

	<b>VDE-AR-E 2802-100-1</b>	<b>VDE</b>
	This specification – <b>only the original German version</b> – is a VDE-Anwendungsregel according to VDE 0022. After completion of the approval procedure adopted by the VDE Supervisory Board it was included in the VDE Specifications Code of safety standards under the VDE number indicated above and announced in the "etz Elektrotechnik + Automation" magazine.	<b>DKE</b>
<p><b>Reproduction prohibited – also for internal use.</b></p> <p>ICS 43.120; 34.040;15.240.60 <span style="float: right;">Supersedes VDE-AR-E 2802-100-1:2017-10</span></p> <p><b>Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118 English translation of VDE-AR-E 2802-100-1:2019-12</b></p> <p>Zertifikats-Handhabung für Elektrofahrzeuge, Ladeinfrastruktur und Backend-Systeme im Rahmen der Nutzung von ISO 15118 Englische Übersetzung von VDE-AR-E 2802-100-1:2019-12</p> <p>Gestion des certificats pour les véhicules électriques, infrastructure de charge et systèmes backend dans le cadre de ISO 15118 Traduction anglaise de VDE-AR-E 2802-100-1:2019-12</p> <p style="text-align: right;">Gesamtumfang 90 Seiten</p> <p style="text-align: center;">Translation by VDE language service In cases of doubt the German original shall prevail</p>		
<p>© VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V. No part of this document may be reproduced without prior permission of VDE, Frankfurt am Main, Germany. Distribution by VDE VERLAG GMBH, 10625 Berlin</p>		

## Date of application

This VDE application guide becomes applicable on 2019-12-01.

No transition period exists for VDE-AR-E 2802-100-1:2017-10.

## Content

	Page
Foreword .....	6
Introduction .....	7
1 Scope .....	9
2 Normative references .....	9
3 Terms, definitions and abbreviated terms .....	10
3.1 Terms and definitions .....	10
3.2 Abbreviations .....	13
4 Public key infrastructure operation .....	15
5 Actors involved in the electric mobility market in the context of Plug & Charge .....	17
5.1 End customers .....	17
5.2 Vehicle manufacturers (OEMs) .....	17
5.3 Mobility operators (MOs) .....	17
5.4 Charge point operators (CPOs) .....	18
5.5 Certificate provisioning service (CPS) operators .....	18
5.6 Contract certificate pool (CCP) operators .....	18
5.7 OEM provisioning certificate pool operators .....	20
5.8 V2G root CA operators .....	20
5.9 Roles not included .....	21
6 Explanation of public key infrastructure as defined in DIN EN ISO 15118-2:2016 08 .....	22
6.1 Plug & Charge for achieving a secure and user-friendly charging experience .....	22
6.2 Certificate types of the PKIs as defined in the context of DIN EN ISO 15118-2:2016-08 .....	22
6.2.1 Overview of certificate types .....	22
6.2.2 V2G root CA certificate .....	23
6.2.3 MO root CA certificate .....	24
6.2.4 Contract certificate .....	24
6.2.5 Charge point certificate (SECC certificate) .....	24
6.2.6 OEM provisioning certificate .....	24
6.2.7 OEM root CA certificate .....	24
6.2.8 Certificate provisioning service (CPS) leaf certificate .....	25
6.2.9 Private operator root CA certificate .....	25
6.3 Non-functional public key infrastructure characteristics .....	25
6.3.1 Non-functional characteristics as a result of different market interests .....	25
6.3.2 Size of a single certificate .....	25

	Page
6.3.3	Length of a certificate chain ..... 25
6.3.4	Number of root CA certificates ..... 26
6.3.5	Period of validity of a V2G root CA certificate ..... 26
6.3.6	Period of validity of sub-CA certificates ..... 27
6.3.7	Validity of an OEM provisioning certificate ..... 27
6.3.8	Validity of contract certificates ..... 27
6.3.9	Validity of charge point certificates ..... 27
7	Validation ..... 27
7.1	Definition of validation ..... 27
7.2	Validity models as requirements for the certificate check ..... 28
7.2.1	Types of validity model ..... 28
7.2.2	Shell model ..... 28
7.2.3	Implementing validations ..... 29
8	Installing certificates ..... 29
8.1	Installing contract certificates ..... 29
8.2	Installing root CA certificates ..... 30
9	Providing public keyinfrastructure certificates ..... 30
9.1	Options for providing contract certificates ..... 30
9.2	Detailed description of categories ..... 31
9.2.1	Category A: Charging interface as defined in DIN EN ISO 15118-2:2016-08 ..... 31
9.2.2	Category B1: OEM backend and telematics link ..... 31
9.2.3	Category B2: Vehicle manufacturer's website ..... 31
9.2.4	Category C1: Vehicle user's mobile end device ..... 32
9.2.5	Category C2: Service interface at the vehicle workshop ..... 32
10	PCID and EMAID structure ..... 32
10.1	Provisioning certificate ID ..... 32
10.2	EMAID ..... 33
11	Processes for provisioning of certificate types for public charging ..... 33
11.1	Overall system with asynchronous data flow ..... 33
11.2	Preparing contract-based public charging and billing ..... 35
11.2.1	Breaking preparation down into sub-processes ..... 35
11.2.2	Providing root certificates for public charging and contract-based billing ..... 35
11.2.3	Producing the vehicle and signing the contract ..... 37
11.2.4	Assigning the vehicle to a contract ..... 40
11.3	Providing a contract certificate for automated billing ..... 42
11.3.1	Relationship between contract and billing as well as vehicle and contract certificate ..... 42
11.3.2	Providing a Contract Certificate Bundle ..... 43
11.3.3	Signing a Contract Certificate Bundle ..... 48
11.3.4	Delivering a contract certificate upon request ..... 53

	Page
11.3.5 Pushing a contract certificate to the OEM backend .....	58
12 Revocation of certificates .....	59
12.1 Motivation .....	59
12.2 Revocation of contract certificates for the Plug & Charge process.....	60
12.2.1 Process of revoking contract certificates.....	60
12.2.2 Pre-requisites .....	60
12.2.3 Having a contract certificate revoked by the mobility operator and generating a certificate revocation list.....	61
13 Message broker.....	62
14 Future developments.....	63
14.1 Procedure for working on unresolved items .....	63
14.2 Installing and using multiple contract certificates in a vehicle.....	63
14.3 Challenge-response authentication in a private environment.....	64
14.4 Requirements for the management of key material at a charge point .....	64
14.5 Verifying the legitimate use of a PCID.....	65
14.6 Usage of OCSP responders vs certificate revocation lists (CRLs) .....	65
Annex A (normative) Cryptographic mechanisms and security parameters .....	66
A.1 Focus on security aspects.....	66
A.2 IT security between electric vehicles and charging infrastructure in general.....	66
A.3 Cryptographic agility .....	67
A.4 Calculating the hash value using SHA-256.....	67
A.5 Elliptic curve cryptography.....	67
A.6 ECDH key exchange method .....	68
A.7 AES-CBC-128 symmetric cryptosystem.....	68
A.8 ECDSA signature method .....	69
A.9 X.509 v3 certificates .....	69
A.10 PKCS#12 .....	69
A.11 OCSP.....	69
A.12 Generating cryptographically secure random numbers .....	70
A.13 Handling static private keys.....	72
Annex B (informative) Motivation for non-functional characteristics from the perspective of a vehicle manufacturer and mobility operator.....	73
B.1 Non-functional characteristics from the perspective of a vehicle manufacturer.....	73
B.2 Non-functional characteristics from the perspective of a mobility operator or PKI operator .....	73
Annex C (informative) Providing PE certificates for charging using private infrastructure .....	75
C.1 Different starting point from public charging.....	75
C.2 Pre-requisites for private charging .....	76
C.3 Providing a private operator root CA certificate for charging using private infrastructure.....	77
C.3.1 Reasons for provisioning.....	77
C.3.2 Types of provisioning.....	77

	Page
C.3.3 Provisioning via private charging infrastructure (Annex E.2.2 of DIN EN ISO 15118-2:2016-08, pairing) .....	77
C.3.3.1 Provisioning process (pairing).....	77
C.3.3.2 Risk analysis for provisioning of the private operator root CA certificate with pairing as per DIN EN ISO 15118-2:2016-08 .....	81
C.3.4 Provisioning of trust anchors (root CA certificates) of a private operator via a central and authentic distribution point and an authentic online connection to the vehicle .....	82
C.4 Provisioning a root CA certificate to authorise an EV for energy transfer .....	88
Bibliography .....	90
<b>Bilder</b>	
Figure 1 – Scope of DIN EN ISO 15118 (all parts) .....	8
Figure 2 – Use of contract data from various CCPs (roaming) .....	20
Figure 3 – Overview of the various certificate types used in accordance with DIN EN ISO 15118 2: 15118-2 in the Plug & Charge authentication and authorisation modes (source: DIN EN ISO 15118 2: 15118-2) .....	23
Figure 4 – Example of validating a CPS leaf certificate as per shell model.....	28
Figure 5 – Options for providing contract certificates.....	30
Figure 6 – Overall system approach to facilitate the Plug & Charge process.....	34
Figure 7 – Breaking the preparation of contract-based public charging and billing down into sub-processes .....	35
Figure 8 – Producing and delivering root certificates used for public charging and contract-based billing (only one root certificate per market role is illustrated).....	36
Figure 9 – Producing the vehicle and signing the contract .....	38
Figure 10 – Assigning the vehicle to a contract .....	41
Figure 11 – Possible contract composition.....	43
Figure 12 – Periodically providing a contract certificate .....	44
Figure 13 – Elements of the Contract Certificate Bundle .....	44
Figure 14 – Elements of the Signed Contract Certificate Bundle.....	45
Figure 16 – Steps for creating the signature of a CertificateInstallationRes .....	51
Figure 17 – Periodically providing a Signed Contract Certificate Bundle.....	52
Figure 18 – Periodically saving contract certificates .....	53
Figure 19 – Delivering a contract certificate upon request.....	56
Figure 20 – Contract certificate revocation via the mobility operator .....	60
Figure C1 – PE pairing as per Annex E2.2 according to DIN EN ISO 15118-2:2016-08 .....	79
Figure C.2 – Example of providing trust anchors (root CA certificates) of a private operator via a central and authentic distribution point and an authentic online connection to the vehicle .....	85
<b>Tabellen</b>	
Table 1 – List of possible status messages exchanged through the message broker .....	62
Table A.1 – Possible classes of random number generators.....	70
Table A.2 – Handling static private keys .....	72
Table C.1 – Example of an implementation of a trust store container for providing CA certificates of the manufacturer of the private supply equipment or of a private operator for a receiver .....	83