PAULETTE
FELLER

IT-Consulting & Audits

Privacy, ISO 27001
ISMS, ITIL

Audit Report Mobile Easykey Manager

For

Domnick+Müller GmbH + Co. KG, Max-Planck-Strasse 11,
61381 Friedrichsdorf

Author: Paulette Feller

Date: 12.03.2020

Version: 1.1

Index

1 SUMMARY

This document describes the results of a review of the "Mobile Easykey Manager" (MEKM) in relation to Data protection through technology design and privacy-friendly defaults.

Data protection through technology design is implemented through a variety of configuration options, and Mobile Easykey Manager implements a number of privacy-friendly presets.

2 INTRODUCTION

This chapter describes the objective of the audit and the methodology.

2.1 GOAL

The purpose of the audit was to determine whether Mobile Easykey Manager provides Data protection through technical design and by data protection-friendly presets (Art. 25 GDPR).

2.2 METHODOLOGY

The following methodology has been used:

Sighting of the manual for Mobile Easykey Database V.1, Mobile Easykey Service 2019.1, Mobile Easykey Manager 2019.1, Mobile Easykey Communicator

Inspection of the Mobile Easykey Manager (MEKM) software

Interview of the developers regarding the technical realisation

3 DATA PROTECTION BY TECHNOLOGY DESIGN AND BY DATA PRIVACY-FRIENDLY PRESETS

The following chapters list all measures to ensure data protection through technology design and privacy-friendly presets.

3.1 MAINTENANCE ACCESS TO PSEUDONYMOUS DATA

Mobile Easykey Manager includes a so-called Service Mode.

3.1.1 Secure login for maintenance accesses via one-time tokens

If a user logs on as a Mobile Easykey Service Administrator (Support staff of Domnick+Müller) with a username and password, the MEK server at Domnick+Müller will receive information about that. A one-time token is now send to the e-mail address stored on the MEK server. This must also be specified by the Mobile Easykey Service Administrator. Only then will registration take place at the MEKM.

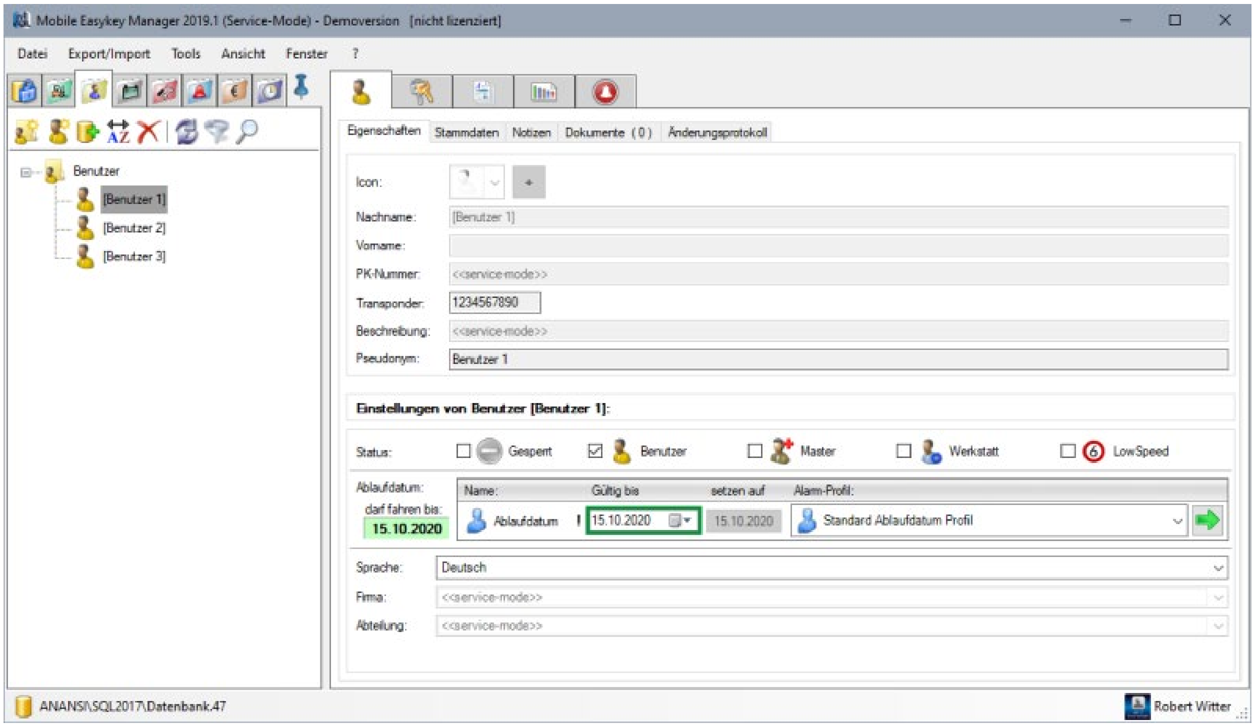
3.1.2 Pseudonymisation of the user interface

Service Mode is automatically activated when a user logs on as a Mobile Easykey Service Administrator or when a remote maintenance session is activated via the Remote Maintenance Feature. As long as the Service Mode is active, the personal data will be displayed exclusively pseudonymously throughout the program and will also be read-only. Only the transponder ID is displayed in plain text so that the customer can establish an assignment if this should be necessary.

The transponder IDs are managed exclusively by the customer, a Mobile Easykey Service Administrator cannot identify any person.

The key used for pseudonymisation is not accessible to a user in the Mobile Easykey Service Administrator role.

The figure below shows the view of a Mobile Easykey Service Administrator during the support access. The last names are pseudonymised, and other information is hidden. Only the transponder ID is displayed in plain text, otherwise support would not be possible.



Icon:

Nachname: [Benutzer 1]

Vorname:

PK-Nummer: <<service-mode>>

Transponder: 1234567890

Beschreibung: <<service-mode>>

Pseudonym: Benutzer 1

Einstellungen von Benutzer [Benutzer 1]:

Status: □ Gesperrt ☑ Benutzer □ Master □ Werkstatt □ LowSpeed

Ablaufdatum:
darf fahren bis:
15.10.2020

Name:	Gültig bis	setzen auf	Alarm-Profil:
Ablaufdatum !	15.10.2020	15.10.2020	Standard Ablaufdatum Profil

Sprache: Deutsch

Firma: <<service-mode>>

Abteilung: <<service-mode>>

Note 1

This is where the active help of the customer is required. The customer must ensure that a Support Employee of Domnick+Müller does not get an insight into the Mobile Easykey Manager, as long as an employee of the customer is logged in there. This applies to both, on-site and remote maintenance.

Note 2

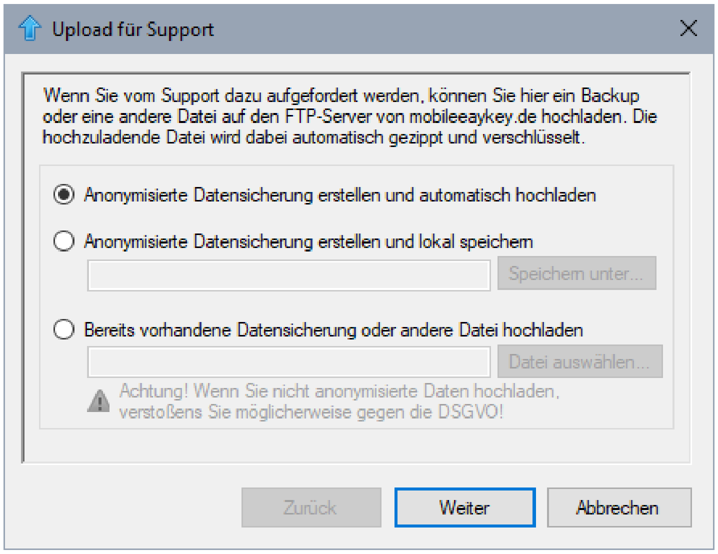
Domnick+Müller's support staff are instructed to access the Mobile Easykey Manager only in the Mobile Easykey Service Administrator role.

3.2 Analysis of the Mobile Easykey Database

There are support cases that require direct access to the Mobile Easykey database. There are basically two ways to do this:

3.2.1 Anonymised backup for support purposes

If the analysis of the database is required for support requests, the customer can create an anonymised backup and make this available to Domnick+Müller via FTP upload (see figure below).



Upload für Support

Wenn Sie vom Support dazu aufgefordert werden, können Sie hier ein Backup oder eine andere Datei auf den FTP-Server von mobileeaykey.de hochladen. Die hochzuladende Datei wird dabei automatisch gezippt und verschlüsselt.

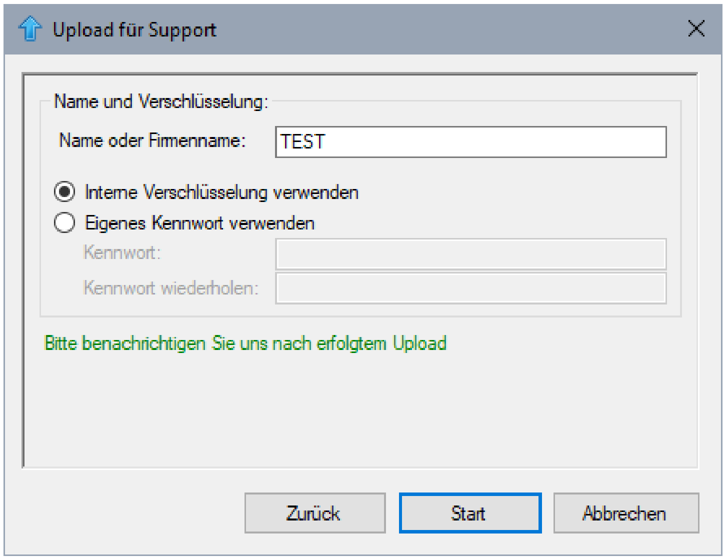
● Anonymisierte Datensicherung erstellen und automatisch hochladen

○ Anonymisierte Datensicherung erstellen und lokal speichern

○ Bereits vorhandene Datensicherung oder andere Datei hochladen

Achtung! Wenn Sie nicht anonymisierte Daten hochladen, verstoßens Sie möglicherweise gegen die DSGVO!

Either the existing internal encryption of the data or a new password is used (see figure below).



Upload für Support

Name und Verschlüsselung:

Name oder Firmenname: TEST

● Interne Verschlüsselung verwenden

○ Eigenes Kennwort verwenden

Kennwort:

Kennwort wiederholen:

Bitte benachrichtigen Sie uns nach erfolgtem Upload

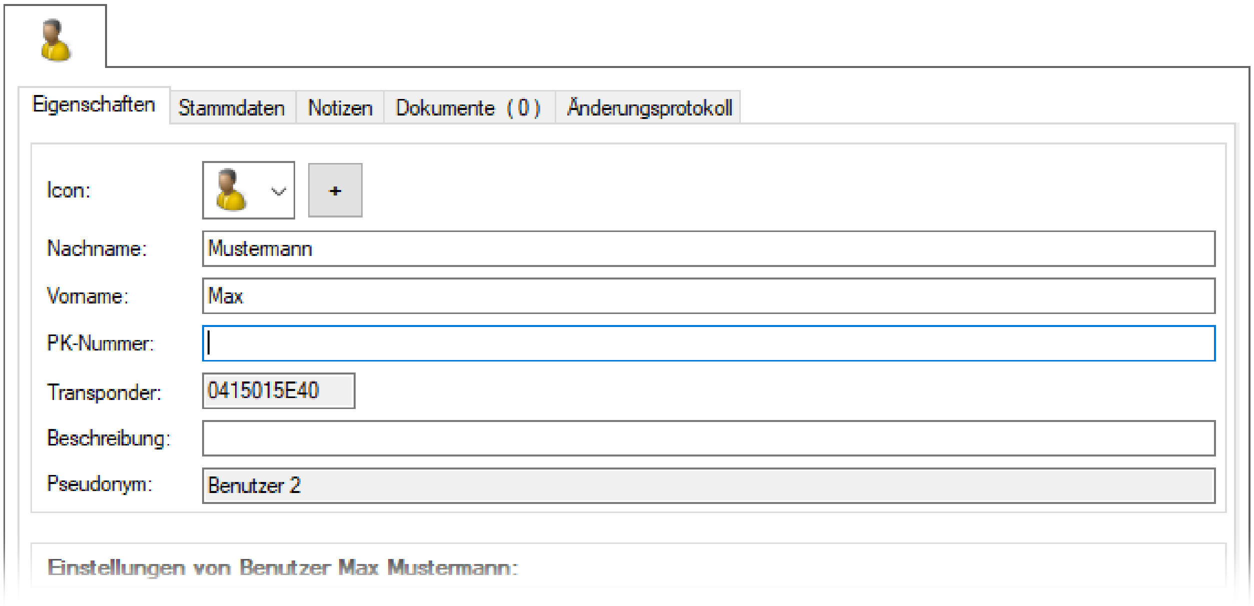
Such an anonymised backup is a backup that contains all the data, but does not hold the key to encrypt the personal data. The anonymised backup is for support purposes only. Such a backup can be completely restored, but all personal data is permanently encrypted (AES 256) and can only be displayed pseudonymously. Decryption is not possible without access to the original database.

3.2.2 Access to the database files

If the customer is unable to create an anonymised backup of the database due to software problems, the original database files must be used for support purposes. These are automatically encrypted at the time of creation, so that even with direct database access, personal data are pseudonymised. The decryption key (de-pseudonymisation) is stored in several parts (see chapter 3.12 Encryption of the database) and is therefore not available for support. Therefore, a support representative can never read the personal data in plain text.

3.3 Data Economy

For the function of the program, only the name, the transponder ID and or if necessary one or more expiration dates (how long the transponder ID is still valid) must be entered. All other information is voluntary.



Icon:

Nachname: Mustermann

Vorname: Max

PK-Nummer:

Transponder: 0415015E40

Beschreibung:

Pseudonym: Benutzer 2

Einstellungen von Benutzer Max Mustermann:

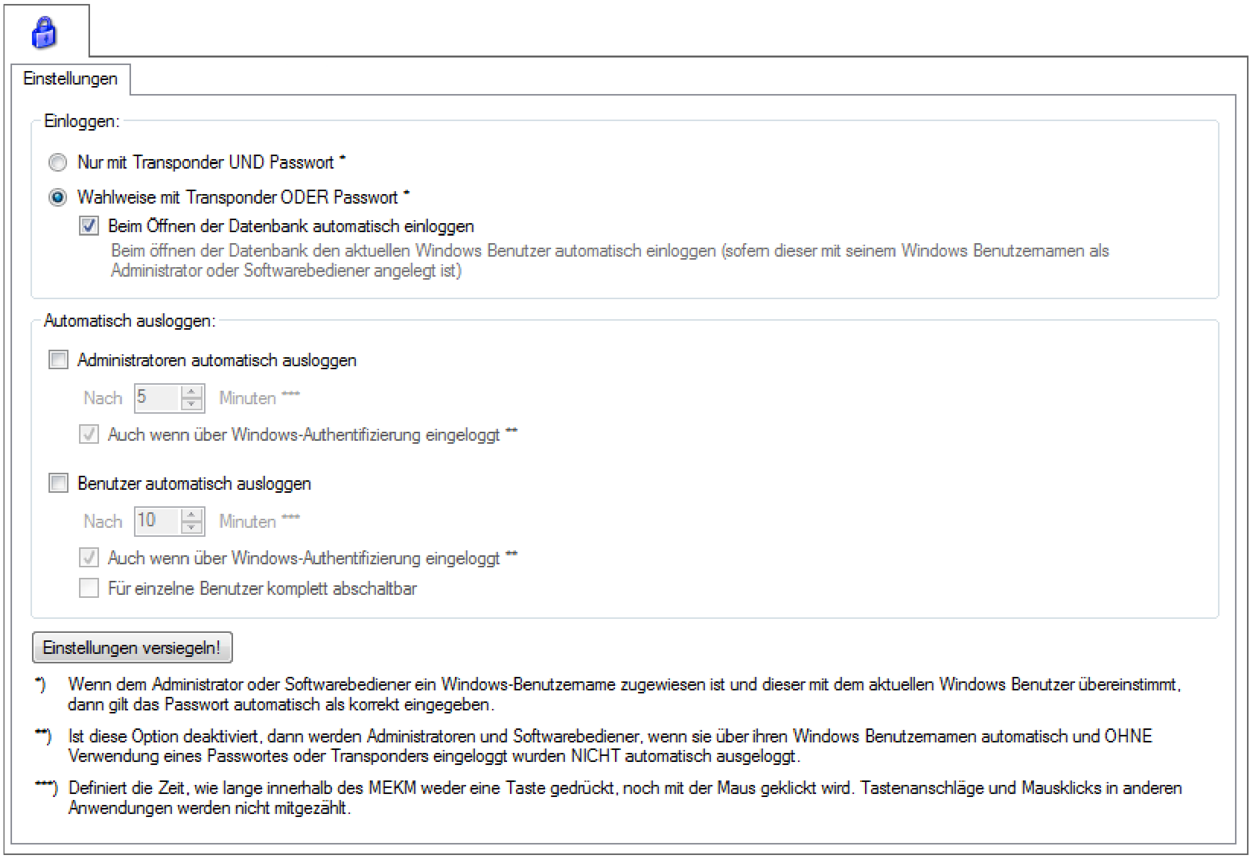
3.4 Strong Authentiction

In the MEKM, it can be determined that users and administrators can or must log in to the Mobile Easykey Manager (login).

□ either only with transponder AND password or
□ optionally with transponder OR password

Only with transponder AND password: With this option, both a transponder and a password must be assigned to the user. If this is not the case, the corresponding user cannot log on.

Optional with transponder OR password: With this option, a user can log in with his transponder or his password.



Einstellungen

Einloggen:

○ Nur mit Transponder UND Passwort *

● Wahlweise mit Transponder ODER Passwort *

☑ Beim Öffnen der Datenbank automatisch einloggen

Beim öffnen der Datenbank den aktuellen Windows Benutzer automatisch einloggen (sofern dieser mit seinem Windows Benutzernamen als Administrator oder Softwarebediener angelegt ist)

Automatisch ausloggen:

☐ Administratoren automatisch ausloggen

Nach 5 Minuten ***

☑ Auch wenn über Windows-Authentifizierung eingeloggt **

☐ Benutzer automatisch ausloggen

Nach 10 Minuten ***

☑ Auch wenn über Windows-Authentifizierung eingeloggt **

☐ Für einzelne Benutzer komplett abschaltbar

Einstellungen versiegeln!

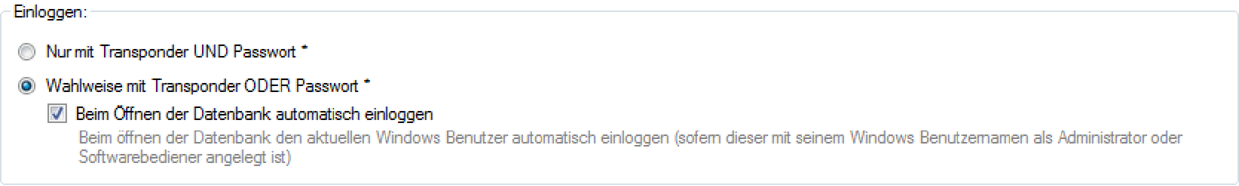
*) Wenn dem Administrator oder Softwarebediener ein Windows-Benutzername zugewiesen ist und dieser mit dem aktuellen Windows Benutzer übereinstimmt, dann gilt das Passwort automatisch als korrekt eingegeben.

**) Ist diese Option deaktiviert, dann werden Administratoren und Softwarebediener, wenn sie über ihren Windows Benutzernamen automatisch und OHNE Verwendung eines Passwortes oder Transponders eingeloggt wurden NICHT automatisch ausgeloggt.

***) Definiert die Zeit, wie lange innerhalb des MEKM weder eine Taste gedrückt, noch mit der Maus geklickt wird. Tastenanschläge und Mausklicks in anderen Anwendungen werden nicht mitgezählt.

3.5 SINGLE SIGN-ON

MEKM offers the option of automatically authenticating a software operator or administrator if the current Windows user name matches the user name stored in MEKM (see figure below).



Einloggen:

○ Nur mit Transponder UND Passwort *

● Wahlweise mit Transponder ODER Passwort *

☑ Beim Öffnen der Datenbank automatisch einloggen

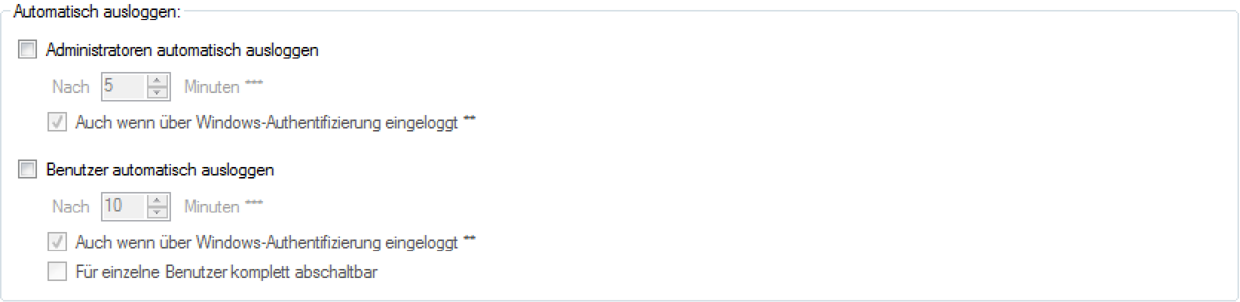
Beim öffnen der Datenbank den aktuellen Windows Benutzer automatisch einloggen (sofern dieser mit seinem Windows Benutzernamen als Administrator oder Softwarebediener angelegt ist)

- In the background, the user is logged on to the SQL database separately. There are two ways to authenticate:
- If the SQL server is a member of the Active Directory, the user logs in via Kerberos. The Users' Kerberos ticket is validated.
- If the server is a Stand Alone SQL Server, the user logs on via NTLM (NT LAN Manager Protocol). The password hash of the user logged on to the Windows client is checked.

In both cases, it is ensured that only legitimate users gain access to the SQL database containing the Mobile Easykey Manager data.

3.6 AUTOMATIC LOG-OFFS

In the MEKM, it can be specified that both administrators and other users are forcibly logged off by the system after a defined time (see figure below).



Automatisch ausloggen:

☐ Administratoren automatisch ausloggen

Nach 5 Minuten ***

☑ Auch wenn über Windows-Authentifizierung eingeloggt **

☐ Benutzer automatisch ausloggen

Nach 10 Minuten ***

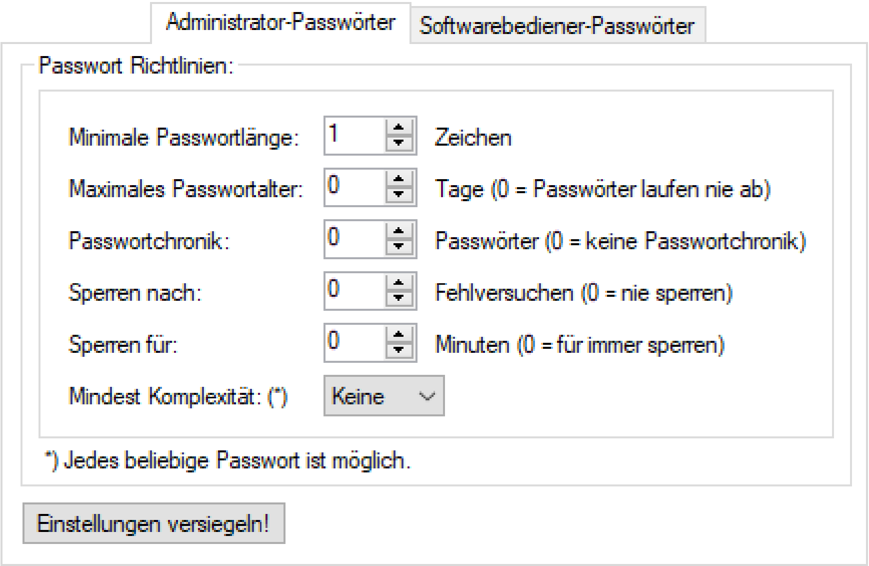
☑ Auch wenn über Windows-Authentifizierung eingeloggt **

☐ Für einzelne Benutzer komplett abschaltbar

3.7 COMPLEX PASSWORD POLICIES

The Mobile Easykey Manager offers the ability to set complex password policies.

Up to 40 characters can be entered as the forced minimum password length. All other settings can take values from 0 to 9999. Details can be found in the following figure.



Passwort Richtlinien:

Minimale Passwortlänge: 1 Zeichen

Maximales Passwortalter: 0 Tage (0 = Passwörter laufen nie ab)

Passwortchronik: 0 Passwörter (0 = keine Passwortchronik)

Sperren nach: 0 Fehlversuchen (0 = nie sperren)

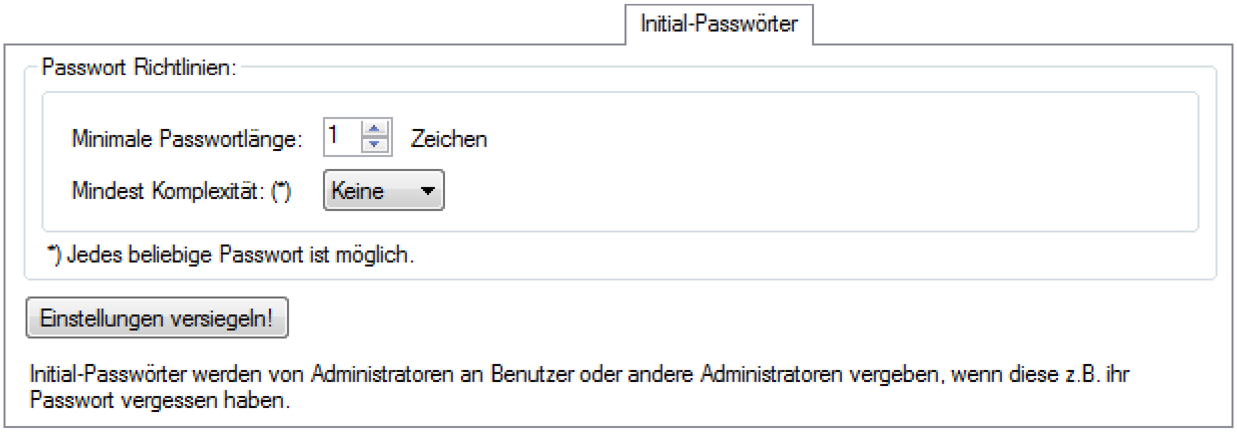
Sperren für: 0 Minuten (0 = für immer sperren)

Mindest Komplexität: (*) Keine

*) Jedes beliebige Passwort ist möglich.

3.8 INITIAL PASSWORDS

Initial passwords are set up for the concerned users, both before you log on for the first time and after a password is reset. After logging on with the initial password, the user must set up a new password.



Initial-Passwörter

Passwort Richtlinien:

Minimale Passwortlänge: 1 Zeichen

Mindest Komplexität: (*) Keine

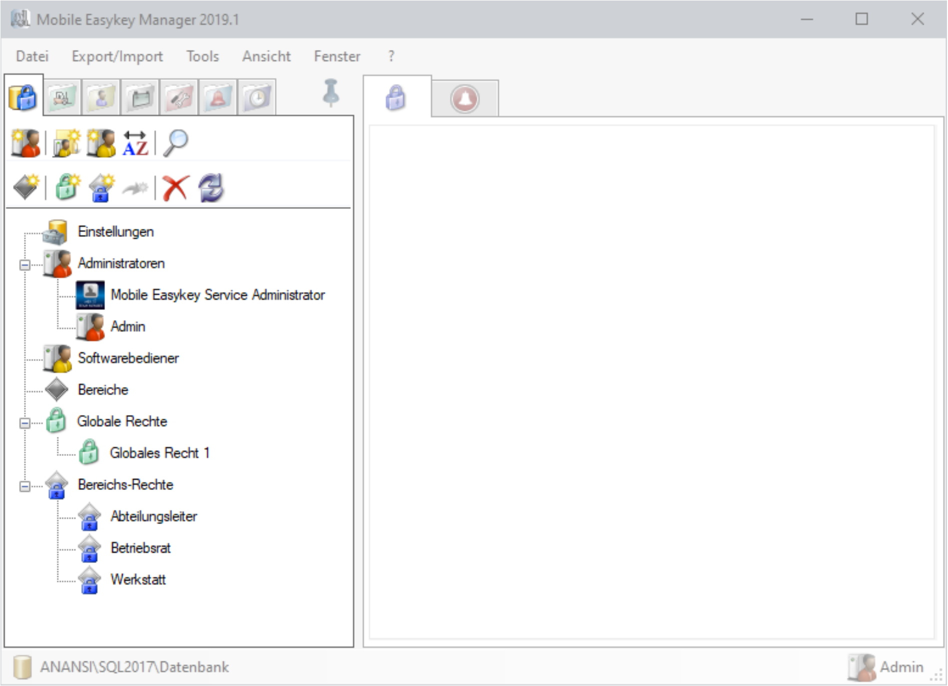
*) Jedes beliebige Passwort ist möglich.

Einstellungen versiegeln!

Initial-Passwörter werden von Administratoren an Benutzer oder andere Administratoren vergeben, wenn diese z.B. ihr Passwort vergessen haben.

3.9 Role and Rights concept (Operating rights)

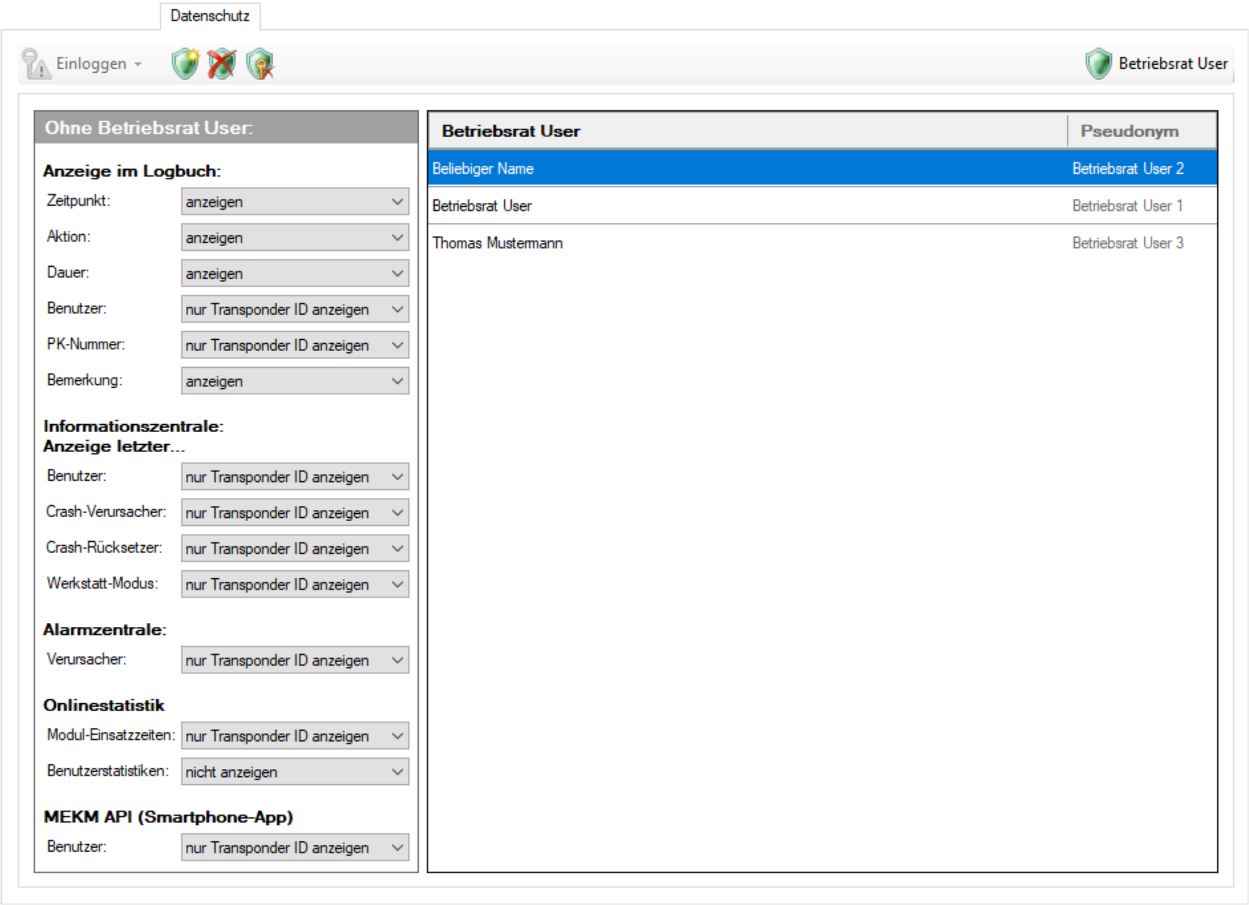
In the MEKM, you can set up your own roles and their operating rights. By default, some roles are preconfigured (see figure below).



3.10 Works Council-User

If the "Works Council User" role is used, personal data for the other user accounts is no longer displayed in plain text in the logbook and in the information center. Instead, only the UID of the transponder of the respective user or the text of the "<<Privacy>>". In order to be able to view the personal data, a User must log in in the "Works Council User" role.

Which personal data is displayed to users without a works council user role can be specified with the help of the operating rights (see figure below).



Ohne Betriebsrat User:

Anzeige im Logbuch:

Zeitpunkt: anzeigen
Aktion: anzeigen
Dauer: anzeigen
Benutzer: nur Transponder ID anzeigen
PK-Nummer: nur Transponder ID anzeigen
Bemerkung: anzeigen

Informationszentrale:
Anzeige letzter...

Benutzer: nur Transponder ID anzeigen
Crash-Verursacher: nur Transponder ID anzeigen
Crash-Rücksetzer: nur Transponder ID anzeigen
Werkstatt-Modus: nur Transponder ID anzeigen

Alarmzentrale:

Verursacher: nur Transponder ID anzeigen

Onlinestatistik

Modul-Einsatzzeiten: nur Transponder ID anzeigen
Benutzerstatistiken: nicht anzeigen

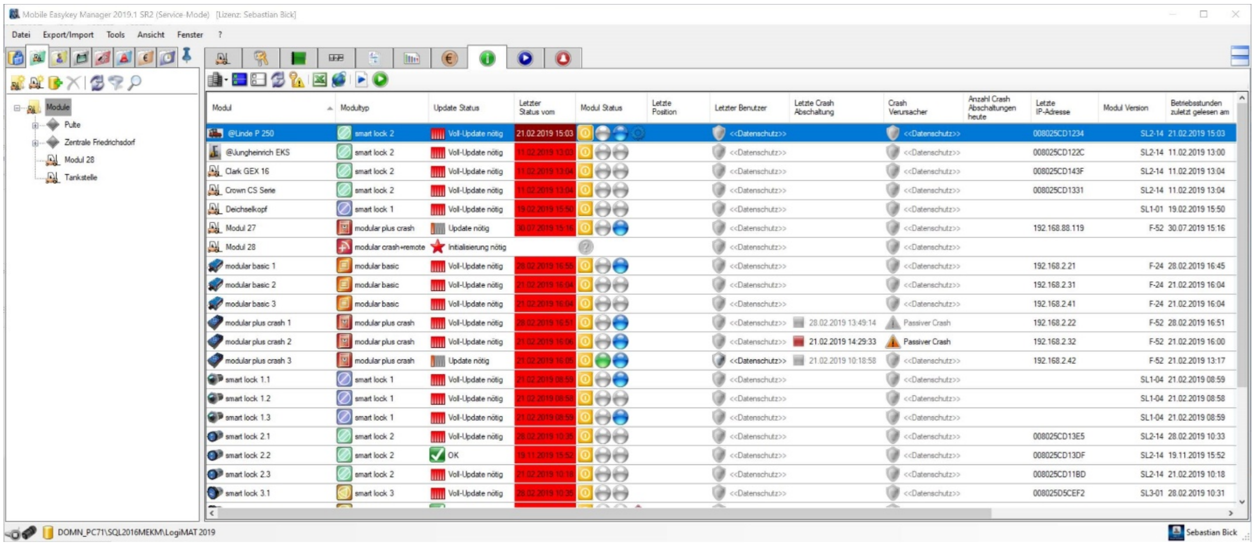
MEKM API (Smartphone-App)

Benutzer: nur Transponder ID anzeigen

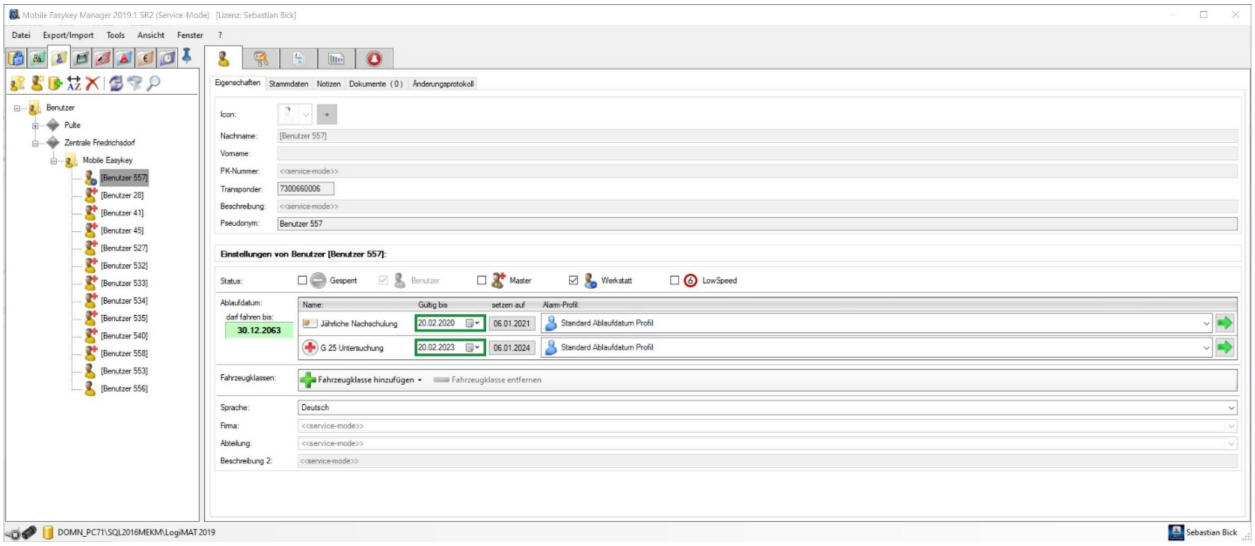
Betriebsrat User	Pseudonym
Beliebiger Name	Betriebsrat User 2
Betriebsrat User	Betriebsrat User 1
Thomas Mustermann	Betriebsrat User 3

In the left column, the components that are displayed without the "Works Council User" role are selected. All components except the UID of the transponder can be deselected.

The following illustrations show that the personal data are hidden from operators who do not have Administrator or Works Council User rights.


Mobile Easykey Manager 2019.1 SR2 (Service-Mode) [Lizenz: Sebastian Bick]
Datei
Export/Import
Tools
Ansicht
Fenster
?
Module
Pulte
Zentrale Friedrichsdorf
Modul 28
Tankstelle
DOMN_PC71\SQL2016MEKM\LogiMAT 2019
Sebastian Bick

Modul	Modultyp	Update Status	Letzter Status vom	Modul Status	Letzte Position	Letzter Benutzer	Letzte Crash Abschaltung	Crash Verursacher	Anzahl Crash Abschaltungen heute	Letzte IP-Adresse	Modul Version	Betriebsstunden zuletzt gelesen am
@Linde P 250	smart lock 2	Voll-Update nötig	21.02.2019 15:03			<<Datenschutz>>		<<Datenschutz>>		008025CD1234	SL2-14	21.02.2019 15:03
@Jungheinrich EKS	smart lock 2	Voll-Update nötig	11.02.2019 13:03			<<Datenschutz>>		<<Datenschutz>>		008025CD122C	SL2-14	11.02.2019 13:00
Clark GEX 16	smart lock 2	Voll-Update nötig	11.02.2019 13:04			<<Datenschutz>>		<<Datenschutz>>		008025CD143F	SL2-14	11.02.2019 13:04
Crown CS Serie	smart lock 2	Voll-Update nötig	11.02.2019 13:04			<<Datenschutz>>		<<Datenschutz>>		008025CD1331	SL2-14	11.02.2019 13:04
Deichselkopf	smart lock 1	Voll-Update nötig	19.02.2019 15:50			<<Datenschutz>>		<<Datenschutz>>			SL1-01	19.02.2019 15:50
Modul 27	modular plus crash	Update nötig	30.07.2019 15:16			<<Datenschutz>>		<<Datenschutz>>		192.168.88.119	F-52	30.07.2019 15:16
Modul 28	modular crash+remote	Initialisierung nötig				<<Datenschutz>>		<<Datenschutz>>				
modular basic 1	modular basic	Voll-Update nötig	28.02.2019 16:55			<<Datenschutz>>		<<Datenschutz>>		192.168.2.21	F-24	28.02.2019 16:45
modular basic 2	modular basic	Voll-Update nötig	21.02.2019 16:04			<<Datenschutz>>		<<Datenschutz>>		192.168.2.31	F-24	21.02.2019 16:04
modular basic 3	modular basic	Voll-Update nötig	21.02.2019 16:04			<<Datenschutz>>		<<Datenschutz>>		192.168.2.41	F-24	21.02.2019 16:04
modular plus crash 1	modular plus crash	Voll-Update nötig	28.02.2019 16:51			<<Datenschutz>>	28.02.2019 13:49:14	Passiver Crash		192.168.2.22	F-52	28.02.2019 16:51
modular plus crash 2	modular plus crash	Voll-Update nötig	21.02.2019 16:06			<<Datenschutz>>	21.02.2019 14:29:33	Passiver Crash		192.168.2.32	F-52	21.02.2019 16:00
modular plus crash 3	modular plus crash	Update nötig	21.02.2019 16:05			<<Datenschutz>>	21.02.2019 10:18:58	<<Datenschutz>>		192.168.2.42	F-52	21.02.2019 13:17
smart lock 1.1	smart lock 1	Voll-Update nötig	21.02.2019 08:59			<<Datenschutz>>		<<Datenschutz>>			SL1-04	21.02.2019 08:59
smart lock 1.2	smart lock 1	Voll-Update nötig	21.02.2019 08:58			<<Datenschutz>>		<<Datenschutz>>			SL1-04	21.02.2019 08:58
smart lock 1.3	smart lock 1	Voll-Update nötig	21.02.2019 08:59			<<Datenschutz>>		<<Datenschutz>>			SL1-04	21.02.2019 08:59
smart lock 2.1	smart lock 2	Voll-Update nötig	28.02.2019 10:35			<<Datenschutz>>		<<Datenschutz>>		008025CD13E5	SL2-14	28.02.2019 10:33
smart lock 2.2	smart lock 2	OK	19.11.2019 15:52			<<Datenschutz>>		<<Datenschutz>>		008025CD13DF	SL2-14	19.11.2019 15:52
smart lock 2.3	smart lock 2	Voll-Update nötig	21.02.2019 10:18			<<Datenschutz>>		<<Datenschutz>>		008025CD11BD	SL2-14	21.02.2019 10:18
smart lock 3.1	smart lock 3	Voll-Update nötig	28.02.2019 10:35			<<Datenschutz>>		<<Datenschutz>>		008025D5CEF2	SL3-01	28.02.2019 10:31



Icon:

Nachname: [Benutzer 557]

Vorname:

PK-Nummer: <<service-mode>>

Transponder: 7300660006

Beschreibung: <<service-mode>>

Pseudonym: Benutzer 557

Einstellungen von Benutzer [Benutzer 557]:

Status: □ Gesperrt ☑ Benutzer □ Master ☑ Werkstatt □ LowSpeed

Ablaufdatum:
darf fahren bis: 30.12.2063

Name:	Gültig bis	setzen auf	Alarm-Profil:
Jährliche Nachschulung	20.02.2020	06.01.2021	Standard Ablaufdatum Profil
G 25 Untersuchung	20.02.2023	06.01.2024	Standard Ablaufdatum Profil

Fahrzeugklassen:

Sprache: Deutsch

Firma: <<service-mode>>

Abteilung: <<service-mode>>

Beschreibung 2: <<service-mode>>

3.11 Encryption of the database

All personal data is encrypted in the database with AES 256. The key to recovering personal data is stored in three parts:

- A part is stored centrally in the database. This part is not copied during the anonymised backup.
- The second part is firmly anchored within the software installation.
- The third part is saved together with the respective user/software operator etc.. This part, in turn, is stored in two versions. Once (Part A) only for the respective name and once (Part B) for all other personal data. Part B is removed upon safe deletion.

Only if all three keys are accessible can the personal data be decrypted and displayed in plain text.

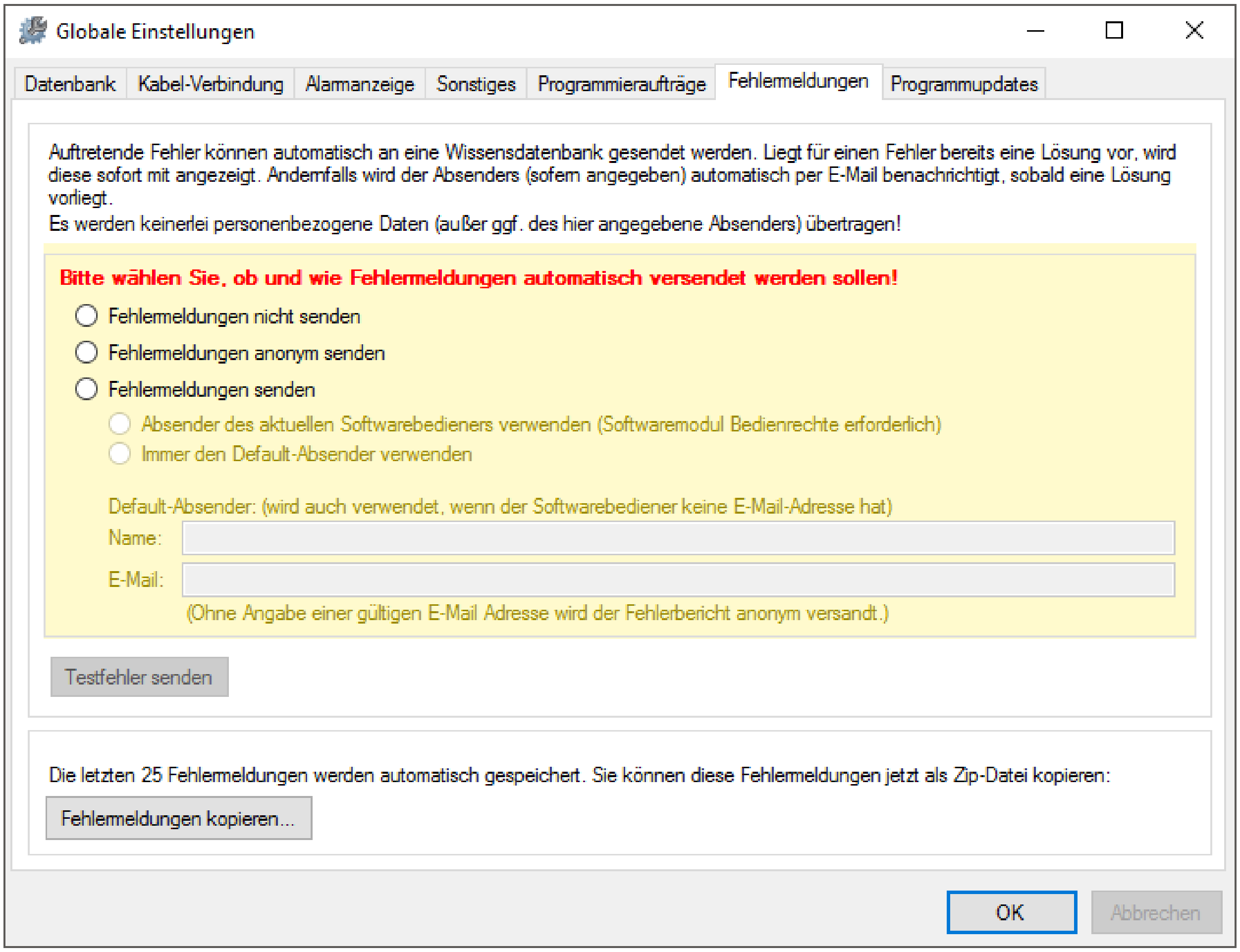
3.12 TRANSFER ERROR REPORTS

Any errors in the MEKM can be automatically send to a knowledge base over the Internet. If the error is already known and there is a solution to it, it is automatically retrieved from the knowledge base and displayed.

If a name and an e-mail address are stored, these contact details are stored together with the error message and the contact person is contacted if further information on the

solution of the problem is required. However, error messages can also be send anonymously only.

The setting for sending the error messages can be changed at any time (see figure below). You can specify that no error messages are transmitted.



Auftretende Fehler können automatisch an eine Wissensdatenbank gesendet werden. Liegt für einen Fehler bereits eine Lösung vor, wird diese sofort mit angezeigt. Andernfalls wird der Absenders (sofern angegeben) automatisch per E-Mail benachrichtigt, sobald eine Lösung vorliegt.

Es werden keinerlei personenbezogene Daten (außer ggf. des hier angegebene Absenders) übertragen!

Bitte wählen Sie, ob und wie Fehlermeldungen automatisch versendet werden sollen!

○ Fehlermeldungen nicht senden

○ Fehlermeldungen anonym senden

○ Fehlermeldungen senden

○ Absender des aktuellen Softwarebedieners verwenden (Softwaremodul Bedienrechte erforderlich)

○ Immer den Default-Absender verwenden

Default-Absender: (wird auch verwendet, wenn der Softwarebediener keine E-Mail-Adresse hat)

Name:

E-Mail:

(Ohne Angabe einer gültigen E-Mail Adresse wird der Fehlerbericht anonym versandt.)

Die letzten 25 Fehlermeldungen werden automatisch gespeichert. Sie können diese Fehlermeldungen jetzt als Zip-Datei kopieren:

3.13 AUTOMATIC DELETION OF OLD LOG ENTRIES

In the various logs within the MEKM, old log entries can be deleted automatically. When the automatic deletion function is activated, the respective log is regularly reduced accordingly.

The individual protocols have the following functions:

Change log: This is recorded when, and by whom (only with activated Operating Rights) which setting has been changed.

Error log: This is where errors that occur in the background are recorded.

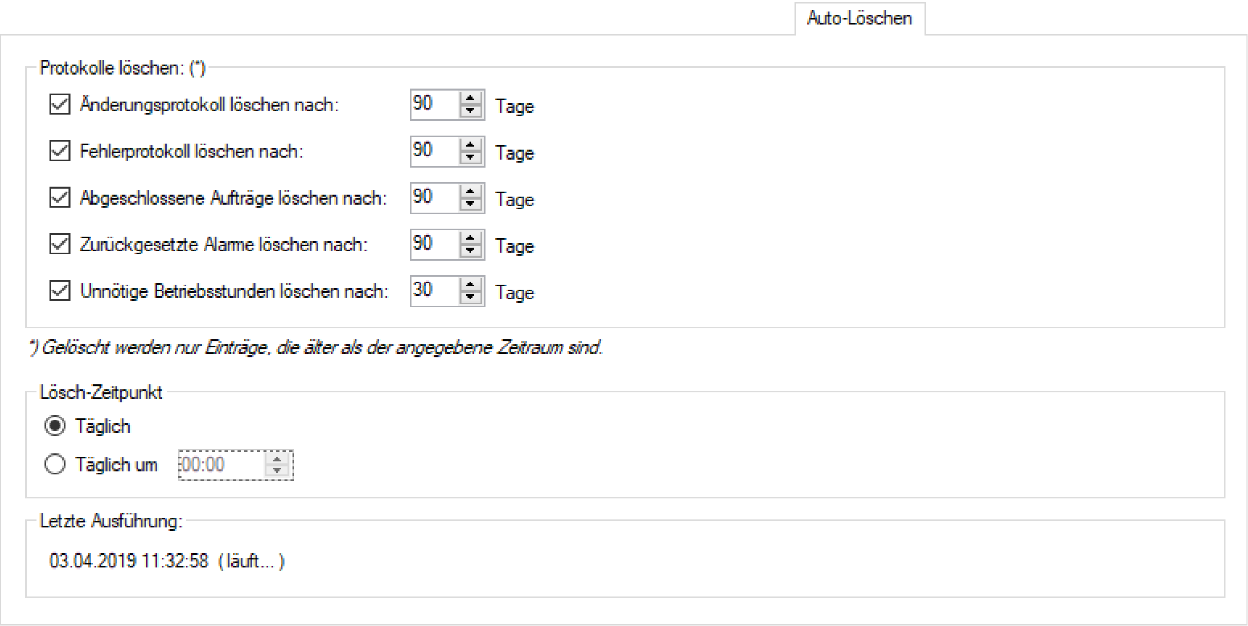
Completed orders: When orders (such as read out logbook) has been completed, the information about it will still be kept for the specified time.

Reset alarms: Alarms are also retained (after the cause of the alarm has been switched off) for the specified time.

Unnecessary operating hours: The modules (from version F) record the operating hours very frequently (every quarter of an hour). However, these quarterly entries are usually no longer important after a few days. Therefore, these can be automatically deleted after the time set here. The operating hours are not deleted at 0:00 a.m. and before or after a new current was applied. Thus, there is still enough data to display the operating hours exactly every day.

In addition, it is possible to specify when this data should be deleted. By default, it is deleted every hour. At each program start and then every hour, it is checked whether there is data to be deleted. This (obsolete) data is then automatically deleted.

In the "daily at" setting, outdated data is deleted only once a day at the specified time.



Protokolle löschen: (*)

☑ Änderungsprotokoll löschen nach: 90 Tage

☑ Fehlerprotokoll löschen nach: 90 Tage

☑ Abgeschlossene Aufträge löschen nach: 90 Tage

☑ Zurückgesetzte Alarme löschen nach: 90 Tage

☑ Unnötige Betriebsstunden löschen nach: 30 Tage

*) Gelöscht werden nur Einträge, die älter als der angegebene Zeitraum sind.

Lösch-Zeitpunkt

● Täglich

○ Täglich um 00:00

Letzte Ausführung:

03.04.2019 11:32:58 (läuft...)

3.14 Secure removal of outdated entries

For database consistency reasons, users (vehicle drivers), software operators, etc. cannot be deleted from the database. Instead, they are marked as deleted and are therefore no longer visible in the Mobile Easykey Manager, but remain in the database.

When deleting a user, software operator, etc., all personal data (except for the name itself) of this user, software operator, etc. are immediately made unrecognisable. This also applies retroactively to the change protocol.

In the database configuration, a time (2 years are default) can be set after which the name of this user is also permanently unrecognisable. If this user still appears in one of the protocols (e.g. the logbook), it will only be displayed there as "<<deleted>>".

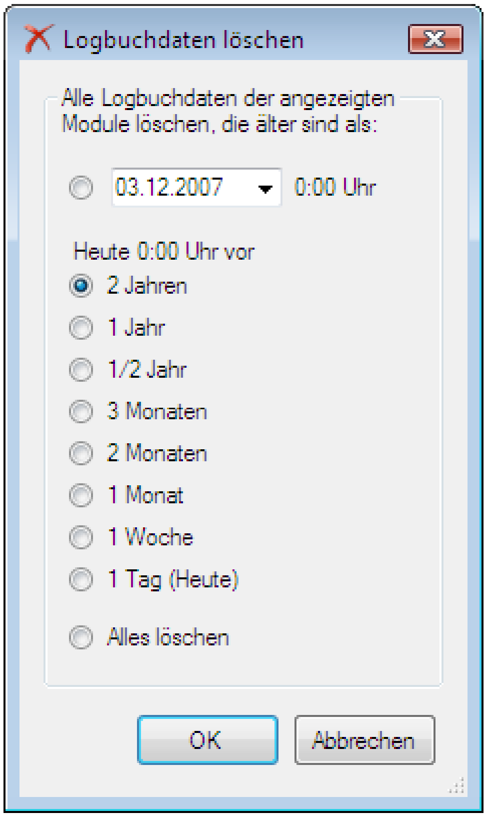
3.15 Delete logbook entries

Because the database size depends mainly on the number of logbook entries, it may be necessary to delete older logbook entries.

For example, if 1 year is selected as the period, all logbook entries older than one year are deleted.

You can also specify any date to delete all logbook entries that are earlier than that date.

You can also delete all existing logbook entries.



Logbuchdaten löschen

Alle Logbuchdaten der angezeigten Module löschen, die älter sind als:

○ 03.12.2007 0:00 Uhr

Heute 0:00 Uhr vor

● 2 Jahren
○ 1 Jahr
○ 1/2 Jahr
○ 3 Monaten
○ 2 Monaten
○ 1 Monat
○ 1 Woche
○ 1 Tag (Heute)

○ Alles löschen

3.16 Microphone on the forklift

The Mobile Easykey microphone is a body sound microphone. This consists of a piezo sensor and measures only the body sound within the "fixed mass" of the forklift. Since the body sound is measured in frequency per Hertz and the pressure level (sound) in dB, Mobile Easykey cannot detect or measure speech. To listen into the driver is therefore excluded.

In addition to the three-axis acceleration sensor, the body sound microphone serves as a second sensor for detecting whether, in addition to the delay, there was also a body sound "impact" to the forklift.

3.17 Protection against unauthorised reading of the modules

In addition to the transponder IDs of the registered drivers, no other personal data is stored in the modules. Without knowledge of the assignment of the transponder IDs to individuals, unauthorised persons can therefore not obtain personal data by unauthorised reading of the modules..