Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Izenpe S.A.
Beato Tomás de Zumárraga
71 – 1ª Planta
01008 Vitoria-Gasteiz, Spanien

für den Vertrauensdienst

CA de Certificados SSL EV

die Erfüllung aller Anforderungen der Norm (EN)

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

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 2016 TÜVIT Trusted Site

Certificate ID: 6757.16

© TÜViT – TÜV NORD GROUP – www.tuvit.de

Zertifikat gültig bis 31.07.2018

Essen, 29.07.2016

Joachim Faulhaber
stellv. 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 – Surveillance Onsite Inspection – ETSI EN 319 411-1, TUVIT-CA6757, CA de Certificados SSL EV“, Version 1.0 vom 26.07.2016, 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

Zusätzlich wurden folgende Kriterien bei dem Audit berücksichtigt:

- “Guidelines for the issuance and management of Extended Validation Certificates”, Version 1.5.7 vom 28.09.2015, CA/Browser Forum

Die anwendbare ETSI Zertifizierungspolitik ist:

- EVCP: Zertifizierungspolitik mit erweiterter Validierung

Prüfgegenstand

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

CA de Certificados SSL EV:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = Izenpe.com Zertifikatsseriennummer: 00 b0 b7 5a 16 48 5f bf e1 cb f5 8b d7 19 e6 7d	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = CA de Certificados SSL EV	6d 71 e2 5b 7b b6 b6 36 4c be a8 48 e3 a4 a9 81

zusammen dem Certification Practice Statement (CPS) des Betreibers:

- „Certification Practice Statement", Version 5.04 vom 01.07.2016, Izenpe

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**

Gegenstand des Nachtrags

Dieser Nachtrag vom 31.07.2017 ergänzt das Zertifikat mit der Certificate ID: 6757.16 vom 29.09.2016 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-CA6757Ü2, CA de Certificados SSL EV“, Version 2.0 vom 26.07.2017, 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:

- EVCP: Zertifizierungspolitik mit erweiterter Validierung

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Vertrauensdienst:

CA de Certificados SSL EV:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = Izenpe.com Zertifikatsseriennummer: 00 b0 b7 5a 16 48 5f bf e1 cb f5 8b d7 19 e6 7d	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = CA de Certificados SSL EV	6d 71 e2 5b 7b b6 b6 36 4c be a8 48 e3 a4 a9 81

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

- „Certification Practice Statement“, Version 6.0 vom 01.06.2017, Izenpe

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 Vertrauensdiensteanbieter (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