Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

JIPDEC
Roppongi First Bldg.
1-9-9 Roppongi, Minato-Ku
Tokyo 106-0032, Japan

für den Zertifizierungsdienst

JCAN Public CA1-G3 (SHA-256)
issued by JCAN Root CA1

die Erfüllung aller Anforderungen der Spezifikation

ETSI TS 102 042 V2.4.1 (2013-02), policy LCP.

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht aus 7 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Ungültig seit 25.07.2016

ETSI TS 102 042 2016 TÜViT® Trusted Site

Certificate ID: 6753.16

17

Zertifikat gültig bis
30.04.2017

Essen, 25.04.2016

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-12022-01-00

Zertifizierungssystem

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH ist bei der „DAkkS Deutsche Akkreditierungsstelle GmbH“ für die Zertifizierung von Produkten in den Bereichen IT-Sicherheit und Sicherheitstechnik nach DIN EN ISO/IEC 17065 akkreditiert. Die Zertifizierungsstelle führt ihre Zertifizierungen auf Basis des folgenden akkreditierten Produktzertifizierungsprogramms durch:

- „Zertifizierungsprogramm (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH”, Version 1.7 vom 18.03.2016, TÜV Informationstechnik GmbH

Prüfbericht

- „Evaluation Report – Surveillance Onsite Inspection – ETSI TS 102 042, JCAN Public CA1 G3 (SHA-256) issued by JCAN Root CA1“, Version 1.1 vom 20.04.2016, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der technischen Spezifikation ETSI TS 102 042 definiert:

- ETSI TS 102 042 V2.4.1 (2013-02): „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates“, Version 2.4.1, 2013-02, European Telecommunications Standards Institute

Die anwendbare ETSI Zertifizierungspolitik ist:

- LCP: Einfache Zertifizierungspolitik

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Zertifizierungsdienst:

JCAN Public CA1-G3 (SHA-256):

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = JCAN Root CA1 Zertifikatsseriennummer: 11 21 43 92 d7 43 01 6f a4 89 ee 65 a4 22 67 b5 e3 f4	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = JCAN Public CA1–G3	11 21 4b b8 01 9e 10 df 4a f2 49 88 36 61 7a 32 8d 41

zusammen mit der Certificate Policy (CP) des Betreibers:

- „JCAN Certificate Policy“, Version 3.1 vom 18.04.2013, JIPDEC

und mit dem Certification Practice Statement (CPS) des Betreibers:

- „JCAN Certification Practice Statement“, Version 3.2 vom 28.03.2014, JIPDEC

Prüfergebnis

- Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien.
- Die im Zertifizierungssystem definierten Zertifizierungs-voraussetzungen sind erfüllt.
- JCAN Zertifikat ist konform zu der japanischen Verordnung „Act on Electronic Signatures and Certification Business“ (Act No. 102 of May 31, 2000, Final Revision: Act No. 102 of March 31st, 2006) Artikel 2 (3), im Besonderen basiert die Sicherheit der elektronischen Signatur auf folgender Schwierigkeit: Faktorisierung in Primfaktoren ≥1024 Bit Integer als ein Produkt zweier Primzahlen, die annähernd gleich groß sind.

Zusammenfassung der Prüfanforderungen

Die ETSI Spezifikation ETSI TS 102 042 enthält folgende Anforderungen:

1 Certification Practice Statement (CPS)

Die CA verfügt über eine Darlegung ihrer Praktiken und Verfahren.

2 Public Key Infrastructure – Schlüsselmanagement-Lebenszyklus

Die CA stellt sicher, dass CA Schlüssel unter kontrollierten Bedingungen erzeugt werden.

Die CA stellt sicher, dass private CA Schlüssel vertraulich bleiben und ihre Integrität beibehalten.

Die CA stellt sicher, dass die Integrität und Authentizität der (öffentlichen) CA Signaturprüfschlüssel und aller zugehörigen Parameter während ihrer Übermittlung an vertrauende Parteien (relying party) erhalten bleiben.

Wenn der Schlüssel für elektronische Signaturen in dem Sinne der Richtlinie 1999/93/EG angewandt wird, dann darf die CA private Signaturschlüssel des Zertifikatsinhabers (subject) nicht in einer Weise aufbewahren, die eine (Reserve) Entschlüsselungsmöglichkeit bietet (gemeinhin als Key Escrow bezeichnet).

Wird eine Kopie des Schlüssels von der CA aufbewahrt, dann sorgt die CA dafür, dass der private Schlüssel geheim gehalten und nur entsprechend befugten Personen zur Verfügung gestellt wird.

Die CA stellt sicher, dass private CA Signaturschlüssel nicht unsachgemäß verwendet werden.

Die CA stellt sicher, dass private CA Signaturschlüssel nicht über das Ende ihres Lebenszyklus hinaus verwendet werden.

Im Falle von NCP stellt die CA sicher, dass die Sicherheit von kryptographischen Geräten während ihres gesamten Lebenszyklus gewährleistet ist.

Die CA stellt sicher, dass jeder Schlüssel, den sie für Zertifikatsinhaber (subject) erzeugt, sicher generiert wird und die Geheimhaltung des privaten Schlüssels des Zertifikatsinhabers sichergestellt ist.

Im Falle von NCP+ stellt die CA sicher, dass die Übergabe der sicheren Signaturerstellungseinheit an den Zertifikatsinhaber (subject) sicher erfolgt, sofern diese von der CA bereitgestellt wird.

Im Fall von EV code signing Zertifikaten werden die Anforderung aus Anhang H, Punkt 10 des Dokuments „Guidelines for the Issuance and Management of Extended Validation Certificates“, Version 1.3, CA/Browser Forum befolgt.

3 Public Key Infrastructure – Zertifikatsmanagement Lebenszyklus

Die CA stellt sicher, dass Nachweise der Identifizierung eines Teilnehmers (subscriber) und Zertifikatsinhabers (subject) sowie der Korrektheit ihrer Namen und die dazugehörigen Daten entweder geeignet als Teil des definierten Services geprüft oder anhand von Bescheinigungen aus geeigneten und zugelassenen Quellen nachgewiesen werden und dass Zertifikatsanträge richtig, autorisiert und vollständig gemäß den gesammelten Nachweisen bzw. Bescheinigungen erfolgen.

Die CA stellt sicher, dass Zertifikatsanträge von Zertifikatsinhabern (subject), die zuvor bei der gleichen CA registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind. Dies beinhaltet Zertifikatsverlängerungen, erneute Schlüsselgenerierung (rekey) nach Sperrung oder vor Ablauf der Gültigkeit oder Aktualisierung aufgrund Attributsänderungen des Zertifikatsinhabers (subject).

Die CA stellt sicher, dass Zertifikate sicher ausgegeben werden, so dass ihre Authentizität erhalten bleibt.

Die CA stellt sicher, dass die allgemeinen Geschäftsbedingungen den Teilnehmer (subscriber) und vertrauenden Parteien (relying party) zur Verfügung gestellt werden.

Die CA stellt sicher, dass Zertifikate den Teilnehmern (subscriber), Zertifikatsinhabern (subject) und vertrauenden Parteien (relying party) im erforderlichen Umfang zur Verfügung gestellt werden.

Die CA stellt sicher, dass Zertifikate kurzfristig anhand von autorisierten und überprüften Sperranfragen gesperrt werden.

4 CA Management und Betrieb

Die Anforderungen des Dokuments „Network Security Requirements“ des CA/Browser Forums finden Anwendung.

Die CA stellt sicher, dass Verwaltungs- und Management-Verfahren angewendet werden, die angemessen sind und anerkannten Normen entsprechen.

Die CA stellt sicher, dass ihre schützenswerte Objekte und Informationen einen angemessenen Schutz erhalten.

Die CA stellt sicher, dass das Personal und die Einstellungsverfahren die Vertrauenswürdigkeit des CA Betriebs verstärken und unterstützen.

Die CA stellt sicher, dass der physische Zugriff auf kritische Dienste kontrolliert wird und physische Risiken der schützenswerten Objekte minimiert werden.

Die CA stellt sicher, dass die CA Systeme sicher sind und ordnungsgemäß betrieben werden mit minimalem Ausfallrisiko.

Die CA stellt sicher, dass der Zugriff auf die CA Systeme auf geeignet autorisierte Personen beschränkt ist.

Die CA soll vertrauenswürdige Systeme und Produkte verwenden, die vor Veränderungen geschützt sind.

Die CA stellt sicher, dass im Falle einer Katastrophe, einschließlich der Kompromittierung des privaten CA Signaturschlüssels, der Betrieb so schnell wie möglich wiederhergestellt wird.

Die CA stellt sicher, dass im Falle der Einstellung des Betriebs der CA potenzielle Störungen von Teilnehmer (subscriber) und vertrauenden Parteien (relying party) minimiert werden und dass der Forterhalt der Aufzeichnungen, die zum Nachweis der Zertifizierung in Gerichtsverfahren benötigt werden, gegeben ist.

Die CA stellt sicher, dass die gesetzlichen Anforderungen eingehalten werden.

Die CA stellt sicher, dass alle relevanten Informationen über ein Zertifikat für einen angemessenen Zeitraum aufgezeichnet werden, insbesondere zum Zweck des Nachweises der Zertifizierung in Gerichtsverfahren.

5 Organisation

Die CA stellt sicher, dass ihre Organisation zuverlässig ist.

6 Weitere Anforderungen

Die CA stellt unterschiedliche Testmöglichkeiten bereit, über die Dritte die Funktion ihrer Zertifikate überprüfen können.

Im Fall von PTC-BR finden die Anforderungen von Anhang C des Dokuments „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ des CA/Browser Forums Anwendung.

Die CA soll alle Cross-Zertifikate offenlegen, in denen die CA als Subjekt geführt wird.

Im Fall von PTC-BR finden die Anforderungen von Abschnitt 8.4 des Dokuments „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ des CA/Browser Forums Anwendung.