Audit Attestation for

DFN Verein e.V.

Reference: AA2019121601

Essen, 2019-12-16

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number “**AA2019121601**” and consists of 9 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	Dr. Bernd Kirsig
Reviewer	Lead Auditor

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	CN = T-TeleSec GlobalRoot Class 2 OU = T-Systems Trust Center O = T-Systems Enterprise Services GmbH C = DE
	SHA-256 fingerprint	91E2F5788D5810EBA7BA58737DE1548A8ECACD014598BC0B143E041B17052552
	Certificate Serial number	01
	Applied policy	policy OVCP & NCP of ETSI EN 319 411-1

[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 T-Systems International GmbH - Reference AA2019072602” as of 2019-07-26.

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	CN = DFN-Verein Certification Authority 2, OU = DFN-PKI, O = Verein zur Foerderung eines Deutschen Forschungsnetzes, e. V., C = DE
	SHA-256 fingerprint	F660B0C256481CB2BFC67661C1EA8FEEE395 B7141BCAC36C36E04D08CD9E1582
	Certificate Serial number	00E30BD5F8AF25D981
	Applied policy	OVCP and NCP of ETSI EN 319 411-1

The audit was performed as full period of time audit at the TSP’s location in Hamburg, Germany. It took place from 2019-11-27 until 2019-11-28 and covered the period from 2018-10-3 until 2019-10-2. 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 1.6.6” 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 4 as of 2019-05-15
2. Erklärung zum Zertifizierungsbetrieb der DFN-PKI – Sicherheitsniveau „Global“ – Version 4 as of 2019-05-15

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.

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

Findings with regard to ETSI EN 319 401:
6.2 Terms and Conditions

The TSP shall approve the Information Security Guideline (Informationssicherheitsleitlinie) and put it into effect. [ETSI EN 310 401, REQ-6.2-01]

6.3 Information Security

The TSP shall document in its CPS the maximum interval between two checks of appropriate system configuration. [ETSI EN 319 401, REQ-6.3-10]

7.9 Incident Management

The TSP shall define typical security incidents and assign a severity rating to the incidents. The TSP shall create lists of security incidents and implement defined reporting structures. Incidents shall be added to the ISMS. [ETSI EN 319 401, REQ-7.9-03]

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 1534580, DFN-PKI: 40 OV certificates with wrong ST: https://bugzilla.mozilla.org/show_bug.cgi?id=1534580.

The remediation measures taken by DFN PKI as described on Bugzilla (see link above) have been accompanied by the auditors and showed to properly address the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
Fraunhofer Service CA - G02	C=DE, ST=Bayern, L=Muenchen, O=Fraunhofer, OU=Fraunhofer Corporate PKI, CN=Fraunhofer Service CA - G02	ACBFAEBDCBCE1AC84C98CF24140B6061A97318E926215409DC0CF4C7BE506620	1B63BAB8CF33FA	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-05-24 to 2031-02-22
Fraunhofer User CA - G02	C=DE, ST=Bayern, L=Muenchen, O=Fraunhofer, OU=Fraunhofer Corporate PKI, CN=Fraunhofer User CA - G02	562CBBCBDEBEEB3CB55946BDCE248CA4A623D2BA6E77B63B754D3A571F67DFA2	1B63BAC68B5242	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-05-24 to 2031-02-22
DFN-Verein Global Issuing CA	C=DE, O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V., OU=DFN-PKI, CN=DFN-Verein Global Issuing CA	1257AAC2F4EEAC6CA4942C2C83F0B67B41A3B47120C4D53429929513ACAD468C	1B63BAD01E2C3D	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-05-24 to 2031-02-22

TU Dortmund Chipcard CA 2	C=DE, O=Technische Universitaet Dortmund, CN=TU Dortmund Chipcard CA 2	E121C1694DA737C17B86448AEDC614EEBD7946A7B4B91FB30025B636070239EA	1B809DBAC8F194EBDD5D27A8	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-06-15 to 2031-02-22
TU Ilmenau CA G2	C=DE, O=Technische Universitaet Ilmenau, CN=TU Ilmenau CA G2	1A5CCD714ABD7C7AF52A0FA946BC9C8F8696BCBF227D81339430E5D3394ECC97	1B9DCD8A84F6517B4758CCF4	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-07-07 to 2031-02-22
RUB-Chipcard CA G2	C=DE, O=Ruhr-Universitaet Bochum, CN=RUB-Chipcard CA G2	709BE4EAB0A3721236F28B2AB80F76FDA251330B3282F515EA5E0B6C79AE6729	1B9DCDA0A1BB20DCD658CFFF	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-07-07 to 2031-02-22
MPG CA - G02	C=DE, ST=Bayern, L=Muenchen, O=Max-Planck-Gesellschaft, CN=MPG CA - G02	FC2245BE59DC6461D4119C3A06EDBEE4D288556BD88C479E30ED5F3E81616469	1C3AD450847EEEF358F88E77	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-11-03 to 2031-02-22

Deutscher Bundestag CA - G02	C=DE, ST=Berlin, L=Berlin, O=Deutscher Bundestag, CN=Deutscher Bundestag CA - G02	4C9E0538F985690DE9D5CE1C38F16C24B4C39A1710C0881CDB06E2AFDB757B4D	1C3AD46FEC82C025CADB5A8D	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-11-03 to 2031-02-22
KIT-CA	C=DE, ST=Baden-Wuerttemberg, L=Karlsruhe, O=Karlsruhe Institute of Technology, CN=KIT-CA	01B9F3D08E31A9E8E1600D118C2ABFD856875EA60827020469865BA242EEBE1C	1C3AD48C24ED922EB0F490AE	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-11-03 to 2031-02-22
TU Dresden CA	C=DE, ST=Sachsen, L=Dresden, O=Technische Universitaet Dresden, CN=TU Dresden CA	E1B295E1465C24E0951EC0B90FBF7DA30B678E9E9CE4417DFFE9F34042DF4386	1C6E34243F3AD82C1BCC9135	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1	*server authentication, signature*	*None*	2016-12-12 to 2031-02-22

Table 1: Sub-CAs issued by the Intermediate CA

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
DFN-Verein Certification Authority 2	C=DE, O = Verein zur Foerderung eines Deutschen Forschungsnetzes e. V., OU = DFN-PKI, CN = DFN-Verein Certification Authority 2	F660B0C256481CB2BFC67661C1EA8FEEE395B7141BCAC36C36E04D08CD9E1582	E30BD5F8AF25D981	OVCP of ETSI EN 319 411-1 NCP of ETSI EN 319 411-1		*None*	2016-02-22 to 2031-02-22

Table 2: Intermediate CA issued by the Root-CA

Modifications record

Version	Issuing Date	Changes
Version 1.0	*2019-12-16*	Initial attestation

End of the audit attestation letter.