

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH  
bescheinigt hiermit dem Unternehmen

**Volkswagen AG**  
**Berliner Ring 2**  
**38436 Wolfsburg**

für den Vertrauensdienst

**VW Car2X PKI**  
**Root-CA, RA und PCA Dienst**

die Erfüllung aller relevanten Anforderungen der  
Zertifizierungspolitik

**(draft) certificate policy for the  
European C-ITS trust model based  
on public key infrastructure**

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht  
aus 4 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.



**Certificate ID: 01113.20**

© TÜVIT - TÜV NORD GROUP - [www.tuvit.de](http://www.tuvit.de)

Zertifikat gültig bis  
29.04.2021

21

Essen, 29.04.2020

Dr. Christoph Sutter  
Leiter Zertifizierungsstelle

**TÜV Informationstechnik GmbH**  
TÜV NORD GROUP  
Langemarckstraße 20  
45141 Essen  
[www.tuvit.de](http://www.tuvit.de)

Zertifikat

## Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Zertifizierungsprogramms durch:

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.0 vom 24.08.2015, TÜV Informationstechnik GmbH

## Prüfbericht

- „Audit Report – Initial Audit – Certificate Policy C-ITS TUVIT.01113.C-ITS, Root-CA service of VW Car2X PKI“, Version 1.1 vom 23.04.2020, TÜV Informationstechnik GmbH
- „Audit Report – Initial Audit – Certificate Policy C-ITS TUVIT.01113.C-ITS, RA and PCA service of VW Car2X PKI“, Version 1.1 vom 23.04.2020, TÜV Informationstechnik GmbH

## Prüfanforderungen

Die Prüfanforderungen sind in dem Dokument: (draft) certificate policy for the European C-ITS trust model based on public key infrastructure (C-ITS CP):

- Anhang 3 der COMMISSION DELEGATED REGULATION (EU) .../... vom 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems, C(2019) 1789 final

für die folgenden Elemente des C-ITS Trust Modells definiert:

- Root-CA,
- Enrolment Authority (EA),
- Authorisation Authority (AA).

## Prüfgegenstand

Der Prüfgegenstand wird charakterisiert durch die Zertifikatsinformation des untersuchten Vertrauensdienstes:

### Root-CA, RA and PCA service of VW Car2X PKI:

#### 1) Root-CA

<u>Aussteller des Zertifikats (id Name):</u> <b>rca.volkswagen.de</b>	
SHA-256 Hashwert: 1CDB077C56197034A5D667A71C87EBF53DD04B6F6126442E C051E7A33B7E6FAA	
ID Name	SHA-256 Hashwert
<b>rca.volksw agen.de</b>	1CDB077C56197034A5D667A71C87EBF53DD04 B6F6126442EC051E7A33B7E6FAA

#### 2) Registration Authority (RA)

<u>Aussteller des Zertifikats (id Name):</u> <b>rca.volkswagen.de</b>	
SHA-256 Hashwert: 1CDB077C56197034A5D667A71C87EBF53DD04B6F6126442E C051E7A33B7E6FAA	
ID Name	SHA-256 Hashwert
<b>VWG_CAR 2X_LIVE_ PRD_CXEA RA_001</b>	D5FCE25DAE2A8C38344D7B0BA89B013A100A 0EF87B7AB3B2C65A9643D9E21774

#### 3) Pseudonym CA (PCA)

<u>Aussteller des Zertifikats (id Name):</u> <b>rca.volkswagen.de</b>	
SHA-256 Hashwert: 1CDB077C56197034A5D667A71C87EBF53DD04B6F6126442E C051E7A33B7E6FAA	
ID Name	SHA-256 Hashwert
<b>VWG_CAR 2X_LIVE_ PRD_CXPS CA_001</b>	1A269B077C20BBD2AD2702B79729DE6FCA4C 9EF1BAE0752EDDC63E576A4F4487

zusammen mit der Dokumentation des Betreibers:

- „Volkswagen Group Product Public Key Infrastructure – Certification Practice Statement (CPS) for the Car2X – Root-CA of the Volkswagen Group Product-PKI“, Version 1.0 vom 20.11.2019, Volkswagen AG
- „Volkswagen AG Car2X Public Key Infrastructure – Certification Practice Statement for the RA and PCA services“, Version 0.5 vom 23.09.2019, Technology Nexus Secured Business Solutions AB

### **Prüfergebnis**

- Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien.
- Die im Zertifizierungsprogramm definierten Zertifizierungsanforderungen sind erfüllt.

## **Zusammenfassung der Prüfanforderungen**

Die C-ITS CP enthält Anforderungen an Vertrauensdienste unter folgenden Überschriften:

- 1 Einleitung**
- 2 Verantwortlichkeiten für Veröffentlichungen und Verzeichnisse**
- 3 Identifizierung und Authentifizierung**
- 4 Betriebsanforderungen für den Lebenszyklus des Zertifikats**
- 5 Anlagen-, Management- und Betriebskontrollen**
- 6 Technische Sicherheitskontrollen**
- 7 Zertifikatsprofile, CRL und CTL**
- 8 Compliance-Audit und andere Bewertungen**
- 9 Sonstige Bestimmungen**
- 10 Referenzen**