

## Anwendungsbeginn

Anwendungsbeginn der VDE-Anwendungsregel ist 2017-10-01.

### Inhalt

	Seite
Vorwort.....	7
Einleitung .....	8
1 Anwendungsbereich .....	10
2 Normative Verweisungen .....	10
3 Begriffe und Abkürzungen .....	11
3.1 Begriffe .....	11
3.2 Abkürzungen .....	12
4 Betrieb einer Public-Key-Infrastruktur (PKI) .....	13
5 Involvierte Akteure im Elektromobilitätsmarkt im Kontext von Plug & Charge.....	15
5.1 Endkunde .....	15
5.2 Automobilhersteller (OEM) .....	15
5.3 Mobility Operator (MO).....	15
5.4 Charge Point Operator (CPO).....	16
5.5 Betreiber des Certificate Provisioning Service (CPS) .....	16
5.6 Betreiber des Contract Certificate Pools (CCP) .....	16
5.7 Betreiber des OEM Provisioning Certificate Pools.....	18
5.8 Betreiber der V2G Root CA .....	18
5.9 Nicht enthaltene Rollen .....	19
6 Beschreibung der aus DIN EN ISO 15118-2 abgeleiteten PKI .....	19
6.1 Plug & Charge zur Erfüllung eines sicheren und nutzerfreundlichen Ladeerlebnisses .....	19
6.2 Zertifikatstypen der im Kontext nach DIN EN ISO 15118-2 definierten PKIs.....	20
6.2.1 Überblick über die Zertifikatstypen .....	20
6.2.2 V2G-Root-CA-Zertifikat .....	21
6.2.3 MO-Root-CA-Zertifikat.....	22
6.2.4 Vertragszertifikat (Contract Certificate) .....	22
6.2.5 Ladestationszertifikat (EVSE Leaf Certificate) .....	22
6.2.6 OEM-Provisioning-Zertifikat (OEM Prov Certificate).....	22
6.2.7 OEM-Root CA-Zertifikat .....	23
6.2.8 Vertrags-Bereitstellungs-Zertifikat (Leaf Prov Certificate).....	23
6.2.9 PE Private-Operator-Root-CA-Zertifikat.....	23
6.3 Nicht-funktionale Eigenschaften der PKI.....	23
6.3.1 Funktionale Eigenschaften als Resultat unterschiedlicher Marktinteressen .....	23
6.3.2 Speichergröße eines einzelnen Zertifikats .....	23

	Seite
6.3.3	Länge einer Zertifikatskette..... 24
6.3.4	Anzahl der Root-CA-Zertifikate ..... 24
6.3.5	Gültigkeitsdauer eines V2G-Root-CA-Zertifikats ..... 24
6.3.6	Gültigkeitsdauer von Zwischenzertifikaten (Sub-CA-Zertifikate) ..... 25
6.3.7	Gültigkeit eines OEM-Provisioning-Zertifikats..... 25
6.3.8	Gültigkeit von Vertragszertifikaten ..... 25
6.3.9	Gültigkeit von Ladestationszertifikaten ..... 25
7	Gültigkeitsprüfung ..... 26
7.1	Definition einer Gültigkeitsprüfung ..... 26
7.2	Gültigkeitsmodelle als Vorgabe für die Zertifikatsprüfung ..... 26
7.2.1	Arten von Gültigkeitsmodellen ..... 26
7.2.2	Kettenmodell ..... 26
7.2.3	Schalenmodell..... 27
7.2.4	Hybridmodell (Kompromissmodell)..... 28
7.2.5	Umsetzung von Gültigkeitsprüfungen ..... 29
8	Installation von Zertifikaten ..... 29
8.1	Installation von Vertragszertifikaten ..... 29
8.2	Installation von Root-CA-Zertifikaten ..... 29
9	Bereitstellung von Zertifikaten der PKI..... 30
9.1	Möglichkeiten der Bereitstellung von Vertragszertifikaten ..... 30
9.2	Detaillierte Beschreibung der Kategorien ..... 31
9.2.1	Bewertungsmatrix für die Installationsvarianten eines Vertragszertifikats..... 31
9.2.2	OEM-Backend und Telematiklink des Automobilherstellers ..... 31
9.2.3	Webseite des Automobilherstellers..... 33
9.2.4	Mobiles Endgerät des Fahrzeugnutzers ..... 33
9.2.5	DIN EN ISO 15118 (alle Teile) Ladeschnittstelle ..... 33
9.2.6	Service-Schnittstelle in der Autowerkstatt..... 33
9.3	PE-Zertifikate für das Laden an privater Infrastruktur bereitstellen ..... 34
9.3.1	Geänderte Ausgangslage gegenüber dem öffentlichen Laden ..... 34
9.3.2	Vorbedingungen für ein privates Laden ..... 35
9.3.3	Private-Operator-Root-CA-Zertifikat für das Laden an der privaten Infrastruktur bereitstellen ..... 36
10	Aufbau der PCID ..... 39
11	Prozesse für die Bereitstellung der Zertifikatstypen für öffentliches Laden ..... 40
11.1	Gesamtsystem mit asynchronem Datenfluss..... 40
11.2	Vertragsbasiertes öffentliches Laden und vertragsbasiertes Abrechnen vorbereiten ..... 41
11.2.1	Vorbereitung in Teilabläufe zerlegen ..... 41
11.2.2	Root-Zertifikate für öffentliches Laden und vertragsbasiertes Abrechnen bereitstellen ..... 42
11.2.3	Fahrzeug produzieren und Vertrag abschließen ..... 44

	Seite
11.2.4 Fahrzeug einem Vertrag zuordnen.....	46
11.3 Vertragszertifikat für die automatisierte Abrechnung bereitstellen.....	48
11.3.1 Zertifikatsbereitstellung in Teilabläufe zerlegen.....	48
11.3.2 Zusammenhang von Vertrag, Abrechnung, Fahrzeug- und Vertragszertifikat .....	48
11.3.3 Vertragszertifikat periodisch bereitstellen .....	50
11.3.4 Vertragszertifikat auf Anfrage ausliefern .....	58
12 Zurückziehen von Zertifikaten (Revocation).....	62
12.1 Motivation .....	62
12.2 Rücknahme von Vertragszertifikaten für das Plug-&-Charge-Verfahren .....	63
12.2.1 Ablauf der Rücknahme von Vertragszertifikaten.....	63
12.2.2 Vorbedingungen .....	63
12.2.3 Vertragszertifikat vom Mobility Operator zurückziehen lassen und Zertifikats-Sperlliste erzeugen.....	63
12.2.4 Zertifikats-Sperlliste für ein zurückgezogenes Vertragszertifikat ausliefern .....	64
13 Ausblick .....	65
13.1 Vorgehensweise bei der Erarbeitung noch offener Punkte.....	65
13.2 Installation und Nutzung mehrerer Vertragszertifikate im Fahrzeug.....	65
13.3 Verwendung von XSD-Schemadateien.....	65
13.4 Challenge-Response Authentifizierung in privater Umgebung (PE).....	67
13.5 Nicht nur Vertragszertifikat auf Anfrage ausliefern sondern definierte Daten bei vorgegebenen Zustandsänderungen .....	67
Anhang A (normativ) Kryptographische Mechanismen und Sicherheitsparameter.....	69
A.1 Fokus auf Securityaspekte .....	69
A.2 IT-Sicherheit zwischen Elektrofahrzeug und Ladeinfrastruktur im Allgemeinen.....	69
A.3 Kryptografische Agilität.....	70
A.4 Hash-Wert-Berechnung mittels SHA-256.....	70
A.5 Elliptische-Kurven-Kryptografie .....	71
A.6 ECDH Schlüsselaustauschverfahren .....	71
A.7 Symmetrisches Kryptoverfahren AES-CBC-128.....	71
A.8 ECDSA Signaturverfahren.....	72
A.9 X.509v3-Zertifikate .....	72
A.10 PKCS#12.....	73
A.11 OCSP.....	73
A.12 Erzeugen von kryptographisch sicheren Zufallszahlen.....	73
Anhang B (normativ) Motivation nicht-funktionaler Eigenschaften aus Sicht eines Automobilherstellers und Mobility Operators .....	75
B.1 Anforderungen aus Sicht eines Automobilherstellers .....	75
B.2 Anforderungen aus Sicht eines Mobility Operators bzw. PKI-Betreibers.....	75
Anhang C (normativ) Gültigkeitsmodelle .....	77
C.1 Kettenmodell.....	77

	Seite
C.2 Schalenmodell.....	77
C.3 Kompromissmodell (Hybridmodell) .....	78
Literaturhinweise .....	80
<b>Bilder</b>	
Bild 1 – Anwendungsbereich DIN EN ISO 15118 (alle Teile) .....	9
Bild 2 – Benutzung von Vertragsdaten aus unterschiedlichen CCPs (Roaming) .....	18
Bild 3 – Überblick über die diversen Zertifikatstypen, welche nach DIN EN ISO 15118-2 beim Plug&Charge-Authentifizierungs- und Autorisierungsmodus zum Einsatz kommen (Quelle: DIN EN ISO 15118-2).....	21
Bild 4 – Beispiel der Gültigkeitsprüfung nach Kettenmodell eines Vertrags-Bereitstellungs-Zertifikats .....	27
Bild 5 – Beispiel der Gültigkeitsprüfung nach Schalenmodell eines Vertrags-Bereitstellungs- Zertifikats.....	27
Bild 6 – Beispiel der Gültigkeitsprüfung nach Kompromissmodell eines Vertrags-Bereitstellungs-Zertifikats .....	28
Bild 7 – Möglichkeiten der Bereitstellung von Vertragszertifikaten .....	30
Bild 8 – Gesamtsystem einer optimierten PKI für das Plug&Charge-Verfahren .....	41
Bild 9 – Vertragsbasiertes öffentliches Laden und vertragsbasiertes Abrechnen vorbereiten in Teilabläufe zerlegen .....	42
Bild 10 – Root-Zertifikate für öffentliches Laden und vertragsbasiertes Abrechnen produzieren, liefern und gleichzeitig Vertrag abschließen .....	43
Bild 11 – Fahrzeug produzieren und Vertrag abschließen .....	44
Bild 12 – Fahrzeug einem Vertrag zuordnen.....	47
Bild 13 – Vertragszertifikat für die automatisierte Abrechnung bereitstellen in Teilabläufe zerlegen .....	48
Bild 14 – Mögliche Zusammensetzung eines Vertrages .....	49
Bild 15 – Vertragszertifikat periodisch bereitstellen (CertificateInstallation) .....	50
Bild 16 – Bestandteile der übertragenen Vertragsdaten .....	51
Bild 17 – Bestandteile der übertragenen SignedContractData .....	51
Bild 18 – Vertragszertifikat periodisch bereitstellen .....	52
Bild 19 – Schritte zur Erstellung der Signatur einer CertificateInstallationRes .....	55
Bild 20 – Vertragsdaten periodisch signieren.....	56
Bild 21 – Vertragszertifikat periodisch speichern .....	58
Bild 22 – Vertragszertifikat auf Anfrage ausliefern .....	61
Bild 23 – Zurückziehen eines Vertragszertifikats über den Mobility Operator .....	63
Bild C.1 – Prüfung nach reinem Kettenmodell (gültig), Sub-CA-Zertifikat ist länger gültig als sein Aussteller.....	77
Bild C.2 – Prüfung nach reinem Kettenmodell (ungültig), Signaturzeitpunkt des Sub-CA 2-Zertifikats nach Ablauf der Gültigkeit des Sub-CA 1 Zertifikats.....	77
Bild C.3 – Prüfung nach Schalenmodell (gültig), Sub-CA-Zertifikate gültig, Authentisierung erfolgreich.....	78
Bild C.4 – Prüfung nach Schalenmodell (ungültig), Sub-CA 1-Zertifikat gesperrt, Massensperrung als Folge.....	78
Bild C.5 – Prüfung nach Kompromissmodell (gültig), Nutzerdokumente nicht länger gültig als ihr Aussteller.....	79

	Seite
Bild C.6 – Prüfung nach Kompromissmodell (ungültig), Nutzerdokumente nicht länger gültig als ihr Aussteller .....	79
<b>Tabellen</b>	
Tabelle 1 – Bewertungsmatrix für die Installationsvarianten eines Vertragszertifikats .....	32