Audit Attestation for

DFN Verein e.V.

Reference: AA2021112501

Essen, 2021-11-25

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 “**AA2021112501**” 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
Am TÜV 1
45307 Essen, Germany
E-Mail: certuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

Dr. Silke Keller
Reviewer

Ralf Schneider
Leadauditor

Identification of the conformity assessment body (CAB):	• TÜV Informationstechnik GmbH[1], Am TÜV 1, 45307 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)". • Insurance Carrier (BRG section 8.2): HDI Global SE • Third-party affiliate audit firms involved in the audit: None.
Identification and qualification of the audit team:	• Number of team members: 1 Lead Auditor, 1 Auditor • Academic qualifications of team members: • All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See "Additional competences of team members" above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications;

[1] In the following termed shortly „TÜViT"
[2] https://www.dakks.de/en/accredited-body.html?id=D-ZE-12022-01-01

	b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective; d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits; b) has adequate knowledge and attributes to manage the audit process; and c) has the competence to communicate effectively, both orally and in writing. • All members are qualified and registered assessors within the accredited CAB. • Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
Identification and qualification of the reviewer performing audit quality management:	• Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 Reviewer • The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

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

Audit Period covered for all policies:	2020-09-19 to 2021-09-02
Audit dates:	2021-08-24 to 2021-08-25 (on site) 2021-08-31 (on site) 2021-09-01 to 2021-09-02 (remote)

Audit Location:	DFN-Verein e. V. c/o DFN-CERT Services GmbH, Nagelsweg 41, 20097 Hamburg, Germany Two external enterprise RAs in Osnabrück, Germany Due to COVID-19 / Sars-CoV-2 influences, two external enterprise RAs in Magdeburg and Braunschweig, both Germany, have been remotely inspected. The locations have not been inspected in person, but the physical security concept was discussed during the audit and identifications were performed on a sampling basis.
Type of audit	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit

Standards considered	European Standards: ☐ ETSI EN 319 411-2, V2.2.2 (2018-04) ☒ ETSI EN 319 411-1, V1.2.2 (2018-04) ☒ ETSI EN 319 401, V2.2.1 (2018-04) CA Browser Forum Requirements: ☐ EV SSL Certificate Guidelines, version 1.7.4 ☒ Baseline Requirements, version 1.7.6 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403 V2.2.2 (2015-08) ☒ ETSI TS 119 403-2 V1.2.4 (2020-11)

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

1. Zertifizierungsrichtlinie der DFN-PKI – Sicherheitsniveau “Global” –, version 9, as of 2021-06-30
2. Erklärung zum Zertifizierungsbetrieb der DFN-PKI – Sicherheitsniveau “Global” –, version 9, as of 2021-06-30

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

This Audit Attestation also covers the following incidents as documented under

- Bugzilla ID = 1705791, Telekom Security: Multiple commonName in certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1705791

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.

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

Table 1: Root-CA

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 AA2021070109” as of 2021-07-01.

Identification of the Intermediate-CA:			
Distinguished Name	C=DE, O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V., OU=DFN-PKI, CN=DFN-Verein Certification Authority 2	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP
SHA-256 fingerprint	F660B0C256481CB2BFC67661C1EA8FEEE395B7141BCAC36C36E04D08CD9E1582		

Table 2: Intermediate-CA in scope of this attestation

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Identification of the audited Sub-CAs					
Distinguished Name	C=DE, ST=Berlin, L=Berlin, O=Deutscher Bundestag, CN=Deutscher Bundestag CA - G02	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined
SHA-256 fingerprint	4C9E0538F985690DE9D5CE1C38F16C24B4C39A1710C0881CDB06E2AFDB757B4D				
Distinguished Name	C=DE, O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V., OU=DFN-PKI, CN=DFN-Verein Global Issuing CA	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined
SHA-256 fingerprint	1257AAC2F4EEAC6CA4942C2C83F0B67B41A3B47120C4D53429929513ACAD468C				
Distinguished Name	C=DE, ST=Bayern, L=Muenchen, O=Fraunhofer, OU=Fraunhofer Corporate PKI, CN=Fraunhofer Service CA - G02	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined
SHA-256 fingerprint	ACBFAEBDCBCE1AC84C98CF24140B6061A97318E926215409DC0CF4C7BE506620				

Distinguished Name	C=DE, ST=Bayern, L=Muenchen, O=Fraunhofer, OU=Fraunhofer Corporate PKI, CN=Fraunhofer User CA - G02	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined
SHA-256 fingerprint	562CBBCBDEBEEB3CB55946BDCE248CA4A623D2BA6E77B63B754D3A571F67DFA2				
Distinguished Name	C=DE, ST=Baden-Wuerttemberg, L=Karlsruhe, O=Karlsruhe Institute of Technology, CN=KIT-CA	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined
SHA-256 fingerprint	01B9F3D08E31A9E8E1600D118C2ABFD856875EA60827020469865BA242EEBE1C				
Distinguished Name	C=DE, ST=Bayern, L=Muenchen, O=Max-Planck-Gesellschaft, CN=MPG CA - G02	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined
SHA-256 fingerprint	FC2245BE59DC6461D4119C3A06EDBEE4D288556BD88C479E30ED5F3E81616469				
Distinguished Name	C=DE, O=Ruhr-Universitaet Bochum, CN=RUB-Chipcard CA G2	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined
SHA-256 fingerprint	709BE4EAB0A3721236F28B2AB80F76FDA251330B3282F515EA5E0B6C79AE6729				
Distinguished Name	C=DE, O=Technische Universitaet Dortmund, CN=TU Dortmund Chipcard CA 2	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined

SHA-256 fingerprint	E121C1694DA737C17B86448AEDC614EEBD7946A7B4B91FB30025B636070239EA				
Distinguished Name	C=DE, ST=Sachsen, L=Dresden, O=Technische Universitaet Dresden, CN=TU Dresden CA	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined
SHA-256 fingerprint	E1B295E1465C24E0951EC0B90FBF7DA30B678E9E9CE4417DFFE9F34042DF4386				
Distinguished Name	C=DE, O=Technische Universitaet Ilmenau, CN=TU Ilmenau CA G2	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP ETSI EN 319 411-1 V1.2.2, OVCP	EKU	Not defined
SHA-256 fingerprint	1A5CCD714ABD7C7AF52A0FA946BC9C8F8696BCBF227D81339430E5D3394ECC97				

Table 3: Sub-CA's issued by the Root-CA or its Sub-CA's

Modifications record

Version	Issuing Date	Changes
Version 1.0	2021-11-25	Initial attestation

End of the audit attestation letter.