Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Fabrica Nacional de Moneda y Timbre – Real Casa de la Moneda
C/Jorge Juan, 106
28009 Madrid, Spanien

für den Zertifizierungsdienst

AC Public Administration

die Erfüllung aller Anforderungen der Spezifikation

ETSI TS 101 456 V1.4.3 (2007-05), policy QCP public.

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

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

ETSI TS 101 456 2016 TÜVIT® Trusted Site

Certificate ID: 6747.16

17

Zertifikat gültig bis 31.07.2017

Essen, 21.06.2016

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 101 456, AC Public Administration“, Version 1.1 vom 16.06.2016, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der technischen Spezifikation ETSI TS 101 456 definiert:

- ETSI TS 101 456 V1.4.3 (2007-05): „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing qualified certificates“, Version 1.4.3, 2007-05, European Telecommunications Standards Institute

Die anwendbare ETSI Zertifizierungspolitik ist:

- QCP public: Zertifizierungspolitik für (öffentlich angebotene) qualifizierte Zertifikate

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikats-information zum untersuchten Zertifizierungsdienst:

AC Public Administration:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): **OU = AC RAIZ FNMT-RCM** **Zertifikatsseriennummer: 5d 93 8d 30 67 36 c8 06 1d 1a c7 54 84 69 07**	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = AC Administración Pública	02
CN = AC FNMT Usuarios	45 5f 3a e1 5c 21 cd ba 54 4f 82 aa 47 51 eb db
CN = AC Representación	61 c2 d4 d4 f6 a9 ae 77 55 92 66 b9 8d af d6 21

zusammen mit der Certificate Policy (CP) des Betreibers:

- „Specific Certification Policies and Practices applicable to Electronic Certification and Signature Services for Public Organizations and Administrations, their Bodies and attached or dependent Entities“, Version 2.3 vom 05.11.2015, FNMT-RCM
- „Specific Certification Practices and Policy for Natural Person Certificates from the AC FNMT Usuarios“, Version 1.0 vom 25.03.2014, FNMT-RCM
- „Specific Certification Practices and Policy of Certificates of Representatives of Legal Entities and of Institutions with no Legal Entity from the AC Representación“, Version 1.2 vom 06.04.2016, FNMT-RCM

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

- „General Certification Practice Statement“, Version 4.3 vom 01.04.2016, FNMT-RCM

Prüfergebnis

- Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien.
- Die im Zertifizierungssystem definierten Zertifizierungs-voraussetzungen sind erfüllt.

Zusammenfassung der Prüfanforderungen

Die ETSI Spezifikation ETSI TS 101 456 enthält folgende Anforderungen:

1 Certification Practice Statement (CPS)

Die CA stellt sicher, dass sie die erforderliche Zuverlässigkeit für die Bereitstellung von Zertifizierungsdiensten darlegt (siehe die Richtlinie 1999/98/EG, Anhang II (a)).

2 Public Key Infrastructure – Schlüsselmanagement-Lebenszyklus

Die CA stellt sicher, dass CA Schlüssel unter kontrollierten Bedingungen erzeugt werden (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass private CA Schlüssel vertraulich bleiben und ihre Integrität beibehalten (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

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 (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Private Signaturschlüssel von Inhabern (subject) dürfen nicht hinterlegt werden, dass eine (Reserve-)Entschlüsselungsmöglichkeit geboten wird, die es autorisierten Stellen unter bestimmten Bedingungen erlaubt, Daten unter Verwendung von Information, die durch einen oder mehrere Beteiligte bereitgestellt werden, zu entschlüsseln (gemeinhin als Key Escrow bezeichnet) (siehe die Richtlinie 1999/93/EG, Anhang II (j)).

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 (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass die Sicherheit der kryptografischen Hardware während ihres gesamten Lebenszyklus gewährleistet ist (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

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 (siehe die Richtlinie 1999/93/EG, Anhang II (f) und Anhang II(j)).

Die CA stellt sicher, dass die Übergabe der sicheren Signaturerstellungseinheit sicher erfolgt, sofern diese Signaturerstellungseinheit der CA bereitgestellt wird (siehe die Richtlinie 1999/93/EG, Anhang III).

3 Public Key Infrastructure – Zertifikatsmanagement Lebenszyklus

Die CA stellt sicher, dass Zertifikatsinhaber (subject) geeignet identifiziert und authentifiziert sind und dass Zertifikatsanträge vollständig, korrekt und ordnungsgemäß autorisiert sind (siehe die Richtlinie 1999/93/EG, Anhang II (d)).

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) (siehe die Richtlinie 1999/93/EG, Anhang II (g)).

Die CA stellt sicher, dass Zertifikate sicher ausgegeben werden, so dass ihre Authentizität erhalten bleibt (siehe die Richtlinie 1999/93/EG, Anhang II (g)).

Die CA stellt sicher, dass die allgemeinen Geschäftsbedingungen den Teilnehmer (subscriber) und vertrauenden Parteien (relying party) zur Verfügung gestellt werden (siehe die Richtlinie 1999/93/EG, Anhang II (k)).

Die CA stellt sicher, dass Zertifikate den Teilnehmern (subscriber), Zertifikatsinhabern (subject) und vertrauenden Parteien (relying party) im erforderlichen Umfang zur Verfügung gestellt werden (siehe die Richtlinie 1999/93/EG, Anhang II (l)).

Die CA stellt sicher, dass Zertifikate kurzfristig anhand von autorisierten und überprüften Sperranfragen gesperrt werden (siehe die Richtlinie 1999/93/EG, Anhang II (b)).

4 CA Management und Betrieb

Die CA stellt sicher, dass Verwaltungs- und Management-Verfahren angewendet werden, die angemessen sind und anerkannten Normen entsprechen (siehe die Richtlinie 1999/93/EG, Anhang II (e), 2. Teil).

Die CA stellt sicher, dass ihre schützenswerte Objekte und Informationen einen angemessenen Schutz erhalten (siehe die Richtlinie 1999/93/EG, Anhang II (e)).

Die CA stellt sicher, dass das Personal und die Einstellungsverfahren die Vertrauenswürdigkeit des CA Betriebs verstärken und unterstützen (siehe die Richtlinie 1999/93/EG, Anhang II (e) 1. Teil).

Die CA stellt sicher, dass der physische Zugriff auf kritische Dienste kontrolliert wird und physische Risiken der schützenswerten Objekte minimiert werden (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA stellt sicher, dass die CA Systeme sicher sind und ordnungsgemäß betrieben werden mit minimalem Ausfallrisiko (siehe die Richtlinie 1999/93/EG, Anhang II (e)).

Die CA stellt sicher, dass der Zugriff auf die CA Systeme auf geeignet autorisierte Personen beschränkt ist (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA soll vertrauenswürdige Systeme und Produkte verwenden, die vor Veränderungen geschützt sind (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA stellt sicher, dass im Falle einer Katastrophe, einschließlich der Kompromittierung des privaten CA Signaturschlüssels, der Betrieb so schnell wie möglich wiederhergestellt wird (siehe die Richtlinie 1999/93/EG, Anhang II (a)).

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, geben ist (siehe die Richtlinie 1999/93/EG, Anhang II (i)).

Die CA stellt sicher, dass die gesetzlichen Anforderungen eingehalten werden (siehe die Richtlinie 1999/93/EG, Artikel 8).

Die CA stellt sicher, dass alle relevanten Informationen über ein qualifiziertes Zertifikat für einen angemessenen Zeitraum aufgezeichnet werden, insbesondere zum Zweck des Nachweises der Zertifizierung in Gerichtsverfahren (siehe die Richtlinie 1999/93/EG, Anhang II (i)).

5 Organisation

Die CA stellt sicher, dass ihre Organisation zuverlässig ist (siehe die Richtlinie 1999/93/EG, Anhang II (a)).