General definition of CDR data structures

Publication of the S.A.F.E. Roaming Working Group

This document is a joint definition of the best practices for a well-functioning roaming operation under the utilization of calibrated metering values and smart meters.

Document Metadata

Status:	Released
Date:	20.03.2020
Version:	1.0

Authors: Sergiu Tcaciuc (Wirelane), Andreas Weber (Allego), Michael Roeder (Chargepoint), Karl Wendrich (reev), Julia Drazic (Chargecloud), Anas Munir (smartlab), Simon Schilling (SMATRICS)

General definition of CDR data structures

Scope

In the established market communication structure, the charging transaction data is sent in the form of Charge Detail Records (CDRs). The MSP as the receiving party needs to be able to parse and validate these CDR messages in order to invoice their customers.

As the market is adopting the meanwhile formalized requirements for the calibration law compliance, the existing roaming protocols need to adopt as well. In particular the CDR formats need to get enabled to carry all relevant information for a calibration law compliant invoicing. Therefore the S.A.F.E. Working Group Roaming evaluated the requirements as well as possible implementation scenarios to propose a common CDR data structure towards all roaming protocols. The focus of the document is on the ease of use and simple adoption for the current roaming market. Additionally the compatibility towards all major roaming protocols has been evaluated to allow for one unified solution.

The following requirements and goal are to be achieved with this data structure definition:

1. The MSP has to inform the customer about the transparency method for the charging session.
2. The MSP needs to receive all necessary information from the CPO to apply the transparency method and validation checks.
3. The MSP needs to be able to perform automated validation checks.

This leads to the minimum on information the MSP needs to have available at the time a CDR is processed and validated:

- **transparency method:** (different variations available, e.g. signature-based, local validation, …) This information is needed to instruct the customer with the right guidance in case they want to validate the invoice and to apply the internal data validation checks.
- **data format and version:** (Multiple known, e.g.: SAFE, SAM, Alfen, ChargePoint, …) This information is needed to apply the right parsing/decoding method for internal validation checks, e.g. selecting the right transparency software.
- **signed data:** (data + signature) The actual signed data to be transmitted to the customer for validating the invoice.
- **public key** If the transparency method relies on a public key it has to be transmitted for automated validation.

Evaluation of central register for implementation variants

The CPO has to communicate information on the calibration law implementation to the MSP (see list above). This is necessary up-front in the POI data as well as after the transaction in the CDR data. There are three possible variants to implement the communication of the calibration law solution:

- Central register: The data describing the solutions is stored in a central register. The register generates and offers unique IDs per solution. The CPO needs to refer to these IDs in the market communication. The MSP uses the register to apply the right business logic depending on the solution the charging transaction was done with.
- Existing IDs: The unique IDs of the solution certification are used in conjunction with the certification date. These IDs are issued by the certifying body. This references one implementation and version of a hardware uniquely. The CPO takes the ID out of the hardware data sheet. The MSP uses the ID to apply the right business logic depending on the solution the charging transaction was done with.
- Descriptive data: The data format describes the implementation by various parameters. The CPO sends a machine readable description of the solution with the roaming data. The MSP applies the (generative) business logic depending on the description.

Applied ratings for the following evaluation:

- very good: ++
- good: +
- neutral: 0
- bad: -
- very bad: --

Criteria	**Central register**	**Existing IDs**	**Descriptive data**
Time to market	--	++	0
Globalization / International scalability	--	+	++
Implementation effort: CPO	--	0	-
Implementation effort: MSP	-	+	--
Implementation effort: roaming platforms	++	++	+
Operation effort: CPO	0	++	-

Operation effort: MSP	+	-	++
Operation effort: roaming platforms	0	0	0
Direct operation costs (Operation of the solution)	--	0	0
Feature flexibility	0	0	--
Independence for new solutions	0	0	++

Based on this evaluation the usage of existing IDs is the most promising implementation. The following section describes a proposal for the usage of existing IDs in CDRs of current roaming protocols.

Validation of a CDR

It is recommended for the MSP to validate any incoming CDR before invoicing it to the customer. The original CDR contains value fields for time, energy and other billing relevant data. The signed data however is added to this original CDR as a separate data element.

This leads to three possible ways for the validation of a incoming CDR:

1. Use original CDR and keep signed data as additional proof in case of an audit. No consistency issues will be detected before invoicing. In case of falsified data the customer will be the first to notice and file an inquiry.
2. Ignore original CDR data and bill on signed data only. The most reliable data is used for invoicing. Billing engines have to be adopted to work with the signed data format. Non-compliant charging stations have to be handled differently than compliant ones.
3. Validate original CDR against signed data and bill on basis of original CDR. The validation effort for the MSP is high as there is no direct mapping of signed data fields to the original CDRs fields available.

Version 2 is seen as the best approach as it is the lowest impact to roaming systems.

1. Validate the signatures of all signed data elements.
2. Validate the content (flags, consistence) of all signed meter elements.

The exact validation steps and methods are dependent on the data format and should be carried out by a oficial transparency software. In case of validation problems it is recommended to reject the CDR.

The MSP should then use the signed data values instead of the unsigned fields of the original CDR for the billing process. The other fields can be used for informative purposes if needed.

CDR Content

- The calibration law compliant CDR has to contain four additional fields:
  - Compliance identification
  - Compliance ID: A unique ID referencing one individual solution. This can be used to link to the instructions for metering data processing. (“Nummer der Baumusterprüfbescheinigung”)
  - Revision number (optional)
  - Validity date
- Metering Data format and version
- Metering Data: An unordered list of zero or more data containers. Data processing according to the Compliance ID.
  - The transmitted format can contain one or more metering samples each.
  - The format needs to contain an identifier for each sample. This identifier is used to declare it as session start, session end etc. value.
  - It is allowed to repeat samples in multiple containers.
  - Should be encoded in a base64 encoded string.
- Public key (only required if not include in metering data set)

General Remarks

Data transfer principles

The data is transmitted in the CDR in the format the charging station produces it. The transparency software defines an additional container format for user convenience. This container can hold the data of a charging session in one or multiple signed objects. It is the decision of the MSP whether the signed data has to be packed into such a container before presenting it to the user.

How to invoice based on signed CDR

When the MSP receives a CDR he should perform the following steps in order to invoice the customer:

1. Validate the signatures of the relevant signed data.

2. Apply the rules defined by the charging station manufacturer and/or data format regarding falsification flags. (Messwertverwendervorschrift)
3. Extract the billing relevant data from the signed data containers.

The MSP should not use the non-signed data fields of the CDR for billing purposes.

How to lookup Compliance identification

It is foreseen that the roaming solution makes the following data available to the MSPs. This can be done through a central data exchange, a dedicated endpoint at the CPO or similar mechanisms. The data must be accessible through a combination of compliance ID, revision number and validity date.

- transparency software
- “Messwertverwendervorschrift”
- user manual

Implementation proposals

Open Chargepoint Interface (OCPI)

The implementation of the above proposal in OCPI can be demonstrated through the following proposal. The basis for the proposal is OCPI 2.2.D-2.

OCPI is structured by modules. One module contains the interfaces for one set of business functionality. The CDRs module contains the interfaces for exchanging charging data between CPO and MSP.

The CDR module defines the CDR Object which is extended in the proposal. Therefore the following new classes are introduced:

- SignedData class
- SignedValue class
- ComplianceID class

Extension of the CDR object

The property signed_data of type SignedData is added to the CDR object. It is an optional property only to be provided if the charging session contains signed data.

Property	Type	Card.	Description
...	...	...	...
compliance_data	ComplianceData	?	Compliance information that belongs to this charging session.

ComplianceData class

This class contains all the information of the compliance relevant data. Which encoding method is used, if needed, the public key and a list of signed values.

Property	Type	Card.	Description
compliance_id	ComplianceID		A unique compliance ID is required to verify the metering data processing will be done according the compliance requirements
metering_data_format	CiString(36)	1	The name of the metering data format used in the signed_values field. This is the name given to the encoding by a company or group of companies. It may also contain a version number if needed. The identification string should be defined by the format definition.
public_key	CiString(512)	?	Public key used to sign the data, base64 encoded.
signed_values	SignedValue	+	One or more signed values.

SignedValue class

This class contains the signed and the plain/unsigned data. By decoding the data, the receiver can check if the content has not been altered.

Property	Type	Card.	Description
nature	CiString(32)	?	Nature of the value, in other words, the event this value belongs to. Possible values at moment of writing: - Start (value at the start of the Session) - End (signed value at the end of the Session) - Intermediate (signed values take during the Session, after Start, before End) - Multiple/mixed Others might be added later. Usually this is handled by the signed data format and should not be repeated on roaming protocol level.
signed_data	CiString(512)	1	Blob of signed data, base64 encoded. The format of the content depends on the metering_data_format field.

ComplianceID class

This class contains the Compliance ID information to reference the correct data handling required based on Eichrecht conformity instruction.

Property	Type	Card.	Description
compliance_id	CiString(32)	1	The Compliance ID is referring to the examination certificate of the specific charger used for this CDR
revision	int	1	Defines the Revision of the Compliance document
issue_date	DateTime	1	Defines the date the compliance document was issued

Open Clearing House Protocol (OCHP)

TBD

Open Intercharge Protocol (OICP)

TBD

EVSE Data

Name	Data Type	Description	M/O	Field Length	Validation
SignedMeteringValueAvailable	enum	This field gives the information that if the EVSEID can generate the Calibration Law data or not. One option out of 3 should be provided "Local" (for eg SAM) "Non Local" (for eg Transperency Software) "Not available" (for eg at the moment no Calibration Law complaint data generated)	M		
CalibrationLawTechnologyInformation	CalibrationLawTechType	If the Calibration Law Complaince field is true then additional information must be provided by CPO.	O/M	100	If CalibrationLawCapliance field has "true" as a value, this field must be provided.

CalibrationLawTechType

Name	Data Type	Description	M/O	Field Length	Validation
CalibrationLawComplainceID	String	The Calibration Law Complaince ID from respective authority along with the revision and issueing date (Complaince ID : Revision : Date) For eg PTB - X-X-XXXX : V1 : 01Jan2020	O/M	100	
PublicKey	String	Unique PublicKey for charging station should be provided here	O/M	1000	
PublicKey_LastUpdated	Date/Time	This field gives the information when PublicKey was last updated	OM	1000	
MeteringSignatureEncodingMethod	String	Format of the data which is provided in Metering Signature	O/M	50	
SignedMeterValueVerificationInfo	MeteringSignatureVerificationInfoType	Instructions needed to verify the transaction using the information provided in the MeteringSignatureValue	O/M		

MeteringSignatureVerificationInfoType

Name	Data Type	Description	M/O	Field Length	Validation
url	String	URL	M	200	
Instruction	String	Additional information	M	400	

CDR

Name	Data Type	Description	M/O	Field Length	Validation
SignedMeteringValue	String	Metering Signature basically contains all metering signature for different status of charging session for eg start, end or inbetween	O	5000	

eMobility Protocol Inter-Operation (eMIP)

TBD