Certificate

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

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

to confirm that its trust service

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

fulfils all requirements defined in the standard (EN)

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

The appendix to the certificate is part of the certificate and consists of 3 pages.

The certificate is valid only in conjunction with the evaluation report.

ETSI EN 319 411-1
TÜViT®
2017
Trusted Site
Certificate ID: 6797.17
© TÜViT – TÜV NORD GROUP – www.tuvit.de

Certificate valid until
2019-05-31

Essen, 2017-05-18

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

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

Certification System

The certification body of TÜV Informationstechnik GmbH is accredited by "DAkkS Deutsche Akkreditierungsstelle GmbH" according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- "Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH", version 2.0 as of 2016-06-06, TÜV Informationstechnik GmbH

Evaluation Report

- "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 as of 2017-05-04, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the standard ETSI EN 319 411-1:

- 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

The applicable ETSI Certificate Policy is:

- OVCP: Organizational Validation Certificate Policy

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected trust service:

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

Issuer of CA certificate (Root CA or intermediate CA): OU = AC RAIZ FNMT-RCM Certificate Serial Number: 5d 93 8d 30 67 36 c8 06 1d 1a c7 54 84 69 07	
Name of CA (as in certificate)	**serial number of certificate**
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

together with the Certification Practice Statements (CPS) of the operator:

- "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 as of 2017-01-03, FNMT-RCM

and

- "SPECIFIC CERTIFICATION POLICY AND PRACTICES APPLICABLE TO COMPONENT CERTIFICATES", version 1.5 as of 2017-01-03, FNMT-RCM

and

- "TRUST SERVICES PRACTICES AND ELECTRONIC CERTIFICATION GENERAL STATEMENT", version 5.1 as of 2017-01-03, FNMT-RCM

Evaluation Result

- The target of evaluation fulfills all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

Summary of the Evaluation Requirements

ETSI EN 319 411-1 contains requirements for Trust Service Providers practice under the following headlines:

1 Publication and repository responsibilities

2 Identification and authentication

3 Certificate Life-Cycle operational requirements

4 Facility, management, and operational controls

5 Technical security controls

6 Certificate, CRL, and OCSP profiles

7 Compliance audit and other assessment

8 Other business and legal matters

9 Other provisions

Scope of the Amendment

This amendment as of 2018-05-11 supplements the certificate with certificate ID: 6797.17 as of 2017-05-18 because of the conducted surveillance audit.

Certification System

The certification body of TÜV Informationstechnik GmbH is accredited by “DAkkS Deutsche Akkreditierungsstelle GmbH” according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- “Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH”, version 2.0 as of 2016-06-06, TÜV Informationstechnik GmbH

Evaluation Report

- “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 as of 2018-05-11, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the standard ETSI EN 319 411-1:

- 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

The applicable ETSI Certificate Policy is:

- OVCP: Organizational Validation Certificate Policy

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected trust service:

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

**Issuer of CA certificate (Root CA or intermediate CA):
OU = AC RAIZ FNMT-RCM
Certificate Serial Number: 5d 93 8d 30 67 36 c8 06 1d 1a c7 54 84 69 07**	

Name of CA (as in certificate)	**serial number of certificate**
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

together with the Certification Practice Statements (CPS) of the operator:

- “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 as of 2017-01-03, FNMT-RCM,
- “SPECIFIC CERTIFICATION POLICY AND PRACTICES APPLICABLE TO COMPONENT CERTIFICATES”, version 1.5 as of 2017-01-03, FNMT-RCM

and

- "TRUST SERVICES PRACTICES AND ELECTRONIC CERTIFICATION GENERAL STATEMENT", version 5.2 as of 2017-10-09, FNMT-RCM

Evaluation Result

- The target of evaluation fulfills all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

Summary of the Evaluation Requirements

ETSI EN 319 411-1 contains requirements for Trust Service Providers practice under the following headlines:

1 **Publication and repository responsibilities**

2 **Identification and authentication**

3 **Certificate Life-Cycle operational requirements**

4 **Facility, management, and operational controls**

5 **Technical security controls**

6 **Certificate, CRL, and OCSP profiles**

7 **Compliance audit and other assessment**

8 **Other business and legal matters**

9 **Other provisions**