Audit Attestation for

DFN-Verein e.V.

Reference: AA2018121902

Essen, 19.12.2018

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 “**AA2018121902**” and consist of 5 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 Reviewer	*Bernd Kirsig* 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 Global Root 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	91 E2 F5 78 8D 58 10 EB A7 BA 58 73 7D E1 54 8A 8E CA CD 01 45 98 BC 0B 14 3E 04 1B 17 05 25 52
	Certificate Serial number	01
	Applied 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 AA2018072003” as of 2018-07-20.

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	F6 60 B0 C2 56 48 1C B2 BF C6 76 61 C1 EA 8F EE E3 95 B7 14 1B CA C3 6C 36 E0 4D 08 CD 9E 15 82
	Certificate Serial number	00 E3 0B D5 F8 AF 25 D9 81
	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 and Munich, Germany. It took place from September 27th, 2018 until September 28th, 2018 in Munich and from October 1st, 2018 until October 2nd, 2018 in Hamburg and covered the period from October 26th, 2017 until October 2nd, 2018. The audit was performed according to the European Standards , “ETSI EN 319 411-1, V1.1.1 (2016-02)” and “ETSI EN 319 401, V2.1.1 (2016-02)” as well “Baseline Requirements, version 1.6.0” 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 3.8 valid from 2018-03-18, DFN Verein
2. Erklärung zum Zertifizierungsbetrieb der DFN-PKI – Sicherheitsniveau Global”, version 3.8 as of 2018-03-18, DFN-Verein

The following non-conformities have been identified during the audit:

- The TSP shall describe how subscribers are informed in case of incidents. [ETSI EN 319 401, 7.9 e)]
- The TSP shall add to the CPS a paragraph that it addresses any critical vulnerabilities within 48 hours after discovery. [ETSI EN 319 401, 7.9 e)]
- The TSP shall prepare a detailed and up-to-date Termination Plan. [ETSI EN 319 401, 7.12 a)].
- The policy NCP for natural person / email certificates shall be added to the CP. [ETSI EN 319 411-1, 7.1 a)]

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in List 2 of CA's of the DFN-PKI", version 1.0 as of 2018-12-19 which is attached to the attestation. 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.

Modifications record

Version	Issuing Date	Changes
Version 1.0	2018-12-19	Initial attestation

End of the audit attestation letter.

List 2 of CA's of the DFN-PKI

Project ID:	TUVIT-CA67122
Certification Service:	DFN-PKI Sicherheitsniveau Global
Operator:	DFN-Verein e. V. (short DFN-Verein) Alexanderplatz 1 10178 Berlin
Sponsor:	DFN-Verein
Certification Body:	TÜV Informationstechnik GmbH Member of TÜV NORD GROUP Certification Body Langemarckstraße 20 45141 Essen, Germany
Date of Audit:	2018-09-27 until 2018-10-02
Evaluation Standard:	ETSI EN 319 411-1, V1.1.1 (2016-02) policy OVCP
Version:	1.0
Author:	Bernd Kirsig
Date of Report:	2018-12-19

.....	.....
Dr. Silke Keller	Bernd Kirsig
Reviewer	Author

TABLE OF CONTENTS

1 Evaluated Certification Authorities 3
1.1 Root-CA 3
1.2 Intermediate CA 3
1.3 SHA-2 Issuing CA's of the DFN-PCA 4
2 Minimum Cryptographic Algorithm and Key Sizes 8
3 List of Abbreviations 11

1 Evaluated Certification Authorities

1.1 Root-CA

The DFN-PKI Sicherheitsniveau Global comprises the following Root CA's as downloaded from the webpage https://www.pki.dfn.de/wurzelzertifikate/globalroot2/. The Root CA is not subject of the inspection.

1. T-TeleSec GlobalRoot Class 2

subject	CN = T-TeleSec GlobalRoot Class 2, OU = T-Systems Trust Center, O = T-Systems Enterprise Services GmbH, C = DE	
issuer	CN = T-TeleSec GlobalRoot Class 2, OU = T-Systems Trust Center, O = T-Systems Enterprise Services GmbH, C = DE	
serial number (hex)	01	
validity	Not Before: 2008-10-01, 10:40:14 UTC	Not After: 2033-10-01, 23:59:59 UTC
public key length	2048 Bit	
signature	2048 Bit RSA with SHA-256	
SHA-256 finger-print	91e2f5788d5810eba7ba58737de1548a8ecacd014598bc0b143e041b17052552	

1.2 Intermediate CA

The DFN-PKI Sicherheitsniveau Global comprises the following intermediate CA as downloaded from the webpages https://www.pki.dfn.de/wurzelzertifikate/globalroot/ and https://www.pki.dfn.de/wurzelzertifikate/globalroot2/.

1. DFN Verein Certification Authority 2

subject	CN = DFN-Verein Certification Authority 2, OU = DFN-PKI O = Verein zur Foerderung eines Deutschen Forschungs-netzes e. V., C = DE	
issuer	CN = T-TeleSec GlobalRoot Class 2, OU = T-Systems Trust Center, O = T-Systems Enterprise Services GmbH, C = DE	
serial number (hex)	00 e3 0b d5 f8 af 25 d9 81	
validity	Not Before: 2016-02-22, 13:38:22 UTC	Not After: 2031-02-22, 23:59:59 UTC
public key length	2048 Bit	
signature	2048 Bit RSA with SHA-256	
SHA-256 finger-print	F6 60 B0 C2 56 48 1C B2 BF C6 76 61 C1 EA 8F EE E3 95 B7 14 1B CA C3 6C 36 E0 4D 08 CD 9E 15 82	

1.3 SHA-2 Issuing CA's of the DFN-PCA

The DFN-PKI Sicherheitsniveau Global comprises the following issuing CA's that are subject of the inspection as provided by DFN-Verein and downloadable from the web page https://info.pca.dfn.de/.

1. Deutscher Bundestag CA - G02

subject	/C=DE/ST=Berlin/L=Berlin/O=Deutscher Bundestag/CN=Deutscher Bundestag CA - G02	
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2	
serial number (hex)	1C 3A D4 6F EC 82 C0 25 CA DB 5A 8D	
validity	notBefore=Nov 3 15:25:19 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	
signature	sha256WithRSAEncryption	
SHA-256 finger-print	4C 9E 05 38 F9 85 69 0D E9 D5 CE 1C 38 F1 6C 24 B4 C3 9A 17 10 C0 88 1C DB 06 E2 AF DB 75 7B 4D	

2. DFN-Verein Global Issuing CA

subject	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Global Issuing CA	
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2	
serial number (hex)	1B 63 BA D0 1E 2C 3D	
validity	notBefore=May 24 11:38:40 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	
signature	sha256WithRSAEncryption	
SHA-256 finger-print	12 57 AA C2 F4 EE AC 6C A4 94 2C 2C 83 F0 B6 7B 41 A3 B4 71 20 C4 D5 34 29 92 95 13 AC AD 46 8C	

3. Fraunhofer Service CA - G02

subject	/C=DE/ST=Bayern/L=Muenchen/O=Fraunhofer/OU=Fraunhofer Corporate PKI/CN=Fraunhofer Service CA - G02
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2
serial number (hex)	1B 63 BA B8 CF 33 FA

validity	notBefore=May 24 11:38:16 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	
signature	sha256WithRSAEncryption	
SHA-256 finger-print	AC BF AE BD CB CE 1A C8 4C 98 CF 24 14 0B 60 61 A9 73 18 E9 26 21 54 09 DC 0C F4 C7 BE 50 66 20	

4. Fraunhofer User CA - G02

subject	/C=DE/ST=Bayern/L=Muenchen/O=Fraunhofer/OU=Fraunhofer Corporate PKI/CN=Fraunhofer User CA - G02	
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2	
serial number (hex)	1B 63 BA C6 8B 52 42	
validity	notBefore=May 24 11:38:30 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	
signature	sha256WithRSAEncryption	
SHA-256 finger-print	56 2C BB CB DE BE EB 3C B5 59 46 BD CE 24 8C A4 A6 23 D2 BA 6E 77 B6 3B 75 4D 3A 57 1F 67 DF A2	

5. KIT-CA

subject	/C=DE/ST=Baden-Wuerttemberg/L=Karlsruhe/O=Karlsruhe Institute of Technology/CN=KIT-CA	
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2	
serial number (hex)	1C 3A D4 8C 24 ED 92 2E B0 F4 90 AE	
validity	notBefore=Nov 3 15:25:48 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	
signature	sha256WithRSAEncryption	
SHA-256 finger-print	01 B9 F3 D0 8E 31 A9 E8 E1 60 0D 11 8C 2A BF D8 56 87 5E A6 08 27 02 04 69 86 5B A2 42 EE BE 1C	

6. MPG CA - G02

subject	/C=DE/ST=Bayern/L=Muenchen/O=Max-Planck-Gesellschaft/CN=MPG CA - G02	
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2	
serial number (hex)	1C 3A D4 50 84 7E EE F3 58 F8 8E 77	
validity	notBefore=Nov 3 15:24:48 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	

signature	sha256WithRSAEncryption
SHA-256 fingerprint	FC 22 45 BE 59 DC 64 61 D4 11 9C 3A 06 ED BE E4 D2 88 55 6B D8 8C 47 9E 30 ED 5F 3E 81 61 64 69

7. RUB-Chipcard CA G2

subject	/C=DE/O=Ruhr-Universitaet Bochum/CN=RUB-Chipcard CA G2	
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2	
serial number (hex)	1B 9D CD A0 A1 BB 20 DC D6 58 CF FF	
validity	notBefore=Jul 7 12:50:24 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	
signature	sha256WithRSAEncryption	
SHA-256 fingerprint	70 9B E4 EA B0 A3 72 12 36 F2 8B 2A B8 0F 76 FD A2 51 33 0B 32 82 F5 15 EA 5E 0B 6C 79 AE 67 29	

8. TU Dortmund Chipcard CA 2

subject	/C=DE/O=Technische Universitaet Dortmund/CN=TU Dortmund Chipcard CA 2	
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2	
serial number (hex)	1B 80 9D BA C8 F1 94 EB DD 5D 27 A8	
validity	notBefore=Jun 15 09:30:18 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	
signature	sha256WithRSAEncryption	
SHA-256 fingerprint	E1 21 C1 69 4D A7 37 C1 7B 86 44 8A ED C6 14 EE BD 79 46 A7 B4 B9 1F B3 00 25 B6 36 07 02 39 EA	

9. TU Dresden CA

subject	/C=DE/ST=Sachsen/L=Dresden/O=Technische Universitaet Dresden/CN=TU Dresden CA	
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2	
serial number (hex)	1C 6E 34 24 3F 3A D8 2C 1B CC 91 35	
validity	notBefore=Dec 12 14:39:16 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	
signature	sha256WithRSAEncryption	
SHA-256 fingerprint	E1 B2 95 E1 46 5C 24 E0 95 1E C0 B9 0F BF 7D A3 0B 67 8E 9E 9C E4 41 7D FF E9 F3 40 42 DF 43 86	

10. TU Ilmenau CA G2

subject	/C=DE/O=Technische Universitaet Ilmenau/CN=TU Ilmenau CA G2	
issuer	/C=DE/O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V./OU=DFN-PKI/CN=DFN-Verein Certification Authority 2	
serial number (hex)	1B 9D CD 8A 84 F6 51 7B 47 58 CC F4	
validity	notBefore=Jul 7 12:50:02 2016 GMT	notAfter=Feb 22 23:59:59 2031 GMT
public key length	2048 bit	
signature	sha256WithRSAEncryption	
SHA-256 finger-print	1A 5C CD 71 4A BD 7C 7A F5 2A 0F A9 46 BC 9C 8F 86 96 BC BF 22 7D 81 33 94 30 E5 D3 39 4E CC 97	

2 Minimum Cryptographic Algorithm and Key Sizes

The ETSI document [ETSI TS 102 176-1] makes the following statements on the suitability (validity) of signature suites (algorithms and key sizes) that are independent of the kind of certificate:

signature suite	2017	2020	2030
sha1-with-rsa	not recommended		
sha256-with-rsa	2048	2048	not recommended
RSASSA-PSS with mgf1SHA-1Identifier	not recommended		
RSASSA-PSS with mgf1SHA-224Identifier	2048	2048	not recommended
RSASSA-PSS with mgf1SHA-256Identifier	2048	2048	3072
sha1-with-dsa	not recommended		
sha1-with-ecdsa	not recommended		
sha224-with-ecdsa	224	not recommended	
sha256-with-ecdsa	256	256	256
sha256-with-dsa	256	256	256

Table 1: Recommended signature suites and key length

The following minimum cryptographic algorithm and key sizes are required by appendix A of [EV Guidelines]. For polies EVCP(+) the document [EV Guidelines] is applied instead of [ETSI TS 102 176-1]:

	validity period begins before end 2010	**validity period begins after end 2010**
Root CA Certificates	MD5[1], SHA-1, SHA-256, SHA-384, SHA-512 RSA 2048[2], ECC NIST P-256, P-384, P-521	SHA-1[3], SHA-256 SHA-384 SHA-512 RSA 2048, ECC NIST P-256, P-384, P-521
	validity period begins before end 2010 and ends before end 2013	**validity period begins after end 2010 or ends after end 2013**
Subordinate CA Certificates	SHA-1, SHA-256, SHA-384, SHA-512 RSA 1024, ECC NIST P-256, P-384, P-521	SHA-1[3], SHA-256 SHA-384 SHA-512 RSA 2048, ECC NIST P-256, P-384, P-521
	validity period ends before end 2013	**validity period ends after end 2013**
Subscriber Certificates	SHA-1[3], SHA-256, SHA-384, SHA-512 RSA 1024, ECC NIST P-256, P-384, P-521	SHA-1[3], SHA-256 SHA-384 SHA-512 RSA 2048, ECC NIST P-256, P-384, P-521

Table 2: Minimum cryptographic algorithm and key sizes

[1] MD5 not recommended

[2] A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as a trust anchor for Subscriber Certificates issued in accordance with these Requirements.

[3] Effective 1 January 2016, CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm. CAs MAY continue to sign certificates to verify OCSP responses using SHA1 until 1 January 2017. CAs MAY continue to use their existing SHA-1 Root Certificates. SHA-2 Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate.
Effective 16 January 2015, CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017.

The following table shows keys and certificates used for the CA operation and highlights the validity according to [ETSI TS 102 176-1] and [EV Guidelines] specifications:

CA type certificate	key algorithm signature suites	Validity
Root-CA Deutsche Telekom Root CA 2	RSA-2048 SHA-1 with RSA-2048	ETSI: not recommended BRG / EV: valid
Root-CA T-TeleSec GlobalRoot Class 2	RSA-2048 SHA-256 with RSA-2048	ETSI: 2020 BRG / EV: valid
Intermediate-CA DFN-Verein PCA Global - G01 DFN-Verein Certification Authority 2	RSA-2048 SHA-256 with RSA-2048	ETSI: 2020 BRG / EV: valid
issuing CA's (active) as listed above	RSA-2048 SHA-256 with RSA-2048	ETSI: 2020 BRG / EV: valid
Subscriber Certificates	RSA-2048 SHA-256 with RSA-2048	ETSI: 2020 BRG / EV: valid

Table 3: Expected applicability of keys and algorithms

3 List of Abbreviations

ARL	Authority Certificate Revocation List
AIDE	Advanced Intrusion Detection Environment
CA	Certification Authority
CAB	CA/Browser [Forum]
CC	Common Criteria
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DAkkS	Deutsche Akkreditierungsstelle
DNI	Spanish eID card (Documento Nacional de Identidad)
EAL	Evaluation Assurance Level
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
EVCP+	Enhanced Extended Validation Certificate Policy (with SUD)
HSM	Hardware Security Module
ISMS	Information Security Management System
ITSEC	Information Technology Security Evaluation Criteria
LCP	Lightweight Certificate Policy
NCP	Normalized Certificate Policy
NCP+	extended Normalized Certificate Policy (with SUD)
NIST	National Institute of Standards and Technology (USA)
OCSP	Online Certificate Status Protocol
PDCA	Plan Do Check Act
PIN	Personal Identification Number

PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
RA	Registration Authority
SOF	Strength Of Function
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
SUD	Secure User Device
TLS	Transport Layer Security
TSS	Time Stamp System