Audit Attestation for

DFN Verein e.V.

Reference: AA2020113001

Essen, 2020-11-30

To whom it may concern,

This is to confirm that “TÜV Informationstechnik GmbH” has audited the CAs of “DFN Verein e.V.” without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “**AA2020113001**” and consist of 7 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,

Dr. Silke Keller	Ralf Schneider
Reviewer	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):	DFN-Verein e. V., Alexanderplatz 1, 10178 Berlin, Germany, registered under 7729NZ" at "Vereinsregister des Amtsgerichts Berlin-Charlottenburg", Berlin, Germany

Identification of the audited Root-CA:	T-TeleSec GlobalRoot Class 2	
	Distinguished Name	C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 2
	SHA-256 fingerprint	91E2F5788D5810EBA7BA58737DE1548A8ECACD014598BC0B143E041B17052552
	Applied policy	ETSI EN 319 411-1 V1.2.2, policy OVCP & NCP

[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 of the Root CA itself is not object of this audit attestation. The Root CA was already successfully audited which is confirmed in the “Audit Attestation for Deutsche Telekom Security GmbH - Reference AA2020071702” as of 2020-07-29.

This audit attestation concerns the Intermediate CA which has been issued under the above mentioned Root CA:

Identification of the audited Intermediate-CA:	DFN-Verein Certification Authority 2	
	Distinguished Name	C=DE, O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V., OU=DFN-PKI, CN=DFN-Verein Certification Authority 2
	SHA-256 fingerprint	F660B0C256481CB2BFC67661C1EA8FEEE39 5B7141BCAC36C36E04D08CD9E1582
	Applied policy	ETSI EN 319 411-1 V1.2.2, policy OVCP & NCP

The audit was performed as full period of time audit at the TSP’s location in Hamburg, Göttingen, Chemnitz and Münster, Germany. It took place from 2020-08-11 until 2020-08-12 in Hamburg, from 2020-08-24 to 2020-08-25 for the sites Göttingen and Chemnitz remotely and on 2020-09-18 in Münster, Germany. It covered the period from 2019-10-3 until 2020-09-18. The audit was performed according to the European Standards, “ETSI EN 319 411-1, V1.2.2 (2018-04)” and “ETSI EN 319 401, V2.2.1 (2018-04)” as well as CA Browser Forum Requirements “Baseline Requirements, version 1.7.0” 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. Zertifizierungsrichtlinie der DFN-PKI – Sicherheitsniveau “Global” –, version 8, as of 2020-09-30
2. Erklärung zum Zertifizierungsbetrieb der DFN-PKI – Sicherheitsniveau “Global” –, version 8, as of 2020-09-30

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in table 1 and that have been covered in this audit.No major non-conformities have been identified during the audit.

No major non-conformities have been identified during the audit.

In the following areas, minor non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
7.4 Human resources & 7.8 Network security

Documentation and implementation of firewall administration shall be improved. [REQ-7.4-03, REQ-7.8-08]

Findings with regard to ETSI EN 319 411-1:
None.

For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as documented under

- Bug 1651132, DFN Verein e.V.: 42 certificates with RSA modulus size in bits not divisable by 8:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1651132

The remediation measures taken by DFN Verein e.V. as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

Distinguished Name	SHA-256 fingerprint	Applied policy	EKU
C=DE, ST=Berlin, L=Berlin, O=Deutscher Bundestag, CN=Deutscher Bundestag CA - G02	4C9E0538F985690DE9D5CE1C38F16C24B4C39A1710C0881CDB06E2AFDB757B4D	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined
C=DE, O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V., OU=DFN-PKI, CN=DFN-Verein Global Issuing CA	1257AAC2F4EEAC6CA4942C2C83F0B67B41A3B47120C4D53429929513ACAD468C	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined
C=DE, ST=Bayern, L=Muenchen, O=Fraunhofer, OU=Fraunhofer Corporate PKI, CN=Fraunhofer Service CA - G02	ACBFAEBDCBCE1AC84C98CF24140B6061A97318E926215409DC0CF4C7BE506620	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined
C=DE, ST=Bayern, L=Muenchen, O=Fraunhofer, OU=Fraunhofer Corporate PKI, CN=Fraunhofer User CA - G02	562CBBCBDEBEEB3CB55946BDCE248CA4A623D2BA6E77B63B754D3A571F67DFA2	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined
C=DE, ST=Baden-Wuerttemberg, L=Karlsruhe, O=Karlsruhe Institute of Technology, CN=KIT-CA	01B9F3D08E31A9E8E1600D118C2ABFD856875EA60827020469865BA242EEBE1C	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined

C=DE, ST=Bayern, L=Muenchen, O=Max-Planck-Gesellschaft, CN=MPG CA - G02	FC2245BE59DC6461D4119C3A06EDBEE4D288556BD88C479E30ED5F3E81616469	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined
C=DE, O=Ruhr-Universitaet Bochum, CN=RUB-Chipcard CA G2	709BE4EAB0A3721236F28B2AB80F76FDA251330B3282F515EA5E0B6C79AE6729	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined
C=DE, O=Technische Universitaet Dortmund, CN=TU Dortmund Chipcard CA 2	E121C1694DA737C17B86448AEDC614EEBD7946A7B4B91FB30025B636070239EA	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined
C=DE, ST=Sachsen, L=Dresden, O=Technische Universitaet Dresden, CN=TU Dresden CA	E1B295E1465C24E0951EC0B90FBF7DA30B678E9E9CE4417DFFE9F34042DF4386	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined
C=DE, O=Technische Universitaet Ilmenau, CN=TU Ilmenau CA G2	1A5CCD714ABD7C7AF52A0FA946BC9C8F8696BCBF227D81339430E5D3394ECC97	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	not defined

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

Modifications record

Version	Issuing Date	Changes
Version 1.0	2020-11-30	Initial attestation

End of the audit attestation letter.