

Volkswagen Public Key Infrastructure

- Anlage 1 zur CP der Volkswagen PKI

Version 1.0.2.5

VOLKSWAGEN

AKTIENGESELLSCHAFT

Change - History			
	Date	Author	Remarks
1.0	20.08.2012	Henning Boost	First Draft
1.0.2.1	02.12.2013	Uwe-Jens Hofmann	CA-Baum aktualisiert
1.0.2.2	31.01.2014	Uwe-Jens Hofmann	Ausgabedatum für CP aktualisiert
1.0.2.3	09.04.2014	Uwe-Jens Hofmann	Kurzbeschreibung der CA-Verwendung zugefügt
1.0.2.4	12.12.2014	Liebe, Michael (K-SIS-O/2)	Kurzbeschreibung der MS-CAs angepasst
1.0.2.5	25.02.2015	Feige, Jan-Patrick	VW-CA-ENCM hinzugefügt

1 Einleitung

Das vorliegende Dokument dient als Anlage zur Certificate Policy für die Volkswagen PKI, [3] und fasst Informationen zusammen, die sich im Laufe der Gültigkeit der CP ändern können.

Die Anlage wird an gleicher Stelle wie die CP veröffentlicht und bei Bedarf aktualisiert.

2 Bereich

Im Folgenden sind die am 01.12.2013 geltenden Informationen dargestellt.

2.1 Ansprechpartner

Die in diesem Kapitel wiedergegebenen Informationen vervollständigen die in Kapitel 1.5.2 der CP dokumentierten Informationen und definieren den Ansprechpartner für die CP.

Ansprechpartner für die Certificate Policy der Volkswagen PKI:

Volkswagen AG

Informationssicherheit Services / Authentication & Encryption Services

Brieffach 1248

38436 Wolfsburg

mailto: pki.r.wob@volkswagen.de

Intranet: <http://intranet.pki.vw.vwg>

2.2 Zertifizierungsstellen (CA)

Die in diesem Kapitel wiedergegebenen Informationen vervollständigen die in Kapitel 1.3.1 der CP dokumentierten Informationen.

In der folgenden Abbildung wird die aktuelle CA-Hierarchie der Volkswagen AG dargestellt und die CAs unterhalb der VW-CA-ROOT (Sub-Cas) benannt. Dabei kennzeichnet <xxxx> den Hauptzweck der durch die CA ausgegebenen Zertifikate, <nn> eine fortlaufende Nummer, <y> eine Gesellschaft der Volkswagen AG und <Vn.n> die durch Microsoft CA-Dienste automatisch vergebene Versionsnummer der CA-Instanz.

VOLKSWAGEN

AKTIENGESELLSCHAFT

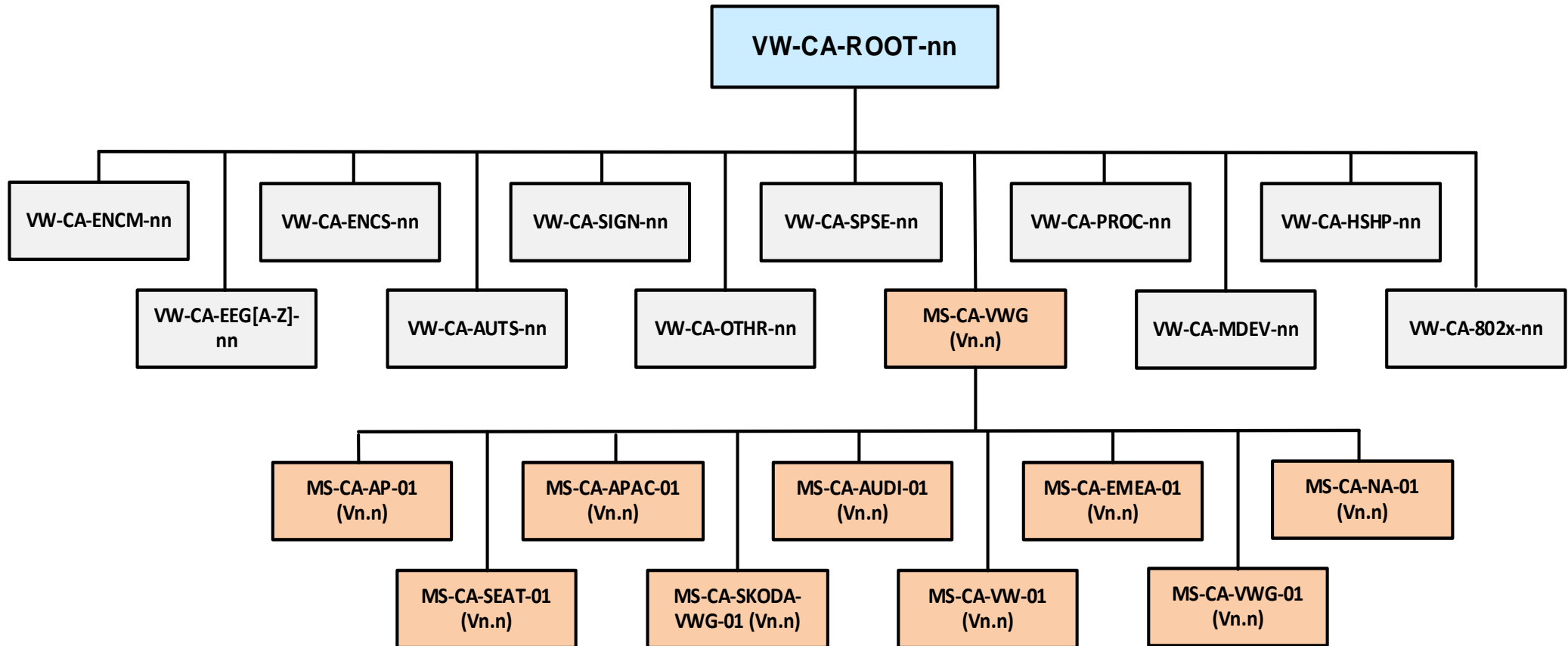


Abbildung 1 – CA Typen-Hierarchie der Volkswagen PKI

Die CAs dienen zur Signierung von Zertifikaten unterschiedliche Anwendungsbereiche: Die Aufgabenbereiche sind hauptsächlich:

VW-CA-ROOT-*nn*

- Sub-CAs
- End-Entitäten, die für die Funktionen der PKI-Software benötigt werden

VW-CA-ENCM-*nn*

Verschlüsselungszertifikate für Normal-Karten

Diese CAs werden erst ab der VW-CA-ROOT-05 verwendet.

VW-CA-EEG[A-Z]-*nn*

[A-Z] ist ein Kennbuchstabe für das jeweilige E-Mail-Verschlüsselungs-Gateway.

- Verschlüsselungszertifikate in E-Mail-Verschlüsselungs-Gateways

VW-CA-ENCS-*nn*

- Verschlüsselungszertifikate für Versandkarten

Diese CAs werden erst ab der VW-CA-ROOT-05 verwendet.

VW-CA-AUTS-*nn*

- Authentifikationszertifikate für Versandkarten

Diese CAs werden erst ab der VW-CA-ROOT-05 verwendet.

VW-CA-SIGN-*nn*

- Signaturzertifikate für Normal-Karten (persönlich übergebene PKI-Karten)

VW-CA-OTHR-*nn*

- Authentifikationszertifikate und Verschlüsselungszertifikate für Normal-Karten (persönlich übergebene PKI-Karten)

VW-CA-SPSE-*nn*

- Software-Zertifikate (Soft-PSEs) für Personen

VW-CA-PROC-nn

- Zertifikate für Anwendungen, Prozesse oder Organisationseinheiten

VW-CA-MDEV-nn

- Zertifikate für mobile Geräte, die nicht die Anforderungen für eine Einwahl in das interne WLAN des Volkswagen Konzerns erfüllen

VW-CA-HSHP-nn

- Authentifikationszertifikate und Verschlüsselungszertifikate für Versandkarten

Diese CAs werden nur bis zur VW-ROOT-CA-04 verwendet.

VW-CA-802x-nn

- Gerätezertifikate für Geräte, die die Anforderungen für eine Verbindung mit dem internen Netz des Volkswagen Konzerns erfüllen und die nicht in einen Microsoft-AD verwaltet werden

MS-CA-VWG (Vn.n)

- Zertifikate für andere CAs, die durch einen Microsoft Certification Service betrieben werden

Diese CA dient als Policy-CA für die CAs, deren Zertifikate von ihr signiert werden.

MS-CA-<x...x>-01 (Vn.n)

<x...x> ist die Bezeichnung der jeweiligen Microsoft Active Directory Domain, innerhalb der die CA betrieben wird.

- Gerätezertifikate für Geräte, die in der lokalen Active Directory Domain verwaltet werden
- Zertifikate für Domain Controller, Exchange Server sowie weitere TLS Anwendungsfälle im jeweiligen Active Directory

2.3 Quellenverzeichnis

Im Folgenden sind die für die CP und die Anlage geltenden Quellen aufgeführt

Nr.	Titel	Genauere Dokumentenbezeichnung, Document-ID (OID, falls vorhanden)	Version, Datum
[1]	Datenschutzrichtlinie	Organisations-Anweisung Nummer 50/1 Sicherung der Informationsverarbeitung	Februar 2006
		Organisations-Anweisung Nummer 51/1 Betriebssicherstellung der Informationsverarbeitung	Juli 2007
[2]	IT-Sicherheitskonzept	Geschäftsprozesshandbuch Informationstechnik (IT)-Sicherheitsregelwerk	November 2013
[3]	Certificate Policy	Certificate Policy für die Volkswagen PKI OID 1.3.6.1.4.1.3210.1883.20.1.1.2.1.1.1.0	Januar 2014