

Audit Attestation for

Atos Information Technology GmbH

Reference: DSC.1036

“Bremen, 2021-06-08”

To whom it may concern,

This is to confirm that datenschutz cert GmbH has audited the CAs of the Atos Information Technology GmbH without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number DSC.1036 and consists of << 21 >> pages.

Kindly find here below the details accordingly.

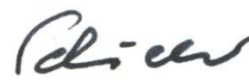
In case of any question, please contact:

Datenschutz cert GmbH
Konsul-Smidt-Strasse 88a
28217 Bremen, Germany
E-Mail: office@datenschutz-cert.de
Phone: +49-421-69663250

With best regards,



Dr. Irene Karper
Reviewer



Klaus-Werner Schröder
Lead Auditor

<p>Identification of the conformity assessment body (CAB) and assessment organization:</p>	<ul style="list-style-type: none"> • datenschutz cert GmbH¹, Konsul-Smidt-Straße 88a, 28217 Bremen, Germany registered under Amtsgericht Bremen HRB 26787 HB • Accredited by Deutsche Akkreditierungsstelle GmbH under registration https://www.dakks.de/files/data/as/pdf/D-ZE-16077-01-00.pdf² 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): ERGO Versicherung AG • Third-party affiliate audit firms involved in the audit: none.
<p>Identification and qualification of the audit team:</p>	<ul style="list-style-type: none"> • Number of team members: 2 • 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 <ol style="list-style-type: none"> 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:

¹ in the following termed shortly “CAB”

² URL to the accreditation certificate hosted by the national accreditation body

	<p>See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in:</p> <ul style="list-style-type: none"> a) knowledge of the CA/TSP standards and other relevant publicly available specifications; 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. <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> 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. • Special skills or qualifications employed throughout audit: none. • Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB. • Auditor’s code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
<p>Identification and qualification of the reviewer performing audit quality management:</p>	<ul style="list-style-type: none"> • Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 • 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):	Atos Information Technology GmbH, Otto-Hahn-Ring 6, 81739 München, Germany, registered under Amtsgericht München HRB 235509
Audit Period covered for all policies:	2020-04-28 to 2021-04-27
Audit dates:	2020-09-23 to 2020-09-24 (on site) 2021-04-21 (remote) 2021-04-22 (on site) 2021-04-23 (remote)
Audit Location:	Bavaria Lower Saxony

Identification of the audited Root-CA:	name of the root, e.g. common Name	
AtosTrustedRoot2011	Distinguished Name	CN = Atos TrustedRoot 2011 O = Atos C = DE
	SHA-256 fingerprint	F356BEA244B7A91EB35D53CA9AD7864ACE018E2D35D5F8F96DDF68A6F41AA474
	Certificate Serial number	5C33CB622C5FB332
	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP
Atos TrustedRoot 1 2019	Distinguished Name	CN = Atos TrustedRoot 1 2019 O = Atos C = DE
	SHA-256 fingerprint	1E462392EEA932A5D605E814B0CE859C680D7580B598C27675A6E0724E8496F9
	Certificate Serial number	4CCA9B2AD999B95BA8
	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP
Atos TrustedRoot 2 2019	Distinguished Name	CN = Atos TrustedRoot 2 2019 O = Atos C = DE
	SHA-256 fingerprint	CED96986E88D86FFF4221F33079ACBE2E126F4CDEFB31E5ADCDAD0A988B99EFE
	Certificate Serial number	0E67855FDB0B59B723

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Identification of the audited Root-CA:	name of the root, e.g. common Name	
	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP
Atos TrustedRoot 3 2019	Distinguished Name	CN = Atos TrustedRoot 3 2019 O = Atos C = DE
	SHA-256 fingerprint	BC0DD3320C194D5E983F18457E21DA12C99F92BD8E92BAF64300D1FF66BA1D55
	Certificate Serial number	48EB671E7CF0226B41
	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP
Atos IoT Root CA 2020	Distinguished Name	CN = Atos IoT Root CA 2020 O = Atos OU = IoT PKI C = DE
	SHA-256 fingerprint	D610385C06085AFDFB98591677219077F3DA25A3A0D590620E881A0F145BF74A
	Certificate Serial number	1B5BCFE58913BAF341D1F0973A44529D
	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP
Atos TrustedRoot Root CA ECC G2 2020	Distinguished Name	CN = Atos TrustedRoot Root CA ECC G2 2020 O = Atos C = DE

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Identification of the audited Root-CA:	name of the root, e.g. common Name	
	SHA-256 fingerprint	E38655F4B0190C84D3B3893D840A687E190A256D98052F159E6D4A39F589A6EB
	Certificate Serial number	0B7328111874301CEF6F0884
	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP
Atos TrustedRoot Root CA RSA G2 2020	Distinguished Name	CN = Atos TrustedRoot Root CA RSA G2 2020 O = Atos C = DE
	SHA-256 fingerprint	78833A783BB2986C254B9370D3C20E5EBA8FA7840CBF63FE17297A0B0119685E
	Certificate Serial number	47BA2946553E169297B0AB40
	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP
Atos TrustedRoot Root CA ECC TLS 2021	Distinguished Name	CN = Atos TrustedRoot Root CA ECC TLS 2021 O = Atos C = DE
	SHA-256 fingerprint	B2FAE53E14CCD7AB9212064701AE279C1D8988FACB775FA8A008914E663988A8
	Certificate Serial number	3D983BA6663D9063F77E26573804EF00
	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP
	Distinguished Name	CN = Atos TrustedRoot Root CA RSA TLS 2021

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Identification of the audited Root-CA:	name of the root, e.g. common Name	
Atos TrustedRoot Root CA RSA TLS 2021		O = Atos C = DE
	SHA-256 fingerprint	81A9088EA59FB364C548A6F85559099B6F0405EFBF18E5324EC9F457BA00112F
	Certificate Serial number	53D5CFE619930BFB2B0512D8C22AA2A4
	Applied policy	ETSI EN 319 411-1 V1.2.2, NCP

The audit was performed as full period of time audit at the TSP's location in Meppen, Lower Saxony, Germany, and Nürnberg/Fürth, Bavaria, Germany. It took place from 2020-09-23 until 2021-04-23 and covered the period from 2020-04-28 until 2021-04-27. 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 "EV SSL Certificate Guidelines, version 1.7.4" and "Baseline Requirements, version 1.7.4" considering the requirements of the "ETSI EN 319 403-1 V2.3.1 (2020-06)" and "ETSI TS 119 403-2 V1.2.4 (2020-11)" for the Trust Service Provider Conformity Assessment.

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Public

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

1. Certification Practice Statement Root CA, Version 2.5.0, 2021-04-07
2. Certification Practice Statement Issuing CA in Version 2.4.0, 2021-04-07

In the following area, a non-conformity has been identified throughout the audit:

Findings with regard to BR 1.7.4, sec. 9.6.3 No 3:

The Subscriber Agreement or Terms of Use do not contain an obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy.

The Subscriber Agreement or Terms of Use shall be improved.

Findings with regard to ETSI EN 319 401:

None.

Findings with regard to ETSI EN 319 411-1:

None.

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as documented under

- Bug 1626355, Atos: Tracking bug for possible audit delays:
https://bugzilla.mozilla.org/show_bug.cgi?id=1626355.
- Bug 1649963, Atos: Incorrect OCSP Delegated Responder Certificate:
https://bugzilla.mozilla.org/show_bug.cgi?id=1649963.

The remediation measures taken by Atos Information Technology GmbH 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.

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 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

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = Atos TrustedRoot Client CA 2011 O = Atos C=DE	140DCFC461F014D0CB5EA59BE0840D6F6EC4558539E12A99531CE7DF938F7AEE	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined
CN = Atos TrustedRoot Client CA 2012 O = Atos C = DE	4CB5CB705D4952497B4ED7C46A8564EA5C9137279F38C86B7BCA8E8883868B09	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined
CN = Atos TrustedRoot Client CA 2013 O = Atos C = DE	E0A4A91C50AFC4FB2CECDEB41ED8CAE72BF0144FB0D628B493FEAC511120FD73	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined
CN = Atos TrustedRoot Issuing CA for Primetals 2015 O = Atos C = DE	574342ADAB4ED79EF7818E8299058E1C071AC0E431FE421CABB62DF4D4E9E4C5	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = Atos TrustedRoot Issuing CA for WWE 2015 O = Atos C = DE	74AFCEECE0731587B45C3CDA7BC210FC917502A323401E932E865BC3D797E7AB	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined
CN = Atos TrustedRoot Client Issuing CA 2015 O = Atos C=DE	40F47955BEA3EA726CADAC5D3FE61297FE7BEBAE5B0509E1EF7B29C838F49D20	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined
CN = Atos TrustedRoot Client CA for equensWorldlineP artner 2017 O = Atos C = DE	7AF4F0DCC03F9D2BD345F264B93E0432EA02260BD618263FC557DCF1266C07AB	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined
CN = Atos TrustedRoot Client-CA for equensWorldlineP artner 2019 O = Atos C = DE	0CE33A4271B1E46CFFB432DB83A4F9C5261AF88BF2451D8AEF9021F60B20BE65	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	1.3.6.1.5.5 .7.3.2 (id- kp- clientAuth) 1.3.6.1.5.5 .7.3.4 (id- kp-

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
			emailProtection)
CN = Atos TrustedRoot Mailgateway CA 2017 O = Atos C = DE	69365C6E42802E0666ABE93096BD4E2E30E012E55E28ECEB0679893048E23A5E	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined
CN = Atos TrustedRoot Mailgateway CA 2019 O = Atos C = DE	6E81509376C93FBCE79472C843A568E883CB5D23ECEEA8299A5CBE9C57BCEE1C	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	1.3.6.1.5.5 .7.3.2 (id-kp-clientAuth) 1.3.6.1.5.5 .7.3.4 (id-kp-emailProtection)
CN = Atos TrustedRoot Server-CA 2013 O = Atos C=DE	AAAFE93E359B149A4C9E0B572D51BF37FDA38A7E9A359BF90359BA9CAA96AADF	ETSI EN 319 411-1 V1.2.2, NCP, DVCP, OVCP	not defined

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = Atos TrustedRoot Server-CA 2017 O = Atos C = DE	831D8FE8989520F4CBA62E4063143850AD7E570385B94B8E958DB48993B8677E	ETSI EN 319 411-1 V1.2.2, NCP, DVCP, OVCP	not defined
CN = Atos TrustedRoot Server-CA 2019 O = Atos C = DE	08FD418B118853484FD1B066F1922A80F571D8FFF7268D598B086DF18B580AD8	ETSI EN 319 411-1 V1.2.2, NCP, DVCP, OVCP	1.3.6.1.5.5 .7.3.1 (id- kp- serverAuth) 1.3.6.1.5.5 .7.3.2 (id- kp- clientAuth)
CN = Atos TrustedRoot CodeSigning-CA 2013 O = Atos C = DE	0A1A5221F38DD458367A20D527DB1880082ACCEEF69A8546FB67D30253F90824	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	not defined

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = Atos TrustedRoot Client-CA for Wintershall Dea 2020 O = Atos C = DE	41ABE8F9A951A8990FBDCD3E14CF479D426401B115F0170189B665E940C3632C	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	1.3.6.1.5.5 .7.3.2 (id- kp- clientAuth) 1.3.6.1.5.5 .7.3.4 (id- kp- emailProte ction) 1.3.6.1.5.5 .7.3.9 (id- kp- OCSPSig ning)
CN = Atos TrustedRoot Client-CA for Worldline 2020 O = Atos C = DE	88AB961F64F9368F4C4D1307F59D4E59C5E570F852A6C5113A8FF28E04315157	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	1.3.6.1.5.5 .7.3.2 (id- kp- clientAuth) 1.3.6.1.5.5 .7.3.4 (id- kp- emailProte ction) 1.3.6.1.5.5 .7.3.9 (id-

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
			kp-OCSPSigning) 1.3.6.1.4.1.311.10.3.4 (szOID_EFS_CRYPTO) 1.3.6.1.4.1.311.10.3.4.1 (szOID_EFS_RECOVERY) 1.3.6.1.4.1.311.20.2.2 (Smartcard Logon)
CN = Atos TrustedRoot Client-CA 2019 O = Atos C = DE	550749FF5E35C407D515D98B327504BC484FDAAE28A713AFE4E2282986BE04E8	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
			1.3.6.1.5.5 .7.3.4 (id- kp- emailProte ction) 1.3.6.1.5.5 .7.3.9 (id- kp- OCSPSig ning) 1.3.6.1.4.1 .311.10.3. 4 (szOID_E FS_CRYP TO) 1.3.6.1.4.1 .311.10.3. 4.1 (szOID_E FS_RECO VERY) 1.3.6.1.4.1 .311.20.2. 2

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
			(Smartcard Logon)
CN=Atos TrustedRoot Client-CA for equensWorldlineP artner 2 2019 O=Atos C=DE	739D0C3A71B6C377CBD1C408AE7CC19732C2CBEF8620D63B16C9FD0185DF9A71	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	1.3.6.1.5.5 .7.3.2 (id- kp- clientAuth) 1.3.6.1.5.5 .7.3.9 (id- kp- OCSPSig ning)
CN = Atos TrustedRoot Client-CA 2020 O = Atos C = DE	5317DF82FB9A88993FA067D8352BC4195B84BBD0C698A1EDD7AF97C9DD90D879	ETSI EN 319 411-1 V1.2.2, NCP	1.3.6.1.5.5 .7.3.2 (id- kp- clientAuth) 1.3.6.1.5.5 .7.3.4 (id- kp- emailProte ction) 1.3.6.1.4.1 .311.10.3. 4 (szOID_E

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
			FS_CRYPTO) 1.3.6.1.4.1.311.10.3.4.1 (szOID_EFS_RECOVERY) 1.3.6.1.4.1.311.20.2.2 (Smartcard Logon)
CN = Atos TrustedRoot Client CA for NordLB 2021 O = Atos C = DE	DBB9EAB4A2C66C77F30B266991DC2CE5E670FD8AE464545E236A9F5FEB4A4EFA	ETSI EN 319 411-1 V1.2.2, NCP	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection)

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = Atos TrustedRoot Client-CA for Wintershall Dea 2 2020 O = Atos C = DE	AA923D9DFCC7982FE4D56A71F53004C92076F1A30DCE9575016AB4FE08DCF820	ETSI EN 319 411-1 V1.2.2, NCP	1.3.6.1.5.5 .7.3.2 (id- kp- clientAuth) 1.3.6.1.5.5 .7.3.4 (id- kp- emailProte ction)
CN = Atos TrustedRoot Client-CA for Worldline 2 2020 O = Atos C = DE	6C5DC34D9D7402E0291416CC8D337B3302E131F1C8543FCEDC14E739153223B1	ETSI EN 319 411-1 V1.2.2, NCP	1.3.6.1.5.5 .7.3.2 (id- kp- clientAuth) 1.3.6.1.5.5 .7.3.4 (id- kp- emailProte ction) 1.3.6.1.4.1 .311.10.3. 4 (szOID_E FS_Cryp TO)

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
			1.3.6.1.4.1 .311.10.3. 4.1 (szOID_E FS_RECO VERY) 1.3.6.1.4.1 .311.20.2. 2 (Smartcar d Logon)
CN = Atos TrustedRoot CodeSign CA 2021 O = Atos C = DE	0D3D8E182C24639A1B7E9A4C32D6DC49EF621ADFD6747E151E289DD08777E094	ETSI EN 319 411-1 V1.2.2, NCP, OVCP	1.3.6.1.5.5 .7.3.3 (id- kp- codeSigni ng)
CN = Atos TrustedRoot Timestamp CA 2020 O = Atos C = DE	BF7EADE06B2F845ACE7BD690BC3476D4F9EB770C63F2893A35CD52EFEAED6EA3	ETSI EN 319 411-1 V1.2.2, NCP	1.3.6.1.5.5 .7.3.8 (id- kp- timeStamp ing)

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

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.

Modifications record

Version	Issuing Date	Changes
Version 1	2021-06-03	Initial attestation
Version 1.1	2021-06-08	Correction due to quality assurance

End of the audit attestation letter.

This attestation is based on the template version 2.8 as of 2021-04-21, that was approved for use by ACAB-c.