Bundesverwaltungsamt

Referat D III 1: Registermodernisierung;
Anschlussunterstützung

Zertifikate für den Anschluss von Data Providern an das Nationale Once-Only-Technical-System (NOOTS)

Version 2.3
11.09.2026

Das vorliegende Dokument wurde durch das Bundesverwaltungsamt in Zusammenarbeit mit der Firma Dataport AöR erstellt.

Ansprechpartner/-in:

Referat D III 1: Registermodernisierung; Anschlussunterstützung
Bundesverwaltungsamt
E-Mail: noots.umsetzung@bva.bund.de

Inhaltsverzeichnis

1. Einleitung 4

2. Zertifikatsbeschaffung: Übersicht über die Zertifikate 6

2.1. Zertifikate für die technische Kommunikation 6

3. Anforderungen an die Zertifikate 9

3.1. Zertifikate für die Kommunikation mit dem NOOTS 11

4. Abkürzungsverzeichnis 15

5. Abbildungsverzeichnis 16

6. Anhang 17

6.1. Vertrauenswürdige Root-Certification-Authorities 17

6.1.1 Häufig genutzte deutsche Root-CAs 17

6.2. Vollständige Liste der Trust Anchors 18

1. Einleitung

Dieses Dokument gibt betrieblich verantwortlichen Stellen eines **Data Provider (DP)** einen Überblick über die bei dem Anschluss an das NOOTS zu erwerbenden Zertifikate zur NOOTS-Kommunikation. Eine Anleitung zur Beschaffung der V-PKI/DOI-CA (Public Key Infrastruktur der Verwaltung) Zertifikate, welche für die NOOTS-Registrierung und technische NOOTS-Kommunikation benötigt werden, sowie ein mögliches Vorgehen zur Signierung des Registrierungsformulars über noots.gov.de sind dem „Vertiefungsleitfaden für die Beschaffung von V-PKI Zertifikaten für Data Consumer und Data Provider für den Anschluss an das NOOTS“ zu entnehmen. Dieses Dokument wird zur Verfügung gestellt, um eine Beschaffung der Zertifikate, welche teilweise mehrere Wochen in Anspruch nehmen kann, frühzeitig zu unterstützen.

DP sind NOOTS-Teilnehmer zur Lieferung von Nachweisen. Data Consumer (DC) sind NOOTS-Teilnehmer zum Abruf von Nachweisen und können Online-Dienste, Fachverfahren und die Intermediäre Plattform sein.

Die Rollen und Zuständigkeiten gliedern sich dabei wie folgt:

- Fachlich Verantwortliche sind die für das technische Verfahren verantwortlichen nachweisanfordernden oder -liefernden Stellen.

- Die das technische Verfahren im Auftrag der fachlich Verantwortlichen Betreibenden sind die betrieblich Verantwortlichen. Sie verantworten den technisch korrekten Betrieb des DC/DP und des Sicheren Anschlussknotens.

Das NOOTS ist ein gemeinsames informationstechnisches System, das aus IT-Komponenten, Schnittstellen und Standards besteht. Es ermöglicht öffentlichen Stellen den Abruf sowie die Übermittlung elektronischer Nachweise und Daten aus öffentlichen Datenbeständen – sowohl national als auch EU-weit – zur Erfüllung ihrer öffentlichen Aufgaben. Das NOOTS 1.0, dessen Produktivsetzung für den 30.11.2026 geplant ist, wird aus den technischen Komponenten Identity und Access Management für Behörden (IAM-B), Registerdatennavigation (RDN) und Vermittlungsstelle (VS) bestehen sowie den Abruf der Identifikationsnummer (IDNr.-Abruf) über das Identity Management für Personen (IDM-P) beinhalten. Darüber hinaus werden Sichere Anschlussknoten (SAK) für DC (SAK-DC) und DP (SAK-DP) zur Verfügung gestellt (Abbildung 1). In der aktuellen

Iteration sind nur Onlinedienste als DC vorgesehen. Die Darstellung ist zur Übersichtlichkeit und Verständlichkeit in ihrer Komplexität vereinfacht.

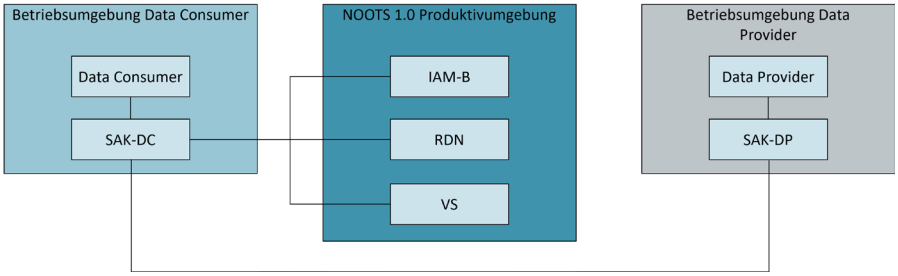

Abbildung 1 - Grobübersicht NOOTS 1.0

In diesem Dokument wird vorausgesetzt, dass das System NOOTS mit seinen Komponenten und Teilnehmenden (z.B. DC) grundsätzlich bekannt ist. Sofern dies nicht der Fall ist, wird hierzu auf die weitere Begleitdokumentation sowie auf die Informationen des Bundesverwaltungsamts und des Bundesministeriums für Digitalisierung und Staatsmodernisierung verwiesen.

Es gibt drei NOOTS-Umgebungen, an die DP aufeinanderfolgend angebunden werden müssen:

- NOOTS Referenzumgebung
- NOOTS Testumgebung
- NOOTS Produktivumgebung

Die zentrale NOOTS-Registrierung der anzuschließenden Teilnehmer und automatisierte Weiterverarbeitung der Anschlussdaten erfolgt über noots.gov.de.

2. Zertifikatsbeschaffung: Übersicht über die Zertifikate

HINWEIS: Für den **Anschluss** an das **NOOTS** benötigen Sie bestimmte **Zertifikate**, die Sie **selbst beschaffen** müssen. Der Erwerb der Zertifikate nimmt eine **gewisse Zeit in Anspruch**, sodass wir Ihnen empfehlen, den Prozess der Beschaffung noch in der Phase der technischen Anschlussvorbereitung anzustoßen.

Für den Anschluss an das NOOTS benötigen Sie unterschiedliche Zertifikate, deren Beschaffung frühzeitig eingeleitet werden sollte. Die Beschaffung übernehmen in der Regel die betrieblich Verantwortlichen in Abstimmung mit bzw. im Auftrag der fachlich Verantwortlichen. Für ein optionales Zertifikat ist abweichend vorgesehen, dass die Beschaffung durch die fachlich Verantwortlichen erfolgt.

Für den Anschluss an das NOOTS benötigen Sie Zertifikate für zwei voneinander unabhängige Zwecke:

- Zur NOOTS-Registrierung
- Für die technische NOOTS-Kommunikation

Die **Zertifikate** für die **NOOTS-Registrierung** werden ausschließlich **im Anschlussprozess** benötigt (die Beschaffung der Zertifikate für die NOOTS-Registrierung wird in diesem Leitfaden nicht weiter berücksichtigt. Eine Schritt-für-Schritt-Anleitung ist hier zu finden: „Vertiefungsleitfaden für die Beschaffung von V-PKI Zertifikaten für Data Consumer und Data Provider für den Anschluss an das NOOTS“.). Die **Zertifikate** für die **technische Kommunikation** sind **dauerhaft** bei erfolgtem Anschluss an das NOOTS im Einsatz.

Hinweis: Bitte berücksichtigen Sie, dass Zertifikate grundsätzlich eine begrenzte Gültigkeitsdauer besitzen. Prüfen Sie daher immer eigenverantwortlich, welche Ihrer verwendeten Zertifikate wann ablaufen und welche Schritte für die rechtzeitige Verlängerung erforderlich sind.

2.1. Zertifikate für die technische Kommunikation

Für die technische Kommunikation mit dem NOOTS benötigen der DC und DP unterschiedliche Zertifikate.

Hier finden Sie einen Überblick für die NOOTS Produktivumgebung:

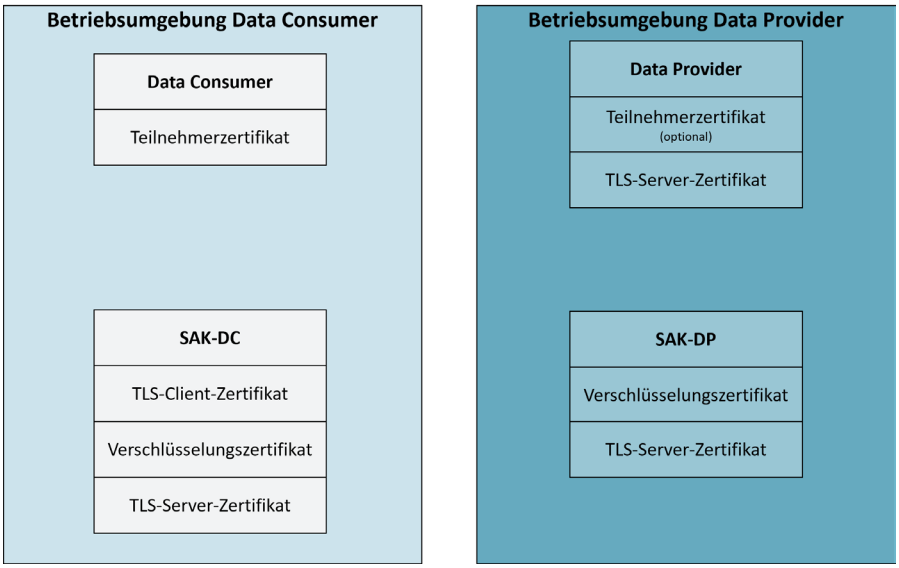

Abbildung 2 - Übersicht Zertifikate NOOTS Produktivumgebung

Für einen DP werden für die Kommunikation mit dem NOOTS insgesamt acht Zertifikate benötigt, von denen eines für Sie bereitgestellt wird. Somit ist die Beschaffung von sieben Zertifikaten zwingend durch Sie erforderlich. Bei dem Teilnehmerzertifikat des DP für alle Umgebungen und dem TLS-Server-Zertifikat des DP für die NOOTS Referenzumgebung handelt es sich um zusätzliche optionale Zertifikate, welche nicht zwingend beschafft werden müssen. Das Verschlüsselungszertifikat des SAK-DP für die NOOTS Referenzumgebung wird Ihnen zur Verfügung gestellt.

NOOTS Referenzumgebung	**NOOTS Testumgebung**	**NOOTS Produktivumgebung**
Teilnehmerzertifikat des DP (optional)	Teilnehmerzertifikat des DP (optional)	Teilnehmerzertifikat des DP (optional)
TLS-Server-Zertifikat des DP (optional)	TLS-Server-Zertifikat des DP	TLS-Server-Zertifikat des DP
TLS-Server-Zertifikat des SAK-DP	TLS-Server-Zertifikat des SAK-DP	TLS-Server-Zertifikat des SAK-DP

Verschlüsselungs-zertifikat des SAK-DP (wird bereitgestellt)	Verschlüsselungs-zertifikat des SAK-DP	Verschlüsselungs-zertifikat des SAK-DP

Tabelle 1 - Übersicht Zertifikate DP

- Mit dem Teilnehmerzertifikat kann der DP den Nachweis siegeln, bevor er ihn als Bestandteil der Nachweisantwort an den SAK-DP übermittelt.
- Das TLS-Server-Zertifikat des DP dient ausschließlich der Kommunikation zwischen dem DP und dem SAK-DP innerhalb der Betriebsumgebung des DP.
- Das TLS-Server-Zertifikat des SAK-DP ermöglicht eine Transportverschlüsselung.
- Das Verschlüsselungszertifikat des SAK-DP ermöglicht zusätzlich zur sicheren mTLS-Verbindung eine Verschlüsselung der vom SAK-DC zum SAK-DP übermittelten Nachweisanfrage.

Die Beschaffung des optionalen Teilnehmerzertifikats des DP ist durch die fachlich Verantwortlichen vorgesehen.

Bei der Registrierung für die NOOTS Test- und Produktivumgebung müssen Sie das Verschlüsselungszertifikat des SAK-DP im PEM-Format angeben.

3. Anforderungen an die Zertifikate

In der nachfolgenden Tabelle finden Sie eine Übersicht über die gestellten Anforderungen, die in den nachfolgenden Abschnitten vertieft werden.

Umgebung	Zertifikat	Anforderung
NOOTS Referenzumgebung	Teilnehmerzertifikat des DP (optional)	für Siegelung geeignetes Zertifikat
	TLS-Server-Zertifikat des DP (optional)	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3)
	TLS-Server-Zertifikat des SAK-DP	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3) (weitere verpflichtende Eigenschaften siehe 3.1)
	Verschlüsselungszertifikat des SAK-DP	Bereitstellung durch Dataport
NOOTS Testumgebung	Teilnehmerzertifikat des DP (optional)	für Siegelung geeignetes Zertifikat
	TLS-Server-Zertifikat des DP	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3)
	TLS-Server-Zertifikat des SAK-DP	gruppenbezogenes Zertifikat (Test) der V-PKI/DOI-CA (CN: *GRP: „Name der Einrichtung“:SAK-DP:“Spezifikation des SAK-DP“,* Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403), TLS 1.3)
	Verschlüsselungszertifikat des SAK-DP	für Verschlüsselung geeignetes Zertifikat (Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403))

NOOTS Produktivumgebung	Teilnehmerzertifikat des DP (optional)	für Siegelung geeignetes Zertifikat
	TLS-Server-Zertifikat des DP	geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung (TLS 1.3)
	TLS-Server-Zertifikat des SAK-DP	gruppenbezogenes Zertifikat der V-PKI/DOI-CA (CN: *GRP: „Name der Einrichtung":SAK-DP:"Spezifikation des SAK-DP",* Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403), TLS 1.3)
	Verschlüsselungszertifikat des SAK-DP	für Verschlüsselung geeignetes Zertifikat (Hash-Algorithmus: SHA256, Schlüsseltyp (Signatur): ECC NIST P-256, Cipher Suite: ecdsa_secp256r1_sha256 (0x0403))

Tabelle 2 – Übersicht Anforderungen Zertifikate DP

Die nachfolgende Abbildung stellt die Kommunikation zwischen DC und DP beispielhaft für die NOOTS Produktivumgebung dar. Diese Darstellung ist zur Übersichtlichkeit und Verständlichkeit in ihrer Komplexität stark vereinfacht. Es sind nur diejenigen Zertifikate erwähnt, die durch DC bzw. DP zu beschaffen sind. Die Pfeile symbolisieren die Richtung des Verbindungsaufbaus.

3.1. Zertifikate für die Kommunikation mit dem NOOTS

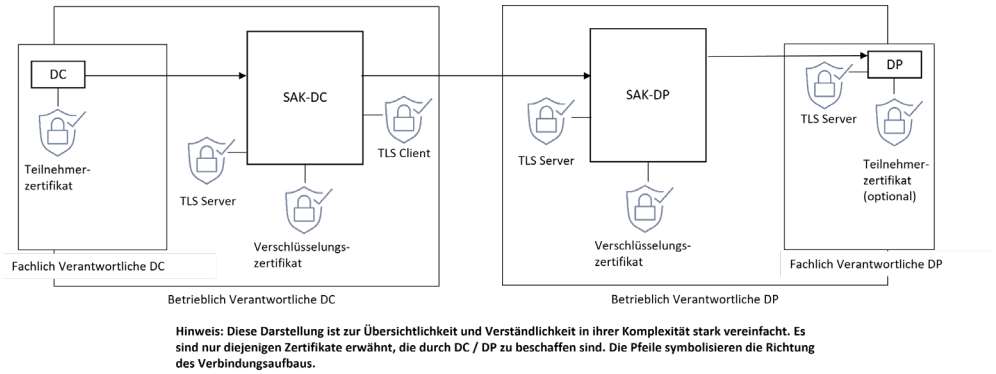

Abbildung 3 – Übersicht Komponenten und Zertifikate zur Beschaffung durch DC/DP in der NOOTS Produktivumgebung

HINWEIS: Generell ist zu beachten, dass für jeden Anwendungsfall ein separates Zertifikat zu beschaffen ist. Eine Wiederverwendung desselben Zertifikats für mehrere Anwendungsfälle ist nicht gestattet.

Beispielsweise ist es nicht zulässig, dasselbe TLS-Server-Zertifikat des SAK-DP für die NOOTS Test- und Produktivumgebung zu verwenden. Auch ist zum Beispiel ein TLS-Zertifikat entweder als Server-Zertifikat oder als Client-Zertifikat zu verwenden, eine gleichzeitige Verwendung für beide Zwecke ist nicht zulässig.

Für die NOOTS Referenzumgebung, NOOTS Test- und Produktivumgebung werden für die Zertifikate des DP in Teilen verschiedene Eigenschaften vorausgesetzt.

NOOTS Referenzumgebung

Bei dem **Teilnehmerzertifikat des DP** muss es sich um ein für Siegelung geeignetes Zertifikat handeln. Dieses Zertifikat ist auf der NOOTS Referenzumgebung nicht verpflichtend. Die Entscheidung über die Verwendung liegt in der Verantwortung des DP.

Das **TLS-Server-Zertifikat des DP** muss ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung sein. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt

den betrieblich Verantwortlichen. Das TLS-Server-Zertifikat des DP ist in der aktuellen Iteration des NOOTS für die NOOTS Referenzumgebung optional.

Bei dem **TLS-Server-Zertifikat des SAK-DP** handelt es sich auch um ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig. Darüber hinaus muss es folgende Anforderungen erfüllen:

- Die Zertifikatskette muss bis zu einer der im Anhang unter 6.1 aufgeführten Root-Certification-Authorities (Root-CAs) zurückverfolgt werden.
- Das End-Zertifikat sowie relevante Intermediate-Zertifikate müssen zum Zeitpunkt der Nutzung gültig sein.
- Das Zertifikat muss für TLS-Client-Authentifizierung geeignet sein (insbesondere EKU/KeyUsage, sofern vorhanden).
- Schlüssel- und Signaturalgorithmen dürfen nicht durch die Java-Sicherheitsrichtlinien gesperrt sein.

Das **Verschlüsselungszertifikat des SAK-DP** wird für die NOOTS Referenzumgebung bereitgestellt.

NOOTS Testumgebung

Bei dem **Teilnehmerzertifikat des DP** muss es sich um ein für Siegelung geeignetes Zertifikat handeln. Dieses Zertifikat ist auf der NOOTS Testumgebung optional. Die Entscheidung über die Verwendung liegt in der Verantwortung des DP.

Das **TLS-Server-Zertifikat des DP** muss ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung sein. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den betrieblich Verantwortlichen.

Das **TLS-Server-Zertifikat des SAK-DP** ist als gruppenbezogenes Zertifikat der V-PKI/DOI-CA zu beziehen. Für den Anschluss an die NOOTS Testumgebung ist in diesem Fall auch ein gruppenbezogenes Test-Zertifikat der V-PKI/DOI-CA zugelassen.

Bei der Beantragung sind als CN, Hash-Algorithmus und Schlüsseltyp folgende Angaben zu machen bzw. auszuwählen:

- CN: *GRP: „Name der Einrichtung“:SAK-DP:“Spezifikation des SAK-DP“*
- Hash-Algorithmus: SHA256

- Schlüsseltyp (Signatur): ECC NIST P-256

Als Cipher Suite ist `ecdsa_secp256r1_sha256 (0x0403)` festzulegen. Weitere Informationen zur Beschaffung der Zertifikate der V-PKI/DOI-CA finden Sie in der Anleitung: „Vertiefungsleitfaden für die Beschaffung von V-PKI Zertifikaten für Data Consumer und Data Provider für den Anschluss an das NOOTS“. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig.

Bei dem **Verschlüsselungszertifikat des SAK-DP** muss es sich um ein für Verschlüsselung der Nachweisanfrage geeignetes Zertifikat handeln. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den betrieblich Verantwortlichen. Es sind jedoch folgende kryptographische Vorgaben einzuhalten:

- Hash-Algorithmus: SHA256
- Schlüsseltyp (Signatur): ECC NIST P-256
- Cipher Suite: `ecdsa_secp256r1_sha256 (0x0403)`

NOOTS Produktivumgebung

Bei dem **Teilnehmerzertifikat des DP** muss es sich um ein für Siegelung geeignetes Zertifikat handeln. Dieses Zertifikat ist auf der NOOTS Produktivumgebung optional. Die Entscheidung über die Verwendung liegt in der Verantwortung des DP.

Bei dem **TLS-Server-Zertifikat des DP** muss es sich um ein geeignetes TLS-Zertifikat zur Gewährleistung der Transportverschlüsselung handeln. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den betrieblich Verantwortlichen.

Das **TLS-Server-Zertifikat des SAK-DP** ist für die NOOTS Produktivumgebung als gruppenbezogenes Zertifikat der V-PKI/DOI-CA zu beziehen.

Bei der Beantragung sind als CN, Hash-Algorithmus und Schlüsseltyp folgende Angaben zu machen bzw. auszuwählen:

- CN: *GRP: „Name der Einrichtung“:SAK-DP:“Spezifikation des SAK-DP“*
- Hash-Algorithmus: SHA256
- Schlüsseltyp (Signatur): ECC NIST P-256

Als Cipher Suite ist `ecdsa_secp256r1_sha256 (0x0403)` festzulegen. Weitere Informationen zur Beschaffung der Zertifikate der V-PKI/DOI-CA finden Sie in der Anleitung: „Vertiefungsleitfaden für die

Beschaffung von V-PKI Zertifikaten für Data Consumer und Data Provider für den Anschluss an das NOOTS“. Es ist ausschließlich die Verwendung von TLS 1.3 zulässig.

Bei dem **Verschlüsselungszertifikat des SAK-DP** muss es sich um ein für Verschlüsselung der Nachweisanfrage geeignetes Zertifikat handeln. Die Entscheidung über den Zertifikatstyp, die Beschaffung und die Installation obliegt den betrieblich Verantwortlichen. Es sind jedoch folgende kryptographische Vorgaben einzuhalten:

- Hash-Algorithmus: SHA256
- Schlüsseltyp (Signatur): ECC NIST P-256
- Cipher Suite: ecdsa_secp256r1_sha256 (0x0403)

4. Abkürzungsverzeichnis

BVA	Bundesverwaltungsamt
NOOTS	National-Once-Only-Technical-System
DC	Data Consumer
DP	Data Provider
IAM-B	Identity und Access Management für Behörden
RDN	Registerdatennavigation
VS	Vermittlungsstelle
ID-Nr.	Identifikationsnummer
IDM-P	Identity Management für Personen
SAK	Sicherer Anschlussknoten
SAK-DC	Sicherer Anschlussknoten für Data Consumer
SAK-DP	Sicherer Anschlussknoten für Data Provider
V-PKI	Public Key Infrastruktur der Verwaltung
DOI-CA	Deutschland Online Infrastruktur Certification Authority
CA	Certification Authority
EKU	Extended Key Usage
SHA	Secure Hash Algorithm
ECC	Elliptic Curve Cryptography
NIST	National Institute of Standards and Technology

5. Abbildungsverzeichnis

Abbildung 1 - Grobübersicht NOOTS 1.0 5
Abbildung 2 - Übersicht Zertifikate NOOTS Produktivumgebung 7
Abbildung 3 – Übersicht Komponenten und Zertifikate zur Beschaffung durch DC/DP in der NOOTS Produktivumgebung 11

6. Anhang

6.1. Vertrauenswürdige Root-Certification-Authorities

Die untenstehende Auflistung vertrauenswürdiger Root-CAs bezieht sich auf das TLS-Server-Zertifikat des SAK-DP für die NOOTS Referenzumgebung.

Wichtig: Die Liste nennt Trust Anchors, nicht einzelne erlaubte End-Zertifikate. Ein Zertifikat wird nicht allein deshalb akzeptiert, weil seine CA hier auftaucht. Die gesamte Zertifikatskette und die Verwendung als TLS-Clientzertifikat müssen gültig sein.

Das Zertifikat muss nicht direkt von der Root-CA ausgestellt sein. Üblich ist Root-CA → Intermediate-CA → Zertifikat.

6.1.1 Häufig genutzte deutsche Root-CAs

In Tabelle A-3 finden Sie häufig verwendete, öffentliche, deutsche Root-CAs:

Root-CA	Typische Einordnung
D-TRUST BR Root CA 1 2020	D-Trust / Bundesdruckerei; verbreitet im deutschen Behörden- und Unternehmensumfeld
D-TRUST BR Root CA 2 2023	Neuerer D-Trust-Vertrauensanker
D-TRUST EV Root CA 1 2020	D-Trust EV-PKI
D-TRUST EV Root CA 2 2023	Neuerer D-Trust-EV-Vertrauensanker
D-TRUST Root Class 3 CA 2 2009	Ältere D-Trust-PKI, weiterhin in vielen bestehenden Ketten relevant
D-TRUST Root Class 3 CA 2 EV 2009	Ältere D-Trust-EV-PKI
T-TeleSec GlobalRoot Class 2	Deutsche Telekom / T-TeleSec
T-TeleSec GlobalRoot Class 3	Deutsche Telekom / T-TeleSec

Telekom Security TLS ECC Root 2020	Telekom Security, ECC-basierte TLS-PKI
Telekom Security TLS RSA Root 2023	Telekom Security, RSA-basierte TLS-PKI

Tabelle A-1 - Häufig verwendete deutsche Root-CAs

Häufig verwendete, öffentliche, internationale, ROOT-CAs sind in Tabelle A-2 aufgelistet:

Root-CA	Typische Einordnung
ISRG Root X1	Let's Encrypt; sehr weit verbreitete öffentliche TLS-PKI
ISRG Root X2	Let's Encrypt; neuere ECC-basierte Root-CA
DigiCert Global Root G2	DigiCert; sehr häufig bei Unternehmens- und öffentlichen TLS-Zertifikaten
GlobalSign Root CA - R3	GlobalSign; weit verbreitete öffentliche PKI
USERTrust RSA Certification Authority	Sectigo / USERTrust; sehr häufige Trust Chain für öffentliche Zertifikate

Tabelle A-2 – Internationale, häufig anzutreffende öffentliche Root-CAs

Hinweis: Maßgeblich für die technische Vertrauensprüfung ist immer die vollständige Liste der Trust Anchors aus Abschnitt 6.2.

6.2. Vollständige Liste der Trust Anchors

In Tabelle 5 ist eine vollständige Liste der Trust Anchors zu finden:

Hinweis: Die SHA-256-Fingerprints dienen zur eindeutigen Identifikation des Root-Zertifikats.

Nr.	Root-CA	Betreiber	Land	gültig bis	Schlüssel	SHA-256
1	AC RAIZ FNMT-RCM	FNMT-RCM	ES	01.01.2030	RSA 4096	EB:C5:57:0C:29:01:8C:4D 67:B1:AA:12:7B:AF:12:F7 03:B4:61:1E:BC:17:B7:DA B5:57:38:94:17:9B:93:FA
2	AC RAIZ FNMT-RCM SERVIDORES SEGUROS	FNMT-RCM	ES	20.12.2043	EC secp384r1	55:41:53:B1:3D:2C:F9:DD B7:53:BF:BE:1A:4E:0A:E0 8D:0A:A4:18:70:58:FE:60 A2:B8:62:B2:E4:B8:7B:CB
3	ACCVRAIZ1	ACCV	ES	31.12.2030	RSA 4096	9A:6E:C0:12:E1:A7:DA:9D BE:34:19:4D:47:8A:D7:C0

						DB:18:22:FB:07:1D:F1:29 81:49:6E:D1:04:38:41:13
4	Actalis Authentication Root CA	Actalis S.p.A./03358520967	IT	22.09.2030	RSA 4096	55:92:60:84:EC:96:3A:64 B9:6E:2A:BE:01:CE:0B:A8 6A:64:FB:FE:BC:C7:AA:B5 AF:C1:55:B3:7F:D7:60:66
5	AffirmTrust Commercial	AffirmTrust	US	31.12.2030	RSA 2048	03:76:AB:1D:54:C5:F9:80 3C:E4:B2:E2:01:A0:EE:7E EF:7B:57:B6:36:E8:A9:3C 9B:8D:48:60:C9:6F:5F:A7
6	AffirmTrust Networking	AffirmTrust	US	31.12.2030	RSA 2048	0A:81:EC:5A:92:97:77:F1 45:90:4A:F3:8D:5D:50:9F 66:B5:E2:C5:8F:CD:B5:31 05:8B:0E:17:F3:F0:B4:1B
7	AffirmTrust Premium	AffirmTrust	US	31.12.2040	RSA 4096	70:A7:3F:7F:37:6B:60:07 42:48:90:45:34:B1:14:82 D5:BF:0E:69:8E:CC:49:8D F5:25:77:EB:F2:E9:3B:9A
8	AffirmTrust Premium ECC	AffirmTrust	US	31.12.2040	EC secp384r1	BD:71:FD:F6:DA:97:E4:CF 62:D1:64:7A:DD:25:81:B0 7D:79:AD:F8:39:7E:B4:EC BA:9C:5E:84:88:82:14:23
9	Amazon Root CA 1	Amazon	US	17.01.2038	RSA 2048	8E:CD:E6:88:4F:3D:87:B1 12:5B:A3:1A:C3:FC:B1:3D 70:16:DE:7F:57:CC:90:4F E1:CB:97:C6:AE:98:19:6E
10	Amazon Root CA 2	Amazon	US	26.05.2040	RSA 4096	1B:A5:B2:AA:8C:65:40:1A 82:96:01:18:F8:0B:EC:4F 62:30:4D:83:CE:C4:71:3A 19:C3:9C:01:1E:A4:6D:B4
11	Amazon Root CA 3	Amazon	US	26.05.2040	EC secp256r1	18:CE:6C:FE:7B:F1:4E:60 B2:E3:47:B8:DF:E8:68:CB 31:D0:2E:BB:3A:DA:27:15 69:F5:03:43:B4:6D:B3:A4
12	Amazon Root CA 4	Amazon	US	26.05.2040	EC secp384r1	E3:5D:28:41:9E:D0:20:25 CF:A6:90:38:CD:62:39:62 45:8D:A5:C6:95:FB:DE:A3 C2:2B:0B:FB:25:89:70:92
13	ANF Secure Server Root CA	ANF Autoridad de Certificacion	ES	30.08.2039	RSA 4096	FB:8F:EC:75:91:69:B9:10 6B:1E:51:16:44:C6:18:C5 13:04:37:3F:6C:06:43:08 8D:8B:EF:FD:1B:99:75:99
14	Atos TrustedRoot 2011	Atos	DE	31.12.2030	RSA 2048	F3:56:BE:A2:44:B7:A9:1E B3:5D:53:CA:9A:D7:86:4A CE:01:8E:2D:35:D5:F8:F9 6D:DF:68:A6:F4:1A:A4:74
15	Atos TrustedRoot Root CA ECC TLS 2021	Atos	DE	17.04.2041	EC secp384r1	B2:FA:E5:3E:14:CC:D7:AB 92:12:06:47:01:AE:27:9C 1D:89:88:FA:CB:77:5F:A8 A0:08:91:4E:66:39:88:A8
16	Atos TrustedRoot Root CA RSA TLS 2021	Atos	DE	17.04.2041	RSA 4096	81:A9:08:8E:A5:9F:B3:64 C5:48:A6:F8:55:59:09:9B 6F:04:05:EF:BF:18:E5:32 4E:C9:F4:57:BA:00:11:2F
17	Autoridad de Certificacion Firmaprofesional CIF A62634068	—	ES	05.05.2036	RSA 4096	57:DE:05:83:EF:D2:B2:6E 03:61:DA:99:DA:9D:F4:64 8D:EF:7E:E8:44:1C:3B:72 8A:FA:9B:CD:E0:F9:B2:6A
18	BJCA Global Root CA1	BEIJING CERTIFICATE AUTHORITY	CN	12.12.2044	RSA 4096	F3:89:6F:88:FE:7C:0A:88 27:66:A7:FA:6A:D2:74:9F B5:7A:7F:3E:98:FB:76:9C 1F:A7:B0:9C:2C:44:D5:AE
19	BJCA Global Root CA2	BEIJING CERTIFICATE AUTHORITY	CN	12.12.2044	EC secp384r1	57:4D:F6:93:1E:27:80:39 66:7B:72:0A:FD:C1:60:0F C2:7E:B6:6D:D3:09:29:79 FB:73:85:64:87:21:28:82
20	Buypass Class 2 Root CA	Buypass AS-983163327	NO	26.10.2040	RSA 4096	9A:11:40:25:19:7C:5B:B9 5D:94:E6:3D:55:CD:43:79 08:47:B6:46:B2:3C:DF:11 AD:A4:A0:0E:FF:15:FB:48
21	Buypass Class 3 Root CA	Buypass AS-983163327	NO	26.10.2040	RSA 4096	ED:F7:EB:BC:A2:7A:2A:38 4D:38:7B:7D:40:10:C6:66 E2:ED:B4:84:3E:4C:29:B4 AE:1D:5B:93:32:E6:B2:4D
22	CA Disig Root R2	Disig a.s.	SK	19.07.2042	RSA 4096	E2:3D:4A:03:6D:7B:70:E9 F5:95:B1:42:20:79:D2:B9 1E:DF:BB:1F:B6:51:A0:63 3E:AA:8A:9D:C5:F8:07:03
23	Certainly Root E1	Certainly	US	01.04.2046	EC secp384r1	B4:58:5F:22:E4:AC:75:6A 4E:86:12:A1:36:1C:5D:9D

						03:1A:93:FD:84:FE:BB:77 8F:A3:06:8B:0F:C4:2D:C2
24	Certainly Root R1	Certainly	US	01.04.2046	RSA 4096	77:B8:2C:D8:64:4C:43:05 F7:AC:C5:CB:15:6B:45:67 50:04:03:3D:51:C6:0C:62 02:A8:E0:C3:34:67:D3:A0
25	Certigna	Dhimyotis	FR	29.06.2027	RSA 2048	E3:B6:A2:DB:2E:D7:CE:48 84:2F:7A:C5:32:41:C7:B7 1D:54:14:4B:FB:40:C1:1F 3F:1D:0B:42:F5:EE:A1:2D
26	Certigna Root CA	Dhimyotis	FR	01.10.2033	RSA 4096	D4:8D:3D:23:EE:DB:50:A4 59:E5:51:97:60:1C:27:77 4B:9D:7B:18:C9:4D:5A:05 95:11:A1:02:50:B9:31:68
27	certSIGN ROOT CA	certSIGN	RO	04.07.2031	RSA 2048	EA:A9:62:C4:FA:4A:6B:AF EB:E4:15:19:6D:35:1C:CD 88:8D:4F:53:F3:FA:8A:E6 D7:C4:66:A9:4E:60:42:BB
28	certSIGN Root CA G2	CERTSIGN SA	RO	06.02.2042	RSA 4096	65:7C:FE:2F:A7:3F:AA:38 46:25:71:F3:32:A2:36:3A 46:FC:E7:02:09:51:71:07 02:CD:FB:B6:EE:DA:33:05
29	Certum EC-384 CA	Asseco Data Systems S.A.	PL	26.03.2043	EC secp384r1	6B:32:80:85:62:53:18:AA 50:D1:73:C9:8D:8B:DA:09 D5:7E:27:41:3D:11:4C:F7 87:A0:F5:D0:6C:03:0C:F6
30	Certum Trusted Network CA	Unizeto Technologies S.A.	PL	31.12.2029	RSA 2048	5C:58:46:8D:55:F5:8E:49 7E:74:39:82:D2:B5:00:10 B6:D1:65:37:4A:CF:83:A7 D4:A3:2D:B7:68:C4:40:8E
31	Certum Trusted Network CA 2	Unizeto Technologies S.A.	PL	06.10.2046	RSA 4096	B6:76:F2:ED:DA:E8:77:5C D3:6C:B0:F6:3C:D1:D4:60 39:61:F4:9E:62:65:BA:01 3A:2F:03:07:B6:D0:B8:04
32	Certum Trusted Root CA	Asseco Data Systems S.A.	PL	16.03.2043	RSA 4096	FE:76:96:57:38:55:77:3E 37:A9:5E:7A:D4:D9:CC:96 C3:01:57:C1:5D:31:76:5B A9:B1:57:04:E1:AE:78:FD
33	CFCA EV ROOT	China Financial Certification Authority	CN	31.12.2029	RSA 4096	5C:C3:D7:8E:4E:1D:5E:45 54:7A:04:E6:87:3E:64:F9 0C:F9:53:6D:1C:CC:2E:F8 00:F3:55:C4:C5:FD:70:FD
34	CommScope Public Trust ECC Root-01	CommScope	US	28.04.2046	EC secp384r1	11:43:7C:DA:7B:B4:5E:41 36:5F:45:B3:9A:38:98:6B 0D:E0:0D:EF:34:8E:0C:7B B0:87:36:33:80:0B:C3:8B
35	CommScope Public Trust ECC Root-02	CommScope	US	28.04.2046	EC secp384r1	2F:FB:7F:81:3B:BB:B3:C8 9A:B4:E8:16:2D:0F:16:D7 15:09:A8:30:CC:9D:73:C2 62:E5:14:08:75:D1:AD:4A
36	CommScope Public Trust RSA Root-01	CommScope	US	28.04.2046	RSA 4096	02:BD:F9:6E:2A:45:DD:9B F1:8F:C7:E1:DB:DF:21:A0 37:9B:A3:C9:C2:61:03:44 CF:D8:D6:06:FE:C1:ED:81
37	CommScope Public Trust RSA Root-02	CommScope	US	28.04.2046	RSA 4096	FF:E9:43:D7:93:42:4B:4F 7C:44:0C:1C:3D:64:8D:53 63:F3:4B:82:DC:87:AA:7A 9F:11:8F:C5:DE:E1:01:F1
38	Comodo AAA Services root	Comodo CA Limited	GB	31.12.2028	RSA 2048	D7:A7:A0:FB:5D:7E:27:31 D7:71:E9:48:4E:BC:DE:F7 1D:5F:0C:3E:0A:29:48:78 2B:C8:3E:E0:EA:69:9E:F4
39	COMODO Certification Authority	COMODO CA Limited	GB	31.12.2029	RSA 2048	0C:2C:D6:3D:F7:80:6F:A3 99:ED:E8:09:11:6B:57:5B F8:79:89:F0:65:18:F9:80 8C:86:05:03:17:8B:AF:66
40	COMODO ECC Certification Authority	COMODO CA Limited	GB	18.01.2038	EC secp384r1	17:93:92:7A:06:14:54:97 89:AD:CE:2F:8F:34:F7:F0 B6:6D:0F:3A:E3:A3:B8:4D 21:EC:15:DB:BA:4F:AD:C7
41	COMODO RSA Certification Authority	COMODO CA Limited	GB	18.01.2038	RSA 4096	52:F0:E1:C4:E5:8E:C6:29 29:1B:60:31:7F:07:46:71 B8:5D:7E:A8:0D:5B:07:27 34:63:53:4B:32:B4:02:34
42	D-TRUST BR Root CA 1 2020	D-Trust GmbH	DE	11.02.2035	EC secp384r1	E5:9A:AA:81:60:09:C2:2B FF:5B:25:BA:D3:7D:F3:06 F0:49:79:7C:1F:81:D8:5A B0:89:E6:57:BD:8F:00:44
43	D-TRUST BR Root CA 2 2023	D-Trust GmbH	DE	09.05.2038	RSA 4096	05:52:E6:F8:3F:DF:65:E8 FA:96:70:E6:66:DF:28:A4 E2:13:40:B5:10:CB:E5:25 66:F9:7C:4F:B9:4B:2B:D1

44	D-TRUST EV Root CA 1 2020	D-Trust GmbH	DE	11.02.2035	EC secp384r1	08:17:0D:1A:A3:64:53:90 1A:2F:95:92:45:E3:47:DB 0C:8D:37:AB:AA:BC:56:B8 1A:A1:00:DC:95:89:70:DB
45	D-TRUST EV Root CA 2 2023	D-Trust GmbH	DE	09.05.2038	RSA 4096	8E:82:21:B2:E7:D4:00:78 36:A1:67:2F:0D:CC:29:9C 33:BC:07:D3:16:F1:32:FA 1A:20:6D:58:71:50:F1:CE
46	D-TRUST Root Class 3 CA 2 2009	D-Trust GmbH	DE	05.11.2029	RSA 2048	49:E7:A4:42:AC:F0:EA:62 87:05:00:54:B5:25:64:B6 50:E4:F4:9E:42:E3:48:D6 AA:38:E0:39:E9:57:B1:C1
47	D-TRUST Root Class 3 CA 2 EV 2009	D-Trust GmbH	DE	05.11.2029	RSA 2048	EE:C5:49:6B:98:8C:E9:86 25:B9:34:09:2E:EC:29:08 BE:D0:B0:F3:16:C2:D4:73 0C:84:EA:F1:F3:D3:48:81
48	DigiCert Assured ID Root CA	DigiCert Inc	US	10.11.2031	RSA 2048	3E:90:99:B5:01:5E:8F:48 6C:00:BC:EA:9D:11:1E:E7 21:FA:BA:35:5A:89:BC:F1 DF:69:56:1E:3D:C6:32:5C
49	DigiCert Assured ID Root G2	DigiCert Inc	US	15.01.2038	RSA 2048	7D:05:EB:B6:82:33:9F:8C 94:51:EE:09:4E:EB:FE:FA 79:53:A1:14:ED:B2:F4:49 49:45:2F:AB:7D:2F:C1:85
50	DigiCert Assured ID Root G3	DigiCert Inc	US	15.01.2038	EC secp384r1	7E:37:CB:8B:4C:47:09:0C AB:36:55:1B:A6:F4:5D:B8 40:68:0F:BA:16:6A:95:2D B1:00:71:7F:43:05:3F:C2
51	DigiCert Global Root CA	DigiCert Inc	US	10.11.2031	RSA 2048	43:48:A0:E9:44:4C:78:CB 26:5E:05:8D:5E:89:44:B4 D8:4F:96:62:BD:26:DB:25 7F:89:34:A4:43:C7:01:61
52	DigiCert Global Root G2	DigiCert Inc	US	15.01.2038	RSA 2048	CB:3C:CB:B7:60:31:E5:E0 13:8F:8D:D3:9A:23:F9:DE 47:FF:C3:5E:43:C1:14:4C EA:27:D4:6A:5A:B1:CB:5F
53	DigiCert Global Root G3	DigiCert Inc	US	15.01.2038	EC secp384r1	31:AD:66:48:F8:10:41:38 C7:38:F3:9E:A4:32:01:33 39:3E:3A:18:CC:02:29:6E F9:7C:2A:C9:EF:67:31:D0
54	DigiCert High Assurance EV Root CA	DigiCert Inc	US	10.11.2031	RSA 2048	74:31:E5:F4:C3:C1:CE:46 90:77:4F:0B:61:E0:54:40 88:3B:A9:A0:1E:D0:0B:A6 AB:D7:80:6E:D3:B1:18:CF
55	DigiCert TLS ECC P384 Root G5	DigiCert, Inc.	US	14.01.2046	EC secp384r1	01:8E:13:F0:77:25:32:CF 80:9B:D1:B1:72:81:86:72 83:FC:48:C6:E1:3B:E9:C6 98:12:85:4A:49:0C:1B:05
56	DigiCert TLS RSA4096 Root G5	DigiCert, Inc.	US	14.01.2046	RSA 4096	37:1A:00:DC:05:33:B3:72 1A:7E:EB:40:E8:41:9E:70 79:9D:2B:0A:0F:2C:1D:80 69:31:65:F7:CE:C4:AD:75
57	DigiCert Trusted Root G4	DigiCert Inc	US	15.01.2038	RSA 4096	55:2F:7B:DC:F1:A7:AF:9E 6C:E6:72:01:7F:4F:12:AB F7:72:40:C7:8E:76:1A:C2 03:D1:D9:D2:0A:C8:99:88
58	e-Szigno Root CA 2017	Microsec Ltd.	HU	22.08.2042	EC secp256r1	BE:B0:0B:30:83:9B:9B:C3 2C:32:E4:44:79:05:95:06 41:F2:64:21:B1:5E:D0:89 19:8B:51:8A:E2:EA:1B:99
59	emSign ECC Root CA - C3	eMudhra Inc	US	18.02.2043	EC secp384r1	BC:4D:80:9B:15:18:9D:78 DB:3E:1D:8C:F4:F9:72:6A 79:5D:A1:64:3C:A5:F1:35 8E:1D:DB:0E:DC:0D:7E:B3
60	emSign ECC Root CA - G3	eMudhra Technologies Limited	IN	18.02.2043	EC secp384r1	86:A1:EC:BA:08:9C:4A:8D 3B:BE:27:34:C6:12:BA:34 1D:81:3E:04:3C:F9:E8:A8 62:CD:5C:57:A3:6B:BE:6B
61	emSign Root CA - C1	eMudhra Inc	US	18.02.2043	RSA 2048	12:56:09:AA:30:1D:A0:A2 49:B9:7A:82:39:CB:6A:34 21:6F:44:DC:AC:9F:39:54 B1:42:92:F2:E8:C8:60:8F
62	emSign Root CA - G1	eMudhra Technologies Limited	IN	18.02.2043	RSA 2048	40:F6:AF:03:46:A9:9A:A1 CD:1D:55:5A:4E:9C:CE:62 C7:F9:63:46:03:EE:40:66 15:83:3D:C8:C8:D0:03:67
63	Entrust Root Certification Authority	Entrust, Inc.	US	27.11.2026	RSA 2048	73:C1:76:43:4F:1B:C6:D5 AD:F4:5B:0E:76:E7:27:28 7C:8D:E5:76:16:C1:E6:E6 14:1A:2B:2C:BC:7D:8E:4C

64	Entrust Root Certification Authority - EC1	Entrust, Inc.	US	18.12.2037	EC secp384r1	02:ED:0E:B2:8C:14:DA:45 16:5C:56:67:91:70:0D:64 51:D7:FB:56:F0:B2:AB:1D 3B:8E:B0:70:E5:6E:DF:F5
65	Entrust Root Certification Authority - G2	Entrust, Inc.	US	07.12.2030	RSA 2048	43:DF:57:74:B0:3E:7F:EF 5F:E4:0D:93:1A:7B:ED:F1 BB:2E:6B:42:73:8C:4E:6D 38:41:10:3D:3A:A7:F3:39
66	Entrust.net Premium 2048 Secure Server CA	Entrust.net	—	24.07.2029	RSA 2048	6D:C4:71:72:E0:1C:BC:B0 BF:62:58:0D:89:5F:E2:B8 AC:9A:D4:F8:73:80:1E:0C 10:B9:C8:37:D2:1E:B1:77
67	ePKI Root Certification Authority	Chunghwa Telecom Co., Ltd.	TW	20.12.2034	RSA 4096	C0:A6:F4:DC:63:A2:4B:FD CF:54:EF:2A:6A:08:2A:0A 72:DE:35:80:3E:2F:F5:FF 52:7A:E5:D8:72:06:DF:D5
68	FIRMAPROFESIONAL CA ROOT-A WEB	Firmaprofesional SA	ES	31.03.2047	EC secp384r1	BE:F2:56:DA:F2:6E:9C:69 BD:EC:16:02:35:97:98:F3 CA:F7:18:21:A0:3E:01:82 57:C5:3C:65:61:7F:3D:4A
69	GDCA TrustAUTH R5 ROOT	GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.	CN	31.12.2040	RSA 4096	BF:FF:8F:D0:44:33:48:7D 6A:8A:A6:0C:1A:29:76:7A 9F:C2:BB:B0:5E:42:0F:71 3A:13:B9:92:89:1D:38:93
70	GlobalSign ECC Root CA - R4	GlobalSign	—	19.01.2038	EC secp256r1	B0:85:D7:0B:96:4F:19:1A 73:E4:AF:0D:54:AE:7A:0E 07:AA:FD:AF:9B:71:DD:08 62:13:8A:B7:32:5A:24:A2
71	GlobalSign ECC Root CA - R5	GlobalSign	—	19.01.2038	EC secp384r1	17:9F:BC:14:8A:3D:D0:0F D2:4E:A1:34:58:CC:43:BF A7:F5:9C:81:82:D7:83:A5 13:F6:EB:EC:10:0C:89:24
72	GlobalSign Root CA	GlobalSign nv-sa	BE	28.01.2028	RSA 2048	EB:D4:10:40:E4:BB:3E:C7 42:C9:E3:81:D3:1E:F2:A4 1A:48:B6:68:5C:96:E7:CE F3:C1:DF:6C:D4:33:1C:99
73	GlobalSign Root CA - R3	GlobalSign	—	18.03.2029	RSA 2048	CB:B5:22:D7:B7:F1:27:AD 6A:01:13:86:5B:DF:1C:D4 10:2E:7D:07:59:AF:63:5A 7C:F4:72:0D:C9:63:C5:3B
74	GlobalSign Root CA - R6	GlobalSign	—	10.12.2034	RSA 4096	2C:AB:EA:FE:37:D0:6C:A2 2A:BA:73:91:C0:03:3D:25 98:29:52:C4:53:64:73:49 76:3A:3A:B5:AD:6C:CF:69
75	GlobalSign Root E46	GlobalSign nv-sa	BE	20.03.2046	EC secp384r1	CB:B9:C4:4D:84:B8:04:3E 10:50:EA:31:A6:9F:51:49 55:D7:BF:D2:E2:C6:B4:93 01:01:9A:D6:1D:9F:50:58
76	GlobalSign Root R46	GlobalSign nv-sa	BE	20.03.2046	RSA 4096	4F:A3:12:6D:8D:3A:11:D1 C4:85:5A:4F:80:7C:BA:D6 CF:91:9D:3A:5A:88:B0:3B EA:2C:63:72:D9:3C:40:C9
77	GLOBALTRUST 2020	e-commerce monitoring GmbH	AT	10.06.2040	RSA 4096	9A:29:6A:51:82:D1:D4:51 A2:E3:7F:43:9B:74:DA:AF A2:67:52:33:29:F9:0F:9A 0D:20:07:C3:34:E2:3C:9A
78	Go Daddy Class 2 CA	The Go Daddy Group, Inc.	US	29.06.2034	RSA 2048	C3:84:6B:F2:4B:9E:93:CA 64:27:4C:0E:C6:7C:1E:CC 5E:02:4F:FC:AC:D2:D7:40 19:35:0E:81:FE:54:6A:E4
79	Go Daddy Root Certificate Authority - G2	GoDaddy.com, Inc.	US	31.12.2037	RSA 2048	45:14:0B:32:47:EB:9C:C8 C5:B4:F0:D7:B5:30:91:F7 32:92:08:9E:6E:5A:63:E2 74:9D:D3:AC:A9:19:8E:DA
80	GTS Root R1	Google Trust Services LLC	US	22.06.2036	RSA 4096	D9:47:43:2A:BD:E7:B7:FA 90:FC:2E:6B:59:10:1B:12 80:E0:E1:C7:E4:E4:0F:A3 C6:88:7F:FF:57:A7:F4:CF
81	GTS Root R2	Google Trust Services LLC	US	22.06.2036	RSA 4096	8D:25:CD:97:22:9D:BF:70 35:6B:DA:4E:B3:CC:73:40 31:E2:4C:F0:0F:AF:CF:D3 2D:C7:6E:B5:84:1C:7E:A8
82	GTS Root R3	Google Trust Services LLC	US	22.06.2036	EC secp384r1	34:D8:A7:3E:E2:08:D9:BC DB:0D:95:65:20:93:4B:4E 40:E6:94:82:59:6E:8B:6F 73:C8:42:6B:01:0A:6F:48
83	GTS Root R4	Google Trust Services LLC	US	22.06.2036	EC secp384r1	34:9D:FA:40:58:C5:E2:63 12:3B:39:8A:E7:95:57:3C 4E:13:13:C8:3F:E6:8F:93 55:6C:D5:E8:03:1B:3C:7D

84	HARICA TLS ECC Root CA 2021	Hellenic Academic and Research Institutions CA	GR	13.02.2045	EC secp384r1	3F:99:CC:47:4A:CF:CE:4D FE:D5:87:94:66:5E:47:8D 15:47:73:9F:2E:78:0F:1B B4:CA:9B:13:30:97:D4:01
85	HARICA TLS RSA Root CA 2021	Hellenic Academic and Research Institutions CA	GR	13.02.2045	RSA 4096	D9:5D:0E:8E:DA:79:52:5B F9:BE:B1:1B:14:D2:10:0D 32:94:98:5F:0C:62:D9:FA BD:9C:D9:99:EC:CB:7B:1D
86	Hellenic Academic and Research Institutions ECC RootCA 2015	Hellenic Academic and Research Institutions Cert. Authority	GR	30.06.2040	EC secp384r1	44:B5:45:AA:8A:25:E6:5A 73:CA:15:DC:27:FC:36:D2 4C:1C:B9:95:3A:06:65:39 B1:15:82:DC:48:7B:48:33
87	Hellenic Academic and Research Institutions RootCA 2015	Hellenic Academic and Research Institutions Cert. Authority	GR	30.06.2040	RSA 4096	A0:40:92:9A:02:CE:53:B4 AC:F4:F2:FF:C6:98:1C:E4 49:6F:75:5E:6D:45:FE:0B 2A:69:2B:CD:52:52:3F:36
88	HiPKI Root CA - G1	Chunghwa Telecom Co., Ltd.	TW	31.12.2037	RSA 4096	F0:15:CE:3C:C2:39:BF:EF 06:4B:E9:F1:D2:C4:17:E1 A0:26:4A:0A:94:BE:1F:0C 8D:12:18:64:EB:69:49:CC
89	Hongkong Post Root CA 3	Hongkong Post	HK	03.06.2042	RSA 4096	5A:2F:C0:3F:0C:83:B0:90 BB:FA:40:60:4B:09:88:44 6C:76:36:18:3D:F9:84:6E 17:10:1A:44:7F:B8:EF:D6
90	IdenTrust Commercial Root CA 1	IdenTrust	US	16.01.2034	RSA 4096	5D:56:49:9B:E4:D2:E0:8B CF:CA:D0:8A:3E:38:72:3D 50:50:3B:DE:70:69:48:E4 2F:55:60:30:19:E5:28:AE
91	IdenTrust Public Sector Root CA 1	IdenTrust	US	16.01.2034	RSA 4096	30:D0:89:5A:9A:44:8A:26 20:91:63:55:22:D1:F5:20 10:B5:86:7A:CA:E1:2C:78 EF:95:8F:D4:F4:38:9F:2F
92	ISRG Root X1	Internet Security Research Group	US	04.06.2035	RSA 4096	96:BC:EC:06:26:49:76:F3 74:60:77:9A:CF:28:C5:A7 CF:E8:A3:C0:AA:E1:1A:8F FC:EE:05:C0:BD:DF:08:C6
93	ISRG Root X2	Internet Security Research Group	US	17.09.2040	EC secp384r1	69:72:9B:8E:15:A8:6E:FC 17:7A:57:AF:B7:17:1D:FC 64:AD:D2:8C:2F:CA:8C:F1 50:7E:34:45:3C:CB:14:70
94	Izenpe.com	IZENPE S.A.	ES	13.12.2037	RSA 4096	25:30:CC:8E:98:32:15:02 BA:D9:6F:9B:1F:BA:1B:09 9E:2D:29:9E:0F:45:48:BB 91:4F:36:3B:C0:D4:53:1F
95	Microsec e-Szigno Root CA 2009	Microsec Ltd.	HU	30.12.2029	RSA 2048	3C:5F:81:FE:A5:FA:B8:2C 64:BF:A2:EA:EC:AF:CD:E8 E0:77:FC:86:20:A7:CA:E5 37:16:3D:F3:6E:DB:F3:78
96	Microsoft ECC Root Certificate Authority 2017	Microsoft Corporation	US	18.07.2042	EC secp384r1	35:8D:F3:9D:76:4A:F9:E1 B7:66:E9:C9:72:DF:35:2E E1:5C:FA:C2:27:AF:6A:D1 D7:0E:8E:4A:6E:DC:BA:02
97	Microsoft RSA Root Certificate Authority 2017	Microsoft Corporation	US	18.07.2042	RSA 4096	C7:41:F7:0F:4B:2A:8D:88 BF:2E:71:C1:41:22:EF:53 EF:10:EB:A0:CF:A5:E6:4C FA:20:F4:18:85:30:73:E0
98	NAVER Global Root Certification Authority	NAVER BUSINESS PLATFORM Corp.	KR	18.08.2037	RSA 4096	88:F4:38:DC:F8:FF:D1:FA 8F:42:91:15:FF:E5:F8:2A E1:E0:6E:0C:70:C3:75:FA AD:71:7B:34:A4:9E:72:65
99	NetLock Arany (Class Gold) Főtanúsítvány	NetLock Kft.	HU	06.12.2028	RSA 2048	6C:61:DA:C3:A2:DE:F0:31 50:6B:E0:36:D2:A6:FE:40 19:94:FB:D1:3D:F9:C8:D4 66:59:92:74:C4:46:EC:98
100	OISTE WISeKey Global Root GB CA	WISeKey	CH	01.12.2039	RSA 2048	6B:9C:08:E8:6E:B0:F7:67 CF:AD:65:CD:98:B6:21:49 E5:49:4A:67:F5:84:5E:7B D1:ED:01:9F:27:B8:6B:D6
101	OISTE WISeKey Global Root GC CA	WISeKey	CH	09.05.2042	EC secp384r1	85:60:F9:1C:36:24:DA:BA 95:70:B5:FE:A0:DB:E3:6F F1:1A:83:23:BE:94:86:85 4F:B3:F3:4A:55:71:19:8D
102	QuoVadis Root CA 1 G3	QuoVadis Limited	BM	12.01.2042	RSA 4096	8A:86:6F:D1:B2:76:B5:7E 57:8E:92:1C:65:82:8A:2B ED:58:E9:F2:F2:88:05:41 34:B7:F1:F4:BF:C9:CC:74
103	QuoVadis Root CA 2	QuoVadis Limited	BM	24.11.2031	RSA 4096	85:A0:DD:7D:D7:20:AD:B7 FF:05:F8:3D:54:2B:20:9D C7:FF:45:28:F7:D6:77:B1 83:89:FE:A5:E5:C4:9E:86

104	QuoVadis Root CA 2 G3	QuoVadis Limited	BM	12.01.2042	RSA 4096	8F:E4:FB:0A:F9:3A:4D:0D 67:DB:0B:EB:B2:3E:37:C7 1B:F3:25:DC:BC:DD:24:0E A0:4D:AF:58:B4:7E:18:40
105	QuoVadis Root CA 3	QuoVadis Limited	BM	24.11.2031	RSA 4096	18:F1:FC:7F:20:5D:F8:AD DD:EB:7F:E0:07:DD:57:E3 AF:37:5A:9C:4D:8D:73:54 6B:F4:F1:FE:D1:E1:8D:35
106	QuoVadis Root CA 3 G3	QuoVadis Limited	BM	12.01.2042	RSA 4096	88:EF:81:DE:20:2E:B0:18 45:2E:43:F8:64:72:5C:EA 5F:BD:1F:C2:D9:D2:05:73 07:09:C5:D8:B8:69:0F:46
107	Sectigo Public Server Authentication Root E46	Sectigo Limited	GB	21.03.2046	EC secp384r1	C9:0F:26:F0:FB:1B:40:18 B2:22:27:51:9B:5C:A2:B5 3E:2C:A5:B3:BE:5C:F1:8E FE:1B:EF:47:38:0C:53:83
108	Sectigo Public Server Authentication Root R46	Sectigo Limited	GB	21.03.2046	RSA 4096	7B:B6:47:A6:2A:EE:AC:88 BF:25:7A:A5:22:D0:1F:FE A3:95:E0:AB:45:C7:3F:93 F6:56:54:EC:38:F2:5A:06
109	Secure Global CA	SecureTrust Corporation	US	31.12.2029	RSA 2048	42:00:F5:04:3A:C8:59:0E BB:52:7D:20:9E:D1:50:30 29:FB:CB:D4:1C:A1:B5:06 EC:27:F1:5A:DE:7D:AC:69
110	SecureSign Root CA12	Cybertrust Japan Co., Ltd.	JP	08.04.2040	RSA 2048	3F:03:4B:B5:70:4D:44:B2 D0:85:45:A0:20:57:DE:93 EB:F3:90:5F:CE:72:1A:CB C7:30:C0:6D:DA:EE:90:4E
111	SecureSign Root CA14	Cybertrust Japan Co., Ltd.	JP	08.04.2045	RSA 4096	4B:00:9C:10:34:49:4F:9A B5:6B:BA:3B:A1:D6:27:31 FC:4D:20:D8:95:5A:DC:EC 10:A9:25:60:72:61:E3:38
112	SecureSign Root CA15	Cybertrust Japan Co., Ltd.	JP	08.04.2045	EC secp384r1	E7:78:F0:F0:95:FE:84:37 29:CD:1A:00:82:17:9E:53 14:A9:C2:91:44:28:05:E1 FB:1D:8F:B6:B8:88:6C:3A
113	SecureTrust CA	SecureTrust Corporation	US	31.12.2029	RSA 2048	F1:C1:B5:0A:E5:A2:0D:D8 03:0E:C9:F6:BC:24:82:3D D3:67:B5:25:57:59:B4:E7 1B:61:FC:E9:F7:37:5D:73
114	Security Communication ECC RootCA1	SECOM Trust Systems CO.,LTD.	JP	18.01.2038	EC secp384r1	E7:4F:BD:A5:5B:D5:64:C4 73:A3:6B:44:1A:A7:99:C8 A6:8E:07:74:40:E8:28:8B 9F:A1:E5:0E:4B:BA:CA:11
115	Security Communication RootCA2	SECOM Trust Systems CO.,LTD.	JP	29.05.2029	RSA 2048	51:3B:2C:EC:B8:10:D4:CD E5:DD:85:39:1A:DF:C6:C2 DD:60:D8:7B:B7:36:D2:B5 21:48:4A:A4:7A:0E:BE:F6
116	SSL.com EV Root Certification Authority ECC	SSL Corporation	US	12.02.2041	EC secp384r1	22:A2:C1:F7:BD:ED:70:4C C1:E7:01:B5:F4:08:C3:10 88:0F:E9:56:B5:DE:2A:4A 44:F9:9C:87:3A:25:A7:C8
117	SSL.com EV Root Certification Authority RSA R2	SSL Corporation	US	30.05.2042	RSA 4096	2E:7B:F1:6C:C2:24:85:A7 BB:E2:AA:86:96:75:07:61 B0:AE:39:BE:3B:2F:E9:D0 CC:6D:4E:F7:34:91:42:5C
118	SSL.com Root Certification Authority ECC	SSL Corporation	US	12.02.2041	EC secp384r1	34:17:BB:06:CC:60:07:DA 1B:96:1C:92:0B:8A:B4:CE 3F:AD:82:0E:4A:A3:0B:9A CB:C4:A7:4E:BD:CE:BC:65
119	SSL.com Root Certification Authority RSA	SSL Corporation	US	12.02.2041	RSA 4096	85:66:6A:56:2E:E0:BE:5C E9:25:C1:D8:89:0A:6F:76 A8:7E:C1:6D:4D:7D:5F:29 EA:74:19:CF:20:12:3B:69
120	SSL.com TLS ECC Root CA 2022	SSL Corporation	US	19.08.2046	EC secp384r1	C3:2F:FD:9F:46:F9:36:D1 6C:36:73:99:09:59:43:4B 9A:D6:0A:AF:BB:9E:7C:F3 36:54:F1:44:CC:1B:A1:43
121	SSL.com TLS RSA Root CA 2022	SSL Corporation	US	19.08.2046	RSA 4096	8F:AF:7D:2E:2C:B4:70:9B B8:E0:B3:36:66:BF:75:A5 DD:45:B5:DE:48:0F:8E:A8 D4:BF:E6:BE:BC:17:F2:ED
122	Starfield Class 2 CA	Starfield Technologies, Inc.	US	29.06.2034	RSA 2048	14:65:FA:20:53:97:B8:76 FA:A6:F0:A9:95:8E:55:90 E4:0F:CC:7F:AA:4F:B7:C2 C8:67:75:21:FB:5F:B6:58
123	Starfield Root Certificate Authority - G2	Starfield Technologies, Inc.	US	31.12.2037	RSA 2048	2C:E1:CB:0B:F9:D2:F9:E1 02:99:3F:BE:21:51:52:C3 B2:DD:0C:AB:DE:1C:68:E5 31:9B:83:91:54:DB:B7:F5

124	Starfield Services Root Certificate Authority - G2	Starfield Technologies, Inc.	US	31.12.2037	RSA 2048	56:8D:69:05:A2:C8:87:08 A4:B3:02:51:90:ED:CF:ED B1:97:4A:60:6A:13:C6:E5 29:0F:CB:2A:E6:3E:DA:B5
125	SwissSign Gold CA - G2	SwissSign AG	CH	25.10.2036	RSA 4096	62:DD:0B:E9:B9:F5:0A:16 3E:A0:F8:E7:5C:05:3B:1E CA:57:EA:55:C8:68:8F:64 7C:68:81:F2:C8:35:7B:95
126	SZAFIR ROOT CA2	Krajowa Izba Rozliczeniowa S.A.	PL	19.10.2035	RSA 2048	A1:33:9D:33:28:1A:0B:56 E5:57:D3:D3:2B:1C:E7:F9 36:7E:B0:94:BD:5F:A7:2A 7E:50:04:C8:DE:D7:CA:FE
127	T-TeleSec GlobalRoot Class 2	T-Systems Enterprise Services GmbH	DE	01.10.2033	RSA 2048	91:E2:F5:78:8D:58:10:EB A7:BA:58:73:7D:E1:54:8A 8E:CA:CD:01:45:98:BC:0B 14:3E:04:1B:17:05:25:52
128	T-TeleSec GlobalRoot Class 3	T-Systems Enterprise Services GmbH	DE	01.10.2033	RSA 2048	FD:73:DA:D3:1C:64:4F:F1 B4:3B:EF:0C:CD:DA:96:71 0B:9C:D9:87:5E:CA:7E:31 70:7A:F3:E9:6D:52:2B:BD
129	Telekom Security TLS ECC Root 2020	Deutsche Telekom Security GmbH	DE	25.08.2045	EC secp384r1	57:8A:F4:DE:D0:85:3F:4E 59:98:DB:4A:EA:F9:CB:EA 8D:94:5F:60:B6:20:A3:8D 1A:3C:13:B2:BC:7B:A8:E1
130	Telekom Security TLS RSA Root 2023	Deutsche Telekom Security GmbH	DE	27.03.2048	RSA 4096	EF:C6:5C:AD:BB:59:AD:B6 EF:E8:4D:A2:23:11:B3:56 24:B7:1B:3B:1E:A0:DA:8B 66:55:17:4E:C8:97:86:46
131	Telia Root CA v2	Telia Finland Oyj	FI	29.11.2043	RSA 4096	24:2B:69:74:2F:CB:1E:5B 2A:BF:98:89:8B:94:57:21 87:54:4E:5B:4D:99:11:78 65:73:62:1F:6A:74:B8:2C
132	TeliaSonera Root CA v1	TeliaSonera	—	18.10.2032	RSA 4096	DD:69:36:FE:21:F8:F0:77 C1:23:A1:A5:21:C1:22:24 F7:22:55:B7:3E:03:A7:26 06:93:E8:A2:4B:0F:A3:89
133	TrustAsia Global Root CA G3	TrustAsia Technologies, Inc.	CN	19.05.2046	RSA 4096	E0:D3:22:6A:EB:11:63:C2 E4:8F:F9:BE:3B:50:B4:C6 43:1B:E7:BB:1E:AC:C5:C3 6B:5D:5E:C5:09:03:9A:08
134	TrustAsia Global Root CA G4	TrustAsia Technologies, Inc.	CN	19.05.2046	EC secp384r1	BE:4B:56:CB:50:56:C0:13 6A:52:6D:F4:44:50:8D:AA 36:A0:B5:4F:42:E4:AC:38 F7:2A:F4:70:E4:79:65:4C
135	Trustwave Global Certification Authority	Trustwave Holdings, Inc.	US	23.08.2042	RSA 4096	97:55:20:15:F5:DD:FC:3C 87:88:C0:06:94:45:55:40 88:94:45:00:84:F1:00:86 70:86:BC:1A:2B:B5:8D:C8
136	Trustwave Global ECC P256 Certification Authority	Trustwave Holdings, Inc.	US	23.08.2042	EC secp256r1	94:5B:BC:82:5E:A5:54:F4 89:D1:FD:51:A7:3D:DF:2E A6:24:AC:70:19:A0:52:05 22:5C:22:A7:8C:CF:A8:B4
137	Trustwave Global ECC P384 Certification Authority	Trustwave Holdings, Inc.	US	23.08.2042	EC secp384r1	55:90:38:59:C8:C0:C3:EB B8:75:9E:CE:4E:25:57:22 5F:F5:75:8B:BD:38:EB:D4 82:76:60:1E:1B:D5:80:97
138	TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK	TR	25.10.2043	RSA 2048	46:ED:C3:68:90:46:D5:3A 45:3F:B3:10:4A:B8:0D:CA EC:65:8B:26:60:EA:16:29 DD:7E:86:79:90:64:87:16
139	TunTrust Root CA	Agence Nationale de Certification Electronique	TN	26.04.2044	RSA 4096	2E:44:10:2A:B5:8C:B8:54 19:45:1C:8E:19:D9:AC:F3 66:2C:AF:BC:61:4B:6A:53 96:0A:30:F7:D0:E2:EB:41
140	TWCA CYBER Root CA	TAIWAN-CA	TW	22.11.2047	RSA 4096	3F:63:BB:28:14:BE:17:4E C8:B6:43:9C:F0:8D:6D:56 F0:B7:C4:05:88:3A:56:48 A3:34:42:4D:6B:3E:C5:58
141	TWCA Global Root CA	TAIWAN-CA	TW	31.12.2030	RSA 4096	59:76:90:07:F7:68:5D:0F CD:50:87:2F:9F:95:D5:75 5A:5B:2B:45:7D:81:F3:69 2B:61:0A:98:67:2F:0E:1B
142	TWCA Root Certification Authority	TAIWAN-CA	TW	31.12.2030	RSA 2048	BF:D8:8F:E1:10:1C:41:AE 3E:80:1B:F8:BE:56:35:0E E9:BA:D1:A6:B9:BD:51:5E DC:5C:6D:5B:87:11:AC:44
143	UCA Extended Validation Root	UniTrust	CN	31.12.2038	RSA 4096	D4:3A:F9:B3:54:73:75:5C 96:84:FC:06:D7:D8:CB:70 EE:5C:28:E7:73:FB:29:4E B4:1E:E7:17:22:92:4D:24
144	UCA Global G2 Root	UniTrust	CN	31.12.2040	RSA 4096	9B:EA:11:C9:76:FE:01:47 64:C1:BE:56:A6:F9:14:B5

						A5:60:31:7A:BD:99:88:39 33:82:E5:16:1A:A0:49:3C
145	USERTrust ECC Certification Authority	The USERTRUST Network	US	18.01.2038	EC secp384r1	4F:F4:60:D5:4B:9C:86:DA BF:BC:FC:57:12:E0:40:0D 2B:ED:3F:BC:4D:4F:BD:AA 86:E0:6A:DC:D2:A9:AD:7A
146	USERTrust RSA Certification Authority	The USERTRUST Network	US	18.01.2038	RSA 4096	E7:93:C9:B0:2F:D8:AA:13 E2:1C:31:22:8A:CC:B0:81 19:64:3B:74:9C:89:89:64 B1:74:6D:46:C3:D4:CB:D2
147	vTrus ECC Root CA	iTrusChina Co.,Ltd.	CN	31.07.2043	EC secp384r1	30:FB:BA:2C:32:23:8E:2A 98:54:7A:F9:79:31:E5:50 42:8B:9B:3F:1C:8E:EB:66 33:DC:FA:86:C5:B2:7D:D3
148	vTrus Root CA	iTrusChina Co.,Ltd.	CN	31.07.2043	RSA 4096	8A:71:DE:65:59:33:6F:42 6C:26:E5:38:80:D0:0D:88 A1:8D:A4:C6:A9:1F:0D:CB 61:94:E2:06:C5:C9:63:87
149	XRamp Global CA Root	XRamp Security Services Inc	US	01.01.2035	RSA 2048	CE:CD:DC:90:50:99:D8:DA DF:C5:B1:D2:09:B7:37:CB E2:C1:8C:FB:2C:10:C0:FF 0B:CF:0D:32:86:FC:1A:A2

Tabelle A-3 – Vollständige Liste der Trust Anchors