Certificate

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

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

to confirm that its certification service

AC Public Administration

fulfils all requirements defined in the technical specification

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

The appendix to the certificate is part of the certificate and consists of 7 pages.

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

ETSI TS 101 456 2016 TÜViT Trusted Site

Certificate ID: 6747.16

Certificate valid until 2017-07-31

Essen, 2016-06-21

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 product certification scheme:

- "Certification Scheme (accredited scope) of the certification body of TÜV Informationstechnik GmbH", version 1.7 as of 2016-03-18, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report – Surveillance Onsite Inspection – ETSI TS 101 456, AC Public Administration", Version 1.1 as of 2016-06-16, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the technical specification ETSI TS 101 456:

- 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

The applicable ETSI Certificate Policy is:

- QCP public: Qualified Certificate Policy for qualified certificates issued to the public

Evaluation Target

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

AC Public Administration:

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 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

together with the Certificate Policy (CP) of the operator:

- "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 as of 2015-11-05, FNMT-RCM
- "Specific Certification Practices and Policy for Natural Person Certificates from the AC FNMT Usuarios", version 1.0 as of 2014-03-25, 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 as of 2016-04-06, FNMT-RCM

and with the Certification Practice Statement (CPS) of the operator:

- "General Certification Practice Statement", version 4.3 as of 2016-04-01, 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

The ETSI specification ETSI TS 101 456 contains the following requirements:

1 Certification Practice Statement (CPS)

The CA shall ensure that it demonstrates the reliability necessary for providing certification services (see the Directive 1999/98/EC, annex II (a)).

2 Public key infrastructure – Key management life cycle

The CA shall ensure that CA keys are generated in controlled circumstances (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

The CA shall ensure that CA private keys remain confidential and maintain their integrity (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

The CA shall ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

Subject private signing keys shall not be held in a way which provides a backup decryption capability, allowing authorized entities under certain conditions to decrypt data using information supplied by one or more parties (commonly called key escrow) (see the Directive 1999/93/EC, annex II (j)).

The CA shall ensure that CA private signing keys are not used inappropriately.

The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

The CA shall ensure the security of cryptographic hardware throughout its lifecycle (see the Directive 1999/93/EC, annex II (f)).

The CA shall ensure that any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured (see the Directive 1999/93/EC, annex II (f) and annex II (j)).

The CA shall ensure that if it issues SSCD this is carried out securely (see the Directive 1999/93/EC, annex III).

3 Public key infrastructure – Certificate Management life cycle

The CA shall ensure that subjects are properly identified and authenticated; and that subject certificate requests are complete, accurate and duly authorized (see the Directive 1999/93/EC, annex II (d)).

The CA shall ensure that requests for certificates issued to a subject who has already previously been registered are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes (see the Directive 1999/93/EC, annex II (g)).

The CA shall ensure that it issues certificates securely to maintain their authenticity (see the Directive 1999/93/EC, annex II (g)).

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties (see the Directive 1999/93/EC, annex II (k)).

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties (see the Directive 1999/93/EC, annex II (l)).

The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests (see the Directive 1999/93/EC, annex II (b)).

4 CA management and operation

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards (see the Directive 1999/93/EC, annex II (e), 2nd part).

The CA shall ensure that its assets and information receive an appropriate level of protection (see the Directive 1999/93/EC, annex II (e)).

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations (see Directive 1999/93/EC, annex II (e) 1st part).

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized (see Directive 1999/93/EC, annex II (f)).

The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure (see the Directive 1999/93/EC, annex II (e)).

The CA shall ensure that CA system access is limited to properly authorized individuals (see the Directive 1999/93/EC, annex II (f)).

The CA shall use trustworthy systems and products that are protected against modification (see the Directive 1999/93/EC, annex II (f)).

The CA shall ensure in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible (see the Directive 1999/93/EC, annex II (a)).

The CA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services as covered by the certificate policy, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings (see the Directive 1999/93/EC, annex II (i)).

The CA shall ensure compliance with legal requirements (see the Directive 1999/93/EC, article 8).

The CA shall ensure that all relevant information concerning a qualified certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings (see the Directive 1999/93/EC, annex II (i)).

5 Organizational

The CA shall ensure that its organization is reliable (see Directive 1999/93/EC, annex II (a)).