

# S.A.F.E. End User Manual Transparency Software 1.2.0

Please note that only the German version is binding. No guarantee is given for the accuracy of the translation.

This document contains all relevant information needed to use the S.A.F.E Transparency Software. Please read these instructions carefully before using the software for the first time.

## 1. Accessing the Transparency Software

#### I.I. System requirements

In order to run the Transparency Software, your system must meet the following requirements:

You must have Java Runtime or the Java Development Kit (JDK) version 16 or later installed. This software may already be pre-installed on your PC. If not, you can download a version at <u>https://jdk.java.net/17/</u> or at https://www.oracle.com/java/technologies/downloads/#java17

At least 50 MB of memory (RAM) must be available to operate the software.

You can look up the additional system requirements at the OpenJDK and Oracle websites <u>https://jdk.java.net</u> or <u>https://www.oracle.com/java/</u>.

## 1.2. Download the S.A.F.E. Transparency Software

The Transparency Software is a computer application that can be operated either on a stationary or mobile PC system. The application is based on the Java framework and as such requires Java being installed on the PC system.

To install and launch the application, please proceed as follows:

1. Download the current version of the Transparency Software to your computer and unpack it into a folder of your choice.

https://www.safe-ev.de/de/transparenzsoftware.php

- 2. Ensure that a current version of the Java framework is installed. If you are unable to open the Transparency Software, it is likely that JAVA is not installed.
- 3. Double click to open the Transparency Software

# 2. Creating Data Tuples in the Charging Device

During a charging procedure at publicly accessible charging systems, a range of values/attributes are captured that are required for invoicing later. Apart from date and energy meter information, this mainly includes Contract ID/Session ID/Transaction ID, which unequivocally link the invoice recipient with the measurement values. These values are collated into what is referred to as a 'data tuple'. The current requirements for the content of a data tuple according to calibration law are set down in the PTB's REA document 6 A.

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

The data tuples are created in the charging device in compliance with calibration law, and then transferred to the invoicing server via OCPP. This is where data are stored long-term, and



the charging system user is invoiced by a Mobility Service Provider [MSP]. The invoice recipient obtains access to this data tuple as part of the invoicing process.

The data tuples are digitally signed so that no modifications/manipulation of calibration lawcompliant attributes can take place during the transfer of data tuples from the charging device to the invoicing server, nor from there to the invoicing process respective the user. The data tuple's public key gives the user the option to verify the validity of the digital signature. Should any attributes have been modified or falsified, verification of the signature cannot return a positive result – which creates transparency between data capture and invoice. A user-friendly way of verifying digital signatures is the objective of the Transparency Software, and is presented here in detail.

## 3. Accessing Public Keys for Data Tuples

In order to verify digitally signed data tuples, you need the following information:

- Digitally signed data tuple (in hexadecimal code or as a file)
- Public key for the charging device

Public keys are calibration law related numerical sequences that are unique to each charge point, and are printed onto measuring devices. They enable charge point users to verify the correctness of remote readings of measurement values. The public key can be a component of the digitally signed data tuple you receive from your EMP. If the public key is not contained in the data tuple, you can access it as follows:

- Printed onto the (local) charging device
- Directly from its MSP
- From the Federal Network Agency's (Bundesnetzagentur) PKI database: <u>https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen</u> <u>\_Institutionen/E-Mobilitaet/Ladesaeulenkarte/start.html</u>

When verifying a digital signature using the Transparency Software, please note that you can check the public key of the charging device, and make sure that you trust the source from which you obtained the key. Public keys printed on invoices or contained in the data tuple itself may be incorrect, and may have to be verified by the user.



# 4. Verifying the Data Tuple

#### 4.3. Transparency Software 1.2.0 interface

When opening the Transparency Software 1.2.0 application, the following interface appears – initially without any data tuple content.

en		Hilfe	oftware für Versorgungseinrichtungen der Elektromobilität - Version: 1.1.0
			Datensatz Details Rohdaten
	C	2	Bitte im Menü "Daten" eine Datei auswählen und öffnen.
	Keine Date	n vorhanden	
L			
Öf	fentlicher So	hlüssel	

Figure 4.1.1: Transparency Software interface without data tuple content

The 'File' tab can be used to conduct verification either by opening a saved file, or by entering sets of measurement value data manually in hexadecimal form:

🍰 Transparenzsoftware für Ver				
Daten	Gehe zu	Hilfe		
Datei öffnen Strg-O				
Manuelle Eingabe Strg-M			È	
Beenden Strg-Q				

Figure 4.1.2: Entering data into the Transparency Software.

By displaying the measurement data in the next step, invoiced items can be compared – thus creating transparency.

#### 4.4. Entering data tuples via saved files

An XML file or Porsche Charging Data file can be opened in the Transparency Software using File  $\rightarrow$  Open file [CTRL-O]. If a live boot medium is being used, external drives such as USB sticks are included in the /run/media/root directory. This is the standard directory displayed on opening.



⊌ Wählen Sie eine Datei aus X			
Suchen <u>i</u> n:	☐ RE_112233_062021_Max_Musterm ▼ 🖪 🔂 🗂 比 🖿	]	
Datentup	pel_RE_112233_062021_Max_Mustermann.xml		
Dateiname:			
Dateityp:	XML-Dateien		
	XML-Dateien		
	Porsche Charging Data Dateien		
	Alle Dateien		

Figure 4.2.1: Dialogue box for opening files.

The following view is displayed after opening the file:

🗧 😑 🔵 Transpar	enzsoftware für Versorgungseinr	ichtungen der Elektromobilität - Version: 1.1.0
Daten Gehe zu Hilfe		
Geöffnete Datensätze Transaktions ID 1 Einzelwert 0 (Parkhaus A9) Transaktions ID 2 Einzelwert 1 (Parkhaus A8) Transaktions ID 3 Einzelwert 2 (Parkhaus B1) Transaktions ID 4 Einzelwert 3 (Ladesäule E77) Transaktions ID 6 Einzelwert 4 (Ladesäule 987)	Reine Daten vorhanden	Datensatz Details Rohdaten   Zählerstand   Zählerstand zu Beginn der Ladetransaktion   25695,9316 kWh   11.08.2020 07:09:11 (lokal) (informativ)   Zählerstand zum Ablesezeitpunkt (Beginn der Ladetransaktion)   25695,9316 kWh   11.08.2020 07:09:20 (lokal) (informativ)   Ladeeinrichtungsnutzungsdauer (informativ)   0h 00m 09s   relevantes Messergebnis für abgegebene Energiemenge   0,0000 kWh
	Öffentlicher Schlüssel	319098b3378bd30891f207679be8b0cd78a824d025d68606872e8d13bf 4e08e0beeb8d41248eae7a613054e81aa767829b70ff7176f8b0ac81f655 9bfd0fcf42
	Seite	: 1 von 5

Figure 4.2.2: Transparency Software interface with XML data sets opened (left hand side).

The content of the data value set of the first transaction as well as the public key are immediately displayed to the user in their unvalidated state. Using Transaction ID/Contract ID/Session ID, the charging procedure in the data tuple is uniquely associated with a specific charging location, charging date, and invoice recipient. The



invoice recipient is then shown this ID at the corresponding invoiced item, and it can then be selected accordingly in the individual values display in the left hand column of the user interface. Selecting it then prompts direct validation of the digital signiture by the Transparency Software. Figure 4.2.3. shows how the green tick indicates successful validation. The data tuple's attributes are still in their original state when signed in the charging device, a process that occurred in compliance with German calibration law.

Daten Gehe zu Hilfe	parenzsoftware für Versorgungseinri	chtungen der Elektromobilität - Version: 1.1.0
Geöffnete Datensätze Transaktions ID 1 Einzelwert 0 (Parkhaus A9) Transaktions ID 2 Einzelwert 1 (Parkhaus A8) Transaktions ID 3 Einzelwert 2 (Parkhaus B1) Transaktions ID 4 Einzelwert 3 (Ladesäule E77) Transaktions ID 6 Einzelwert 4 (Ladesäule 987)	Ihre Daten wurden verifiziert	Datensatz Details Rohdaten   Zählerstand   Zählerstand zu Beginn der Ladetransaktion   25695,9316 kWh 11.08.2020 07:09:11 (lokal) (informativ)   Zählerstand zum Ablesezeitpunkt (Beginn der Ladetransaktion)   25695,9316 kWh   11.08.2020 07:09:20 (lokal) (informativ)   Zahlerstand zum Ablesezeitpunkt (Beginn der Ladetransaktion)   25695,9316 kWh   11.08.2020 07:09:20 (lokal) (informativ)   Zahlerstand zum zum zungsdauer (informativ)   0h 00m 09s   relevantes Messergebnis für abgegebene Energiemenge   0,0000 kWh
	Öffentlicher Schlüssel	319098b3378bd30891f207679be8b0cd78a824d025d68606872e8d13bf 4e08e0beeb8d41248eae7a613054e81aa767829b70ff7176f8b0ac81f655 9bfd0fcf42
	Seite	1 von 5

Figure 4.2.3: Transparency Software interface with XML data sets opened (left hand side).

The user is shown a translation of the content of the hexadecimal data tuple, including information relevant to the charging procedure, such as start/end and amount of charge, and of course furnished with the respective time stamps for retrieval as well as charging duration. The user can verify these items by comparing directly against the respective invoice items.

- **Important:** The file may contain only one set of data values, in which case a selection from multiple options in the left column is not available, and the digital signature is verified directly on opening the file.
- **Important:** A range of data tuple formats are on the market, which means that the way their content is displayed may vary.
- **Important:** The public key of the data tuple can always be verified in its hexadecimal form see the box at the bottom of the window.

The 'Details' tab allows the user to access further information regarding signed data tuple content.



	Da	atensatz Details Rohdaten	
Geöffnete Datensätze	Datensatznummer:	17	
Transaktions ID 1	OBIS-ID Datensatzkontext	81 80 81 62 00 FF (Start der Ladetransaktion)	
Einzelwert 0 (Parkhaus A9)	Serverld:	09 01 49 53 41 00 00 00 00 01	
Transaktions ID 2 Einzelwert 1 (Parkhaus A8) Transaktions ID 3 Einzelwert 2 (Parkhaus B1) Transaktions ID 4 Einzelwert 3 (Ladesäule E77) Transaktions ID 6 Einzelwert 4 (Ladesäule 987)	Kontrakt ID/Kundenmerkmal:	00 01 02 03 04 05 06 07 08 09 0A 08 0C 0D 0E 0F 10 11 12 13 14 15 16 1 7 18 19 1A 18 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 28 2C 2D 2E 27 30 31 32 33 34 35 36 37 38 39 3A 38 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 AA 48 4C 4D 4E 4F 50 51 52 53 54 55 55 75 78 59 5A 5B 5C 5 D 5E 5F 60 61 62 63 64 65 66 67 68 69 6A 68 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F	
	Beginn der Ladetransaktion		
	- OBIS-ID:	01 00 01 08 00 80	
	– Ablesezeitpunkt:	11.08.2020 07:09:11	
	- Zählerstand:	25695,9316 kWh	
	- Zählerstand (HEX):	00 00 00 00 0F 50 E3 54	
	- Status:	00 00 04 00 00 00 00 18	
	Ablesezeitpunkt (Beginn der Ladetransaktion):		

Figure 4.2.4: Transparency Software interface with further information on verified sets of data values.

The 'Dataset' tab allows the hexadecimal display of the data tuple being viewed as a single string.

# 4.3. Entering data tuples using manual data entry

Dialogue window opens via → Manual data entry [CTRL-M]



Figure 4.3.1: Interface window for manual data entry (without data).

The hexadecimal values for the data tuple ('Raw data') and the public key can now be entered using copy&paste.



	Dateneingabe
	Datentupel (Rohdaten)
757F620163BEF8007605000 5F32280153003C53003C757 2131415161718191A1B1C11 4C4D4E4F50515253545556 108008069000040000000 101FF010101018106808182 F5900000000F50E3548404 A7E1EC48522514FBD36C5EC	00006201620072650000010176010A504373746174696FF6E053132413808901495341000000000172810816200F72620155009 000076201620072650000071770A504373746174696FF6E059014953410000000001078180816200F7262037365 77078182815401FF0172620373655F3227F753003C53003C01018802000102030405060708090A080C000E0F1011 91E1F202122232425262728292A282C2D2E2F303132333435363738393A383C3D3E3F40414243445464748494A4 758595A585C5D555F606162636465666768696A6886C6D6E6F707172737475777777879A787C7D7EF7017707100 1187262025557324417621E52FF590000000000750E3540177078180C7F040FF011010165500000011017707818081 183845586378889848886208E8F8909129301770701100010800FF6900004000000187262026557324420621E52 F7C151AD8FFB0F6019F58C167331E7963E1CFDDC53450D0C065AC892ED82721D277A1A9FA64099B882529FE2 F7C151AD8FFB0F6019F58C167331E7963E1CFDDC53450D0C065AC892ED82721D277A1A9FA64095D882529FE2 50558589C1E0800A3840F1CF07180275641557687306A30F639500004000080620162007265000002017101638C 79
	Öffentlicher Schlüssel
319098b3378bd30891f2076 fd0fcf42	79be8b0cd78a824d025d68606872e8d13bf4e08e0beeb8d41248eae7a613054e81aa767829b70ff7176f8b0ac81f6559
	Überprüfen

Figure 4.3.2: Interface window for manual data entry (with data).

Following an additional click on 'Verify', the digital signature is verified, and the signed data tuple is displayed in translated form – see Chapter 4.2.

# 4.4. Error messages in the Transparency Software

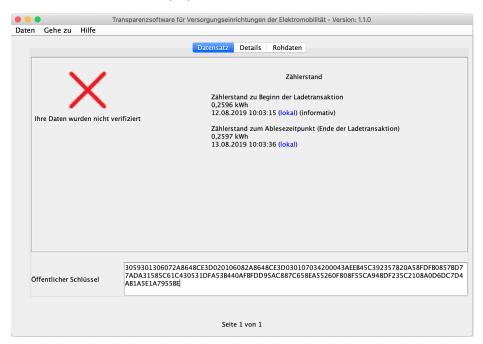
Should the entered data contain errors, the user receives an error message and an error code on a red background. In principle, this means that an error has occurred with the signed measurement data or the digital signing process, and that transparent invoice verification cannot be performed. Error messages are displayed in the same place on all three tabs.



en Gehe zu Hilfe	ransparenzsoftware für Versorgungseinrichtungen der Elektromobilität - Version: 1.1.0
	Datensatz Details Rohdaten
Reine Daten vorhanden	Bitte im Menü "Daten" eine Datei auswählen und öffnen.
Keine Daten vomanden	
	319098b3378bd30891f207679be8b0cd78a824d025d68606872e8d13bf4e08e0beeb8d41248eae7a613054e
Öffentlicher Schlüssel	1aa767829b70ff7176f8b0ac81f6559bfd0fcf42
	Fehler 1305: Unbekanntes Datenformat
	Seite 1 von 5

Figure 4.4.: Error message display on the Transparency Software interface.

If the digital data signature cannot be verified because of an incorrect public key or modified data, the green tick is replaced with a red 'X', and the error message 'Your data has not been verified' is displayed:



**Important:** In this case, please immediately contact your EMP (invoice issuer) and mention the error code. A customer service unit will then clarify the issue.



# 4.5. **Further functions of the Transparency Software**

Version information can be obtained via the 'Help / About' menu options. This shows which version of the software is currently being used, a checksum (SHA-256) for the software, as well as a list of the range of libraries used within the software.

The functions 'Go to / Next entry' (or CTRL-N) and 'Previous entry' (or CTRL-P) can be used to switch between different transactions – as long as the file or data set contains more than one transaction. If no list or tree diagram with transactions is displayed on the right hand side, then only one transaction is included, and the switching functions are not activated.

The menu option 'Help / Help' contains a link to the S.A.F.E. association's website.

The menu option 'Data / Close' can be used to close the application.



#### List of error codes:

- Error code Error message
- Error 1101 Invalid length for ALFEN data sets
- Error 1102 Invalid ALFEN data
- Error 1201 Unable to create %s file
- Error 1202 Unable to write %s file
- Error 1203 Output format error
- Error 1301 Invalid base 32 data
- Error 1302 Invalid base 64 data
- Error 1303 Invalid Hex data
- Error 1304 Unknown encoding type detected
- Error 1305 Unknown data format
- Error 1306 Invalid XML format for data entered
- Error 1307 Invalid curve name
- Error 1308 Unable to read input parameters
- Error 1309 Invalid embedded public key
- Error 1310 Invalid public key
- Error 1311 Invalid length of signature data
- Error 1401 No data entry file entered
- Error 1402 No public key found to verify data (this can also occur if unable to read data)
- Error 1403 Invalid OCMF signature algorithm
- Error 1404 Invalid OCMF version
- Error 1405 Invalid OCMF data
- Error 1204 Unable to create output file because it already exists.
- Error 1406 Unable to parse use data
- Error 1407 The indicated path does not lead to a file
- Error 1501 Unable to read file
- Error 1502 PCDF invalid, missing signature



- Error 1503 Invoicing not allowed
- Error 1504 Invalid charging procedure counter
- Error 1505 Invalid charging duration
- Error 1506 Invalid consumption data
- Error 1507 Data missing in tuple
- Error 1508 Invalid DCMeter type
- Error 1509 End marker missing in data tuple
- Error 1510 <ETX> missing
- Error 1511 Incorrect charging data format
- Error 1512 Incorrect hardware serial number length
- Error 1513 Incorrect OBIS code
- Error 1514 Invalid charging procedure ID
- Error 1515 Invalid length of charging procedure ID
- Error 1516 Invalid length of software checksum
- Error 1517 Invoicing not allowed
- Error 1518 <STX> missing
- Error 1519 Corrupted time information
- Error 1520 Invalid length of time information
- Error 1521 Invalid time signal
- Error 1522 Invalid PCDF signature
- Error 1601 SML data incomplete for verification
- Error 1602 Invalid measuring value unit in SML data set
- Error 1603 Invalid Server ID value transmitted
- Error 1604 Invalid signature in XML file
- Error 1605 No measurement values transmitted in XML
- Error 1606 Time stamp missing for measurement value
- Error 1607 Time stamp missing for measurement value
- Error 1608 Invalid SML, missing Customer ID
- Error 1609 Invalid SML, missing logbook entry index
- Error 1610 Invalid SML, missing meter reading



- Error 1611 Invalid SML, missing OBIS identifier
- Error 1612 Invalid SML, missing pagination
- Error 1613 Invalid SML, missing seconds count
- Error 1614 Invalid SML, missing Server ID
- Error 1615 Invalid SML, missing signature
- Error 1616 Invalid SML, missing time stamp
- Error 1617 Invalid SML, time stamp missing for Customer ID
- Error 1618 Invalid SML data
- Error 1701 Unknown encoding
- Error 1702 Validating error when processing data
- Error 1703 Public key missing in entered data
- Error 1704 Entered data do not contain digitally signed data
- Error 1705 No measurement values in transaction start value
- Error 1706 No start value in transaction
- Error 1707 No measurement values in transaction end data
- Error 1708 No end value in transaction
- Error 1709 Selected file contains no value fields
- Error 1710 Unable to decode public key entered
- Error 1711 No data in public key entered
- Error 1712 Unknown public key format
- Error 1713 Unable to decode entered signature
- Error 1714 No information in entered digitally signed data
- Error 1715 Unknown digitally signed data format
- Error 1716 Unknown format in signed data
- Error 1717 More than one starting value in transaction
- Error 1718 More than one end value in transaction
- Error 1719 Unable to verify data
- Error 1720 Unable to translate Mennekes entry format
- Error 1721 Data contains no unique public key