Geben Sie das neue ein	info line 2 - password changing	input new password:
Menüeintrag Anzeige USB-Host Firmwareve...	Firmware	menue item firmware version	firmware
Menüeintrag Seriennummer des USB-Stick	Seriennummer	menue item serial number	usb serial number
Überschrift Infobox	USB-Host	headline info box usb-host	USB-Host
Infotext keine Fehler Zeile 1 (M)	\tÜbertragung erfolgreich\r\tabgeschl...	message no transfer errors	\tTransfer ready\r\tsuccessful.
Infotext Fehler Zeile 1 (M)	\tBei der Übertragung sind\r\tFehler a...	message error during transfer	\tErrors occured\r\tduring transfer.
Fehlermeldungen		error messages	
Überschrift Dialogbox	Fehler	error	error
Lesefehler	\tLesen	read error	\tread
Schreibfehler	\tSchreiben	write error	\twrite
Kommunikationsfehler USB Host Zeile 1	Kommunikationsfehler USB Host	communication error	communication fail
Kommunikationsfehler USB Host Zeile 2 ...	Code	error number	code
Dateifehler USB Host Zeile 1	Dateifehler USB Host	file error	File error
Dateifehler USB Host Zeile 2 mit Fehlern...	Code	error only with number	code
Medienfehler Zeile 1 (M)	\tUSB Host Fehler\r\tKein USB Memor...	no usb memory stick plugged	\tNo usb memory stick plugged.

Work within the lists with single mouse clicks only. NO double-clicks! Select a line from the list with a single click.

With another single click on the column User (Description/…) or User (Message/…) the cursor is displayed in this field.

Now you can enter or edit the text. When you finish the entry, the description form the column Default (Description/…) is taken over and you can edit it as well.
You can find prepared .dfl-files on the Datafox DVD.

☞ **Note:**
Cyrillic and Chinese characters can not be displayed.

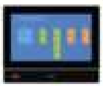
You find different language file.dfl on our product DVD:

Englisch, Niederländisch, Französisch
Default setting is German. German is always included in the firmware file.

Datafox DVD\MasterIV_EVO_TimeboyIV\Datafox Geräte\Datafox Software MasterIV-04.03.07\Datafox Studio-IV_und_Firmware\Sprachdateien der Firmware
https://www.datafox.de/d67/unternehmen/downloads/software/master4-v4/Datafox_Softwarepaket_MasterIV-V04.03.21.zip
(Laden Sie immer das aktuelle Release)
Beispiel: Datafox Software-MasterIV V04.03.19.zip

2.4. Displaydesigner

scope of application:

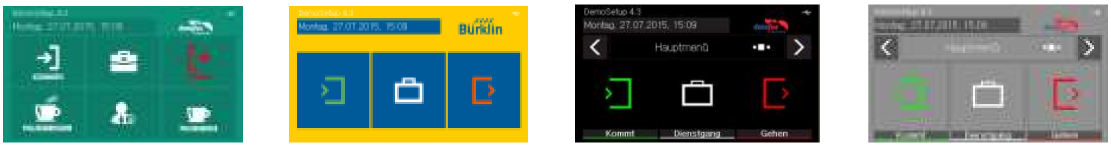
V4	V4	V4		EVO 2.8 / 3.5			ZK / IO Box V4	Mobil-Box V4	Docking V2	FDL V2	 EVO-IPC	ZK-Plus	ZK-Knoten
☒	☒	☒	☒	☒								☒	

For the devices AE-MasterIV V4, PZE-MasterIV V4 and PZE-MasterIV Basic V4 the Designer Is only usable with the optional color display.

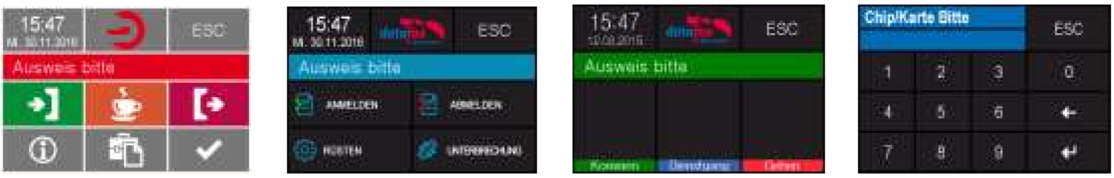
With the Display-Designer, Datafox offers the possibility for partners and users to customize the display according to your requirements. But due to the necessary operating sequences, this cannot be a completely free design, but things like headlines, menu structures and footers have to be guaranteed. The aim of the display designer is to enable the feasible settings with minimal effort.

We are looking forward to many users and recommend:
Create an individual Display-Design for your Company:

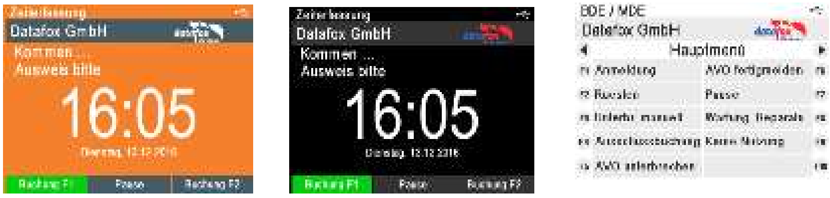
Example picture for EVO 4.3



Example picture for EVO 2.8 / 3.5

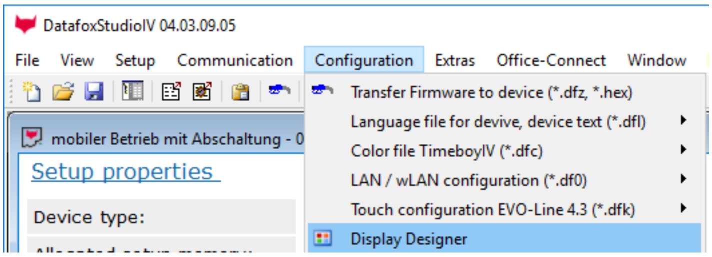


Example picture for PZE-/ AE- Master V4 with color display

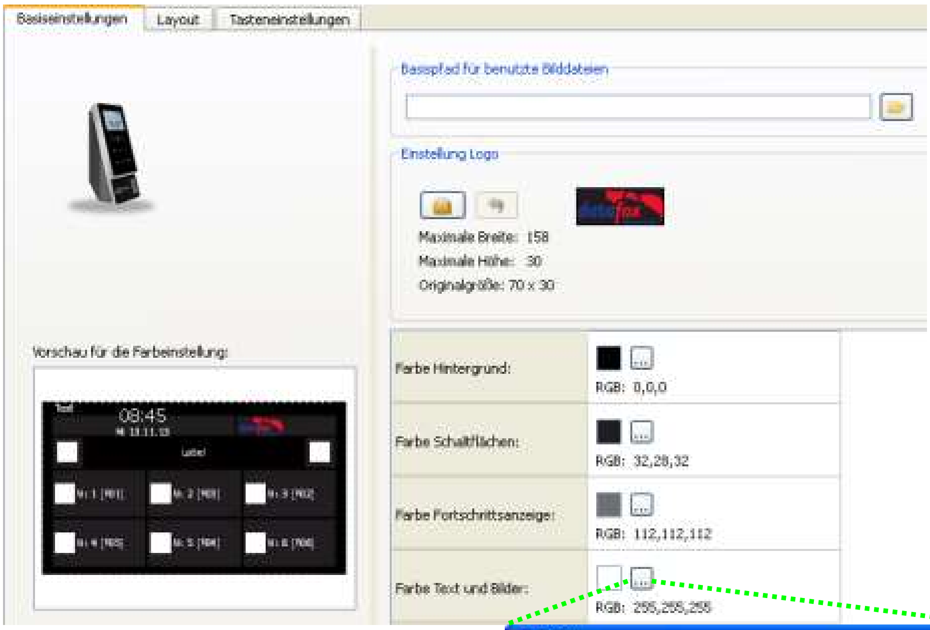


To create an individual discplay design for your device, you need at least the DatafoxStudioIV 04.03.09.05.

The display designer can be opened via the Configuration menu or directly from the setup edit mask.


DatafoxStudioIV 04.03.09.05
File
View
Setup
Communication
Configuration
Extras
Office-Connect
Window
Transfer Firmware to device (*.dfz, *.hex)
Language file for devive, device text (*.dfl)
Color file TimeboyIV (*.dfc)
LAN / wLAN configuration (*.df0)
Touch configuration EVO-Line 4.3 (*.dfk)
Display Designer
mobiler Betrieb mit Abschaltung - 0
Setup properties
Device type:

2.4.1. Color Setting for the Displays of the EVO 4.3 Multifunctional Terminal / 2.8 and 3.5 Pure



Basispfad für benutzte Bilddateien

Einstellung Logo

Maximale Breite: 158
Maximale Höhe: 30
Originalgröße: 70 x 30

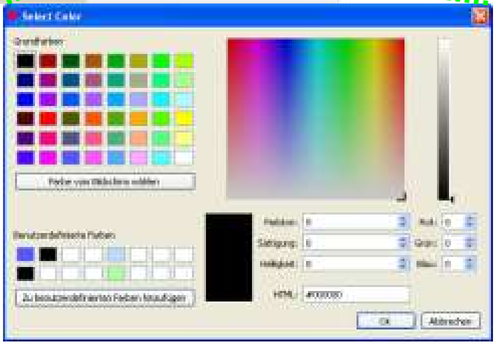
Vorschau für die Farbeinstellung:

Farbe Hintergrund: RGB: 0,0,0

Farbe Schaltflächen: RGB: 32,28,32

Farbe Fortschrittsanzeige: RGB: 112,112,112

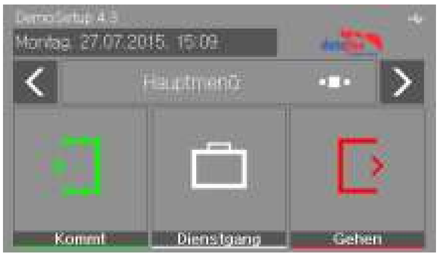
Farbe Text und Bilder: RGB: 255,255,255



Select Color
Grundfarben
Farbe vom Bildschirm wählen
Benutzerdefinierte Farben
Zu benutzerdefinierten Farben hinzufügen
OK
Abbrechen

Farbton: 0
Sättigung: 0
Helligkeit: 0
Rot: 0
Grün: 0
Blau: 0
HTML: #000000

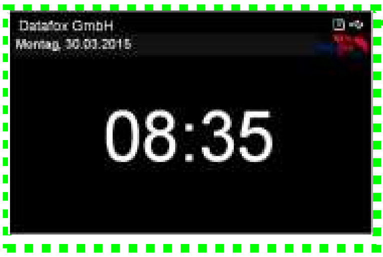
Example Picture:

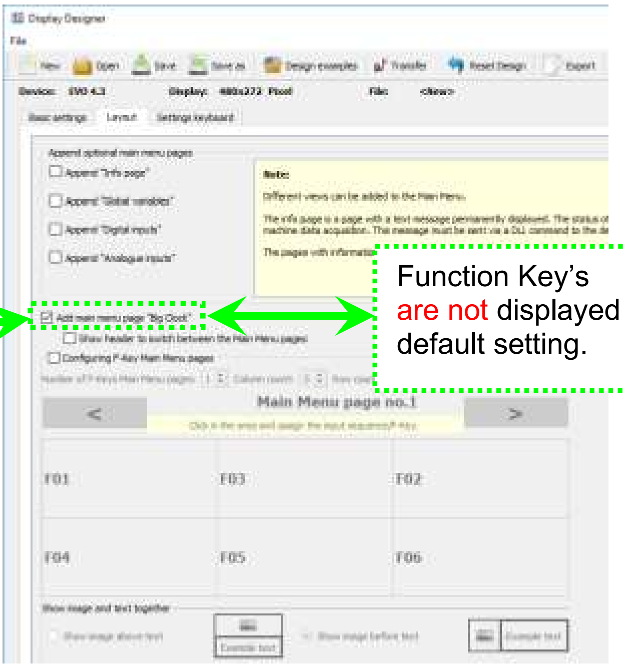


2.4.2. Default Setting

The device is delivered in the default „PZE“-design.

This design is also set as default when you first create a new theme in Display Designer.





Device: EVO 4.3 Display: 480x272 Pixel File: <New>

Append optional main menu pages

□ Append "Info page"

□ Append "Global variables"

□ Append "Digital inputs"

□ Append "Analogue inputs"

Note:

Different views can be added to the Main Menu.

The info page is a page with a text message permanently displayed. The status of machine data acquisition. This message must be sent via a DLL command to the de

The pages with informatio

☑ Add main menu page "Big Clock"

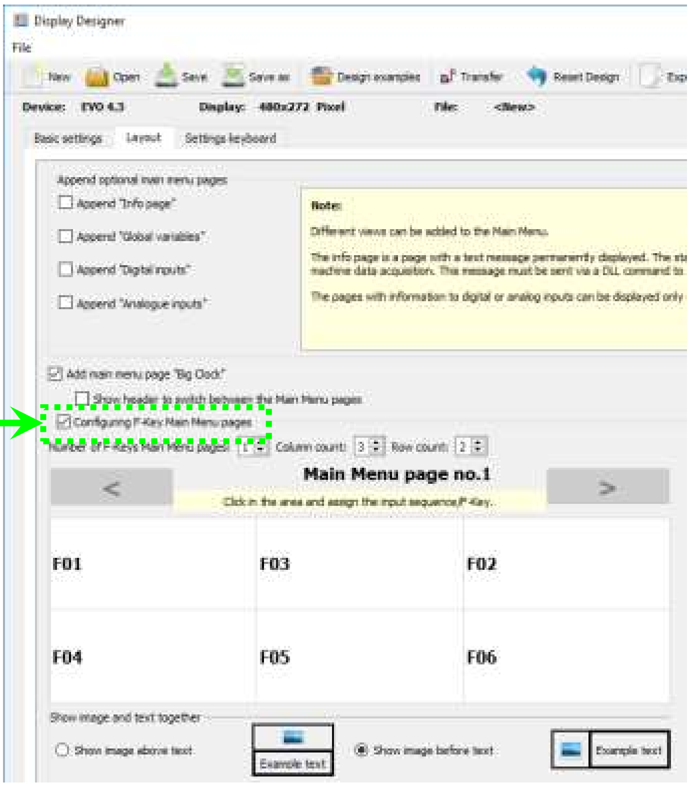
□ Show header to switch between the Main Menu pages

□ Configuring F-Key Main Menu pages

Function Key's **are not** displayed in the default setting.

2.4.3. Display function buttons on the EVO 4.3 Multifunctional Terminal / 2.8 und 3.5 Pure display

By showing the function buttons from the setup, the number of buttons displayed in the display can be adjusted.



Display Designer

Device: EVO 4.3 **Display:** 480x272 Pixel **File:** <New>

Append optional main menu pages

☐ Append "Info page"

☐ Append "Global variables"

☐ Append "Digital inputs"

☐ Append "Analogue inputs"

Note:

Different views can be added to the Main Menu.

The info page is a page with a text message permanently displayed. The st machine data acquisition. This message must be sent via a DLL command to

The pages with information to digital or analog inputs can be displayed only

☑ Add main menu page "Big Clock"

☐ Show header to switch between the Main Menu pages

☑ Configuring F-Key Main Menu pages

Number of F-Keys Main Menu pages: 1 Column count: 3 Row count: 2

Main Menu page no.1

Click in the area and assign the input sequence/F-Key.

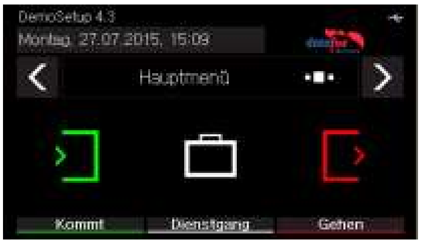
F01	F03	F02
F04	F05	F06

Show image and text together

○ Show image above text

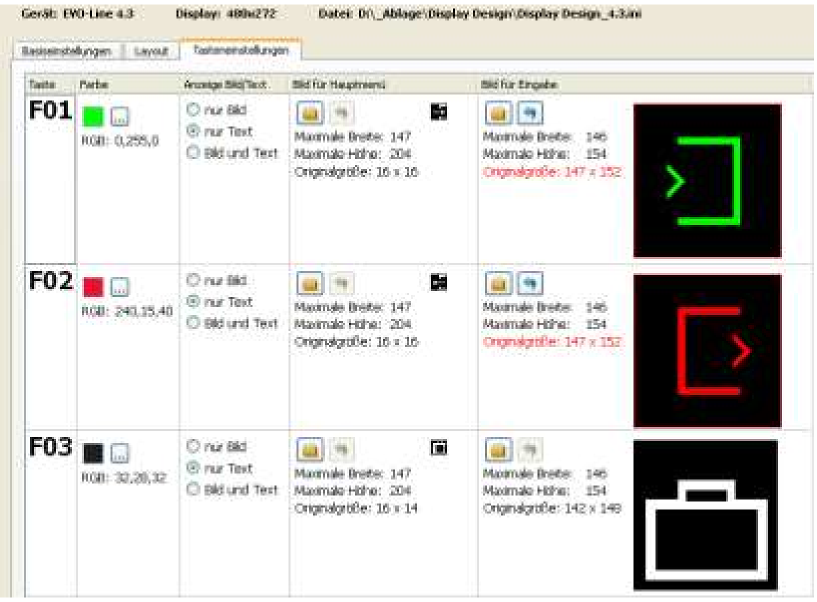
● Show image before text

Example:



2.4.4. Upload images for function buttons of EVO 4.3 Multifunctional Terminal / 2.8 / 3.5 Pure

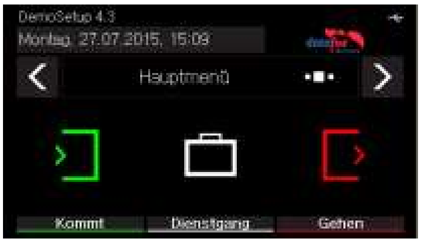
Under this menu item "Key settings" you can import the image file for each function key.



Gerät: EVO-Line 4.3 **Display:** 480x272 **Datei:** D:_Ablage\Display Design\Display Design_4.3.ini

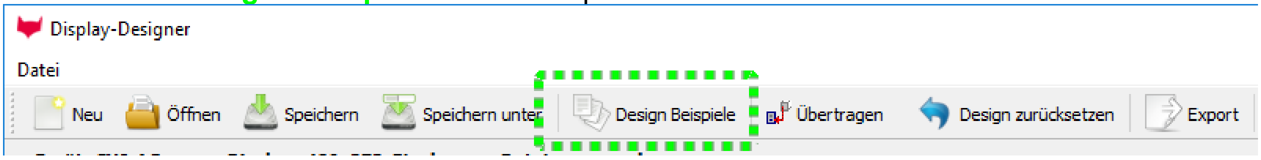
Taste	Farbe	Anzeige Bild/Text	Bild für Hauptmenü	Bild für Eingabe
F01	🟩 RGB: 0,255,0	○ nur Bild ● nur Text ○ Bild und Text	Maximale Breite: 147 Maximale Höhe: 204 Originalgröße: 16 x 16	Maximale Breite: 146 Maximale Höhe: 154 Originalgröße: 147 x 152
F02	🟥 RGB: 240,15,40	○ nur Bild ● nur Text ○ Bild und Text	Maximale Breite: 147 Maximale Höhe: 204 Originalgröße: 16 x 16	Maximale Breite: 146 Maximale Höhe: 154 Originalgröße: 147 x 152
F03	■ RGB: 32,28,32	○ nur Bild ● nur Text ○ Bild und Text	Maximale Breite: 147 Maximale Höhe: 204 Originalgröße: 16 x 14	Maximale Breite: 146 Maximale Höhe: 154 Originalgröße: 142 x 148

Sample picture for the key figures:

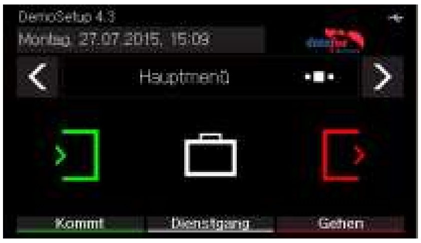


2.4.5. Design examples in the designer

With the installation of the DatafoxStudioIV you get several design examples for the devices. Click on the **"Design Examples"** button to open them.



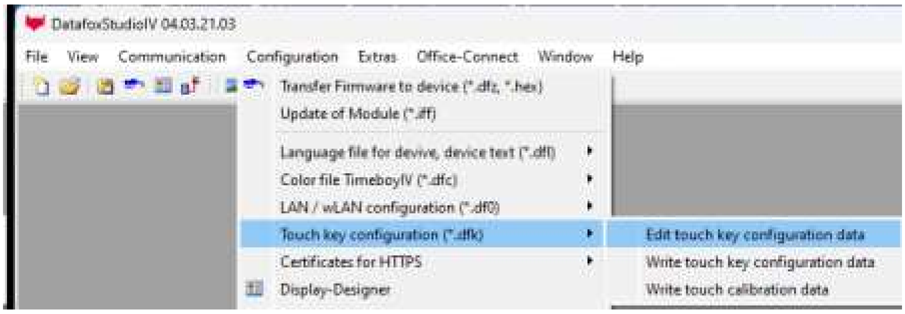
Datafox gradually extends the examples.
If you have any suggestions or wishes, please let us know.



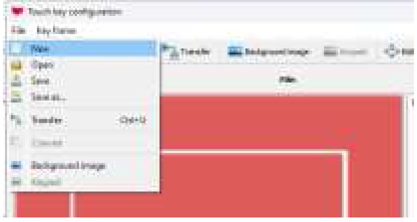
2.5. Individual touch layout for EVO 5.0 Pure and 4.6 FlexKey

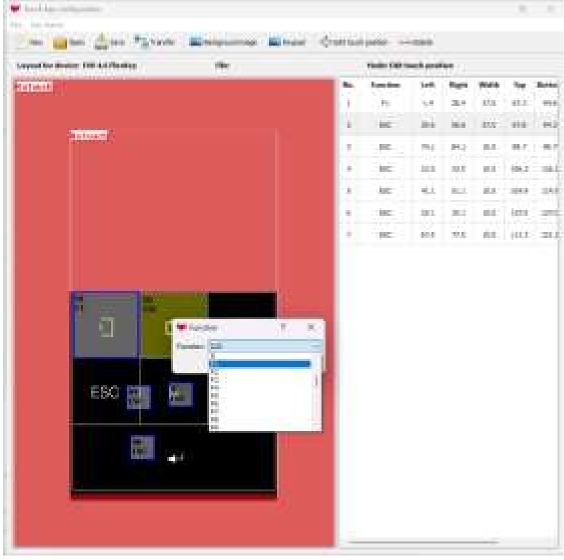
In the devices EVO 5.0 Pure and EVO 4.6 FlexKey, you can individually design the touch surfaces. For this purpose, an image for the keyboard is stored and displayed on the device. With Datafox-StudioIV you can then place the desired keys on the image.

You can open the Touch menu:


DatafoxStudioIV 04.03.21.03
File
View
Communication
Configuration
Extras
Office-Connect
Window
Help
Transfer Firmware to device (*.dfz, *.hex)
Update of Module (*.dff)
Language file for devive, device text (*.dfl)
Color file TimeboyIV (*.dfc)
LAN / wLAN configuration (*.df0)
Touch key configuration (*.dfk)
Certificates for HTTPS
Display-Designer
Edit touch key configuration data
Write touch key configuration data
Write touch calibration data

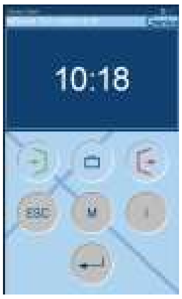
With „New“ can you create a touch-config.





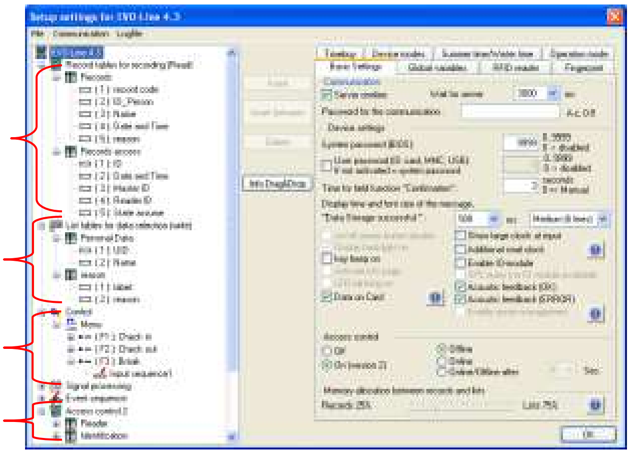
You find a description in the Manual DatafoxStudio.

This is what your display could look like.



3. Creation of a setup (program)

The creation of the setup is done with the free of charge "Datafox StudioIV" tool.
The structure of the tables for master data and bookings as well as the operating procedures, are freely definable. **There are no programming skills required.**



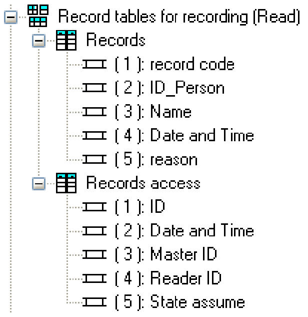
1. bookings

2. master data

3. operating + signal Processing

4. access control

1. Insert the data structure of the tables individually for bookings



- Record tables for recording (Read)
  - Records
    - [1]: record code
    - [2]: ID_Person
    - [3]: Name
    - [4]: Date and Time
    - [5]: reason
  - Records access
    - [1]: ID
    - [2]: Date and Time
    - [3]: Master ID
    - [4]: Reader ID
    - [5]: State assume

Record table: Records (Data description)

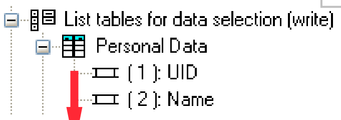
record code	ID_Person	Name	date and time	reason
K	656556	M. Müller	21.02.2013 12:31:15	0
K	656556	F. Muster	21.02.2013 12:32:45	0

Access Tabelle: Records access (Data description)

ID	date and time	Master ID	Reader ID	State
0566236654	21.02.2013 12:31:15	1	010	20
-	21.02.2013 12:32:45	1	010	42
1566959651	21.02.2013 14:12:05	1	020	20
-	21.02.2013 16:55:14	1	020	42

2. Define the structure of the tables for master data.

There can be: 20 record tables and 20 list tables be defined, each with 25 fields



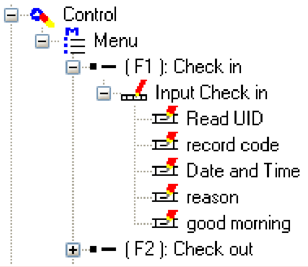
- List tables for data selection (write)
  - Personal Data
    - [1]: UID
    - [2]: Name

Table: Personal Data (description)

UID	Name
00799611485215	M. Mustermann

Lists are for example Master or order data that already exist and in a defined shape (list description) are transferred to the device. For example, HR master, cost centers, production orders, etc .. These data support the data acquisition by allowing a choice to carry out from a list or to compare data with a list (plausibility check).

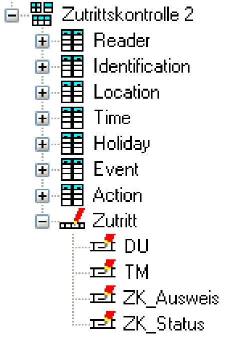
3. Specify the operation and signal processing.



- Control
  - Menu
    - [F1]: Check in
      - Input Check in
        - Read UID
        - record code
        - Date and Time
        - reason
        - good morning
    - [F2]: Check out

- menus
- show text
- Show list
- submenus
- RFID-methods
- Type of inputs

4. Create the Access Control



- Zutrittskontrolle 2
  - Reader
  - Identification
  - Location
  - Time
  - Holiday
  - Event
  - Action
  - Zutritt
    - DU
    - TM
    - ZK_Ausweis
    - ZK_Status

- Detection order
- Status
- online / offline

5. Transfer the setup to the terminal.

6. Collect data

4. Device key and security

There are different techniques for the Datafox devices to protect the device from unqualified access.

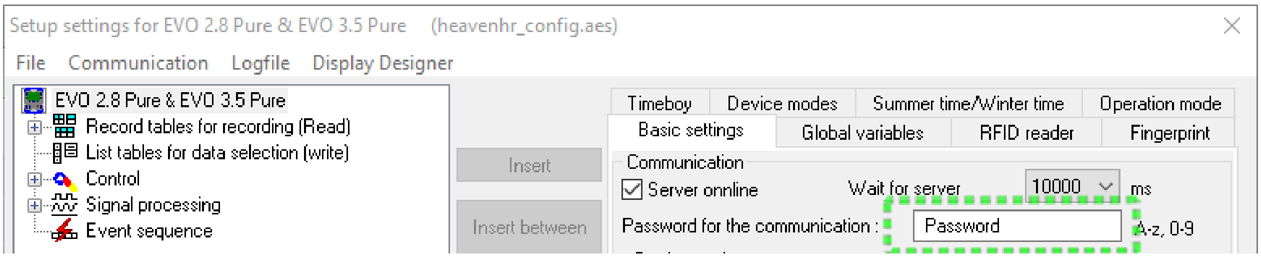
4.1. Device passwords

Device passwords are used to prevent devices from being unintentionally / accidentally or intentionally read or manipulated in the settings for communication or data.

These settings are only intended to ensure the operational safety of the devices and should be part of the standard.
These settings do not have the encryption passwords.
Please see the chapter on encryption via http and DLL.

4.1.1. Communication password

Our software "Datafox StudioIV" is freely available on the homepage.
The devices are configured by our partners.
To prevent misuse or manipulation by users, a communication password can be stored in the device. Only those who know this can change the configuration of the device.
The **Password** is transferred to the device with the configuration (setup file).



Setup settings for EVO 2.8 Pure & EVO 3.5 Pure (heavenhr_config.aes)

☑ Server onnline

Wait for server: 10000 ms

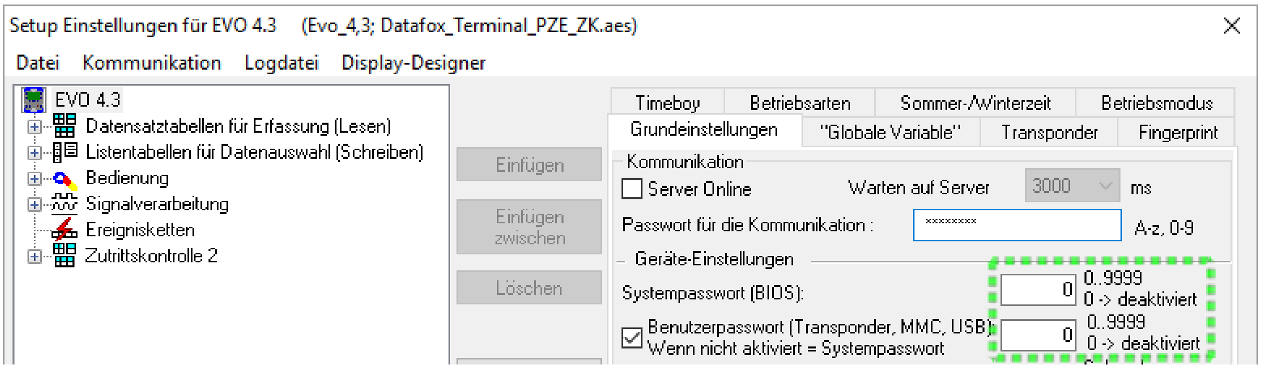
Password for the communication : Password A-z, 0-9

4.1.2. Bios Menu Password

All display devices have a bios menu.
Settings can be made as followed:

IP - address
The type of Communication (GPRS, USB, TCP/IP) etc.
Display brightness, volume etc.

To prevent access to the bios menu, a password can be entered here.
This password is then transferred to the device with the configuration (setup).



Setup Einstellungen für EVO 4.3 (Evo_4,3; Datafox_Terminal_PZE_ZK.aes)

□ Server Online

Warten auf Server: 3000 ms

Passwort für die Kommunikation : ******** A-z, 0-9

Geräte-Einstellungen

Systempasswort (BIOS): 0 — 0..9999, 0 -> deaktiviert

☑ Benutzerpasswort (Transponder, MMC, USB) Wenn nicht aktiviert = Systempasswort: 0 — 0..9999, 0 -> deaktiviert

4.2. Wireless security

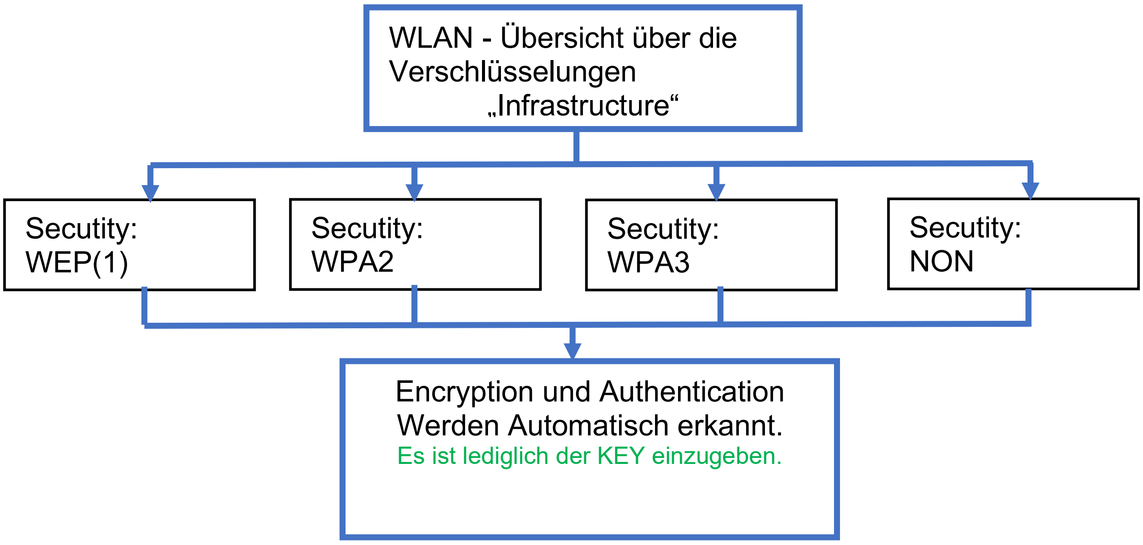
4.2.1. M111_WLAN ESP32-c3 ML01 (WLAN-Modul DF-WL03)

This overview shows you which WLAN methods are supported.

The DF-WL03 module automatically detects the encryption of the AP. Therefore, only the Security parameter needs to be set. The other parameters (Encryption and Authentication) are detected automatically.

Routers that operate WPA3/WPA2 in mixed mode can already be used now.

Supported is here the 2.4Ghz band.


WLAN - Übersicht über die Verschlüsselungen „Infrastructure“
Secutity: WEP(1)
Secutity: WPA2
Secutity: WPA3
Secutity: NON
Encryption und Authentication Werden Automatisch erkannt.
Es ist lediglich der KEY einzugeben.

! **Attention:**
We cannot test every Access point on the market.
Therefore, it is not possible for us to guarantee a connection to every AP..

4.2.2. Texas Instruments TI-CC3135 (Generation 2)

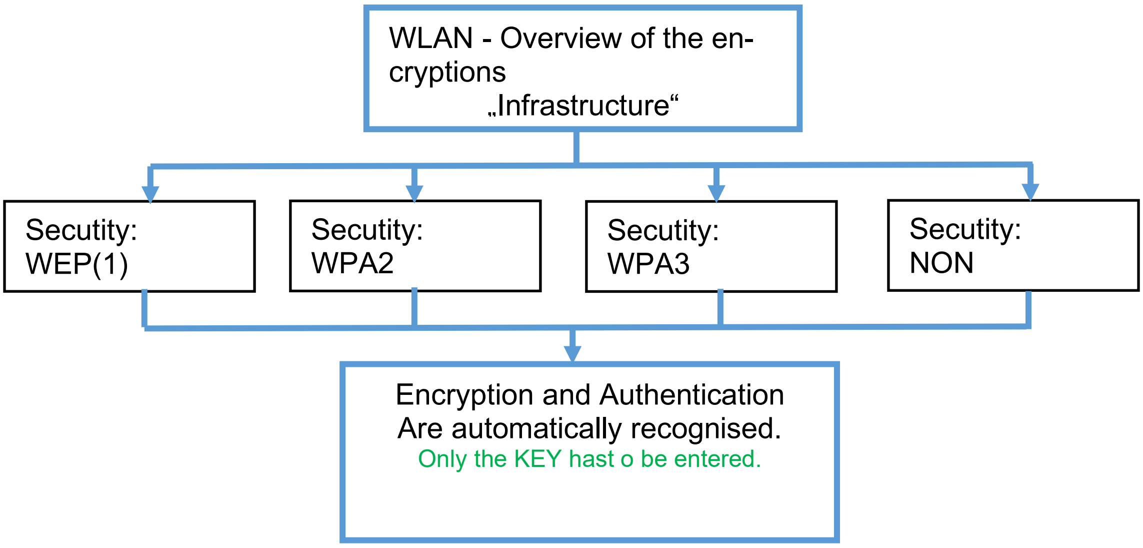
The module is currently not available for the Universal

This overview shows you which WLAN methods are supported.

The TI-CC3135 module automatically detects the encryption of the AP. Therefore, only the Security parameter needs to be set. The other parameters (Encryption and Authentication) are detected automatically.

Routers that operate WPA3/WPA2 in mixed mode can already be used now.

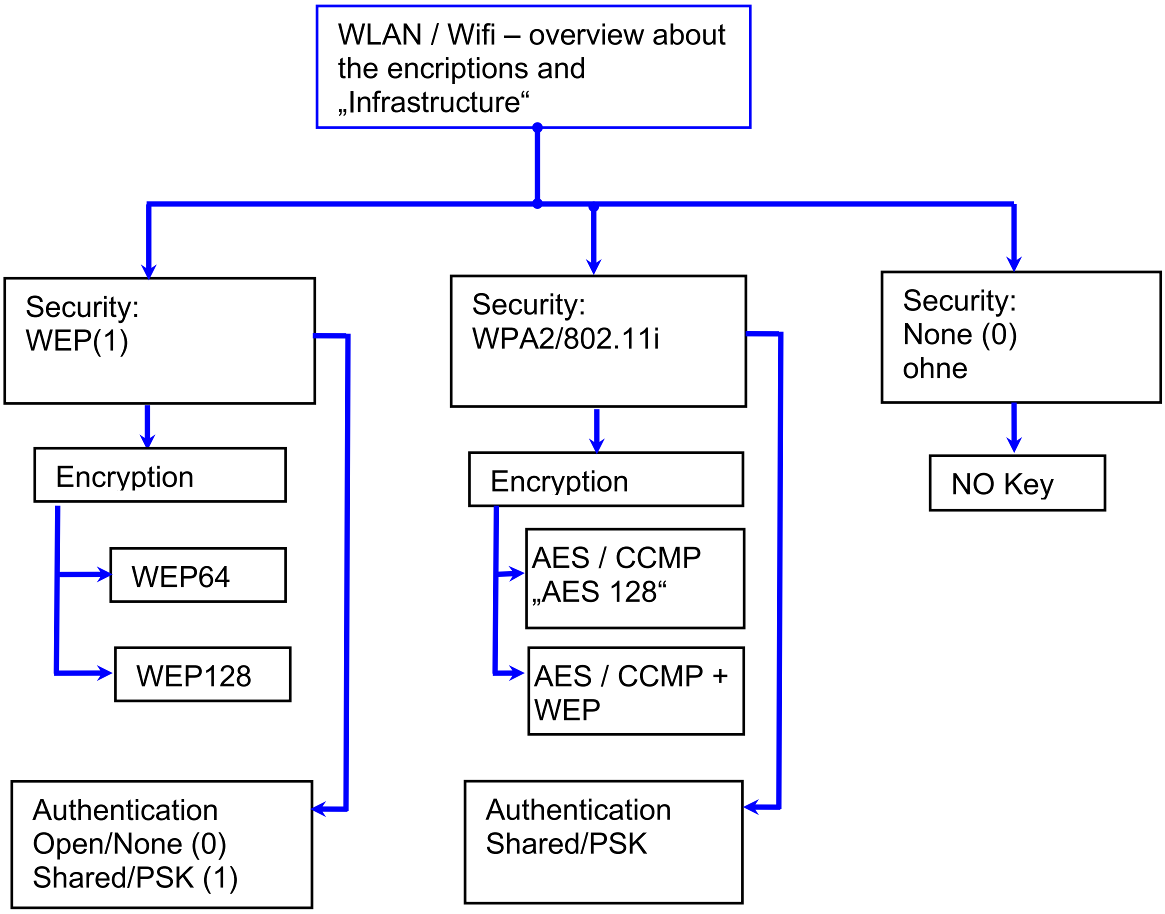
If the networks in the 5Ghz and 2.4Ghz bands have the same name, the network with the better reception quality is selected. This is usually the network in the 2.4Ghz band.


WLAN - Overview of the encryptions
„Infrastructure“
Secutity: WEP(1)
Secutity: WPA2
Secutity: WPA3
Secutity: NON
Encryption and Authentication
Are automatically recognised.
Only the KEY hast o be entered.

! **Attention:**
We cannot test every Access point on the market.
Therefore, it is not possible for us to guarantee a connection to every AP..

4.2.3. Redpine (Generation 1)

This overview shows you which WLAN methods are supported.
Not supported is WPA (Predecessor of WPA2).
Not supported is multiple-input multiple-output (MIMO)
5 GHz connections are **not supported** and no mixed operation 2.4 GHz / 5 GHz.
Authentication via WPA2 Enterprise according to IEEE 802.1x is **not supported.**



! **Attention:**
We cannot test every available Access-Point on the market.
Therefore, it is not possible for us to guarantee a connection to any AP.

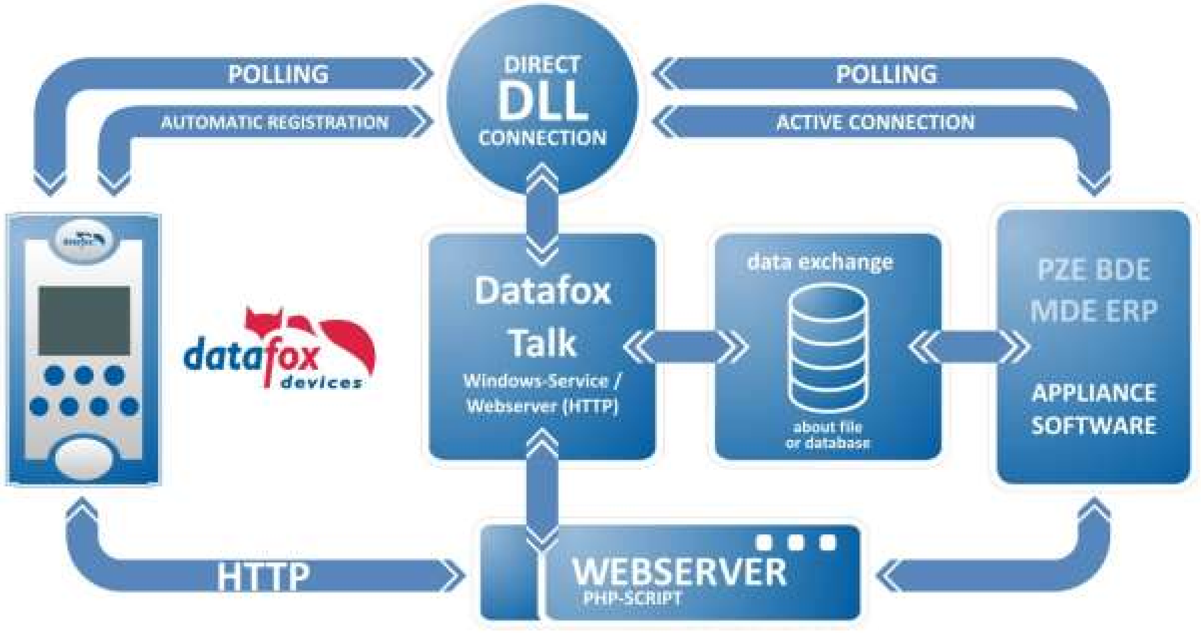
! **Attention:**
multiple-input multiple-output (MIMO) is not supported. If you change the AP from b/g/n to b/g, only SISO is automatically used.
https://en.wikipedia.org/wiki/Single-input_single-output_system

When setting the encryption AES or WEP, only one type is used at a time.
The setting AES+WEP means for some access points that AES encryption is performed first and then additionally encrypted with WEP.
In this case, only set AES.

5. Description of the different communication techniques

5.1. Overview of the communications technologies

This overview is valid for all microcontroller devices of MasterIV series and EVO series, as well as for the embedded modules integrated into the Industrial PC. (Note: The built-in Embedded modules inside the Industrial PCs can also be operated in HID mode.)



DLL integration „Passive-mode“ = Polling
(free of charge)

DLL integration „Active-mode“
Permanent Active connection to the terminal
(free of charge)

„Datafox-Talk“
Data exchange via file storage or database with a service
(License Required)

„http“
Level 1
Automatic sending of data to a Web Server and transfer list to the device
(free of charge)

In order to enable the respective communication, the main communication must be set in the BIOS of the device. How to enter the BIOS menu, please see the respective manuals in the chapter "Display structure and Bios".

5.2. Function overview of communication techniques

access to:	description	DLL integration Polling	DLL active-mode	http Level 1	Datafox Talk
Data sets	Generated data from the data acquisition	✓	✓	✓	✓
Transfer master data	-staff lists -Article Master -orders	✓	✓	✓	✓
System	-Firmware -Language -Colour/Display	✓	✓	✓	✗
System	-Setup	✓	✓	✓	✗
GV global variables	8 x free use	✓	✓	✓	✗
System-variables	GPRS COM I/O	✓	✓	✓	✗
Message to The device	Direct display of text on the display	✓	✓	✓	✗
Online Mode		✓	✓	✓	✗
Online Mode access	All access authorizations are decided directly from the server	✓	✓	✓	✗
Access control alternating online offline	In case the server is ofline: automatic change to Offline-Mode	✓	✓	✓	✗
Access control oflline	The device uses its own access control lists	✓	✓	✓	✓
Access control with assisted onl	The device check self in the list and send the result to the server. the server then checks	✓	✓	✓	✗
Timeliness of data ca. in seconds	How fast is the generated data available	Depending on how often the data is retrieved	Message "data sets exist" <1s	<1s HTTP via Lan, 1-2s via GPRS	300s or more depending on the setting; 300s rec.
Download Hinweise Zusatzinfo		Downlaod: Windows Linux	Downlaod: Windows Linux	Download Hinweise/Info	

6. Communication via DLL

6.1. Program library [Dynamic Link Library (DLL)] - General information

6.1.1. What is a program library?

"A program library referred in programming as a set of subroutines that provides solutions to thematically related problems. Libraries, unlike programs, are not stand-alone units, but auxiliary modules that are requested or called by programs."

Wikipedia about program library

In order to address the functions (subroutines) of the program library, it must be integrated into your software solution. Depending on the development environment a certain procedure is required. In principle, all have one thing in common: the required functions have to be announced to your software solution (they must be declared).

6.1.2. Advantages of a program library in DLL or so-form.

Here specifically for the Datafox DLL.

- The integration of a DLL is easier and faster than the direct integration of a protocol.
- Can be used independently of the programming language..
- Single Programming Interface (API) to the different Datafox devices.
- The DLL shows defined error messages if operations can not be performed correctly.
- The DLL automatically writes log files for debugging.
- Updateable without rebuilding your software solution. Downwards compatible.

6.1.3. The communication library is available for the following systems:

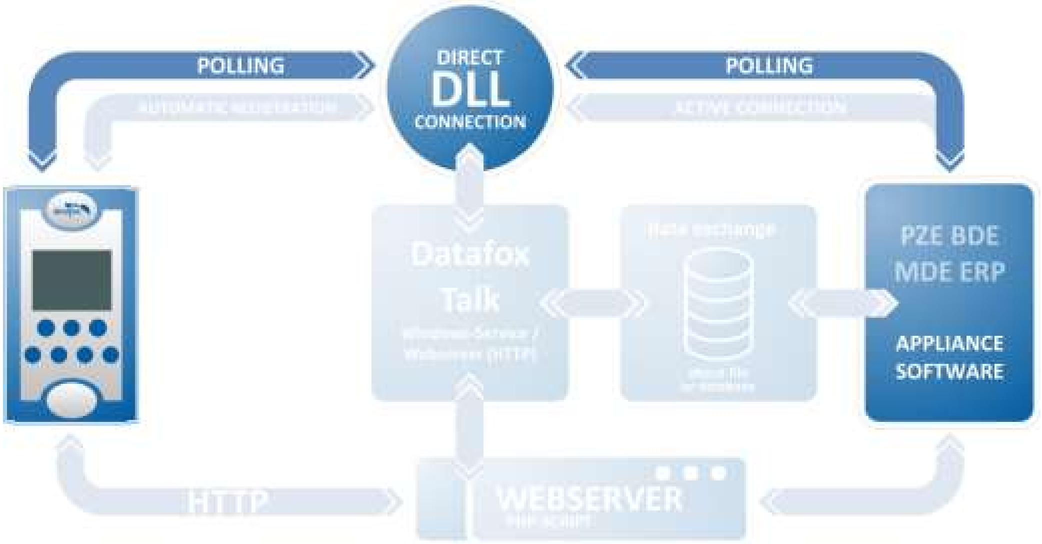
As DLL for Windows 32bit, DFComDLL.dll; 64bit, DFCom_x64.dll
As Shared Library or Static Library for Linux 32/64bit libDFCom.so (Makefile)

https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.21-Dokumentation.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.21-Source.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.21-x64.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.21-x86.zip

6.1.4. Program library (DLL) - Integration Passive mode (polling)

In the passive mode the communication link is established starting from the program library to the devices. For this you need a single function to establish connections and another for disconnection.

Functional principle when transferring the bookings:
The application queries the device via the DLL regularly to collect the data.



The following connection types are supported by the passive mode:

RS232 (via converter also RS485)
USB (via virtual COM-Port)
Modem (analog / GSM)
TCP / IP (LAN / WAN / WLAN)

An exemplary query of a device serial number in an device connected via TCP / IP using the C programming language:

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

advantages:

- All connection types and device types are supported.
- All functions of the program library are fully available.

disadvantages:

- If you want to receive the generated data sets immediately after creation, a constant communication with the device is necessary (polling). In TCP / IP networks, this, depending on the number of units, may lead to an undesirable loss of bandwidth.
- Not recommended for mobile communications as it may cause high costs.

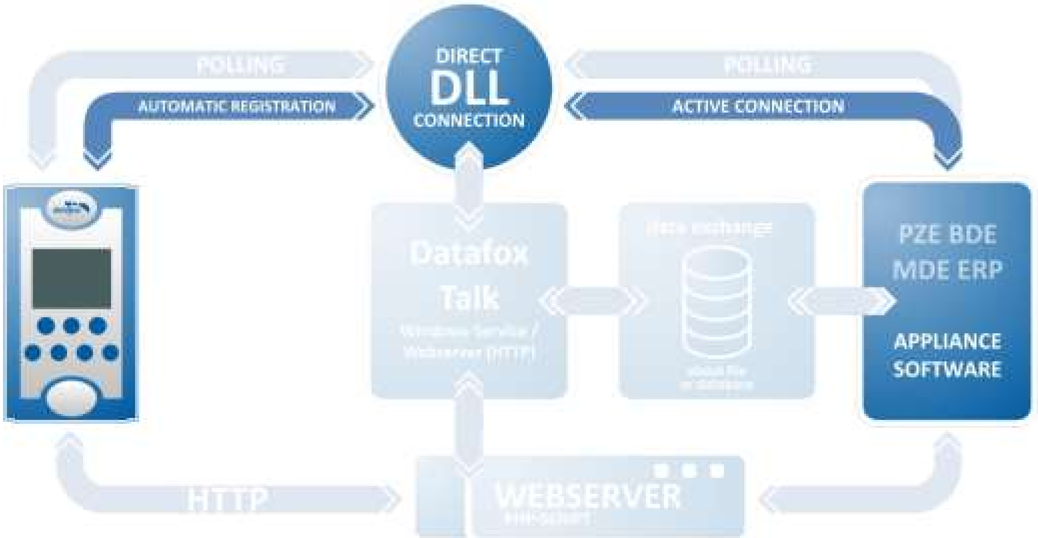
6.2. Program library (DLL) - Integration active mode (active connection)

In Active mode, the communication link from the devices to the program library is made. Prior to this, the devices must be informed at the time of installation where they are to be connected. In the program library, you need a single function to start the active mode and another to end the active mode.

The "DFCStartActiveConnection" function in this case replaces the function "DFComOpenIV" in passive mode.
After activation of active mode in the program library this waits for incoming connections and is then making them available for further processing in your application.

Functional principle when transferring the bookings:

The devices sign in to the DLL. This writes a list of registered devices. If a device has a booking, this sends a trigger to the DLL. The application responds to the trigger and fetches the booking. The necessary connection data is available in the registration list. The collection of the booking is made with the same functions as with polling. As a result, polling and active connection upon collection of the data differ only slightly.



The following connection types are supported by the active mode:

- TCP / IP (LAN, WAN, WLAN, GPRS)

advantages:

- The device log on independently and also report existing records.
- The application does not require a device list, since the devices sign in automatically into the DLL and the DLL provides a list of active devices.
- All functions of the program library are fully available.

disadvantages:

- Here, since the multi-master principle is necessary, only connections by connection type TCP / IP are supported.

More information and documentation can be found here:
https://www.datafox.de/d67/unternehmen/downloads/software/master4-v4/Datafox_Softwarepaket_MasterIV-V04.03.21.zip

6.3. Encrypting the data when using the DFCom.dll

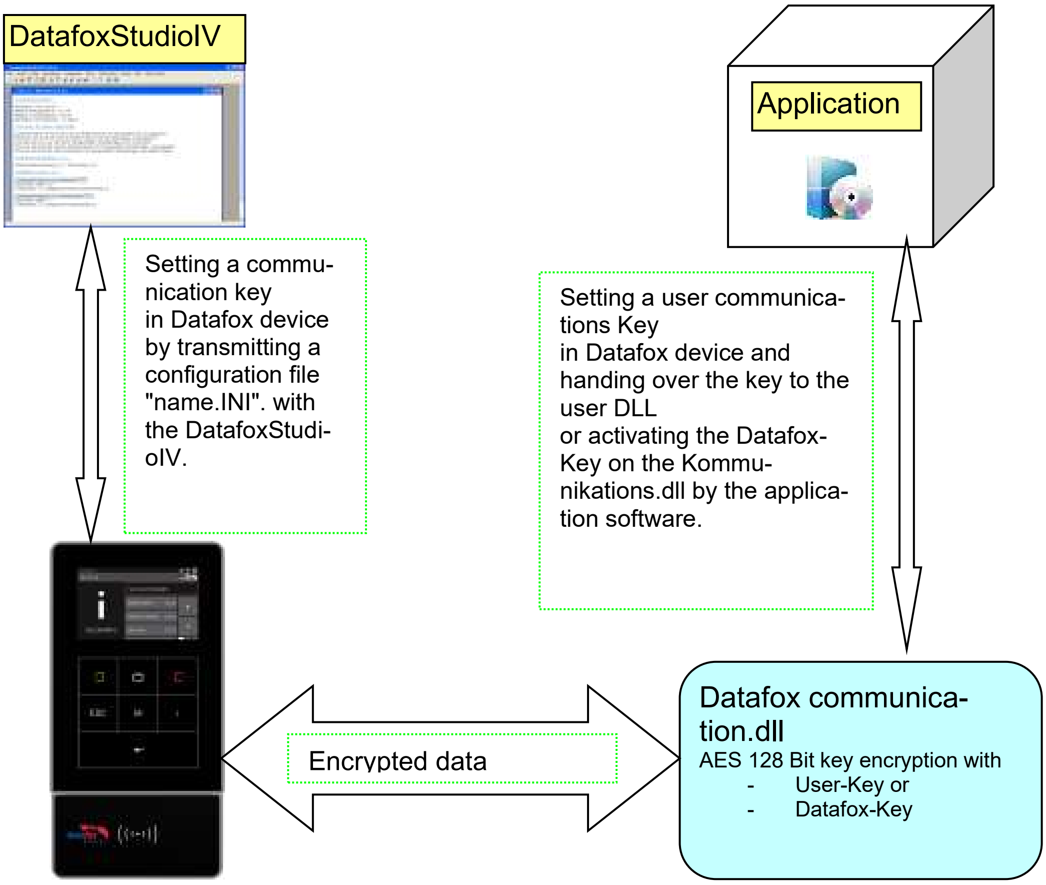
When using the Datafox communication DLL all data coming from the device or sent to the device may be transferred with an AES 128-bit encryption.

Thus, there are only 3 types of communication:

1. Unencrypted communication
2. Encrypt with Datafox-Key
3. Encrypt with user-Key

When integrating the Datafox DFCom.dll from the application side, only a user communication key is handed over to the .dll. The effort of integration of encryption is thus very low.

Overview of the encryption, schematic illustration.



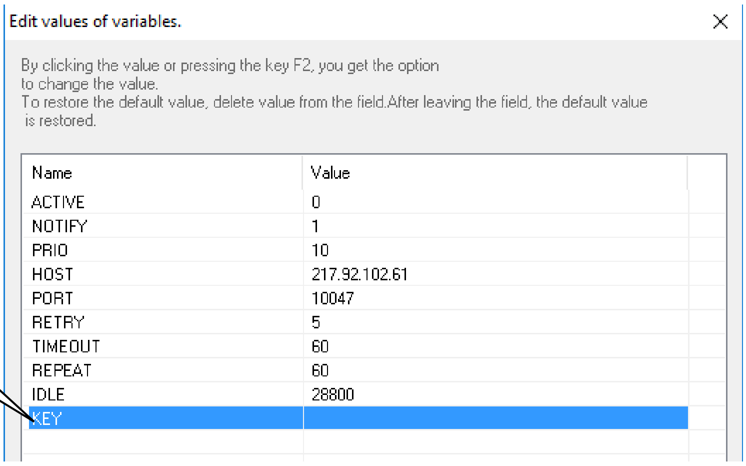
DatafoxStudioIV
Application
Setting a communication key in Datafox device by transmitting a configuration file "name.INI". with the DatafoxStudioIV.
Setting a user communications Key in Datafox device and handing over the key to the user DLL or activating the Datafox-Key on the Kommunikations.dll by the application software.
Encrypted data
Datafox communication.dll
AES 128 Bit key encryption with
- User-Key or
- Datafox-Key

A detailed description of how the handover of the key takes place, you will find:

- for Datafox StudioIV in the manual in the chapter "encrypt communication with MasterIV devices"
- and for the DLL in the DLL documentation

6.3.1. Create and save a communication key for the device

In the menu „Configuration“ -> “System variables active mode “open the configuration file to edit. For example: „active.ini“.



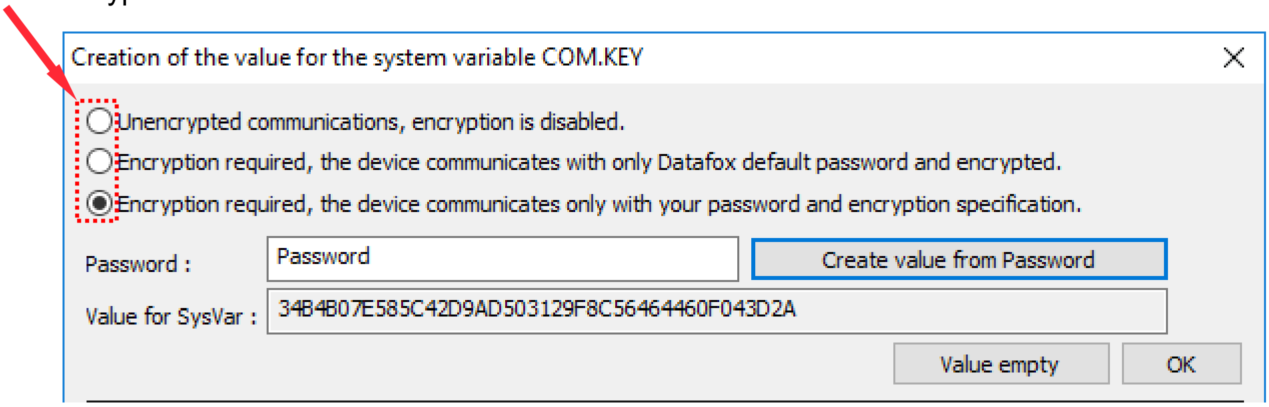
Click on the line “Key” to open a new window and to create a key.

Edit values of variables.

By clicking the value or pressing the key F2, you get the option to change the value.
To restore the default value, delete value from the field.After leaving the field, the default value is restored.

Name	Value
ACTIVE	0
NOTIFY	1
PRIO	10
HOST	217.92.102.61
PORT	10047
RETRY	5
TIMEOUT	60
REPEAT	60
IDLE	28800
KEY	

Select the type of communication.



Creation of the value for the system variable COM.KEY

○ Unencrypted communications, encryption is disabled.

○ Encryption required, the device communicates with only Datafox default password and encrypted.

● Encryption required, the device communicates only with your password and encryption specification.

Password : Password

Value for SysVar : 34B4B07E585C42D9AD503129F8C56464460F043D2A

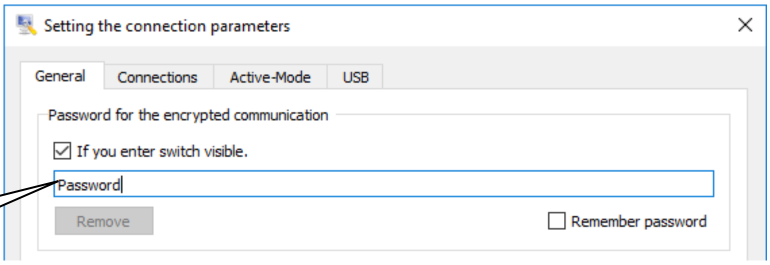
If you want the communication to be encrypted with your own stored password, enter a password and click on the button "Create value from password".

A communication key is now created. Finish the entry with "OK".
After a key has been created and the active. ini file has been transferred, communication with the device is only allowed if the password is entered.

6.3.2. Save the communication key in the Datafox StudioIV

If a device is using a communication key, then the Datafox StudioIV needs the same key. Otherwise no communication with the device would be possible,
In the menu „Communication -> Settings“ you may edit the key for the Communication.

The password is used for all types of communication.



Setting the connection parameters

Password for the encrypted communication

☑ If you enter switch visible.

Password

□ Remember password

Enter your password here.

The plaintext input is only possible at the first input.
If you reopen the window you won’t see the plaintext.

6.3.3. Transfer the communication key for DFComDLL

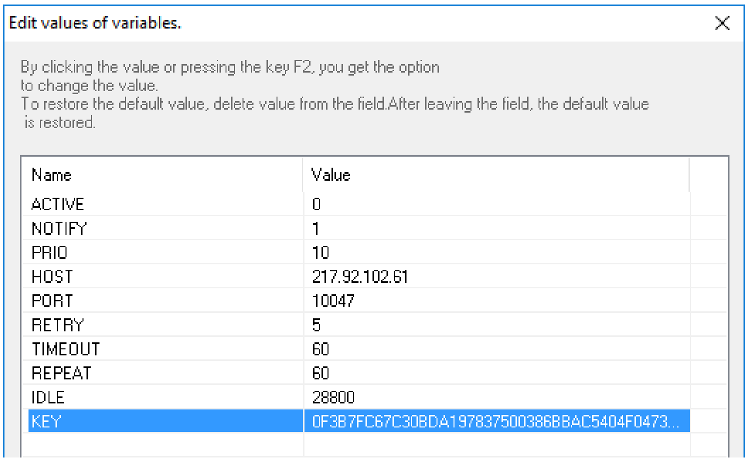
The key for the communication transferred to the DLL is called “DFCSetCommunicatioPassword”.
The key has to be in plaintext (**123456**) and not the created key of the Datafox StudioIV.

More information can be found in the documentation of the DFComDLL.

6.3.4. Clear the communikation key

If created a communication key and transferred to the device then clear this key as follows:

Click on “KEY” to edit.

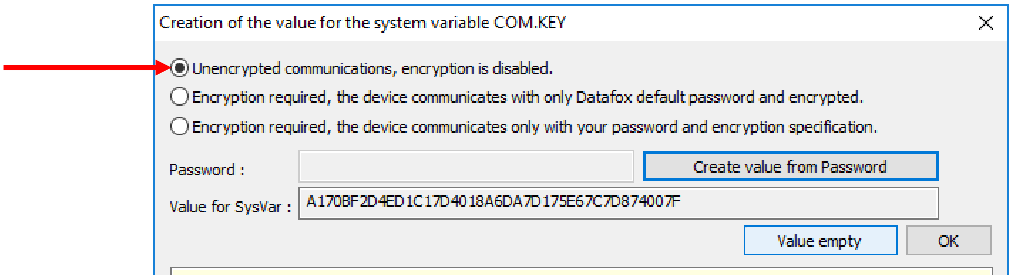


Edit values of variables.

By clicking the value or pressing the key F2, you get the option to change the value.
To restore the default value, delete value from the field.After leaving the field, the default value is restored.

Name	Value
ACTIVE	0
NOTIFY	1
PRIO	10
HOST	217.92.102.61
PORT	10047
RETRY	5
TIMEOUT	60
REPEAT	60
IDLE	28800
KEY	0F3B7FC67C30BDA197837500386BBAC5404F0473...

Switch to unencrypted communication.



Creation of the value for the system variable COM.KEY

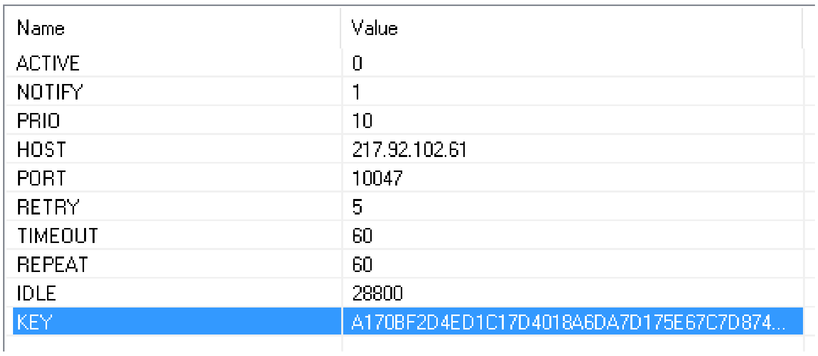
● Unencrypted communications, encryption is disabled.
○ Encryption required, the device communicates with only Datafox default password and encrypted.
○ Encryption required, the device communicates only with your password and encryption specification.

Password :

Value for SysVar : A170BF2D4ED1C17D4018A6DA7D175E67C7D874007F

Click on: “Value empty“.
Then click on: “Create value from Password“. The created Value from the empty Password is necessary to clear the old key in the device.

Save the file and transfer to the device.



Name	Value
ACTIVE	0
NOTIFY	1
PRIO	10
HOST	217.92.102.61
PORT	10047
RETRY	5
TIMEOUT	60
REPEAT	60
IDLE	28800
KEY	A170BF2D4ED1C17D4018A6DA7D175E67C7D874...

After this you can clear the created key from the .ini file.

7. http Level 1

7.1. Requirements

Required for data transfer via http Level 1:
Hardware V4:
- Device with TCP/IP (LAN / WLAN) or mobile radio
- min. Firmware 04.03.10. XX

Software:
- Server must accept an http request and give an active response
- Server must provide master data such as personnel lists or order lists for downloading

☞ **Note:**
If you still have older devices, they can be converted.

http Level 0 you find in the SDK http(s)

7.1.1. Request

Request from the client to the server.

7.1.2. Method: GET

For communication via http level 1, Datafox has developed a specific context that applies only to Datafox devices.
The GET method is used for http communication.
The context now offers extensive possibilities for exchanging data quickly and conveniently with Datafox devices.

Function overview via GET:

Parameter name	Meaning
df_table	Name of data set description
df_record_state	online / offline state of the records
df_col_{Feldname}	Name of the data field and value. According to the device configuration „Setup“.

7.1.3. Response

The server's response to the client.
Each dataset from a Datafox device must be acknowledged by the server.
The confirmation is carried out with:
df_api=1 und HTTP–Result „200 OK“

7.1.3.1. Optional parameter specifications for the response

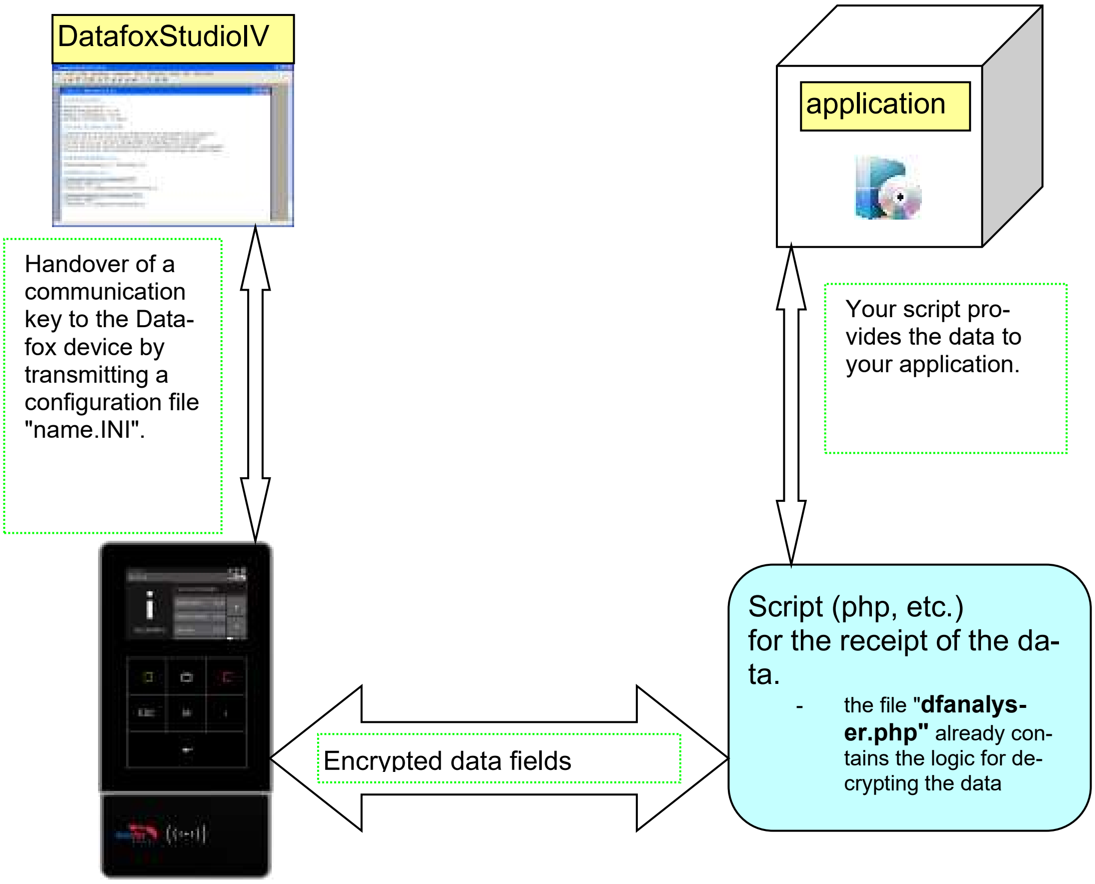
Instruction Name	Meaning
df_time=2016-11-17T12:13:14	Set the date and time on the device.
df_beep=1 (1-11)	OK signal / generate beep on the device
df_service=1,www.datafox.de,10047	Connect to the DLL. Also possible with the Datafox StudioIV. Specification of IP/URL and port possible.
df_var=setup.1,wert	Change the value of a global variable in the setup.
df_ek=name	Trigger an action in the device. Start an input chain in signal processing.
df_msg=This\ris\ra\rMessage,5,1,0	Send a text message to the display.
df_msg_icon=2	Defines the icon to be used when showing a message in the device. The icon is taken from the design and associate to an input sequence (F2 in this example)
df_backlight=0,5,255,255,0,192	Defines the colour of a device’s backlight – for a certain period of time as a RGBW value.
df_info_msg=Info\rMessage,0	Defines the text of an info message.
df_ac2=010,1,10,20,5	AC = access control. Trigger access control actions.
df_custom_msg_ac2=010,1,1,0,Hello%20World	Sends a message to a device that is connect to the access control bus.
df_ao_ac2=0,1234	Acknowledges an action of the pre-checked access control.
df_trigger_ac2=1,011,6543210,0	Simulates a clocking performed at an access control RFID reader.
df_kvp=var,ID	Instructs the device to send the value of a system variable. The value is sent as a key-value-pair to the server.
df_set_relay=2,close,5	Defines the state of a relay for given period of time that is not handled by the access control module.
df_toggle_relay=2,5	Changes the state of a relay for a given period of time. The relay may not be handled by the access control module.
df_load_file=/path/on/server	Instructs the device to download a file from the server.
df_send_file=/logs/,syslog,0	Instructs the device to upload a file to the server.

Instruction Name	Meaning
df_remove_file=root:datafox.cert	Instructs the device to delete a specific file.
df_remove_finger=1980,all	Remove fingers from a fingerprint sensor.
df_setup_list=Personal,/path/to/list.txt	Give the device a new list of personnel, for example.
df_ac2_list=Identification,/path/to/list.txt	Give the device a new access control list.
df_table_count=list.PID	Counts the number of entries within a list stored on the device.
df_table_select=list.PID,/upload/form,Unit=Development,PID=5	Selects on or more entries from a list and uploads them to the server.
df_table_append=list.PID,9999,,Visitor,	Appends a record to a list stored on the device.
df_table_update=list.PID,,,Unit=	Changes values within a list stored on the device.
df_table_delete=list.PID,Unit=Development	Removes rows from a list stored on the device.

7.1.4. Encryption of the data fields when sending via HTTP

If data records are sent via HTTP, the field contents can be transmitted in encrypted form. The data fields of the data set are then encrypted using a RC4 encryption. The so encrypted characters are transferred as field contents in hexadecimal.

Overview of encryption with HTTP; schematic representation:



DatafoxStudioIV

Handover of a communication key to the Datafox device by transmitting a configuration file "name.INI".

application

Your script provides the data to your application.

Script (php, etc.) for the receipt of the data.

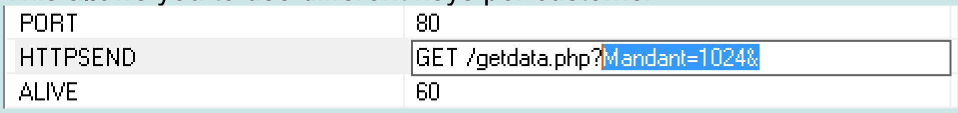
- the file **"dfanalyser.php"** already contains the logic for decrypting the data

Encrypted data fields

A detailed description of how the handover of the key takes place, can be found:

- in the manual of Datafox StudioIV Chapter „5.4.5. "Encryption of the data fields when sending via HTTP"
- and the file "dfanalyser.php" can be found on the Datafox DVD or in the download - Software for Windows

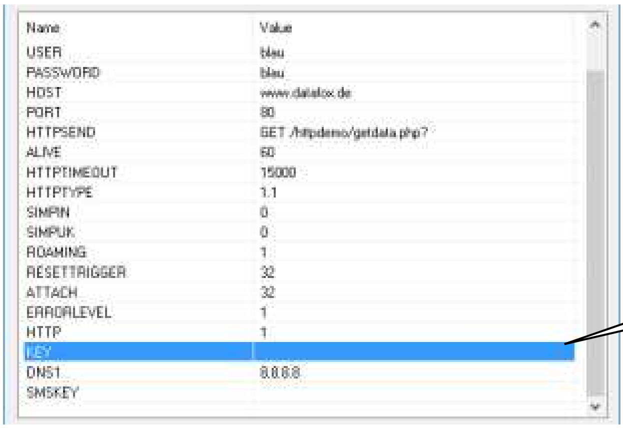
Note:
If you use encryption for several customers, you have to pass a customer ID into the plain text.
This allows you to use different keys per customer.



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

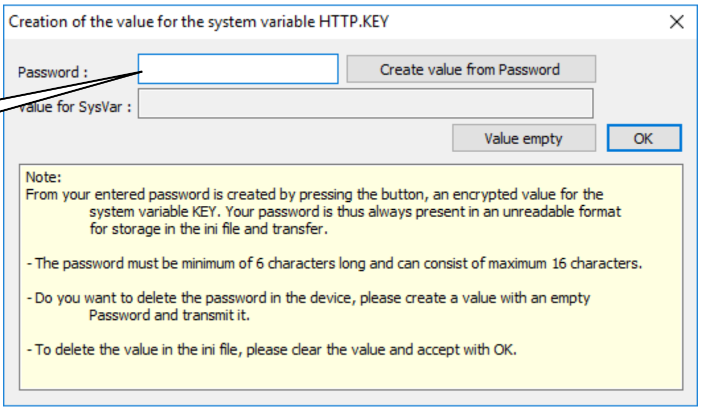
Activating Encryption via Datafox StudioIV

Open the configuration file (e.g. GPRS.ini) for editing via the menu entry Configuration "GPRS / HTTP - Configuration".



Name	Value
USER	blau
PASSWORD	blau
HOST	www.datafox.de
PORT	80
HTTPSEND	GET /httpdemo/getdata.php?
ALIVE	60
HTTPTIMEOUT	15000
HTTPTYPE	1.1
SIMPIN	0
SIMPUK	0
ROAMING	1
RESETTRIGGER	32
ATTACH	32
ERRORLEVEL	1
HTTP	1
KEY	
DNS1	8.8.8.8
SMSKEY	

By clicking on the line “KEY”, the window for creating the key opens.



Creation of the value for the system variable HTTP.KEY
Password :
Create value from Password
Value for SysVar :
Value empty
OK

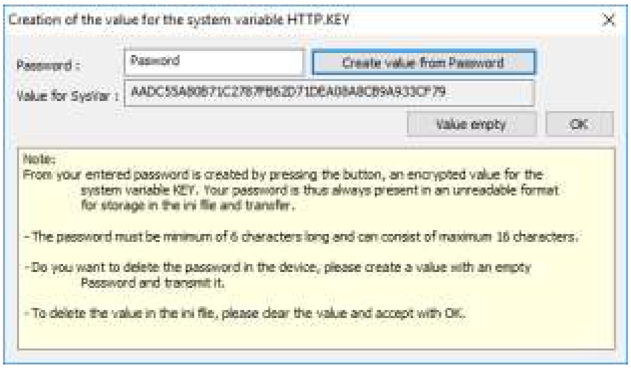
Note:
From your entered password is created by pressing the button, an encrypted value for the system variable KEY. Your password is thus always present in an unreadable format for storage in the ini file and transfer.

- The password must be minimum of 6 characters long and can consist of maximum 16 characters.

- Do you want to delete the password in the device, please create a value with an empty Password and transmit it.

- To delete the value in the ini file, please clear the value and accept with OK.

Enter your password here.



Creation of the value for the system variable HTTP.KEY
Create value from Password
Value empty
OK

Password : Pasword

Value for SysVar : AADC55A80B71C2787FB62D71DEA08A8CB9A933CF79

Note:
From your entered password is created by pressing the button, an encrypted value for the system variable KEY. Your password is thus always present in an unreadable format for storage in the ini file and transfer.

- The password must be minimum of 6 characters long and can consist of maximum 16 characters.

- Do you want to delete the password in the device, please create a value with an empty Password and transmit it.

- To delete the value in the ini file, please clear the value and accept with OK.

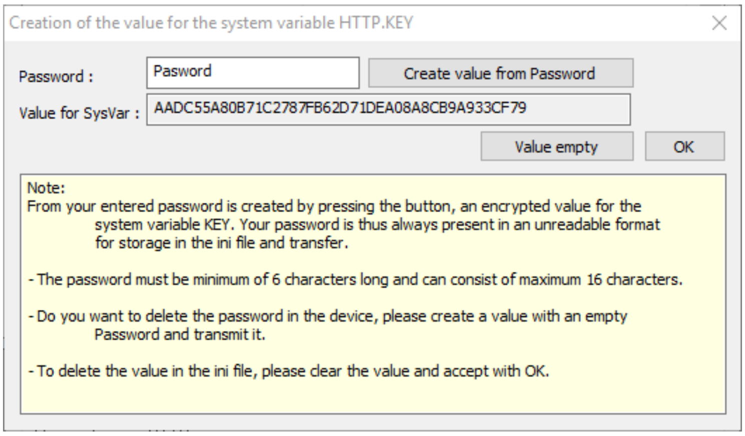
By clicking the button "Create value from password", a key for transfer is generated.

Click "OK" to take the key over.
Subsequently, you can save the settings and transfer them to the Datafox device.

Disable encryption

To deactivate the key which has been transferred to the device, it is necessary to create an empty password field with the button "Clear value" and to transfer this empty key to the device.

Click on „Value empty“



Creation of the value for the system variable HTTP.KEY

Password : Pasword

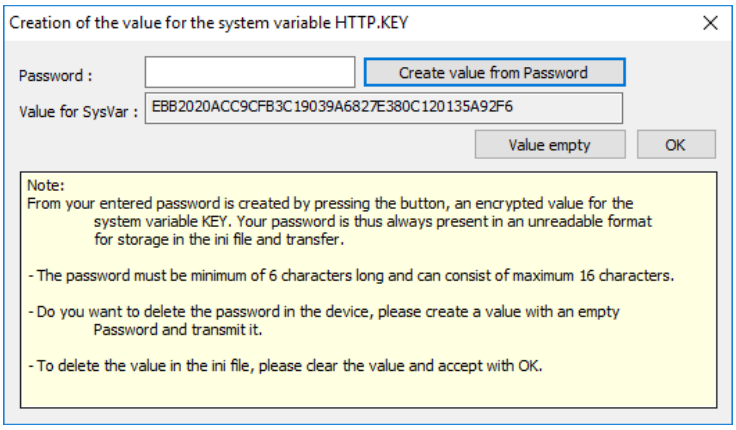
Value for SysVar : AADC55A80B71C2787FB62D71DEA08A8CB9A933CF79

Note:
From your entered password is created by pressing the button, an encrypted value for the system variable KEY. Your password is thus always present in an unreadable format for storage in the ini file and transfer.

- The password must be minimum of 6 characters long and can consist of maximum 16 characters.

- Do you want to delete the password in the device, please create a value with an empty Password and transmit it.

- To delete the value in the ini file, please clear the value and accept with OK.



Creation of the value for the system variable HTTP.KEY

Password :

Value for SysVar : EBB2020ACC9CFB3C19039A6827E380C120135A92F6

Note:
From your entered password is created by pressing the button, an encrypted value for the system variable KEY. Your password is thus always present in an unreadable format for storage in the ini file and transfer.

- The password must be minimum of 6 characters long and can consist of maximum 16 characters.

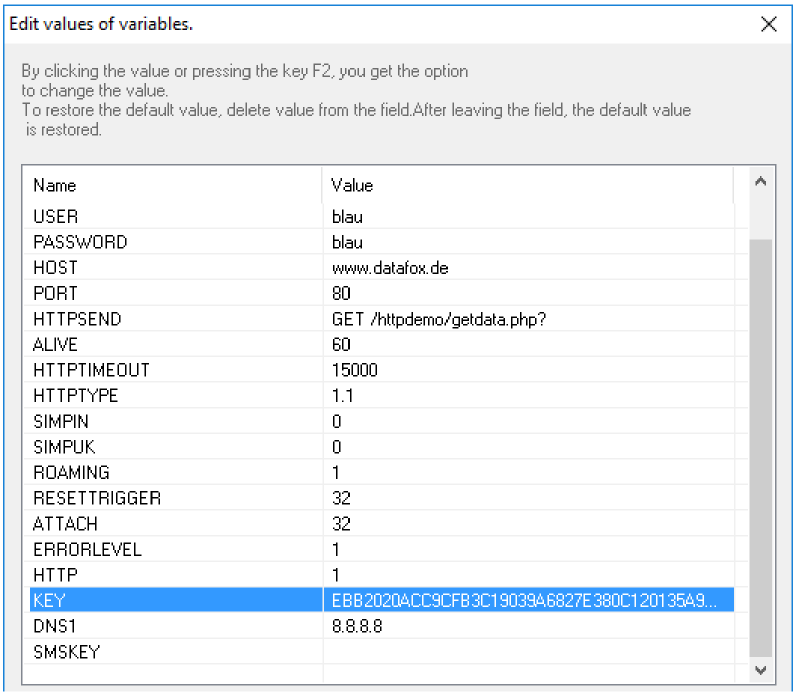
- Do you want to delete the password in the device, please create a value with an empty Password and transmit it.

- To delete the value in the ini file, please clear the value and accept with OK.

Click on "Create value from Password“.

and then on „OK“

Save this file with the new key.



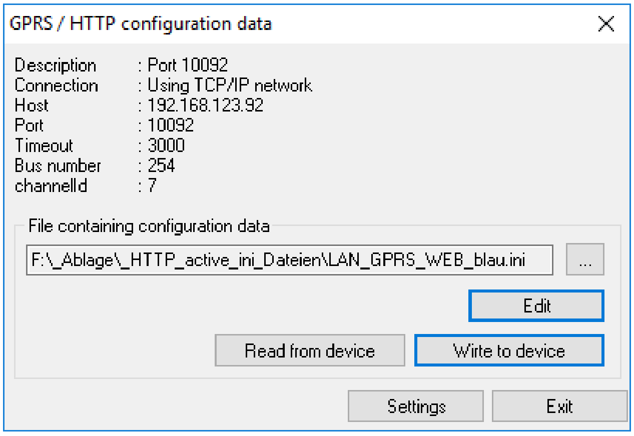
Edit values of variables.

By clicking the value or pressing the key F2, you get the option to change the value.
To restore the default value, delete value from the field.After leaving the field, the default value is restored.

Name	Value
USER	blau
PASSWORD	blau
HOST	www.datafox.de
PORT	80
HTTPSEND	GET /httpdemo/getdata.php?
ALIVE	60
HTTPTIMEOUT	15000
HTTPTYPE	1.1
SIMPIN	0
SIMPUK	0
ROAMING	1
RESETTRIGGER	32
ATTACH	32
ERRORLEVEL	1
HTTP	1
KEY	EBB2020ACC9CFB3C19039A6827E380C120135A9...
DNS1	8.8.8.8
SMSKEY	

Klick on “Write to device“

Now the key in the device is deleted.



GPRS / HTTP configuration data

Description : Port 10092
Connection : Using TCP/IP network
Host : 192.168.123.92
Port : 10092
Timeout : 3000
Bus number : 254
channelId : 7

File containing configuration data

F:_Ablage_HTTP_active_ini_Dateien\LAN_GPRS_WEB_blau.ini

In order to deactivate the key transferred to the device, you must create an empty password field by clicking the button "Empty value" and transfer the empty key to the device.
The data records are then sent unencrypted.

The data fields of the data set can be encrypted using a stream cipher RC4. The field contents are then transferred to their hexadecimal representation.

parameter name	**importance**
df_cb	The parameter specifies that all these fields until and including df_ce have encrypted field contents. The value of df_cb contains the four-digit (1000-9999) public key of the applicable password for the stream cipher.
df_ce	The parameter indicates that all the following fields are not encrypted any more. If the value is decrypted correctly it must match the value of df_cb.

7.1.4.1. Illustrate the GET request

In plain text (unencrypted) and encrypted:

Plaintext request
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
Plaintext Reply
df_api=1&df_time=2017-11-22T08:24:00
Encrypted request
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
encrypted response
df_api=1&df_cb=6102&df_time=e1ba6575855619c4d634f7865c01c4b2bc2ec138670ac2&df_ce=a414ebd6

7.1.4.2. Encryption detection

To see whether the data fields are sent encrypted, the initial encryption is with ‘df_cb’ (Datafox Crypt Begin) in and with ‘df_ce’ (Datafox crypt end) in the end. ‘df_cb’ the first field in the request and ‘df_ce’ the last field in the request is.

The value of the field ‘df_cb’, itself is transmitted in plain text and is ‘public key’. It is a random number between 1000 and 9999. The value must be used in conjunction with the communication password for the encryption and decryption.

7.2. https Communication

7.2.1. Requirements

Requirement for using an SSL certificate (https):
Hardware V4:
- Device with TCP/IP (LAN / WLAN) or mobile radio

Minimum firmware 04.03.11. XX (currently usable as prototype firmware)
Software:
- Server must accept an https request and give an active response

A detailed description of your development can be found here:Link: https://www.datafox.de/d67/unternehmen/downloads/software/master4-v4/datafox-sdk-http.zip

7.2.2. Elements of the https infrastructure

Like http, https is a client-server protocol. The client establishes a connection to the port of the https server via TCP/IP, the data stream is encrypted to protect it against listeners.

Both asymmetric encryption (negotiation of the connection) in the form of a server certificate and symmetric encryption for (later) data exchange are used.

7.2.3. Use of encryption / certificates

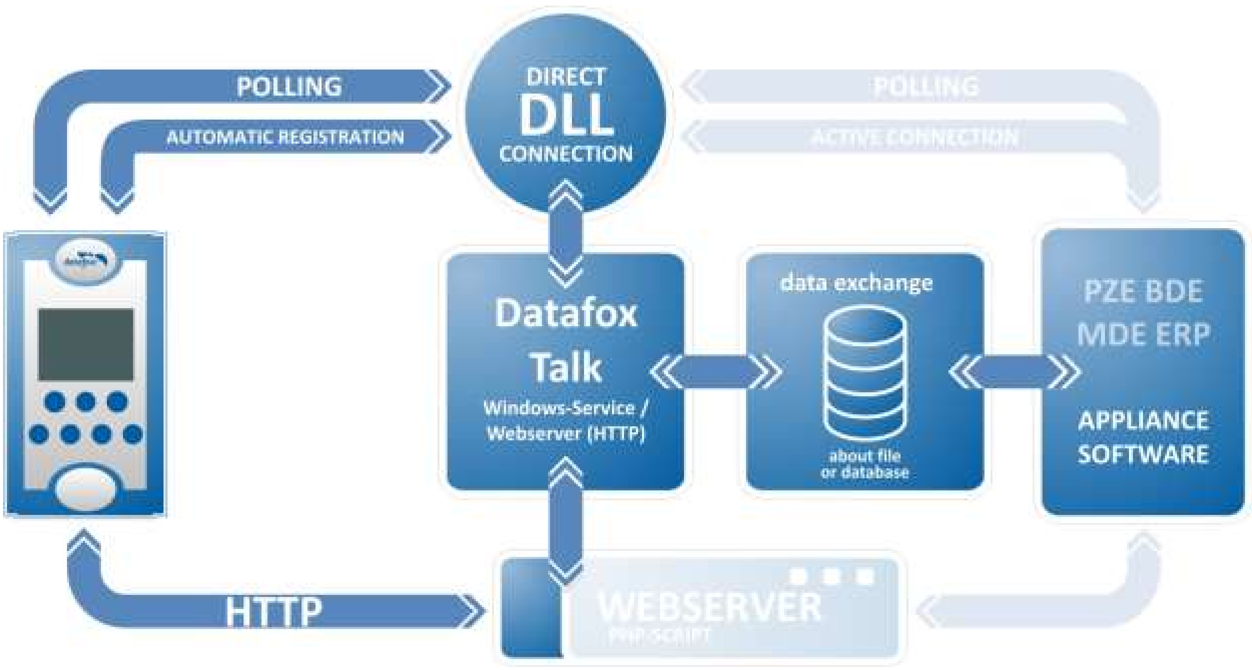
Several certificates can be stored in the Datafox devices for communication.
You can use a certificate signed by Datafox or your own certificate.

The firmware rejects the use of the encryption methods according to specification TLS 1.0, which are no longer considered to be up-to-date (because they are unsafe). Only procedures introduced as of TLS 1.1 are accepted.

Certificates are transferred with the DatafoxStudioIV
The menu item is available as of StudioIV version 04.03.11. XX.
You will find them under: "Configuration>Transfer Certificates".

8. Talk

Datafox - Talk enables the exchange of data with Datafox AEIII +, Timeboy and the Master IV - Series on file and database level. It therefore represents an alternative to communication via DLL and has the great advantage that no programming is required. Lists and devices can be transferred manually or by timer settings data can be read. At extra cost calculation a direct access to customer databases can be provided. Here, the customer determines which database tables and fields are linked.
Datafox- Talk supports all functions for transmitting data.



8.1. Advantages and disadvantages with Datafox Talk

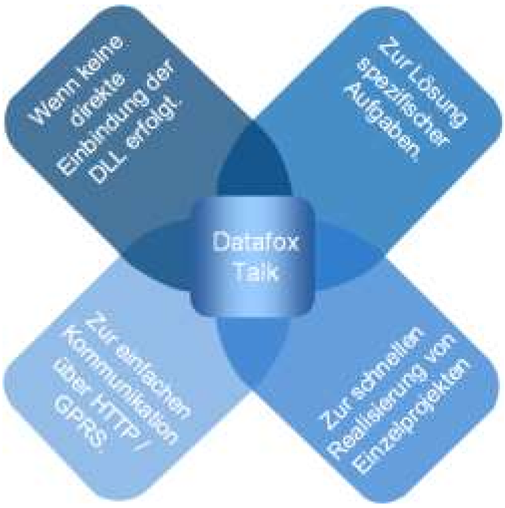
advantages:

Easy data exchange via file storage or database
Automatic fetching of the data via services
Integrated web server to accept data via http
No programming required
Simple updating of master data

disadvantages:

No access to system variables
No online functionality

8.2. When do I use Talk?

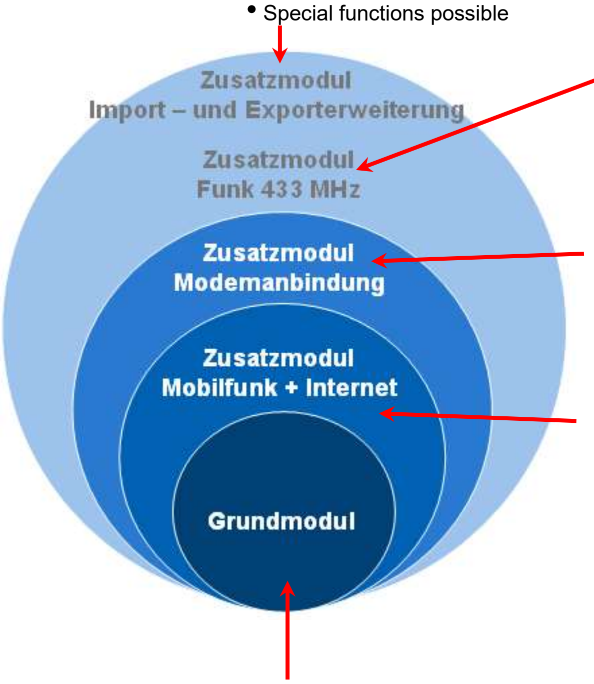

Wenn keine direkte Einbindung der DLL erfolgt.
Zur Lösung spezifischer Aufgaben
Datafox Talk
Zur einfachen Kommunikation über HTTP / GPRS
Zur schnellen Realisierung von Einzelprojekten

advantages:

- Expanded use possibilities of the devices
- Simplifies commissioning and maintenance
- No programming skills required
- Communication with any application software
- No need to create a special interface
- Data can be run directly into the application

8.3. Overview of the Function Modules Talk

- Free formatting of the output files
- ODBC connection to external databases and XML interfaces
- Special functions possible



- Wireless data transmission with 433 MHz
- Wireless network with multiple access points possible
- Management of radio addresses
- Protocol monitoring only for TimeboyIII

- Data transfer via analogue, ISDN or GSM modem.

- Data transfer directly to the Talk-data server and Maintenance Server on Windows
- Data transfer from your web server via a text file with FTP access. PHP necessary.
- Data transfer from your web server via MySQL database with access to the database.
- Data transfer from your web server via MySQL database with access via http

- time control
- Data transmission for all Datafox devices via RS232, RS485 and TCP / IP
- Storage of read data as an ASCII file, Excel, XML, dBase, Access
- Loading lists and access lists from ASCII files.

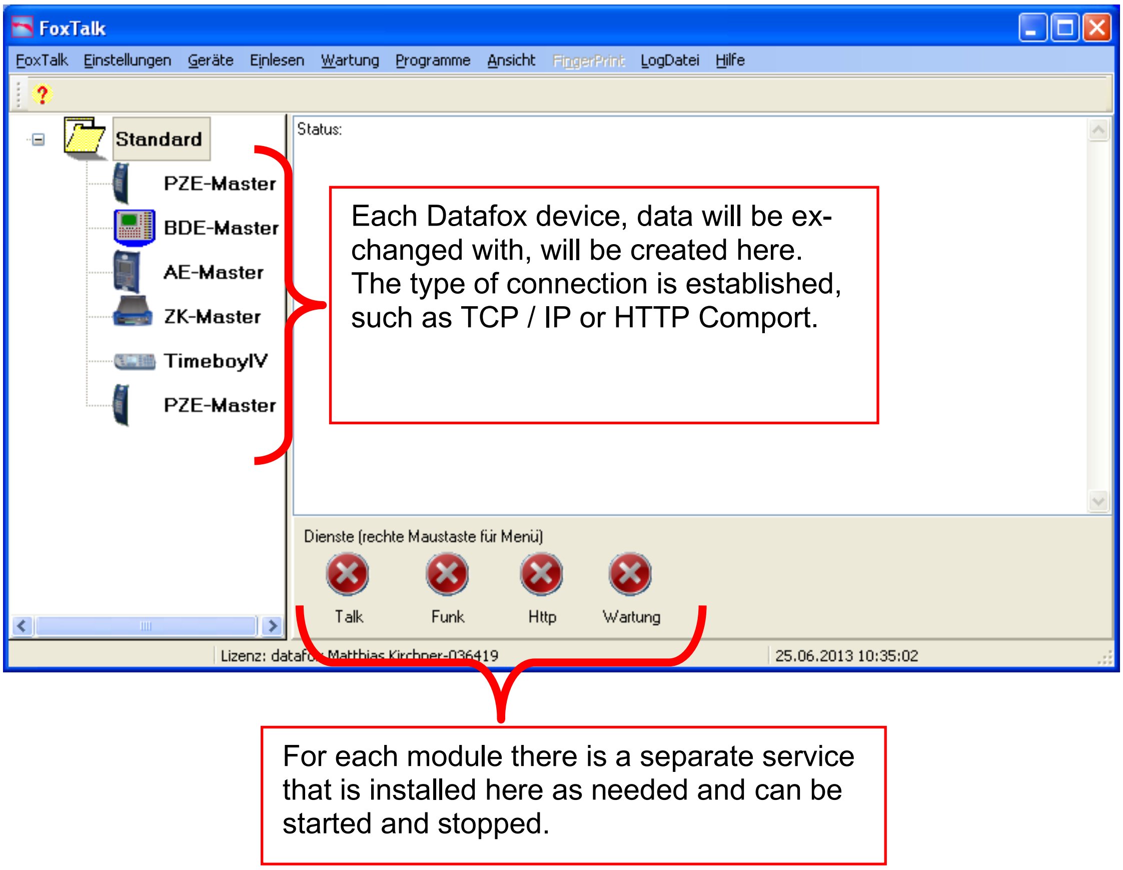
8.4. Establishment of Talk

For the establishment of Talk, we recommend a training by Datafox.
Current training dates can be found on our website:
https://www.datafox.de/support/datafox-akademie

The Datafox Talk Manual can be found on the homepage.
https://www.datafox.de/d67/unternehmen/downloads/software/datafox-talk/datafox-talk-handbuch.pdf

A quick tour of setting up Datafox Talk.

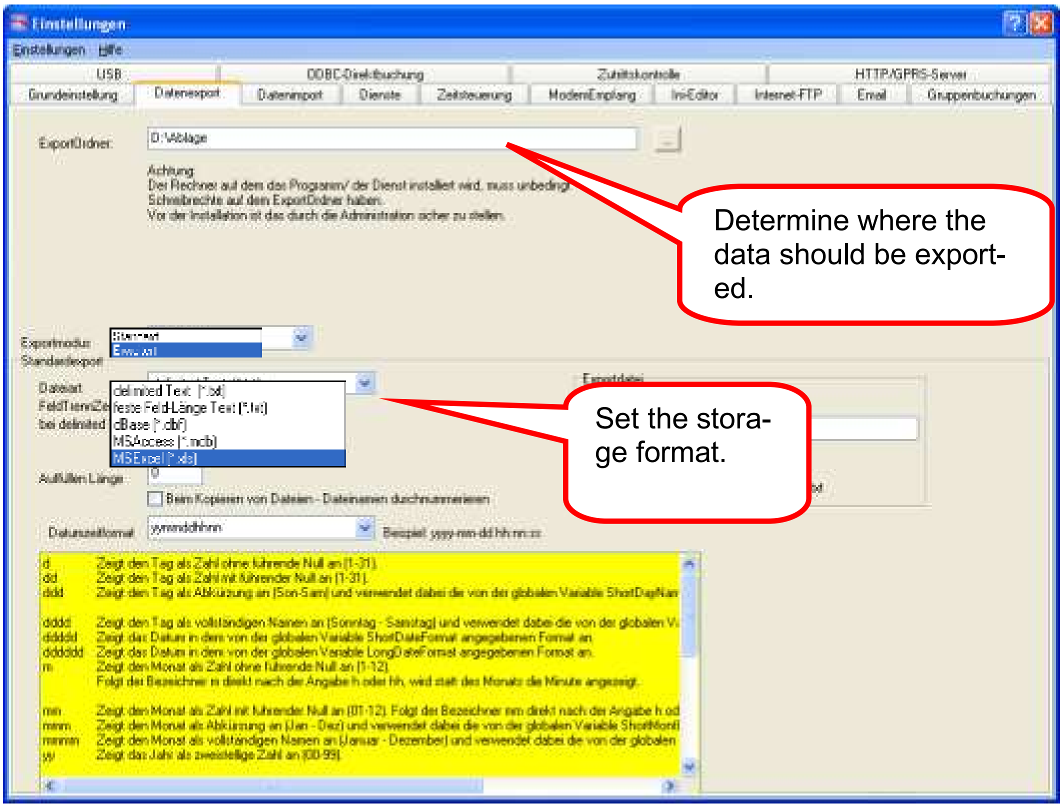
User interface:


FoxTalk
FoxTalk Einstellungen Geräte Einlesen Wartung Programme Ansicht FingerPrint LogDatei Hilfe
Standard
PZE-Master
BDE-Master
AE-Master
ZK-Master
TimeboyIV
PZE-Master
Status:
Dienste (rechte Maustaste für Menü)
Talk
Funk
Http
Wartung
Lizenz: datafox Matthias Kirchner-036419
25.06.2013 10:35:02

Each Datafox device, data will be exchanged with, will be created here. The type of connection is established, such as TCP / IP or HTTP Comport.

For each module there is a separate service that is installed here as needed and can be started and stopped.

Settings for data export:



Einstellungen
Einstellungen Hilfe
USB | ODBC-Direktbuchung | Zutrittskontrolle | HTTP/GPRS-Server
Grundeinstellung | Datenexport | Datenimport | Dienste | Zeitsteuerung | ModemEmpfang | Ini-Editor | Internet-FTP | Email | Gruppenbuchungen

ExportOrdner: D:\Ablage

Achtung:
Der Rechner auf dem das Programm/ der Dienst installiert wird, muss unbedingt
Schreibrechte auf dem ExportOrdner haben.
Vor der Installation ist das durch die Administration sicher zu stellen.

Exportmodus: Standard / Excel xml
Standardexport

Dateiart: delimited Text (*.txt) / feste Feld-Länge Text (*.txt) / dBase (*.dbf) / MSAccess (*.mdb) / MSExcel (*.xls)

FeldTrennZei...
bei delimited

Exportdatei

Auffüllen Länge: 0

☐ Beim Kopieren von Dateien - Dateinamen durchnummerieren

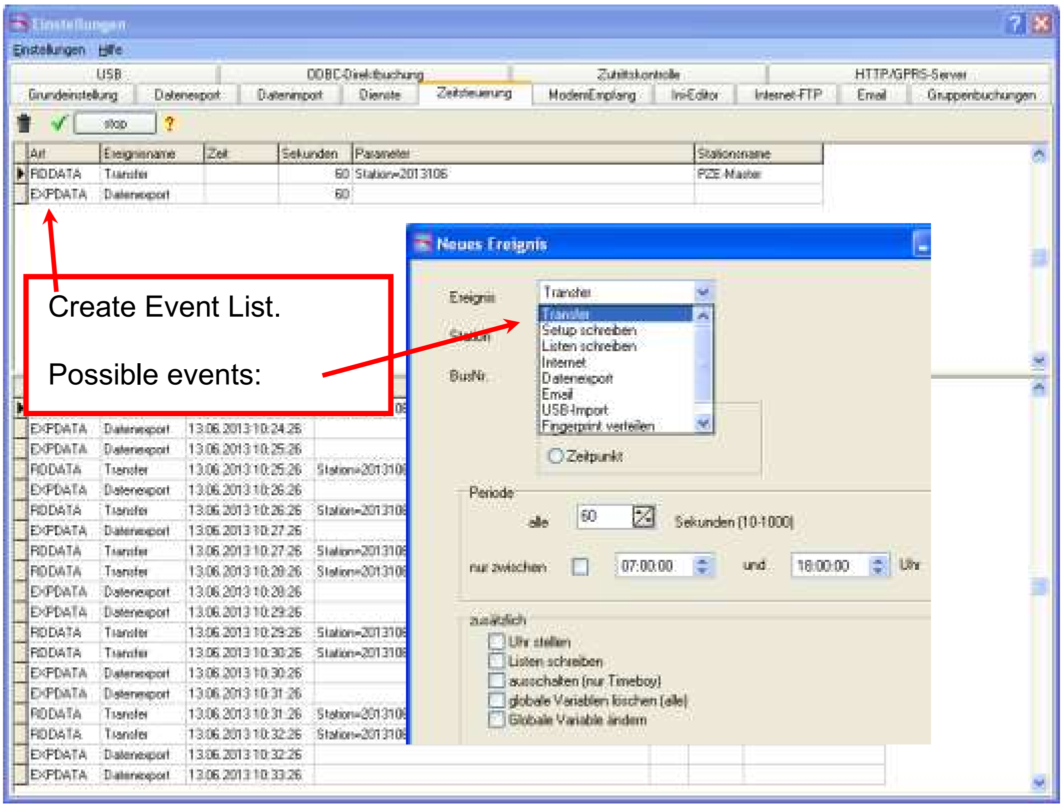
Datumzeitformat: yymmddhhnn Beispiel: yyyy-mm-dd hh:nn:ss

```
d       Zeigt den Tag als Zahl ohne führende Null an (1-31).
dd      Zeigt den Tag als Zahl mit führender Null an (1-31).
ddd     Zeigt den Tag als Abkürzung an (Son-Sam) und verwendet dabei die von der globalen Variable ShortDayNan

dddd    Zeigt den Tag als vollständigen Namen an (Sonntag - Samstag) und verwendet dabei die von der globalen V
ddddd   Zeigt das Datum in dem von der globalen Variable ShortDateFormat angegebenen Format an
dddddd  Zeigt das Datum in dem von der globalen Variable LongDateFormat angegebenen Format an.
m       Zeigt den Monat als Zahl ohne führende Null an (1-12).
        Folgt der Bezeichner m direkt nach der Angabe h oder hh, wird statt des Monats die Minute angezeigt.

mm      Zeigt den Monat als Zahl mit führender Null an (01-12). Folgt der Bezeichner mm direkt nach der Angabe h od
mmm     Zeigt den Monat als Abkürzung an (Jan - Dez) und verwendet dabei die von der globalen Variable ShortMontl
mmmm    Zeigt den Monat als vollständigen Namen an (Januar - Dezember) und verwendet dabei die von der globalen
yy      Zeigt das Jahr als zweistellige Zahl an (00-99).
```

Determine where the data should be exported.

Set the storage format.

Settings for time control of the service:
Here are all tasks that the service performs time controlled are created.



Einstellungen
Einstellungen Hilfe
USB | ODBC-Direktbuchung | Zutrittskontrolle | HTTP/GPRS-Server
Grundeinstellung | Datenexport | Datenimport | Dienste | Zeitsteuerung | ModemEmpfang | Ini-Editor | Internet-FTP | Email | Gruppenbuchungen
stop

Art	Ereignisname	Zeit	Sekunden	Parameter	Stationsname
RDDATA	Transfer		60	Station=2013106	PZE-Master
EXPDATA	Datenexport		60		

EXPDATA	Datenexport	13.06.2013 10:24:26	
EXPDATA	Datenexport	13.06.2013 10:25:26	
RDDATA	Transfer	13.06.2013 10:25:26	Station=201310
EXPDATA	Datenexport	13.06.2013 10:26:26	
RDDATA	Transfer	13.06.2013 10:26:26	Station=201310
EXPDATA	Datenexport	13.06.2013 10:27:26	
RDDATA	Transfer	13.06.2013 10:27:26	Station=201310
RDDATA	Transfer	13.06.2013 10:28:26	Station=201310
EXPDATA	Datenexport	13.06.2013 10:28:26	
EXPDATA	Datenexport	13.06.2013 10:29:26	
RDDATA	Transfer	13.06.2013 10:29:26	Station=201310
RDDATA	Transfer	13.06.2013 10:30:26	Station=201310
EXPDATA	Datenexport	13.06.2013 10:30:26	
EXPDATA	Datenexport	13.06.2013 10:31:26	
RDDATA	Transfer	13.06.2013 10:31:26	Station=201310
RDDATA	Transfer	13.06.2013 10:32:26	Station=201310
EXPDATA	Datenexport	13.06.2013 10:32:26	
EXPDATA	Datenexport	13.06.2013 10:33:26	

Neues Ereignis

Ereignis: Transfer
Transfer / Setup schreiben / Listen schreiben / Internet / Datenexport / Email / USB-Import / Fingerprint verteilen

Station

BusNr.

○ Zeitpunkt

Periode
alle 60 Sekunden (10-1000)
nur zwischen ☐ 07:00:00 und 18:00:00 Uhr

zusätzlich
☐ Uhr stellen
☐ Listen schreiben
☐ ausschalten (nur Timeboy)
☐ globale Variablen löschen (alle)
☐ Globale Variable ändern

Create Event List.

Possible events:

9. Appendix

9.1. All importent Download-links

9.1.1. Manuals for the devices

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 4.6 FlexKey-DE.pdf
https://www.datafox.de/download/Datafox EVO 4.6 FlexKey-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 PZE-MasterIV V4-DE.pdf
https://www.datafox.de/download/Datafox PZE-MasterIV V4-EN.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 TimeboyIV-DE.pdf
https://www.datafox.de/download/Datafox TimeboyIV-EN.pdf
https://www.datafox.de/download/Datafox Timeboy Mobil PZE-DE.pdf

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

9.1.2. Software and SDK (Interface descriptions)

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%2004.03.21-Dokumentation.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.21-Source.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.21-x64.zip
https://www.datafox.de/download/Datafox%20DFComDLL%2004.03.21-x86.zip

9.1.3. Other important 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. All news in a compact form

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. Information for HTTPS

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

HTTPS is used for establish-ing encrypted connections as well as for encrypted transmission of data via LAN, WLAN or mobile radio.
This document describes the functionality in princi-pal, gives hints for the im-plementation and back-ground information on the technologies used.

Datafox Devices implements **TLS** (Transport Layer security) using the mbed-TLS library. With this implementation the devices provide TLS 1.1 and TLS 1.2 functionality, TLS 1.3 is not available currently (May 2020).

This document does not analyse if the data transported between Datafox Devices and an OEM application is with the cost of “cracking” the encryption. This evaluation is left to the reader. However since clocking events are personal data without a doubt, the GDPR requires protecting these data elements – seldom they are matter of secrecy.

Establishing an HTTPS communication
HTTPS communication takes two phases:

- During the TLS handshake client and server check the authen-ticity of their corresponding communication partner. This phase uses the Diffie-Hellmann-Algorithm. After the verifica-tion an encryption key for the exchange of data is established. This process takes place whenever a communication is being negotiated.
- During data exchange, all communication is done encryptedly using the previously established key.

During the TLS handshake asymmetric cryptography is used, during data exchange symmetric cryptographic algorithms are used. Typically RSA (named after Rivest, Shamir and Adleman, who specified the algorithm) or ECC (Elliptic curve cryptography) are used for the handshake, AES (Advanced encryption standard) for data exchange. This makes HTTPS a “hybrid cryptographic algo-rithm.”

Asymmetric vs. Symmetric cryptography
Asymmetric algorithms use different keys for encryption and de-cryption – symmetric algorithms use the same key for encryption and decryption. Using different keys at asymmetric methods allows creating a public and private part of the key – as required for a “Public key infrastructure” (PKI). Splitting the key typically results in higher resource consumption of the algorithm (computation time as well as memory) when comparing to symmetric cryptog-raphy.

Key factors influencing cryptographic security
The security of encrypted data exchange depends on different factors:

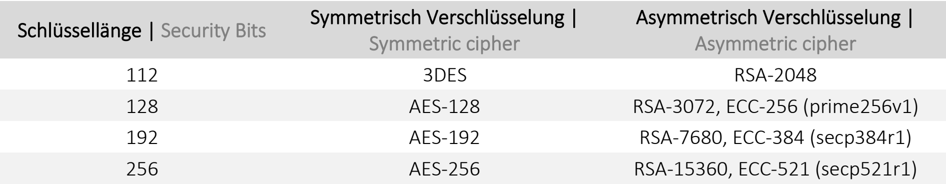
- Safety of the algorithm,
- Length of the key,
- Safety of the systems that exchange data,
- Safety of the infrastructure used to exchange data.

Typically not all above mentioned aspects can be influenced by the user. Algorithms are implemented as soft- or hardware, safety of a server system may be in your hands, that of the client typically is not as well as the infrastructure used for communication – if it is a non-private network. The key length seems to be the essential parameter of control.

Comparison of Algorithms

Additionally it has to be considered that different algorithms offer different security. To make algorithms comparable they are pro-jected onto an ideal block cipher and the resulting key length (named “Security bits”) of this cipher is used to compare algo-rithms. Since TLS uses asymmetric as well as symmetric ciphers, the minimal security bits of both algorithms is a good figure for the overall security of the hybrid algorithm.

Microchip [2] provides the following comparison for AES, RSA and ECC algorithms, citing the NSA as source.



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)

The BSI (Germany federal agency for IT safety) gives the following recommendations:

- Until end of 2022 100 security bits shall be sufficient,
- From 2023 on 120 security bits are recommended (BSI TR-02102-1 from 2020-03-24, page 14, see [1])

Using different certificates/keys on a single server

If you require to use different certificates/keys on the same physical server-host (hardware) and to access the services by a common port, TLS offers **SNI** as a mechanism comparable to virtual hosts in plain HTTP communication. The TLS handshake offers Server Name Indication (SNI, see [7] and [9]), which is supported by Datafox Devices. Using SNI the selection of the correct HTTPS server pro-cess (Software) is done already during the handshake.

Enabling SNI differs between web server implementations. A guide-line how to use SNI with a Microsoft IIS is available at [8]. Should you be using reverse proxies or load balancers, please ensure that they support SNI – detailing this here is way beyond the scope of this document. Please consult you network admins as well.

Using SNI you can e.g. associate different TLS certificates/keys to your ERP system and Datafox Devices using the same server infra-structure. Datafox Devices may use a 2048 bit or 3072 bit key whereas you may see to tighter security concerns of the ERP system by using a 4096 bit key – if you have the requirement concerning security.

Summary

We recommend to use an ECC-bases certificate with a 256 bit key together with Datafox devices. This is conform to the BSI recom-mendation for 2023. Compared to comparable RSA certificates you increase the performance of the devices and need less memory.

Information on creation and usage of RSA- or ECC-based certif-icates are available at [9].

Detailed considerations on symmetric and asymmetric cryp-tography will follow in the appendix.

With SNI you may use cryptography with different key sizes on a single host – if you should require stronger security for some services. SNI is a standardized method used by many cloud platforms.

Appendix

Standards in use

The cryptography standards TLS 1.1 and TLS 1.2 define a set of ciphers and signature algorithms. These algorithms are subject to cryptographic analysis, which results in aging of the algo-rithms – a method considered safe 10 years ago may not be safe anymore – due to algorithmic weaknesses or the increase of computational power available. Thus our devices do not support TLS 1.0 or even older standards SSLv2 and SSLv3 intentionally.

Asymmetric cryptography

Asymmetric cryptography is used during the TLS handshake when authenticating client and server. The key parts (public and private) are represented as X509.3 certificates. For en-cryption and decryption both key parts are needed. If one of the parts is unknown the computational requirement is signifi-cantly higher and the results of decryption will be ambiguous.

The private part of the key is the fragment to be safeguarded. All devices that have access to the private key can use it to prove their authenticity – a client cannot distinguish servers by cryptographic methods if the servers are using the same key.

To mitigate the problems that arise from loss of a key, the X509.3 certificate includes a validity period, enables hierarchic certificates and supports revocation lists. Please be aware that certificates at the top of a certificate hierarchy have a very long validity period, typically 10 years or more. The “real” server certificate offers a shorter validity period ranging from 90 days to 2 years typically. Obviously a certificate authority (CA) deserves a higher amount of trust than us using key concerning safeguarding keys – as far as the algorithm is concerned.

TLS authentication is design in a way, so that not all public certificates are needed when verifying authenticity. The CA’s certificate is sufficient. This makes short validity periods of a server’s certificate bearable at the client side since the CA certificates (see above) have a long validity period.

Comparable to checking the server authenticity by the client, the server may check the client authenticity during the TLS handshake. For this a so-called client-certificate may be used.

Once authentication is completed, the symmetric cipher algo-rithm and its key are negotiated. Details on the functionality of the Diffie-Hellmann-Algorithm are described in many places on the World Wide Web, the documents at [5] seem to be good entry point.

Symmetric cryptography

Typically the AES algorithm is used as symmetric cipher. This algorithm is specified for key lengths of 128, 192 or 256 bits – which seems rather short when comparing it to typical RSA key lengths. Hence the AES algorithm is well studied which led to some non-dramatic weaknesses of the algorithm.

Estimates on necessary computational power for cracking a 128 bit AES key are
- 30 years using an ideal quantum computer (~10 Seconds if the key has only 100 bits)
- 2.15 * 1012 years on hardware currently available (~6000 years for a 100 bit key)

Our sun has an estimated lifetime of 5 * 109 years.

The symmetric encryption is negotiated with every handshake. An HTTPS connection is disconnected by the infrastructure typically after being idle for 30 seconds. So, cracking the sym-metric channel encryption requires computation resources after each re-negotiation of the communication.

Attack scenarios
Currently no feasible attack on an established AES encrypted channel using current hardware is known, so attacking TLS focuses on the handshake as well as the algorithms in use. Some of these attacks made it to be internally renown by now:

- Heartbleed (OpenSSL < 1.0.1g: A client could retrieve data from the server – potentially the server’s key.)
- FREAK (faulty implementation of US export regulation could lead to accepting very short keys for asym metric cryptography)
- BEAST (TLS < 1.1: Implementation issues of symmetric encryption)

Exploits that may be used over the network are of particular interest – the system attacked is not aware of that attack typically.

Attacking the Handshake
During attacks on the handshake, either negotiating the algo-rithm or the key to be used may be influenced (resulting in either weaker symmetric cipher or a key with some “known” bits).

Attacking the Handshake
During attacks on the handshake, either negotiating the algo-rithm or the key to be used may be influenced (resulting in either weaker symmetric cipher or a key with some “known” bits).

Compromised client or server
If an attacker has access to client or server, it may be possible that the key is retrieved or changed.

Random number generator attack
Many encryption and signature algorithms use “entropy” to harden the algorithm against attacks. Entropy typically is part of a negotiated key as well. Having a system that does not produce “good” random numbers and knowing their distribu-tion is helpful when determining the encryption key.

Timing attacks
In many algorithms there is a time difference between checking an incorrect key and checking a correct key. These deviations may be observed externally and harvested to deduce the proximity of the test key and the real key.

Attacking the encrypted channel
Attacking an established channel encryption is difficult if the attacker may not influence either side of the communication. The key space of algorithms used currently is too big to deter-mine the key by guessing (“brute force”). In addition to the guess work it is necessary to know the content of a transac-tion in order to determine the right key.

Padding oracle attacks
Many symmetric ciphers are encoding a fixed length of data (“block”). Consequently, a message which has a length not dividable by the block length will be padded. Some algorithmic implementations have weak padding algorithms that may be used to have an own message encoded.

Exploiting weaknesses of an algorithm
If an algorithm has weaknesses, these may be exploited when decrypting a message. The AES-128 bit algorithm has weak-nesses that reduce the key space roughly to the billionth part of the original key space – which is a vast reduction for a brute force attack.

If the algorithm has no additional weaknesses, that allow guessing additional parts of the key, it may still be put to use. In the case of AES-128 there are still roughly 1030 keys left.

Guessing the key by brute force
Brute force attacks are typically not usable on today’s algo-rithms.

However, [6] details the steps in chronological order that lead to the DES algorithm with a key length of 56 bit being consid-ered unsecure. A substantial part in this is attributed to in-creased computational power since 1975 which resulted in brute force attacks being feasible when using distributed com-puting.
It is likely that quantum computing – when being available – will lead to a comparable situation with current cipher algo-rithms.

Key length considerations in PKI
In addition to above mentioned security aspects, that should be considered when exchanging data, the key length remains the main factor of security.

Today typically RSA and ECC based algorithms are used.

RSA
The BSI recommends using a key with at least 2000 bits. A key of this length is expected to provide reasonable security until end of 2022 (see [1]: BSI TR-02102-1, March 24th 2020)

RSA and the symmetric cipher being used are compared con-cerning the security bits of an equivalent ideal block cipher. The BSI recommends a key length equivalent to 100 security bits (roughly 1900 bit RSA) to be used currently, from 2023 the key length should be at least 120 bits (roughly 2800 bit RSA).

Microchip [2] uses the same scale for its recommendations and reaches the same conclusions as the BSI. The Microchip table shows that a key length increase does not result in a proportional increase in security bits. To reach the security level of an AES 256 algorithm, a hypothetical RSA key of equivalent strength should have 15360 bits.

The time estimates for factorizing (“cracking”) a 2048 bit RSA key deviate when checking web, please check [3] and [4].

The estimates seem to emphasize, that a 2048 bit certificate still has enough security reserves to be safe against attacks with reasonable effort. BSI sees RSA as a technology on the way to obsolescence and suggests migration towards ECC base algo-rithms.

ECC
Algorithms based on ECC reach a security level comparable to RSA with shorter keys (see [2]). We have additionally measured memory consumption while comparing RSA-2048, RSA-3072 and ECC-256 ciphers during the TLS handshake and we have seen that ECC-256 consumes
- 6 % less memory than RSA-2048 and
- 22% less memory than RSA-3072.

We came to the conclusion that ECC based cipher’s resource efficiency is worth using the ciphers, despite RSA is widely considered industry standard. Thus we recommend using 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