Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

FNMT – Real Casa de la Moneda
C/Jorge Juan, 106
28009 Madrid, Spanien

für den Vertrauensdienst

Autoridades de certificación para la expedición de certificados de autenticación de sitios web

die Erfüllung aller Anforderungen der Norm (EN)

ETSI EN 319 411-1 V1.1.1 (2016-02), policy OVCP.

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht aus 3 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

ETSI EN 319 411-1 2017 TÜViT® Trusted Site

Certificate ID: 6797.17

Zertifikat gültig bis 31.05.2019

Essen, 18.05.2017

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 Zertifizierungssystems durch:

- „Zertifizierungssystem (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH”, Version 2.0 vom 06.06.2016, TÜV Informationstechnik GmbH

Prüfbericht

- „Evaluation Report – Initial Certification – ETSI EN 319 411-1, TUVIT-CA6797, Autoridades de certificación para la expedición de certificados de autenticación de sitios web“, Version 2.0 vom 04.05.2017, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der Norm ETSI EN 319 411-1 definiert:

- ETSI EN 319 411-1 V1.1.1 (2016-02): „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements“, Version 1.1.1, 2016-02, European Telecommunications Standards Institute

Die anwendbare ETSI Zertifizierungspolitik ist:

- OVCP: Zertifizierungspolitik mit Organisationsvalidierung

Prüfgegenstand

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

Autoridades de certificación para la expedición de certificados de autenticación de sitios web:

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**
OU = AC Componentes Informáticos	34 c6 ab 04 4e 36 99 12 51 c8 25 0b 6c 94 d6 c0
CN = AC Administración Pública serialNumber=Q2826004J	02

zusammen mit den Certification Practice Statements (CPS) des Betreibers:

- „SPECIFIC CERTIFICATION POLICIES AND PRACTICES APPLICABLE TO ELECTRONIC CERTIFICATION AND SIGNATURE SERVICES FOR PUBLIC ORGANIZATIONS AND ADMINISTRATIONS, THEIR PUBLIC BODIES AND PUBLIC LAW ENTITIES“, Version 3.0 vom 03.01.2017, FNMT-RCM

und

- „SPECIFIC CERTIFICATION POLICY AND PRACTICES APPLICABLE TO COMPONENT CERTIFICATES “, Version 1.5 vom 03.01.2017, FNMT-RCM

und

- “TRUST SERVICES PRACTICES AND ELECTRONIC CERTIFICATION GENERAL STATEMENT”, Version 5.1 vom

03.01.2017, FNMT-RCM

Prüfergebnis

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

Zusammenfassung der Prüfanforderungen

ETSI EN 319 411-1 enthält Anforderungen für Vertrauensdienstanbieter (VDA) bzgl. der Tätigkeit des VDAs unter folgenden Überschriften:

1 Verantwortlichkeiten bzgl. Veröffentlichung und öffentlichem Verzeichnis

2 Identifizierung und Authentifizierung

3 Betriebsanforderungen an den Zertifikatslebenszyklus

4 Anforderungen an Einrichtung, Verwaltung und Betrieb

5 Technische Sicherheitsanforderungen

6 Zertifikats-, Sperrlisten- (CRL-) und OCSP-Profile

7 Compliance-Audit und andere Bewertungen

8 Sonstige geschäftliche und rechtliche Angelegenheiten

9 Sonstige Maßnahmen

Gegenstand des Nachtrags

Dieser Nachtrag vom 11.05.2018 ergänzt das Zertifikat mit der Certificate ID: 6797.17 vom 18.05.2017 aufgrund des durchgeführten Überwachungsaudits.

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 Zertifizierungssystems durch:

- „Zertifizierungssystem (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 2.0 vom 06.06.2016, TÜV Informationstechnik GmbH

Prüfbericht

- „Evaluation Report – Surveillance Onsite Inspection – ETSI EN 319 411-1, TUVIT.6797.TSP A1, Autoridades de certificación para la expedición de certificados de autenticación de sitios web“, Version 1.0 vom 11.05.2018, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der Norm ETSI EN 319 411-1 definiert:

- ETSI EN 319 411-1 V1.1.1 (2016-02): „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements“, Version 1.1.1, 2016-02, European Telecommunications Standards Institute

Die anwendbare ETSI Zertifizierungspolitik ist:

- OVCP: Zertifizierungspolitik mit Organisationsvalidierung

Prüfgegenstand

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

Autoridades de certificación para la expedición de certificados de autenticación de sitios web:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = xxx yy Zertifikatsseriennummer:	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = AC Administración Pública	02
CN = AC Componentes Informáticos	34 c6 ab 04 4e 36 99 12 51 c8 25 0b 6c 94 d6 c0

zusammen mit den Certificate Practice Statements (CPS) des Betreibers:

- „SPECIFIC CERTIFICATION POLICIES AND PRACTICES APPLICABLE TO ELECTRONIC CERTIFICATION AND SIGNATURE SERVICES FOR PUBLIC ORGANIZATIONS AND ADMINISTRATIONS, THEIR PUBLIC BODIES AND PUBLIC LAW ENTITIES", Version 3.0 vom 03.01.2017, FNMT-RCM,
- „SPECIFIC CERTIFICATION POLICY AND PRACTICES APPLICABLE TO COMPONENT CERTIFICATES", Version 1.5 vom 03.01.2017, FNMT-RCM

und

- „TRUST SERVICES PRACTICES AND ELECTRONIC CERTIFICATION GENERAL STATEMENT“, Version 5.2 vom 09.10.2017, FNMT-RCM

Prüfergebnis

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

Zusammenfassung der Prüfanforderungen

ETSI EN 319 411-1 enthält Anforderungen für Vertrauensdienste-anbieter (VDA) bzgl. der Tätigkeit des VDAs unter folgenden Überschriften:

1 Verantwortlichkeiten bzgl. Veröffentlichung und öffentlichem Verzeichnis

2 Identifizierung und Authentifizierung

3 Betriebsanforderungen an den Zertifikatslebenszyklus

4 Anforderungen an Einrichtung, Verwaltung und Betrieb

5 Technische Sicherheitsanforderungen

6 Zertifikats-, Sperrlisten- (CRL-) und OCSP-Profile

7 Compliance-Audit und andere Bewertungen

8 Sonstige geschäftliche und rechtliche Angelegenheiten

9 Sonstige Maßnahmen