S.A.F.E. End-Nutzer-Handbuch Transparenzsoftware 1.4.2

In dieser Dokumentation finden Sie alle relevanten Informationen, welche für die Nutzung der S,A.F.E.-Transparenzsoftware erforderlich sind. Bitte lesen Sie sich die Anleitung vor der ersten Inbetriebnahme der Software aufmerksam durch.

1. Zugang zur Transparenzsoftware

1.1. Systemanforderungen

Für den Betrieb der Transparenzsoftware muss Ihr System zumindest die folgenden Systemanforderungen erfüllen:

Es muss eine Java Runtime oder das Java Development Kit (JDK) ab Version 17 installiert sein. Diese Software ist evtl. bereits auf dem PC installiert. Falls nicht kann eine Version hier heruntergeladen werden: https://jdk.java.net/17/ oder unter https://www.oracle.com/java/technologies/downloads/#java17

Für den Betrieb der Software sind mindestens 50 MB freier Speicher (RAM) notwendig.

Die weiteren Systemanforderungen können auf der OpenJDK bzw. Oracle Webseite https://jdk.java.net oder https://www.oracle.com/java/ nachgelesen werden.

1.2. Download S.A.F.E. Transparenzsoftware

Die Transparenzsoftware ist eine Computeranwendung, welche auf einem stationärem oder mobilem PC- System betrieben werden kann. Die Anwendung basiert zudem auf dem JAVA Framework, welches eine Installation von JAVA auf dem PC-System erfordert.

Für die Installation und Inbetriebnahme der Anwendung gehen Sie bitte wie folgt vor:

1. Laden Sie die jeweils aktuelle Version der Transparenzsoftware auf Ihren Computer und entpacken Sie diese in einen beliebigen Ordner
   https://www.safe-ev.de/de/transparenzsoftware.php
2. Stellen Sie sicher, dass das JAVA Framework in einer aktuellen Version installiert ist. Können Sie die Transparenzsoftware nicht starten, ist JAVA voraussichtlich nicht installiert.
3. Öffnen Sie die Transparenzsoftware mittels Doppelklick

2. Erstellung des Datentupels in der Ladeeinrichtung

Während eines Ladevorgangs an öffentlich zugänglichen Ladeeinrichtungen werden unterschiedliche Werte/Attribute erfasst, die für eine zeitlich versetzte Rechnungsstellung erforderlich sind. Neben Datums- und Energiezählerinformationen sind das vor allem die sog. Contract-ID/Session-ID/Transaktions-ID, die einen Rechnungsempfänger eineindeutig mit den Messwerten in Verbindung setzt. Diese Werte werden in ein sogenanntes Datentupel zusammengefasst. Die aktuellen Anforderungen an den Inhalt eines Datentupels

im Sinnes des Mess- und Eichgesetzes werden aktuell im REA-Dokument 6 A der PTB festgelegt.

https://oar.ptb.de/files/download/58d8ffad4c9184f55a2f94e3

Die Datentupel werden in der Ladeeinrichtung eichrechtskonform erstellt und über OCPP an einen Abrechnungsserver übertragen. Hier findet die langfristige Speicherung und die Rechnungsstellung gegenüber dem Nutzer der Ladeeinrichtung durch einen Mobility Service Provider [MSP] statt. Der Rechnungsempfänger erhält in der Rechnungsstellung Zugang zu diesem Datentupel.

Damit auf dem Transport der Datentupel von der Ladeeinrichtung zum Abrechnungsserver und von dort zur Rechnungsstellung ggü. dem Nutzer der Ladeeinrichtung keine Veränderungen/Manipulationen der eichrechtskonform erfassten Attribute stattfindet, werden die Datentupel digital versiegelt. Mit dem öffentlichen Signaturschlüssel des Datentupels hat der Verwender die Möglichkeit die Versiegelung auf Echtheit zu überprüfen. Sollten Attribute verändert oder verfälscht worden sein, dann kann keine positive Versiegelungsprüfung stattfinden – es wird somit Transparenz zwischen Erfassung und Rechnung hergestellt. Eine nutzerfreundliche Versiegelungsprüfung ist Aufgabe der Transparenzsoftware, dessen Verfahren hier vorgestellt wird.

3. Zugang öffentlichen Schlüssel Datentupel

Um digital versiegelte Datentupel prüfen zu können, benötigen Sie die folgenden Informationen:

- Digital versiegeltes Datentupel (als Hexadezimal-Code oder Datei)
- Öffentlicher Schlüssel (Public Key) der Ladeeinrichtung

Public Keys sind auf Messeinrichtungen aufgedruckte, eichrechtsrelevante Zahlenfolgen, die pro Ladepunkt eineindeutig vergeben werden. Sie ermöglichen Nutzern des Ladepunkts, fernausgelesene Messwerte auf ihre Richtigkeit zu überprüfen. Der öffentliche Schlüssel kann Bestandteil des digital versiegelten Datentupels sein, der Ihnen von Ihrem EMP bereitgestellt wird. Ist der öffentliche Schlüssel im Datentupel nicht enthalten, können Sie Zugang über folgende Wege erhalten:

- Von der Beschriftung der Ladeeinrichtung (vor Ort)
- Direkt vom entsprechenden MSP
- Aus der PKI Datenbank der Bundesnetzagentur: https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/E-Mobilitaet/Ladesaeulenkarte/start.html

Bitte beachten Sie bei der Durchführung der Versiegelungsprüfung in der Transparenzsoftware, dass Sie den öffentlichen Schlüssel der Ladeeinrichtung überprüfen können und Sie der Quelle des Schlüssels vertrauen. Öffentliche Schlüssel, die auf der Rechnung aufgedruckt wurden oder im Datentupel direkt enthalten sind, können nicht korrekt sein und müssen durch den Nutzer noch einmal abgeglichen werden.

4. Prüfung des Datentupels

4.3. Oberfläche Transparenzsoftware 1.4.2

Beim Öffnen der Anwendung Transparenzsoftware 1.4.2 erfolgt nachfolgende Oberfläche, zunächst noch ohne Datentupelinhalt.

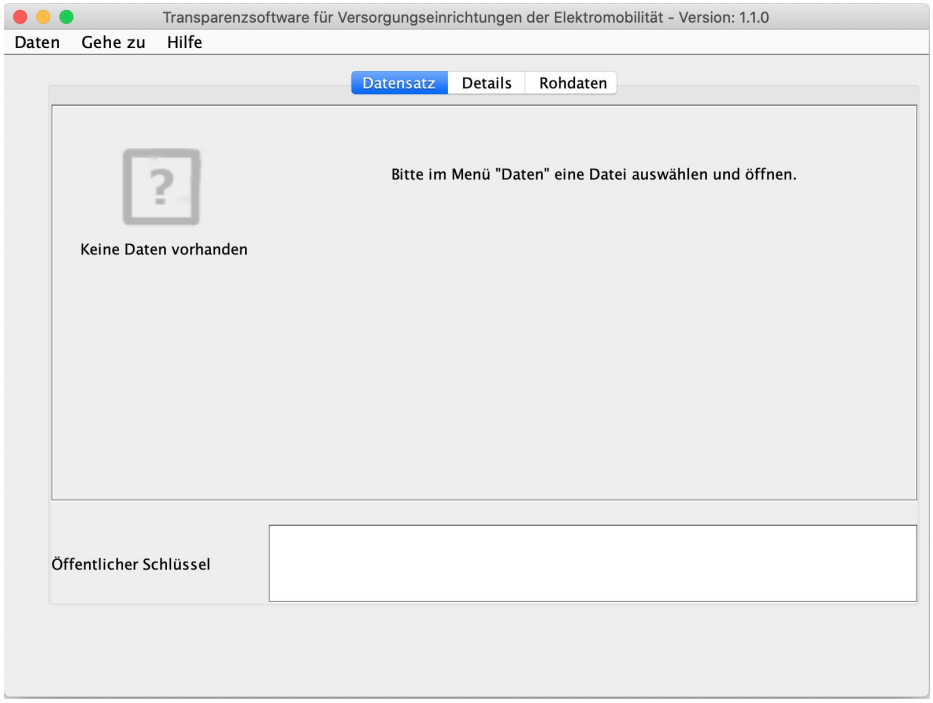


Abbildung 4.1.1: Oberfläche Transparenzsoftware ohne Datentupelinhalte

Über den Reiter Daten besteht die Möglichkeit entweder mit dem Öffnen einer gespeicherten Datei oder mit der manuellen Eingabe der Datenwertsätze in hexadezimaler Form die Prüfung durchzuführen:

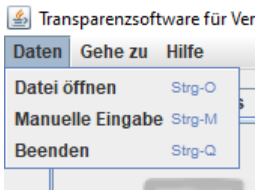


Abbildung 4.1.2.: Dateneingabe in die Transparenzsoftware.

Mit der anschließenden Darstellung der Messdaten, können dann die Rechnungspositionen verglichen werden – es wird Transparenz hergestellt.

4.4. Eingabe Datentupel via gespeicherte Datei

Über Daten ➡ Datei-Öffnen [STRG-O], kann die zuvor am PC abgespeicherte XML-Datei oder Porsche Charging Data Datei in der Transparenzsoftware geöffnet

werden. Wenn das Live-Medium genutzt wird, werden externe Laufwerke wie USB-Sticks im Verzeichnis /run/media/root eingebunden. Das ist das Standardverzeichnis, das beim Öffnen angezeigt wird.

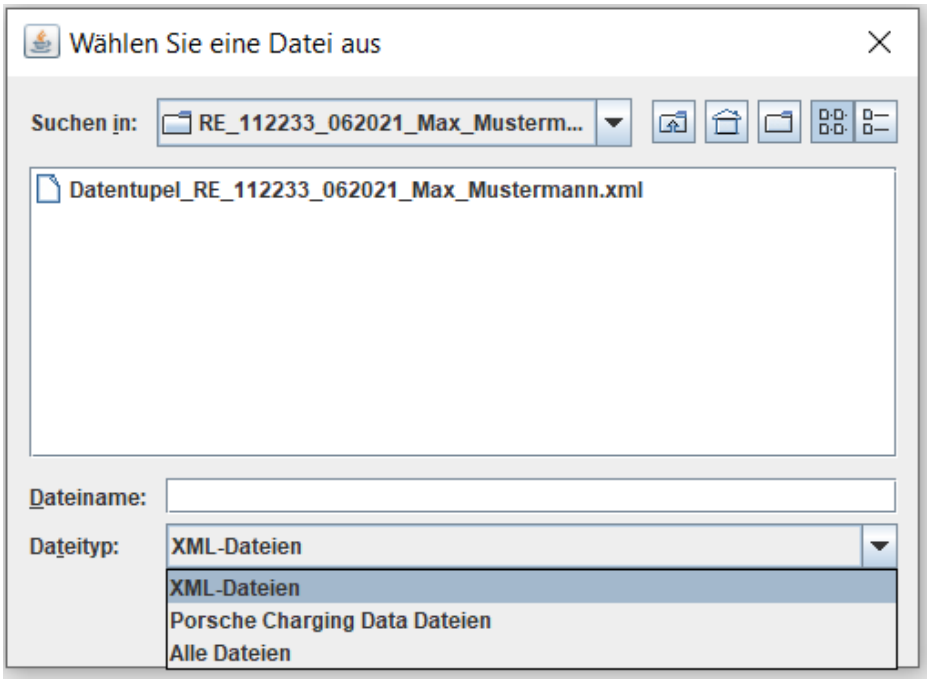


Abbildung 4.2.1.: Dialogfenster zum Datei öffnen.

Nach dem Öffnen der Datei erfolgt nachfolgende Ansicht:

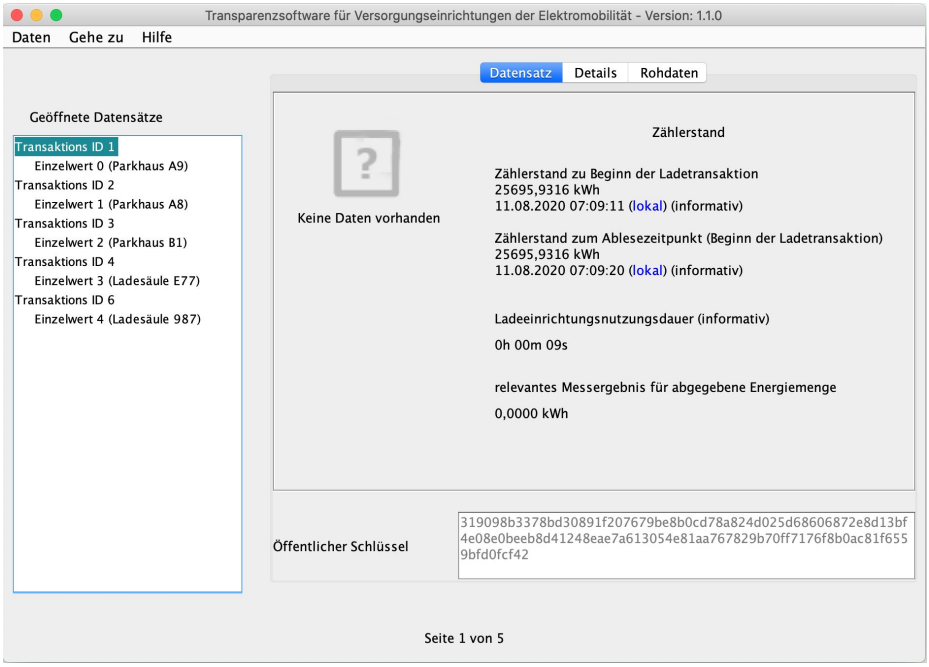


Abbildung 4.2.2.: Oberfläche Transparenzsoftware mit geöffneten XML-Datensätzen (links).

Der Datenwertsatzinhalt der ersten Transaktion sowie der öffentliche Schlüssel werden dem Nutzer bereits ungeprüft dargestellt. Mittels der Transaktions-ID/Contract-ID/Session-ID wird der Ladevorgang im Datentupel eineindeutig einem Ladeort, Ladedatum und Rechnungsempfänger zugewiesen. Diese ID wird dem Rechnungsempfänger an der entsprechenden Rechnungsposition angezeigt und kann dann in der Einzelwertdarstellung in der linken Spalte der Benutzeroberfläche entsprechend ausgewählt werden. Mit der Auswahl erfolgt dann direkt die Versiegelungsprüfung durch die Transparenzsoftware. Abbildung 4.2.3. veranschaulicht mit grünem Haken, dass die Prüfung erfolgreich war. Die Attribute des Datentupels sind noch immer im Ursprungszustand der Versiegelung in der Ladeeinrichtung, die konform zum deutschen Mess- und Eichgesetz erfolgte.

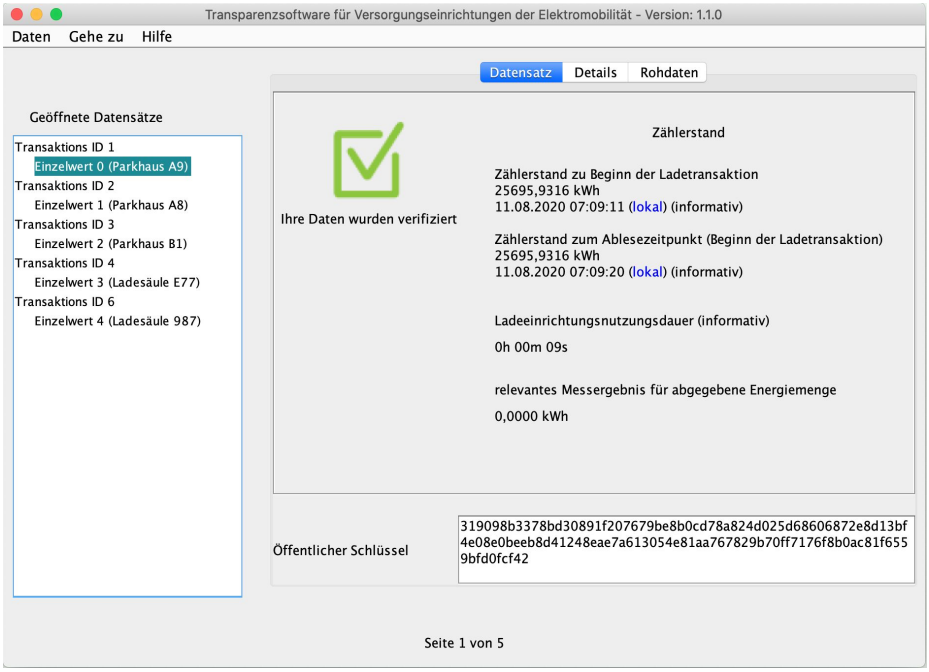


Abbildung 4.2.3.: Oberfläche Transparenzsoftware mit geöffneten XML-Datensätzen (links).

Der Nutzer bekommt die Übersetzung des Inhalts des hexadezimalen Datentupels angezeigt in die für den Ladevorgang relevanten Informationen, wie Start-/Ende oder Menge der Ladesitzung und natürlich versehen mit den entsprechenden Zeitstempeln des Abrufes sowie der Ladedauer. Diese Positionen können vom Nutzer direkt mit den jeweiligen Rechnungspositionen geprüft werden.

Wichtig: In der Datei kann auch nur ein Datenwertsatz sein, dann ist keine Mehrfachauswahl – linke Spalte – möglich und es findet direkt nach Öffnung eine Versiegelungsprüfung statt.

Wichtig: Es gibt verschiedene Datentupel-Formate im Markt, weshalb die Darstellung des Inhaltes leicht voneinander abweichen kann.

Wichtig: Der öffentliche Schlüssel des Datentupels kann als hexadezimal-Darstellung immer überprüft werden – siehe unteres Kästchen der Ansicht.

Im Reiter – Details - hat der Nutzer die Möglichkeit sich weitere Information zum Inhalt des Datentupels anzeigen zu lassen.

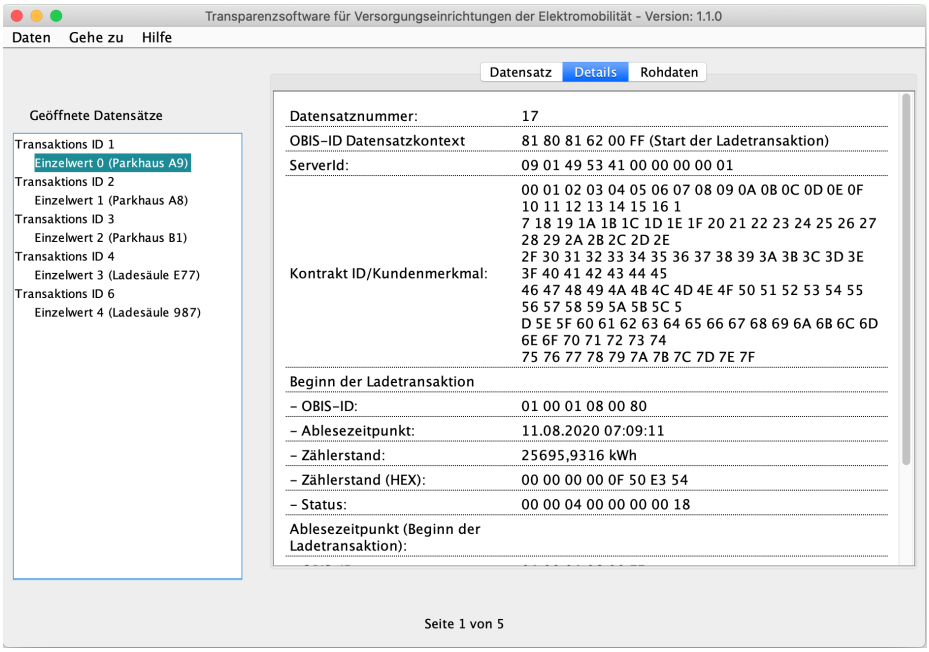


Abbildung 4.2.4.: Oberfläche Transparenzsoftware verifizierter Datenwertsatz weitere Informationen.

Der Reiter – Rohdaten – ermöglicht noch einmal einen Blick auf die hexadezimale Darstellung des Datentupels als kompletten String.

4.3. Eingabe Datentupel via manuelle Eingabe

Über Daten ➡ Manuelle Eingabe [STRG-M] öffnet sich ein Dialogfenster



Abbildung 4.3.1: Oberfläche Dialogfenster manuelle Dateneingabe – ohne Daten.

Über die Funktion copy&paste können nun die Hexadezimalwerte für das Datentupel bei Rohdaten und der öffentliche Schlüssel eingefügt werden.

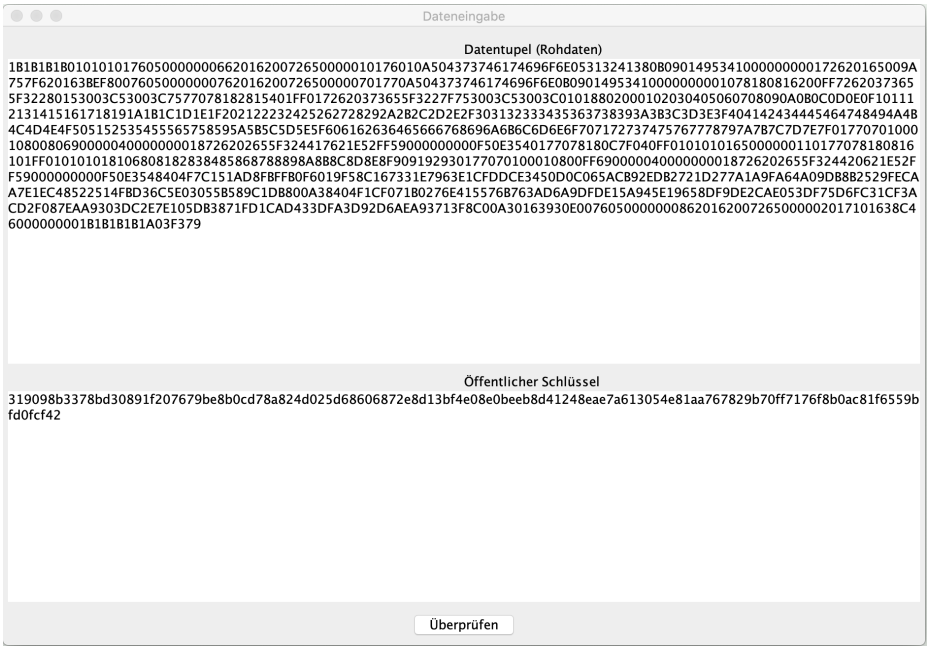


Abbildung 4.3.2.: Oberfläche Dialogfenster manuelle Dateneingabe – mit Daten.

Mit dem anschließenden Klick auf Überprüfen findet dann die Versiegelungsprüfung sowie die Anzeige des übersetzten versiegelten Datentupels statt – siehe Kapitel 4.2.

4.5. Fehlermeldungen der Transparenzsoftware

Sollte in den eingelesenen Daten Fehler enthalten sein, dann erhält der Nutzer rot hinterlegt einen Fehlercode und eine Fehlermeldung angezeigt. Das bedeutet grundsätzlich das an den versiegelten Messdaten oder der Versiegelung ein Fehler entstanden ist und man keine transparente Rechnungsprüfung durchführen kann. Die Fehlermeldung wird auf allen drei Reitern immer an der gleichen Stelle zu Verfügung gestellt.

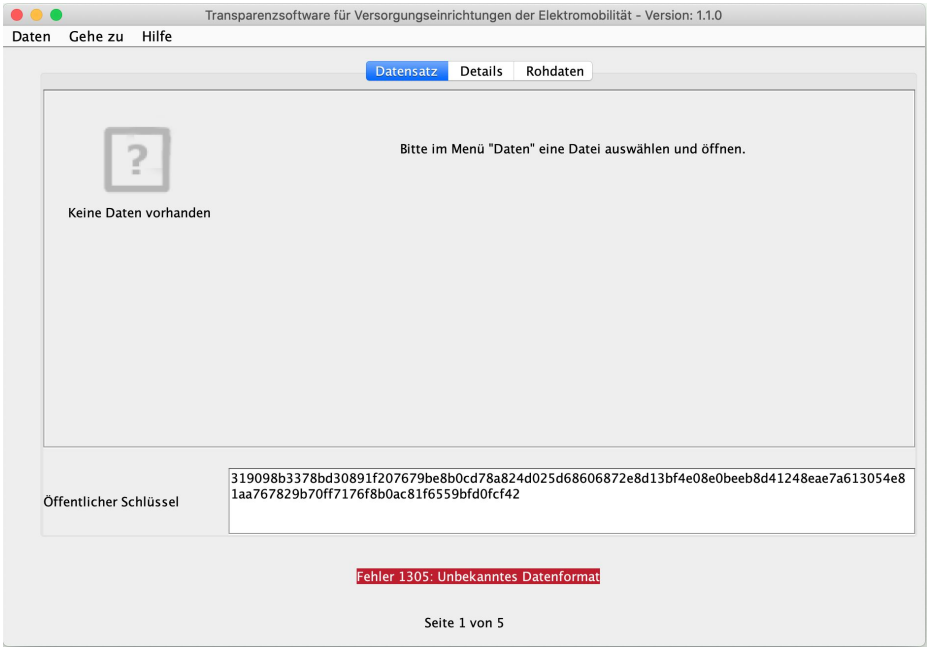
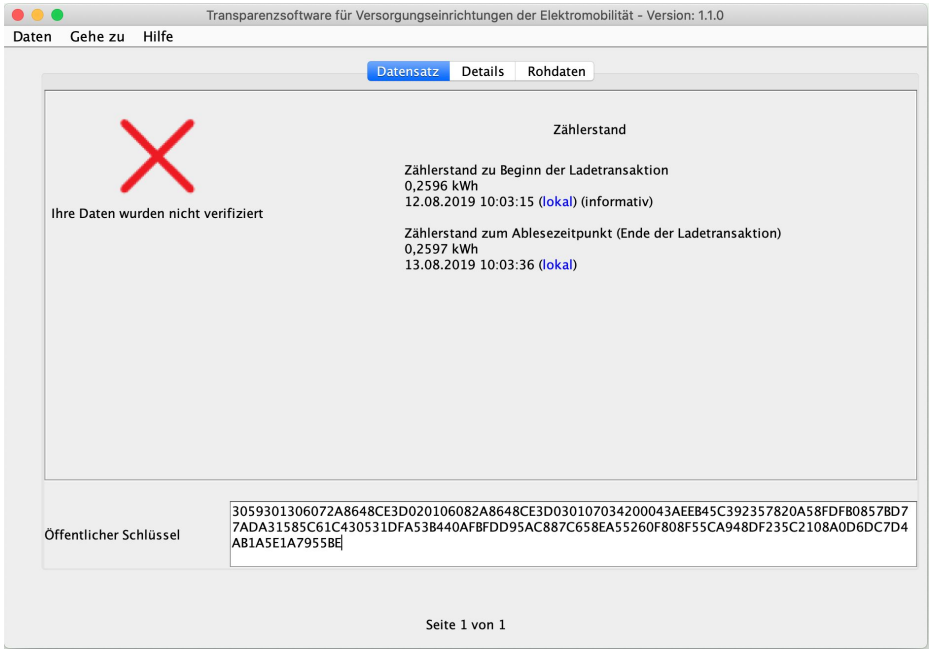


Abbildung 4.4.: Anzeige Fehlermeldungen in der Oberfläche der Transparenzsoftware.

Konnte die Versiegelung wegen eines falschen Schlüssels oder veränderter Daten nicht überprüft werden, wird an Stelle des grünen Hakens ein rotes X und der Fehler "Ihre Daten wurden nicht überprüft" angezeigt:



Wichtig: Wenden Sie sich in diesem Fall unmittelbar an Ihren EMP (Rechnungssteller) und geben bei der Kommunikation den Fehlercode an. Über eine Clearing-Stelle wird der Sachverhalt dann geklärt.

4.5. Weitere Funktionen der Transparenzsoftware

Unter dem Menupunkt "Hilfe / Über" können Versionsinformationen abgerufen werden. Dort wird angezeigt, welche Version der Software aktuell verwendet wird, eine Prüfsumme (SHA-256) über die Software sowie eine Liste mit verschiedene Bibilotheken, die in der Software verwendet werden.

Mit den Funktionen ”Gehe zu / Nächster Eintrag” (oder Strg-N) und ”Vorheriger Eintrag” (oder Strg-P) kann zwischen verschiedenen Transaktionen gewechselt werden, wenn in der Datei oder den Daten mehrere Transaktionen enthalten sind. Wird auf der rechten Seite keine Liste bzw. Baumstruktur mit Transaktionen angezeigt, ist nur eine Transaktion enthalten und die Funktionen zum Weiterschalten sind nicht aktiviert.

Unter dem Menupunkt "Hilfe / Hilfe" befindet sich ein Link auf die Webseite des S.A.F.E. Vereins.

Mit dem Menupunkt "Daten / Beenden" kann das Programm beendet werden.

Liste der Fehlercodes:

Fehlercode	Fehlertext
Fehler 1101	Ungültige Länge für ALFEN Datensätze
Fehler 1102	Ungültige Daten im Alfen-Format
Fehler 1201	Ausgabedatei %s kann nicht erstellt werden
Fehler 1202	Ausgabedatei %s konnte nicht geschrieben werden
Fehler 1203	Fehler beim Erzeugen des Ausgabeformates
Fehler 1301	Ungültige Base 32 Daten
Fehler 1302	Ungültige Base 64 Daten
Fehler 1303	Ungültige Hex Daten
Fehler 1304	Es liegt ein unbekannter Encodingtyp vor
Fehler 1305	Unbekanntes Datenformat
Fehler 1306	Die Eingabedaten sind kein gültiges XML-Format
Fehler 1307	Ungültiger Kurvenname
Fehler 1308	Eingabeparameter konnten nicht ausgelesen werden
Fehler 1309	Ungültiger eingebetteter, öffentlicher Schlüssel
Fehler 1310	Ungültiger öffentlicher Schlüssel
Fehler 1311	Ungültige Länge der Signaturdaten
Fehler 1401	Es wurde keine Eingabedatei angegeben
Fehler 1402	Es konnte kein öffentlicher Schlüssel gefunden werden, um die Daten zu verifizieren (dies kann auch auftreten wenn Daten nicht gelesen werden können)
Fehler 1403	Ungültiger Signatur-Algorithmus für OCMF
Fehler 1404	Ungültige OCMF Version
Fehler 1405	Ungültige Daten im OCMF-Format
Fehler 1204	Ausgabedatei kann nicht erstellt werden, da sie bereits existiert.
Fehler 1406	Nutzdaten konnten nicht geparsed werden
Fehler 1407	Der angegebene Pfad führt nicht zu einer Datei
Fehler 1501	Die Datei kann nicht gelesen werden
Fehler 1502	PCDF ungültig, Signatur fehlt
Fehler 1503	Abrechnung nicht erlaubt

Fehler 1504	Ladevorgangszähler ist ungültig
Fehler 1505	Ladevorgangsdauer ist ungültig
Fehler 1506	Verbrauchdaten sind ungültig
Fehler 1507	Fehlende Felder im Datentupel
Fehler 1508	Ungültiger DCMeter Typ
Fehler 1509	Datentupel enthält keine Endmarkierung
Fehler 1510	<ETX> fehlt
Fehler 1511	Formatierung der Ladedaten ist falsch
Fehler 1512	Hardware Serial Number hat eine falsche Länge
Fehler 1513	Falscher OBIS-Code
Fehler 1514	Ladevorgang-ID ist ungültig
Fehler 1515	Länge der Ladevorgangs-ID ist ungültig
Fehler 1516	Software-Prüfsumme hat eine falsche Länge
Fehler 1517	Abrechnung nicht erlaubt
Fehler 1518	<STX> fehlt
Fehler 1519	Korrupte Zeit Information
Fehler 1520	Zeit Information Länge ist ungültig
Fehler 1521	Zeitsignal ist ungültig
Fehler 1522	PCDF Signatur ungültig
Fehler 1601	Die SML Daten sind nicht vollständig für eine Prüfung
Fehler 1602	Ungültige Einheit für Messwert im SML Datensatz
Fehler 1603	Es wurde ein ungültiger Wert als Server-ID übergeben
Fehler 1604	Ungültige Signatur in der XML Datei
Fehler 1605	Es wurden keine Messwerte im XML Übertragen
Fehler 1606	Es wurde kein Zeitstempel im Messwert angegeben
Fehler 1607	Es wurde kein Zeitstempel im Messwert angegeben
Fehler 1608	Ungültiges SML, Kunden-ID ist nicht vorhanden
Fehler 1609	Ungültiges SML, Logbuch-Eintrags-Index ist nicht vorhanden
Fehler 1610	Ungültiges SML, Zählerstand ist nicht vorhanden
Fehler 1611	Ungültiges SML, OBIS Kennzahl ist nicht vorhanden
Fehler 1612	Ungültiges SML, Paginierung ist nicht vorhanden

Fehler 1613	Ungültiges SML, Sekunden-Index ist nicht vorhanden
Fehler 1614	Ungültiges SML, Server ID ist nicht vorhanden
Fehler 1615	Ungültiges SML, Signatur ist nicht vorhanden
Fehler 1616	Ungültiges SML, Zeitstempel ist nicht vorhanden
Fehler 1617	Ungültiges SML, Zeitstempel der Kunden-ID ist nicht vorhanden
Fehler 1618	Ungültige Daten im SML-Format
Fehler 1701	Unbekanntes Encoding
Fehler 1702	Validierungsfehler beim Verarbeiten der Daten
Fehler 1703	Die eingegebenen Daten enthalten keinen öffentlichen Schlüssel
Fehler 1704	Die eingegebenen Daten enthalten keine signierten Daten
Fehler 1705	Transaktionsstartwert enthält keine Messwerte
Fehler 1706	Transaktion enthält keinen Startwert
Fehler 1707	Transaktionstopwert enthält keine Messwerte
Fehler 1708	Transaktion enthält keinen Stopwert
Fehler 1709	Die ausgewählte Datei enthält keine Wert-Felder
Fehler 1710	Der angegebene öffentliche Schlüssel kann nicht decodiert werden
Fehler 1711	Der angegebene öffentliche Schlüssel enthält keine Daten
Fehler 1712	Der angegebene öffentliche Schlüssel liegt in einem unbekannten Format vor
Fehler 1713	Die angegebene Signatur kann nicht decodiert werden
Fehler 1714	Die angegebenen signierten Daten enthalten keine Informationen
Fehler 1715	Die angegebenen signierten Daten enthalten ein unbekanntes Codierungsformat
Fehler 1716	Die angegebenen signierten Daten enthalten ein unbekanntes Format
Fehler 1717	Transaktion enthält mehr als einen Startwert
Fehler 1718	Transaktion enthält mehr als einen Stopwert
Fehler 1719	Daten konnten nicht verifiziert werden
Fehler 1720	Das Mennekes Eingabe Format konnte nicht transformiert werden.
Fehler 1721	Die Daten enthalten keinen eindeutigen öffentlichen Schlüssel