IT-Consulting & Audits

Datenschutz, ISO 27001
ISMS, ITIL

Prüfbericht Mobile Easykey Manager

für

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

Autorin: Paulette Feller

Datum: 12.03.2020

Version: 1.1

Inhaltsverzeichnis

1 ZUSAMMENFASSUNG

Das vorliegende Dokument beschreibt die Ergebnisse der Prüfung von „Mobile Easykey Manager“ (MEKM) im Hinblick auf die Realisierung des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.

Der Datenschutz durch Technikgestaltung ist durch vielfältige Konfigurationsmöglichkeiten implementiert, und in Mobile Easykey Manager sind eine Reihe von datenschutzfreundlichen Voreinstellungen realisiert.

2 EINLEITUNG

In diesem Kapitel wird das Ziel der Prüfung und die Methodik beschrieben.

2.1 ZIEL

Die Prüfung diente der Bewertung der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO).

2.2 METHODIK

Folgende Methodik wurde angewendet:

- Sichtung des Handbuchs für Mobile Easykey Database V.1, Mobile Easykey Service 2019.1, Mobile Easykey Manager 2019.1, Mobile Easykey Communicator
- Inaugenscheinnahme der Software Mobile Easykey Manager (MEKM)
- Interview der Entwickler bezüglich der technischen Realisierung

3 DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Die nachfolgenden Kapitel führen alle Maßnahmen zur Gewährleistung des Datenschutzes durch Technikgestaltung und zur Umsetzung von datenschutzfreundlichen Voreinstellungen auf.

3.1 WARTUNGSZUGRIFF AUF PSEUDONYME DATEN

Mobile Easykey Manager beinhaltet einen so genannten Service Mode.

3.1.1 Sichere Anmeldung bei Wartungszugriffen per Einmal-Token

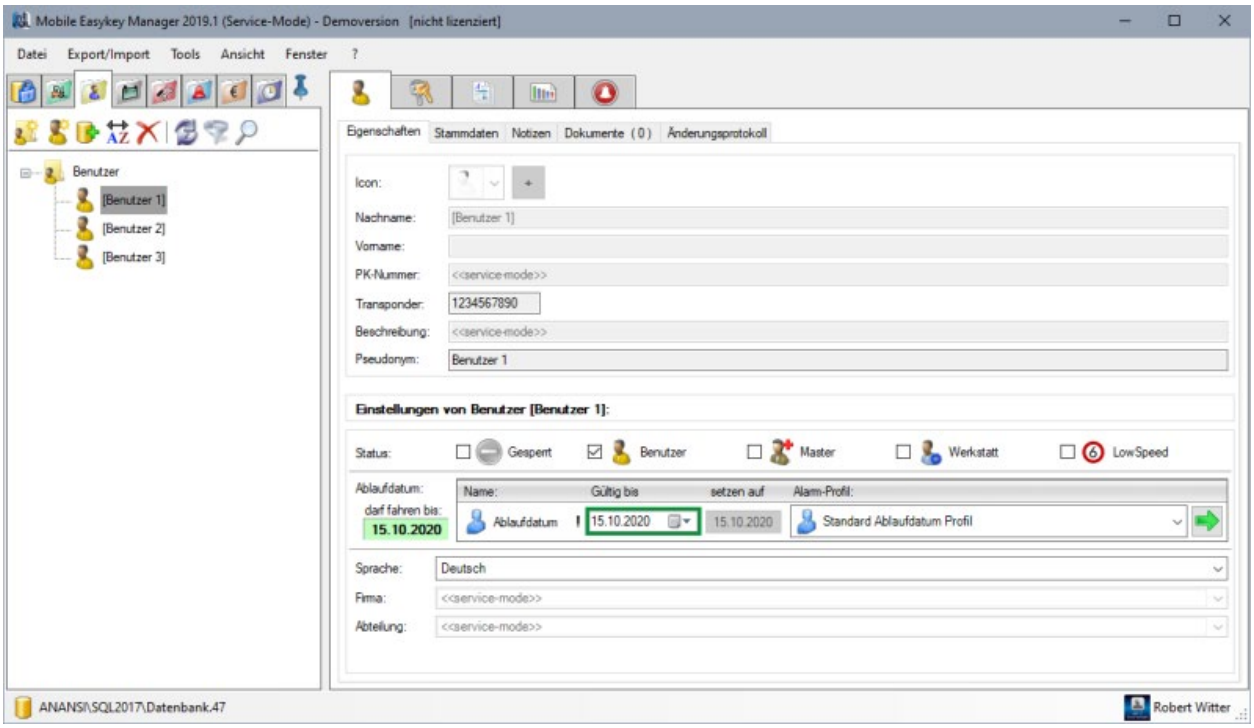
Meldet sich ein Benutzer als Mobile Easykey Service Administrator (Support Mitarbeiter von Domnick+Müller) mit Benutzernamen und Kennwort an, so erhält der MEK Server bei Domnick+Müller darüber eine Information. Es wird nun an die am MEK Server hinterlegte E-Mail-Adresse ein Einmal-Token gesendet. Dieses muss der Mobile Easykey Service Administrator zusätzlich angeben. Erst dann erfolgt die Anmeldung am MEKM.

3.1.2 Pseudonymisierung der Bedienoberfläche

Der Service Mode wird automatisch aktiviert, sobald sich ein Benutzer als Mobile Easykey Service Administrator anmeldet oder wenn über die Funktion Fernwartung eine Fernwartungssitzung aktiviert wird. So lange der Service Mode aktiv ist, werden im gesamten Programm die personenbezogenen Daten ausschließlich pseudonymisiert angezeigt und sind zusätzlich schreibgeschützt. Lediglich die Transponder-ID wird im Klartext angezeigt, damit der Kunde eine Zuordnung herstellen kann, falls dies erforderlich sein sollte. Die Transponder-IDs werden ausschließlich vom Kunden verwaltet, ein Mobile Easykey Service Administrator kann daraus keine Person identifizieren.

Der Schlüssel, der zur Pseudonymisierung verwendet wird, ist einem Benutzer in der Rolle „Mobile Easykey Service Administrator“ nicht zugänglich.

Die nachfolgende Abbildung zeigt die Sicht eines Mobile Easykey Service Administrators während des Supportzugriffs. Die Nachnamen sind pseudonymisiert, und weitere Angaben sind ausgeblendet. Lediglich die Transponder-ID wird im Klartext angezeigt, weil sonst ein Support nicht möglich wäre.



Anmerkung 1

Hier ist die aktive Mithilfe des Kunden erforderlich. Der Kunde muss sicherstellen, dass ein Support-Mitarbeiter von Domnick+Müller keinen Einblick in den Mobile Easykey Manager erhält, solange ein Mitarbeiter des Kunden dort angemeldet ist. Dies gilt sowohl für Vor-Ort- als auch für Fernwartung.

Anmerkung 2

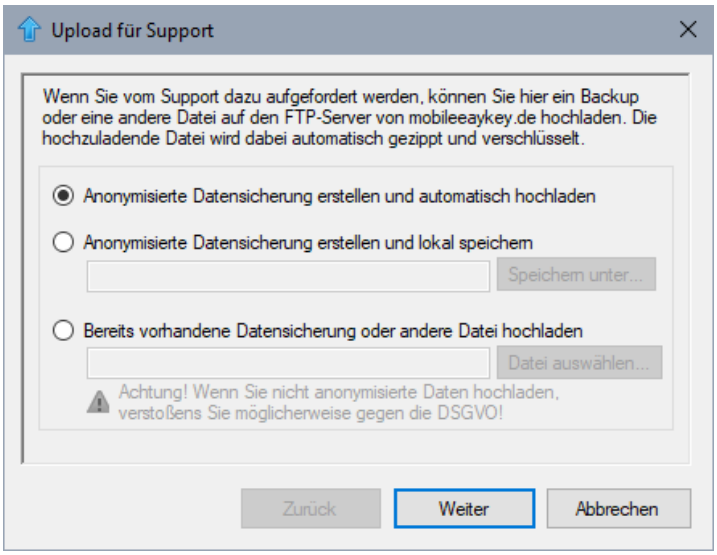
Die Support Mitarbeiter von Domnick+Müller sind instruiert, Zugriffe auf den MobileEasykey Manager ausschließlich in der Rolle „Mobile Easykey Service Administrator“ vorzunehmen.

3.2 Support durch Zugriff auf die Mobile Easykey Datenbank

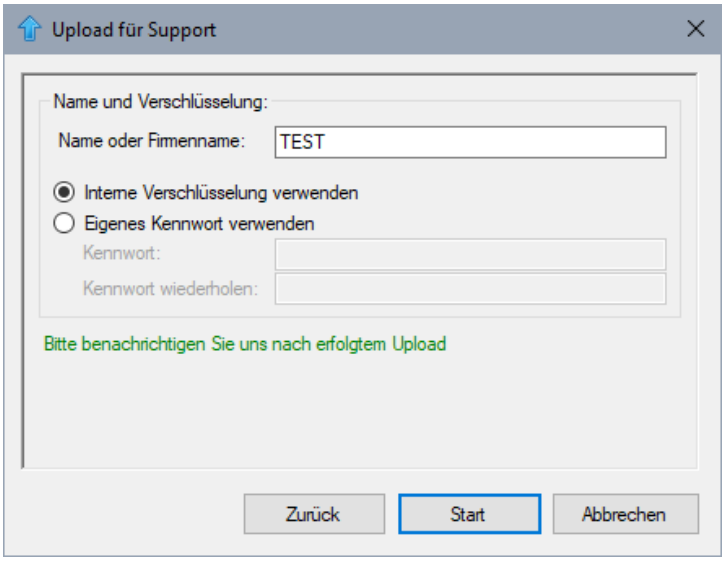
Es gibt Supportfälle, die einen direkten Zugriff auf die Mobile Easykey-Datenbank erforderlich machen. Hierfür gibt es grundsätzlich zwei Wege:

3.2.1 Anonymisierte Sicherung für Supportzwecke

Ist für Supportanfragen die Analyse der Datenbank erforderlich, so kann der Kunde ein anonymisiertes Backup erstellen und dieses Domnick+Müller per FTP-Upload zur Verfügung stellen (siehe nachfolgende Abbildung).



Dabei wird entweder die bereits vorhandene interne Verschlüsselung der Daten genutzt oder ein neues Kennwort verwendet (siehe nachfolgende Abbildung).



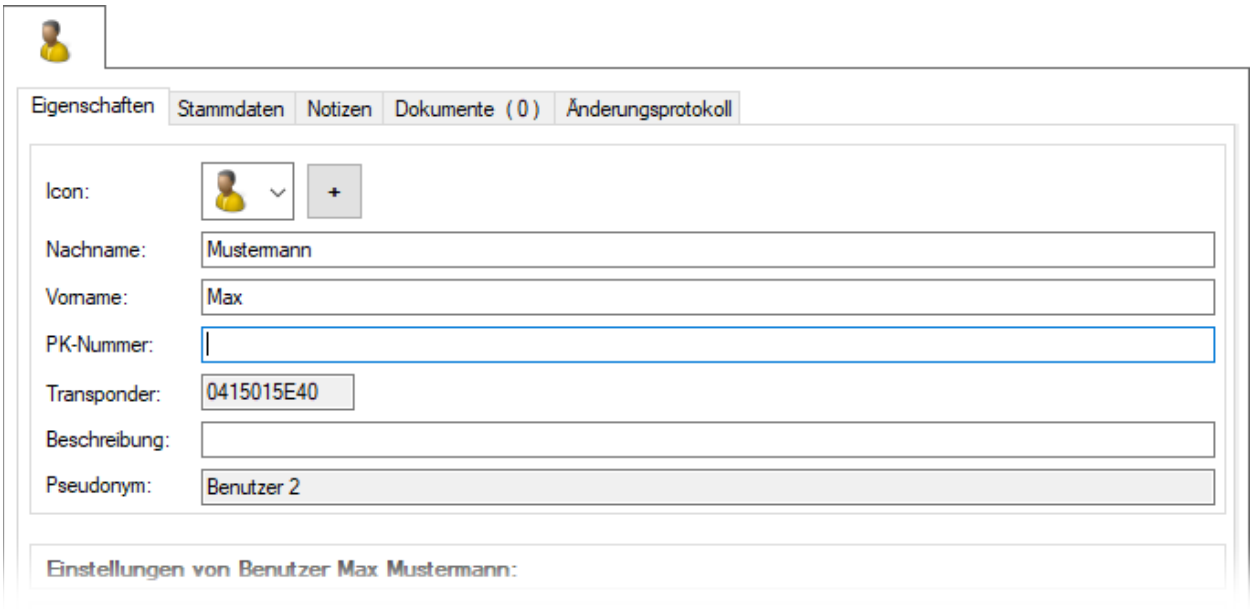
Ein solches anonymisiertes Backup ist ein Backup, in dem zwar alle Daten enthalten sind, nicht jedoch der Schlüssel für die Verschlüsselung der personenbezogenen Daten. Das anonymisierte Backup dient ausschließlich Support-Zwecken. Ein solches Backup kann zwar komplett wiederhergestellt werden, sämtliche personenbezogene Daten sind aber dauerhaft (AES 256) verschlüsselt und können nur noch pseudonymisiert angezeigt werden. Ein Entschlüsseln ist ohne Zugriff auf die Original-Datenbank nicht möglich.

3.2.2 Zugriff auf die Datenbank-Dateien

Sollte der Kunde aufgrund von Software-Problemen nicht in der Lage sein, eine anonymisierte Sicherung der Datenbank zu erstellen, so müssen die Original-Datenbank-Dateien für Supportzwecke verwendet werden. Diese werden bereits bei der Erstellung automatisch verschlüsselt, so dass auch bei direktem Datenbank-Zugriff personenbezogene Daten pseudonymisiert sind. Der Schlüssel zur Entschlüsselung (Ent-Pseudonymisierung) wird in mehreren Teilen gespeichert (siehe Kapitel 3.12 Verschlüsselung der Datenbank) und steht somit für den Support nicht zur Verfügung. Daher kann ein Support Mitarbeiter die personenbezogenen Daten niemals im Klartext lesen.

3.3 DATENSPARSAMKEIT

Für die Funktion des Programms müssen ausschließlich der Name, die Transponder-ID und ggf. ein oder mehrere Ablaufdaten (wie lange die Transponder-ID noch gültig ist) eingegeben werden. Alle anderen Angaben sind freiwillig.



3.4 STARKE AUTHENTIFIZIERUNG

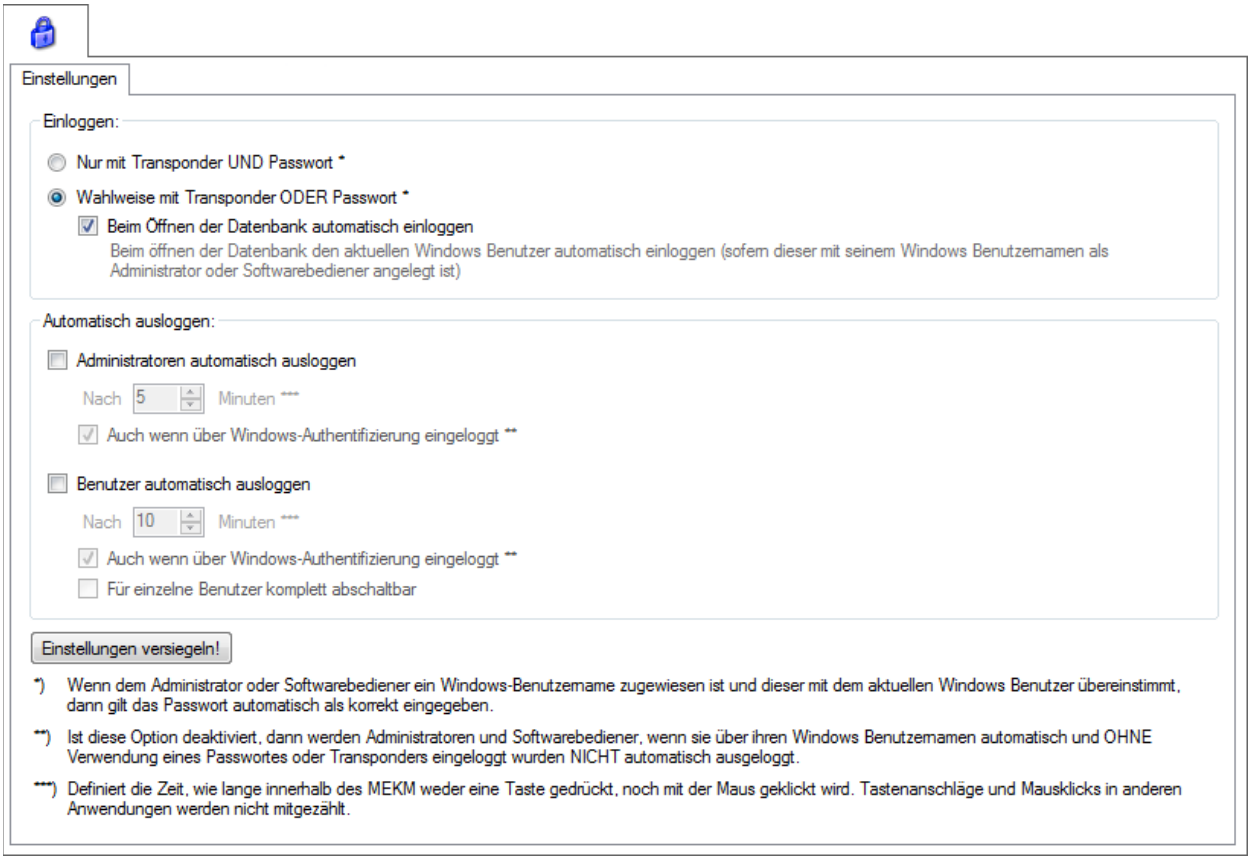
Im MEKM kann festgelegt werden, dass sich Benutzer und Administratoren

- entweder nur mit Transponder UND Passwort oder
- wahlweise mit Transponder ODER Passwort

am Mobile Easykey Manager anmelden (einloggen) können/müssen.

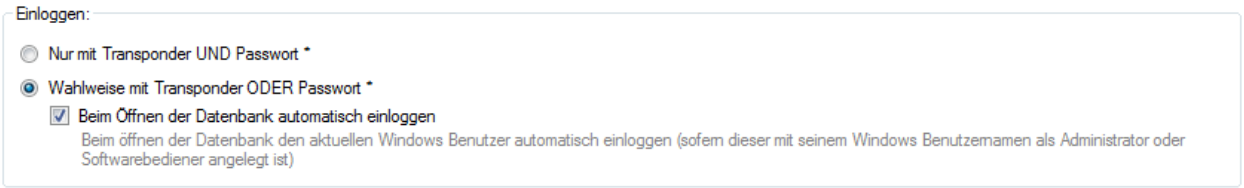
Nur mit Transponder UND Passwort: Bei dieser Option muss dem Benutzer sowohl ein Transponder als auch ein Passwortzugeordnet sein. Ist das nicht der Fall, so kann sich der entsprechende Benutzer nicht anmelden.

Wahlweise mit Transponder ODER Passwort: Bei dieser Option kann sich ein Benutzer mit seinem Transponder oder seinem Passwort anmelden.



3.5 SINGLE SIGN-ON

MEKM bietet die Möglichkeit, einen Softwarebediener oder Administrator automatisch anzumelden, wenn der aktuelle Windows-Benutzernamen mit dem in MEKM hinterlegten Benutzernamen übereinstimmt (siehe nachfolgende Abbildung).



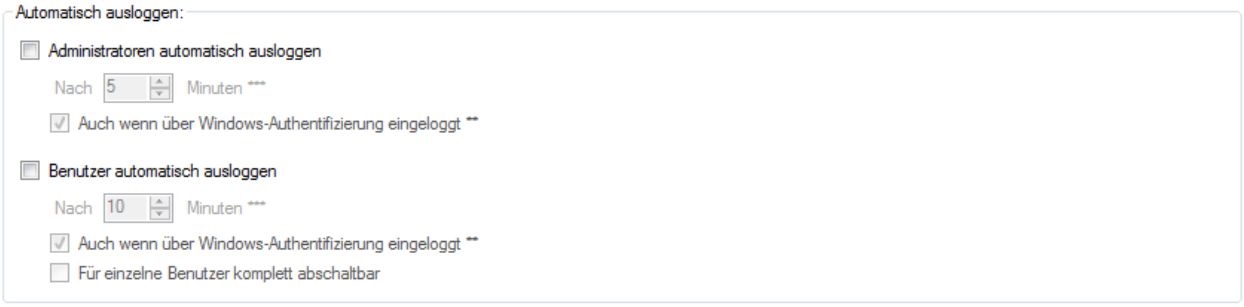
Im Hintergrund wird der Benutzer separat nochmals an der SQL-Datenbank angemeldet. Hier gibt es zwei Möglichkeiten der Authentifizierung:

- Wenn der SQL-Server Mitglied des Active Directory ist, erfolgt die Benutzer-Anmeldung per Kerberos. Dabei wird das Kerberos-Ticket des Benutzers validiert.
- Wenn es sich um einen Stand Alone SQL-Server handelt, erfolgt die Benutzer-Anmeldung per NTLM (NT LAN Manager Protokoll). Dabei wird der Passwort-Hash des am Windows-Client angemeldeten Benutzers geprüft.

In beiden Fällen ist sichergestellt, dass nur legitime Benutzer Zugriff auf die SQL-Datenbank mit den Daten des Mobile Easykey Managers erhalten.

3.6 Automatische Abmeldung

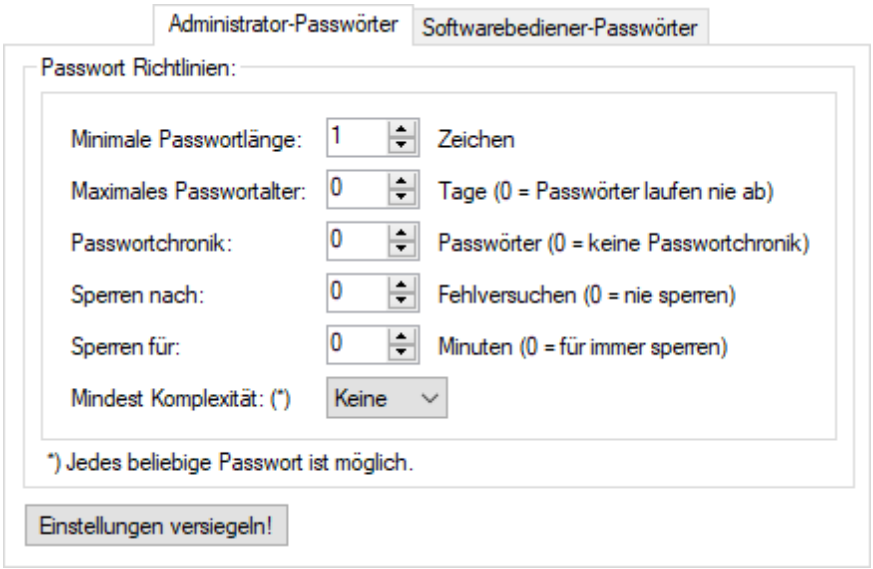
Im MEKM kann vorgegeben werden, dass sowohl Administratoren als auch sonstige Benutzer nach einer definierten Zeit vom System zwangsweise abgemeldet werden (siehe nachfolgende Abbildung).



3.7 Komplexe Kennwortrichtlinien

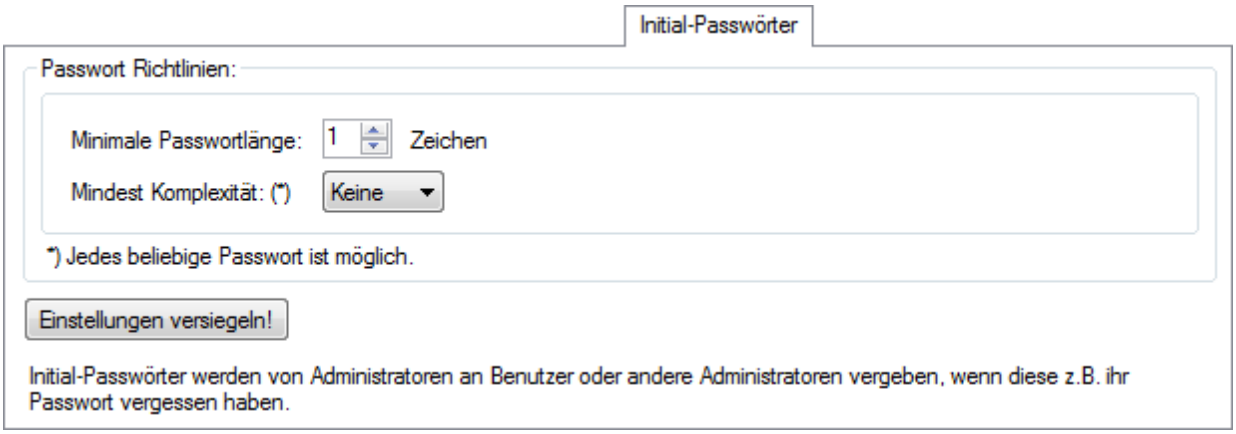
Der Mobile Easykey Manager bietet die Möglichkeit, komplexe Kennwortrichtlinien vorzugeben.

Als erzwungene minimale Passwortlänge können bis zu 40 Zeichen eingegeben werden. Alle anderen Einstellungen können Werte von 0 bis 9999 annehmen. Details sind der folgenden Abbildung zu entnehmen.



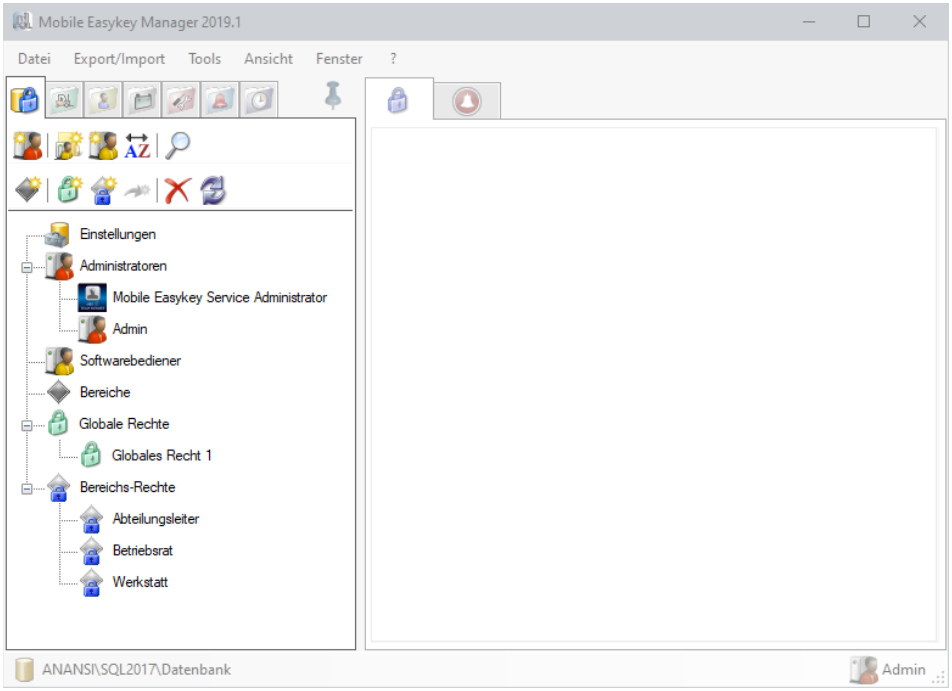
3.8 Initial-Kennwörter

Sowohl vor der Erstanmeldung als auch nach Zurücksetzen eines Kennwortes werden für die betroffenen Benutzer Initial-Kennwörter eingerichtet. Nach Anmeldung mit dem Initial-Kennwort muss der Benutzer selbst ein neues Kennwort einrichten.



3.9 Rollen- und Rechtekonzept (Bedienrechte)

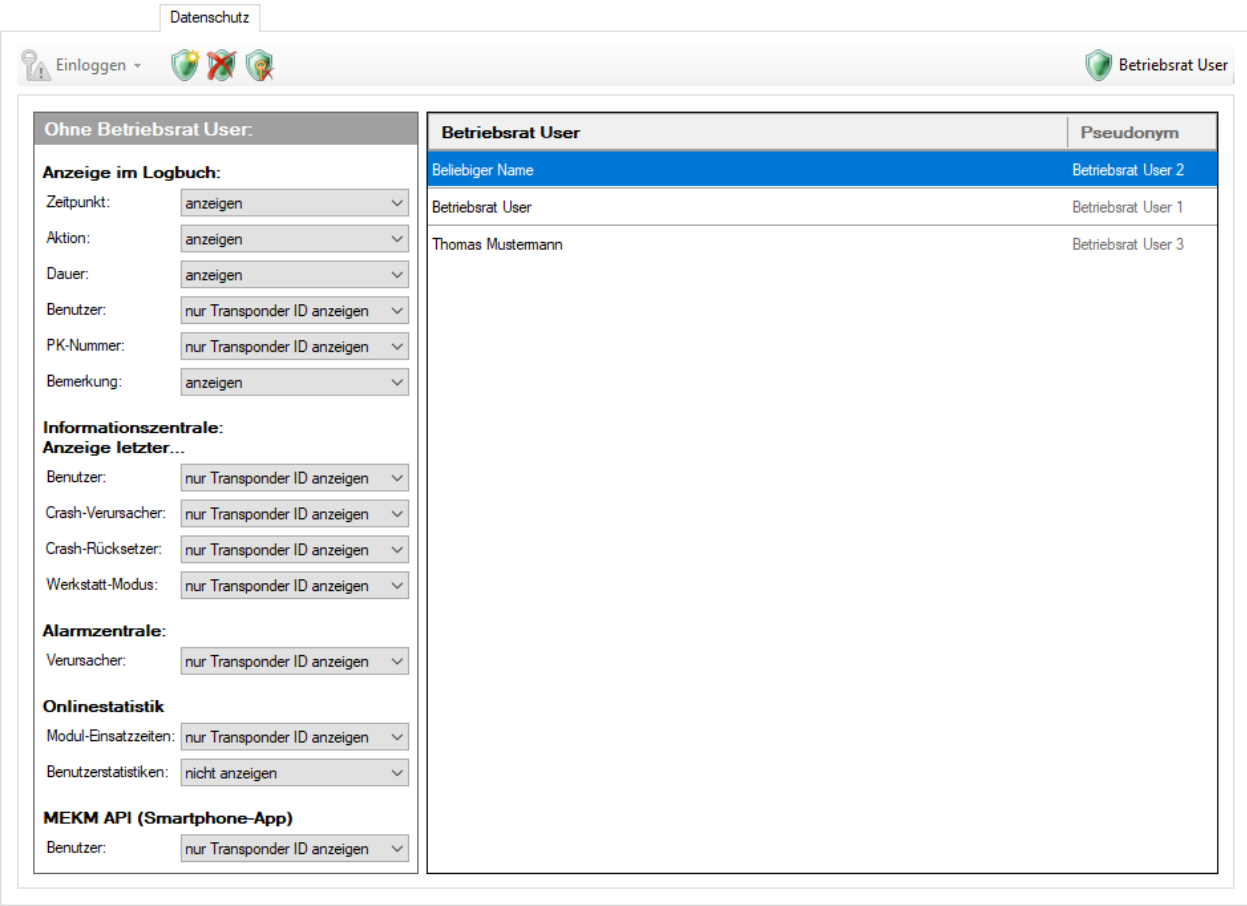
Im MEKM können eigene Rollen und deren Bedienrechte eingerichtet werden. Standardmäßig sind einige Rollen vorkonfiguriert (siehe nachfolgende Abbildung).



3.10 Betriebsrat-User

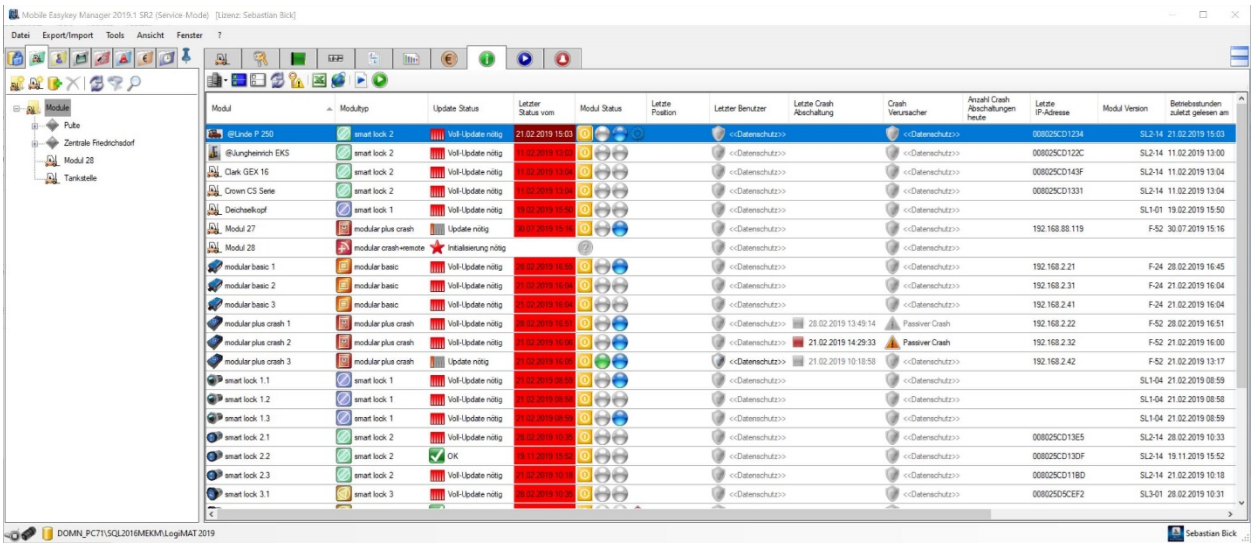
Wenn die Rolle „Betriebsrat User“ verwendet wird, werden für die anderen Benutzerkonten personenbezogene Daten im Logbuch und in der Informationszentrale nicht mehr im Klartext angezeigt. Stattdessen wird dort nur die UID des Transponders des jeweiligen Benutzers oder der Text „<<Datenschutz>>“ angezeigt. Um die personenbezogenen Daten anzeigen zu können, muss sich ein Benutzer mit der Rolle „Betriebsrat User“ anmelden.

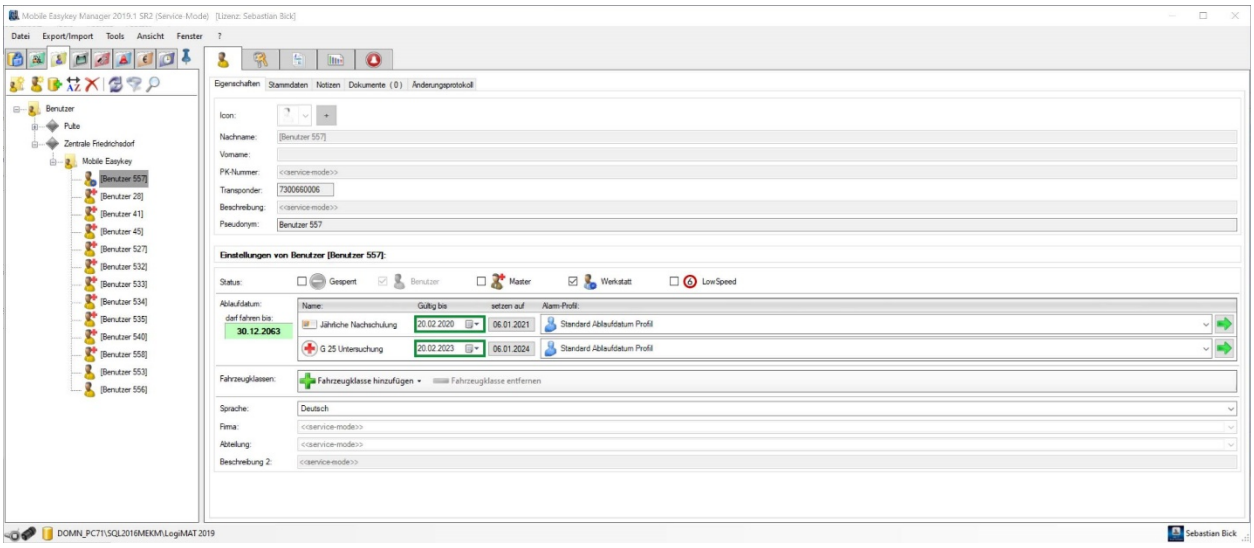
Welche personenbezogenen Daten den Benutzern ohne Betriebsrat-User- Rolle angezeigt werden, kann mit Hilfe der Bedienrechte vorgegeben werden (siehe nachfolgende Abbildung).



In der linken Spalte werden die Komponenten ausgewählt, die ohne die Rolle „Betriebsrat-User“ angezeigt werden. Es können alle Komponenten abgewählt werden außer der UID des Transponders.

Die nachfolgenden Abbildungen zeigen, dass die personenbezogenen Daten bei Bedienern ausgeblendet werden, die nicht über Administrator- oder Betriebsrat-User-Rechte verfügen.





3.11 Verschlüsselung der Datenbank

Alle personenbezogene Daten werden in der Datenbank mit AES 256 verschlüsselt. Der Schlüssel zur Wiederherstellung der personenbezogenen Daten wird dabei in drei Teilen gespeichert:

- Ein Teil wird in der Datenbank zentral abgelegt. Dieser Teil wird beim anonymisierten Backup nicht mit kopiert.
- Der zweite Teil ist fest innerhalb der Software-Installation verankert.
- Der dritte Teil wird zusammen mit dem jeweiligen Benutzer/Softwarebediener etc. gespeichert. Dieser Teil wiederum wird in zwei Versionen gespeichert. Einmal (Teil A) nur für den jeweiligen Namen und einmal (Teil B) für alle übrigen personenbezogenen Daten. Dieser Teil B wird beim sicheren Löschen entfernt.

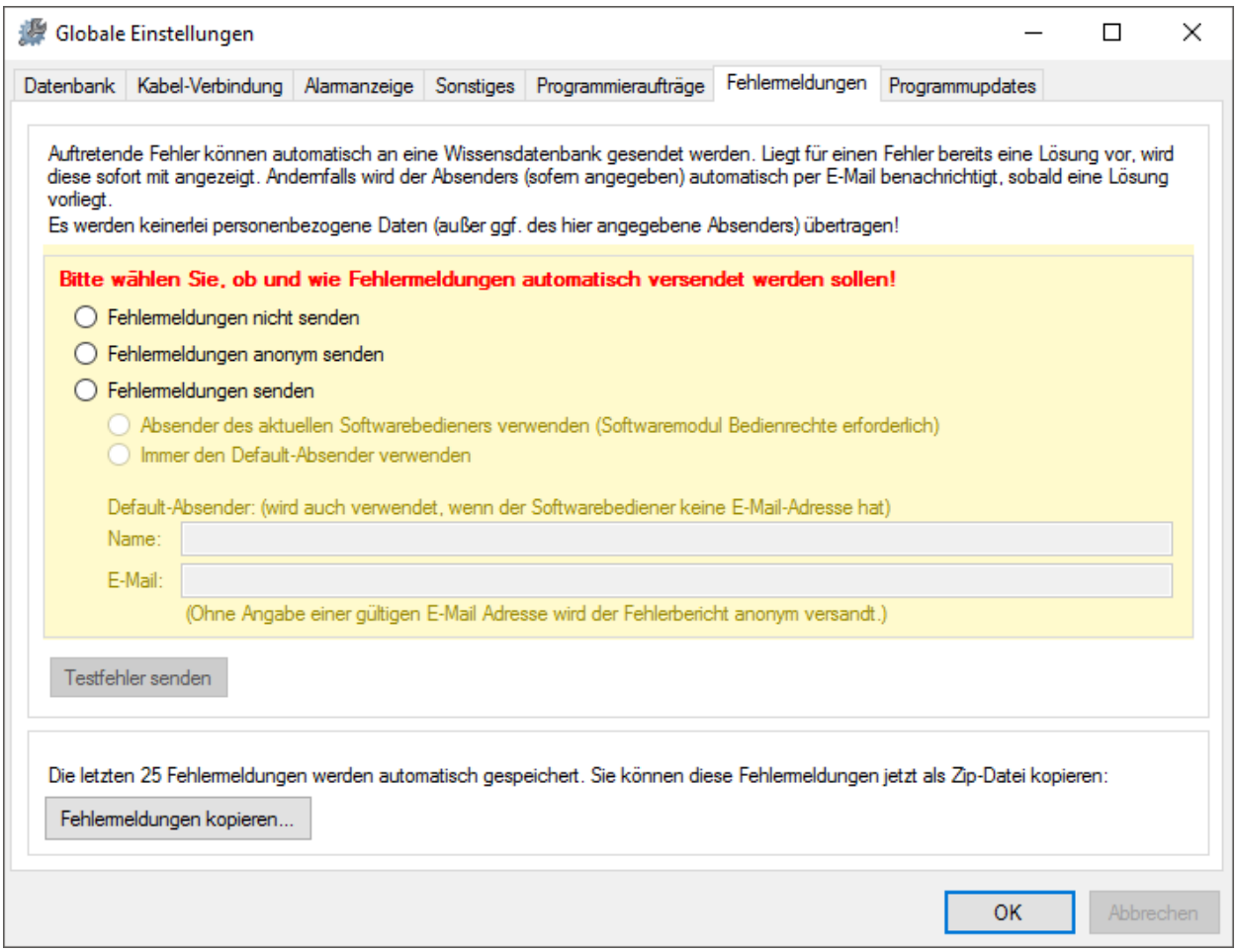
Nur wenn auf alle drei Schlüssel Zugriff besteht, können die personenbezogenen Daten entschlüsselt und im Klartext angezeigt werden.

3.12 Fehlerberichte übertragen

Eventuell auftretende Fehler im MEKM können automatisch über das Internet in eine Wissensdatenbank gesendet werden. Sollte der Fehler bereits bekannt sein und es eine Lösung dazu geben, wird diese automatisch aus der Wissensdatenbank abgerufen und angezeigt.

Wenn ein Name und eine E-Mail-Adresse hinterlegt werden, werden diese Kontaktdaten mit dem Fehler zusammen gespeichert und der Ansprechpartner wird ggf. kontaktiert, wenn weitere Informationen zur Lösung des Problems erforderlich sind. Fehlermeldungen können aber auch ausschließlich anonym gesendet werden.

Die Einstellung für das Senden der Fehlermeldungen kann jederzeit geändert werden (siehe nachfolgende Abbildung). Es kann festgelegt werden, dass keine Fehlermeldungen übertragen werden.



3.13 Automatisches Löschen alter Protokolleinträge

In den verschiedenen Protokollen innerhalb des MEKM können alte Protokolleinträge automatisch gelöscht werden. Wenn die automatische Löschfunktion aktiviert ist, wird das jeweilige Protokoll regelmäßig entsprechend verkleinert.

Die einzelnen Protokolle haben die folgenden Funktionen:

Änderungsprotokoll: Hier wird erfasst wann, und von wem (nur bei aktivierten Bedienrechten) welche Einstellung geändert wurde.

Fehlerprotokoll: Hier werden im Hintergrund aufgetretene Fehler erfasst.

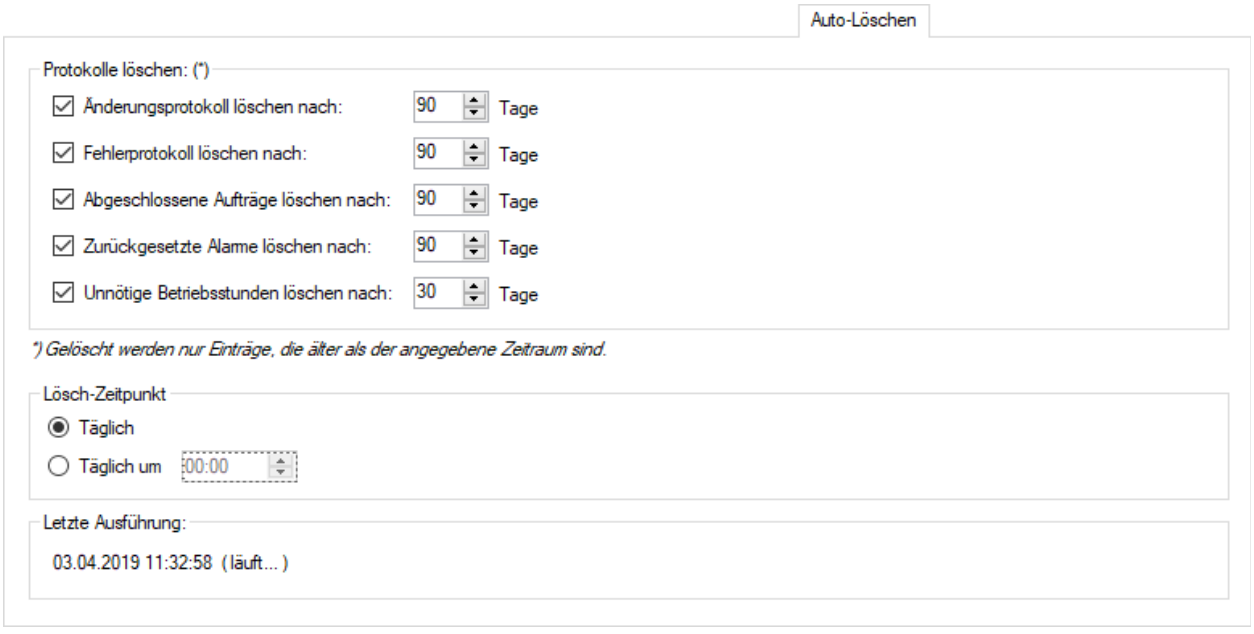
Abgeschlossene Aufträge: Wenn Aufträge (wie z.B. Logbuch auslesen) komplett ausgeführt wurden, wird die Information darüber trotzdem noch für die angegebene Zeit aufbewahrt.

Zurückgesetzte Alarme: Auch Alarme werden (nach Abstellen der Alarm-Ursache) noch für die angegebene Zeit aufbewahrt.

Unnötige Betriebsstunden: Mit den Modulen (ab der Version F) werden die Betriebsstunden-Stände sehr häufig (jede Viertelstunde) erfasst. Diese viertelstündlichen Einträge sind jedoch in der Regel nach ein paar Tagen nicht mehr wichtig. Daher können diese automatisch nach der hier eingestellten Zeit gelöscht werden. Nicht gelöscht werden dabei die Betriebsstunden-Stände jeweils um 0:00 Uhr und vor, bzw. nach einem Neubestromen. Somit bleiben trotzdem genügend Daten vorhanden, um die Betriebsstundenden tagesgenau darzustellen.

Zusätzlich kann angegeben werden, wann diese Daten gelöscht werden sollen. Standardmäßig erfolgt stündlich eine Löschung. Dabei wird bei jedem Programmstart und danach stündlich überprüft, ob zu löschende Daten vorliegen. Diese (veralteten) Daten werden dann automatisch gelöscht.

In der Einstellung „Täglich um“ werden nur einmal am Tag zur angegebenen Uhrzeit veraltete Daten gelöscht.



3.14 Sicheres Entfernen veralteter Einträge

Aus Gründen der Datenbank-Konsistenz können Benutzer (Fahrer), Softwarebediener etc. nicht aus der Datenbank gelöscht werden. Sie werden stattdessen als gelöscht markiert und sind damit im Mobile Easykey Manager nicht mehr sichtbar, verbleiben jedoch in der Datenbank.

Beim Löschen eines Benutzers, Softwarebedieners etc. werden unmittelbar sämtliche personenbezogenen Daten (bis auf den Namen selbst) dieses Benutzers, Softwarebedieners etc. unkenntlich gemacht. Dies gilt dabei auch rückwirkend für das Änderungsprotokoll.

In der Datenbankkonfiguration kann eine Zeit (Standard sind 2 Jahre) festgelegt werden, nach der auch der Name dieses Benutzers endgültig unkenntlich ist. Kommt dieser Benutzer noch in einem der Protokolle (z.B. dem Logbuch) vor, wird er dort nur nach als „<<gelöscht>>“ angezeigt.

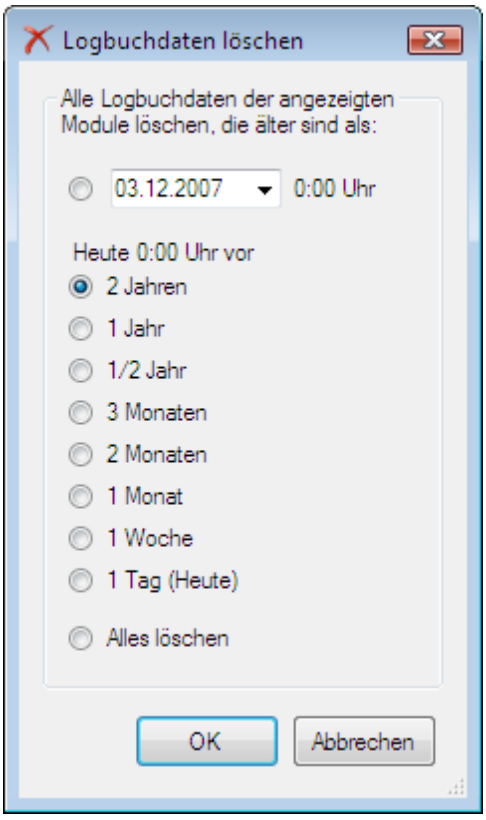
3.15 Logbucheinträge löschen

Da die Datenbankgröße hauptsächlich von der Anzahl der Logbucheinträge abhängt, kann es nötig sein, ältere Logbucheinträge zu löschen.

Wenn als Zeitraum beispielsweise 1 Jahr auswählt wird, so werden alle Logbucheinträge gelöscht, die älter als ein Jahr sind.

Es kann auch ein beliebiges Datum angegeben werden, um alle Logbucheinträge zu löschen, die vor diesem Datum liegen.

Ebenso können alle vorhandenen Logbucheinträge gelöscht werden.



3.16 Mikrofon am Gabelstapler

Bei dem Mobile Easykey Mikrofon handelt es sich um ein Körperschall Mikrofon. Dieses besteht aus einem Piezo Sensor und misst nur den Körperschall innerhalb der „festen Masse“ des Flurförderzeuges. Da der Körperschall in Frequenz pro Hertz gemessen wird und der Druckpegel (Schall) in dB, kann Mobile Easykey keine Sprache erkennen oder messen. Ein Belauschen des Fahrers ist somit ausgeschlossen.

Das Körperschall Mikrofon dient neben dem dreiachsigen Beschleunigungssensor als zweiter Sensor zum Erkennen ob neben der Verzögerung auch ein Körperschall „Anschlag“ am Flurförderzeug stattfand.

3.17 Schutz vor unberechtigtem Auslesen der Module

In den Modulen werden außer den Transponder-IDs der angemeldeten Fahrer keine weiteren personenbezogenen Daten gespeichert. Ohne Kenntnis der Zuordnung der Transponder-IDs zu Individuen können Unbefugte also keine personenbezogenen Daten durch unbefugtes Auslesen der Module erhalten.