Audit Attestation for

Fabrica Nacional de Moneda y Timbre – Real Casa de la Moneda

Reference: AA2018041201

Essen, 12.04.2018

To whom it may concern,

This is to confirm that "TÜV Informationstechnik GmbH" has successfully audited the CAs of the "**Fabrica Nacional de Moneda y Timbre – Real Casa de la Moneda**" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "**AA2018041201**" and consist of 6 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Certification Body
Langemarckstr. 20
45141 Essen, Germany
E-Mail: certuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Matthias Wiedenhorst
Reviewer

Mirco Przybylinski
Leadauditor

Identification of the conformity assessment body (CAB):	TÜV Informationstechnik GmbH[1], Langemarckstraße 20, 45141 Essen, Germany registered under HRB 11687, Amtsgericht Essen, Germany Accredited by DAkkS under registration D-ZE-12022-01[2] for the certification of trust services according to "DIN EN ISO/IEC 17065:2013" and "ETSI EN 319 403 V2.2.2 (2015-08)".

Identification of the trust service provider (TSP):	Fabrica Nacional de Moneda y Timbre – Real Casa de la Moneda, C/Jorge Juan, 106, Madrid, Spain, registered under Q2826004J at Registro comercial, Madrid, Spain

Identification of the audited Root-CA:	AC RAIZ FNMT-RCM	
	Distinguished Name	OU = AC RAIZ FNMT-RCM O = FNMT-RCM C = ES
	SHA-256 fingerprint	eb c5 57 0c 29 01 8c 4d 67 b1 aa 12 7b af 12 f7 03 b4 61 1e bc 17 b7 da b5 57 38 94 17 9b 93 fa
	Certificate Serial number	5d 93 8d 30 67 36 c8 06 1d 1a c7 54 84 69 07
	Applied policy	OVCP of ETSI EN 319 411-1 QCP-n of ETSI EN 319 411-2 QCP-l of ETSI EN 319 411-2 TSS of ETSI EN 319 421

[1] In the following termed shortly „TÜViT"
[2] http://www.dakks.de/en/content/accredited-bodies-dakks?Regnr=D-ZE-12022-01-01

The audit was performed as full period of time audit at the TSP's location in Madrid, Spain. It took place from 2017-11-20 until 2017-11-23 with additional document checks performed until 2018-01-13 and covered the period from 2017-01-13 until 2018-01-12. The audit was performed according to the European Standards "ETSI EN 319 411-2, V2.1.1 (2016-02)", "ETSI EN 319 411-1, V1.1.1 (2016-02)" and "ETSI EN 319 401, V2.1.1 (2016-02)" as well as CA Browser Forum Requirements "Baseline Requirements, version 1.5.5" considering the requirements of the "ETSI EN 319 403, V2.2.2 (2015-08)" for the Trust Service Provider Conformity Assessment.

The audit was based on the following policy and practice statement documents of the TSP:

1. TRUST SERVICES PRACTICES AND ELECTRONIC CERTIFICATION GENERAL STATEMENT, Version 5.2 as of 2017-10-09,
2. SPECIFIC CERTIFICATION PRACTICES AND POLICY FOR NATURAL PERSON CERTIFICATES FROM THE "AC FNMT USUARIOS", Version 1.2 as of 2017-01-03,
3. SPECIFIC CERTIFICATION PRACTICES AND POLICY OF CERTIFICATES OF REPRESENTATIVES OF LEGAL ENTITIES AND OF INSTITUTIONS WITH NO LEGAL ENTITY FROM THE "AC REPRESENTACIÓN", Version 1.4 as of 2017-01-03,
4. 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,
5. SPECIFIC CERTIFICATION POLICY AND PRACTICES APPLICABLE TO COMPONENT CERTIFICATES, Version 1.5 as of 2017-01-03,
6. CERTIFICATION PRACTICES AND POLICIES STATEMENT ON CENTRALISED ELECTRONIC SIGNATURE CERTIFICATES FOR PUBLIC EMPLOYEES, Version 1.0 as of 2017-05-17,
7. TS POLICIES AND PRACTICES OF THE QUALIFIED TIME STAMPING SERVICE, Version 1.0 as of 2017-01-03.

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. The TSP assured that all non-revoked Sub-CA's that are technically capable of issuing server or email certificates and that have been issued by this Root-CA are in the scope of regular audits. It has been explicitly assured by the TSP and verified during the audit that the CA's "AC FNMT Usuarios" and "AC Representacion" do not issue SSL / TLS certificates (ExtendedKeyUsage 1.3.6.1.5.5.7.3.1 – TLS web server authentication).

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy	Service	EKU	Validity
AC Administración Pública	CN = AC Administración Pública, SERIALNUMBER = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES	83 0f f2 05 ae 69 48 50 59 c3 fb 23 76 a7 f2 f9 ee 1c 2a 61 de 25 9d d0 9d 0b b6 ad 69 f8 88 32	02	OVCP QCP-n QCP-l	server authentication, signatures, seals	Not defined	2010-05-21 until 2022-05-21
AC Componentes Informáticos	OU = AC Componentes Informáticos, O = FNMT-RCM, C = ES	f0 38 42 1f 07 f2 0d 63 a2 0d 36 91 e5 a1 78 ab 84 59 eb e5 70 c1 64 7b 76 90 55 4e f2 38 76 ab	34 c6 ab 04 4e 36 99 12 51 c8 25 0b 6c 94 d6 c0	OVCP QCP-l TSS	server authentication, seals, time stamp units	Not defined	2013-06-24 until 2028-06-24
AC FNMT Usuarios	CN = AC FNMT Usuarios, OU = Ceres, O = FNMT-RCM, C = ES	60 12 93 ca 20 b0 9a 03 29 5d 19 62 56 c6 95 3f f9 eb a8 11 db 8e 3c e1 40 41 3c 1b ff e9 a8 69	45 5f 3a e1 5c 21 cd ba 54 4f 82 aa 47 51 eb db	QCP-n	signatures	Not defined	2014-10-28 until 2029-10-28

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy	Service	EKU	Validity
AC Representación	CN = AC Representación OU = CERES O = FNMT-RCM C = ES	8f d1 6a 17 99 44 d5 d1 d4 20 af 09 40 5e da 7a bf 2a 9c 74 28 83 e8 c2 f8 9e 0d 90 af af 75 4b	61 c2 d4 d4 f6 a9 ae 77 55 92 66 b9 8d af d6 21	QCP-n	signatures	Not defined	2015-06-30 until 2029-12-31

Table 1: Sub-CA's issued by the Root-CA

Modifications record

Version	Issuing Date	Changes
Version 1	2018-04-12	Initial attestation

End of the audit attestation letter.