BERICHT

BEGUTACHTUNG ZUR SYSTEMFÖRDERUNG

Atos TrustedRoot CA
ETSI TS 102 042 V2.4.1 (2013-02)

Applied Certificate Policy:
NORMALIZED CERTIFICATE POLICY (NCP)
IN DEN VARIANTEN DVCP UND OVCP

ATOS INFORMATION TECHNOLOGY GMBH

LUXEMBURGER STRAßE 3
45131 ESSEN

DATUM DES AUDITS
09. - 18.05.2016
AZ: 334220

DQS GmbH Deutsche Gesellschaft zur Zertifizierung von Managementsystemen
August-Schanz-Straße 21, 60433 Frankfurt a. M., Germany

Inhaltsverzeichnis

1 Zertifizierungsempfehlung

Wir danken Ihnen für die vertrauensvolle Zusammenarbeit im Rahmen des kürzlich abgeschlossenen Audits in Ihrem Unternehmen. Der vorliegende Bericht beinhaltet die Ergebnisse der Begutachtung, inklusive aller Stärken, Chancen und Schwächen. Der Unternehmensleitung wurde die Auswertung bereits in der Abschlussbesprechung des Audits vorgestellt. Sie kann nun von Ihnen zur Verbesserung der Effektivität Ihres Managementsystems verwendet werden. Wir freuen uns, Sie auf dem Weg zu einem nachhaltigem Unternehmenserfolg begleiten zu dürfen.

Das Auditteam empfiehlt der DQS für das Regelwerk ETSI TS 102 042 V2.4.1 (2013-02):

- ☐ die Erteilung des Zertifikats
- ☐ die Erteilung des Zertifikates, sobald die Umsetzung der Korrekturmaßnahmen nachgewiesen ist
- ☒ die Aufrechterhaltung des Zertifikats
- ☐ die Aufrechterhaltung des Zertifikats, sobald die Umsetzung der Korrekturmaßnahmen nachwiesen ist
- ☐ trifft nicht zu, da außerordentlicher Bericht

Bitte denken Sie daran, die DQS möglichst frühzeitig über wesentliche Änderungen des Managementsystems zu informieren, damit wir gemeinsam geeignete Maßnahmen zur Aufrechterhaltung der Zertifizierung vereinbaren können.

Gesamteindruck

- Trust Center von Atos mit profundem PKI-Know-how
- Struktur im ATC an Best Practices aus bisherigen Projekten orientiert
- IS-Awareness bei allen Beteiligten auf hohem Niveau
- Alle Anforderungen der ISO 27001:2013 werden von dem System erfüllt

Ergebnis ETSI TS 102 042 V2.4.1 (2013-02):

- Das System konnte auch im Vergleich zum Vorjahr weiterentwickelt werden.
- Alle identifizierten Potentiale wurden bearbeitet und entsprechend umgesetzt.
- Das System hat seinen hohen Reifegrad aufrechterhalten.
- Umzug in das Rechenzentrum in Nürnberg ist bereits in den ersten Zügen abgeschlossen.
- Das Rechenzentrum in Nürnberg / Fürth entspricht den erwarteten Anforderungen.
- Eine eigene Zertifizierung des Trustcenters nach ISO 27001:2013 konnte erreicht werden.

2 Das Managementsystem

2.1 Bewertung PDCA-Zyklus

DQS-Begutachtungen nutzen Plan - Do - Check - Act, kurz den PDCA-Zyklus. Er kann auf einzelne Prozesse, ein System oder eine geführte Organisation angewendet werden.

Plan:	Aktivitäten werden mit Zielen, Prozessen und Ressourcen geplant.
Do:	Die Planung wird verwirklicht.
Check:	Ergebnisse werden mit Zielen und Erwartungen verglichen.
Act:	Benötigte Verbesserungen und Veränderungen werden definiert und geplant - siehe 1. Schritt “Plan”.

Zusammenfassend wurden die Prozesse, die Organisation, die Verfahren und die Technologie der Atos TrustedRoot CA (ATC) als auditierte Certification Authority (CA) wie folgt bewertet:

Folgende Anforderungen wurden u. a. im Rahmen dieses Audits geprüft:

- Alle Anforderungen, die an eine CA Practice gem. Kapitel 7 des Regelwerkes sind im Sinne der gewählten Certificate Policy (NCP) umgesetzt und die darin geforderten Maßnahmen sind implementiert.
- Die auditierte CA hat auch dann die Verantwortung zur Erfüllung der Normforderungen, wenn CA-Funktionen von Vertragspartnern erbracht werden.
- Die CA erbringt die Zertifizierungsdienste gemäß den Festlegungen des Certificate Practice Statement.
- Die Certificate Policy ist Teil eines effektiven Certificate Policy Management mit Regelungen zu Verantwortlichkeiten, Kommunikation und PDCA-Zyklus.[1]
- Die Umsetzung der in dem letzten Audit der DQS identifizierten Potentiale.

3 Certification Authority Practice

3.1 Certificate Practice Statement (CPS) [7.1]

Im CPS sind die angewendeten Verfahren und Prozesse gemäß den Forderungen des RFC 3647 (Internet X.509 Public Key Infrastructure, November 2003) dargelegt. Wo in den Abschnitten [4 bis 6, sowie 8] der zu Grunde gelegten Norm Forderungen an die Prozesse, die Organisation, die Verfahren oder die Technologie der Certification Authority (CA) bezüglich der Definition von Begriffen, vertraglichen Regelungen oder Berücksichtigung in einem übergeordneten Policy Statement stellt, wird im CPS darauf verwiesen.

Die angewendete Certificate Policy ist die **N**ormalized **C**ertificate **P**olicy (NCP). Der Geltungsbereich umfasst das Atos TrustedRoot CA (ATC) für drei CAs:

1. **Atos TrustedRoot Server CA**
2. **Atos TrustedRoot Client CA**
3. **Atos TrustedRoot CodeSigning CA**

Die Umsetzung, Einhaltung und Aufrechterhaltung der angewendeten Verfahren und Prozesse wird durch die Einbettung der CA-Prozesse in das AIMS (Atos Integrated Management System) gewährleistet.

[1] Inhalte einer Certificate Policy (gem. RFC 3647, Internet X.509 Public Key Infrastructure, November 2003) wurden im CPS berücksichtigt. Von daher wurde kein separates Dokument zur Certificate Policy CPS erstellt.

3.2 Public key infrastructure: Key management lifecycle [7.2]

CA Schlüssel werden unter kontrollierten Bedingungen erzeugt, die im Sicherheitskonzept näher spezifiziert sind. Dies bezieht sich bei der Schlüsselerzeugung sowohl auf die technische Konfiguration des Gerätes, als auch auf die Wahl des verwendeten Algorithmus hinsichtlich Art und Länge, die dem gängigen Industriestandard folgen.

Die Vertraulichkeit und Integrität privater CA Signaturschlüssel wird mittels geeigneter kryptographischer Technologie gewährleistet und aufrechterhalten. Zutritt, Zugang und Zugriff zur eingesetzten kryptographischen Technologie, sowie die dazugehörigen Verfahren zur Speicherung, Datensicherung und Wiederherstellung sind nur einem streng limitierten Personenkreis mit hoher persönlicher Integrität möglich. Sämtliche Operationen an der kryptographischen Technologie folgen dem 4-Augen-Prinzip und werden aufgezeichnet. Regelungen zu vorgenannten Vorgehensweisen sind im Sicherheitskonzept dargelegt.

Nach denselben Prinzipien werden die Integrität und Authentizität der öffentlichen CA Signaturschlüssel und aller zugehörigen Parameter während ihrer Übermittlung an die vertrauenden Instanzen („Relying parties“) aufrechterhalten.

Der private CA Signaturschlüssel wird nur zum Zwecke der Wiederherstellung vertraulich aufbewahrt und vor unbefugtem Zugriff geschützt. Die Wiederherstellung des CA Signaturschlüssels folgt demselben Ablauf wie bei der initialen Beantragung. Dies ist in der Arbeitsanweisung *Key Recovery* geregelt.

Private CA Signaturschlüssel, die zur Erzeugung von CA Zertifikaten verwendet werden, werden auch nur für diesen Zweck eingesetzt. Die Erzeugung von CA Zertifikaten geschieht in physisch sicheren Bereichen.

Private CA Signaturschlüssel werden nicht über das Ende ihres Lebenszyklus hinaus verwendet. Der zugehörige Prozess ist in der Arbeitsanweisung *Zertifikatssperrung* geregelt.

Die Sicherheit von kryptographischen Geräten wird während ihres gesamten Lebenszyklus durch die Anwendung und Einhaltung der IS-Vorgaben für IT-Systeme, wie z. B. Sicherheitskonzepte für dedizierte IT-Systeme mit und ohne Sicherheitsfunktionen, gewährleistet. Dies schließt die unbefugte Handhabung während des Versandes, der Lagerung, sowie der Installation, Aktivierung, Rücknahme, Backup und Wiederherstellung der CA Signaturschlüssel unter Wahrung des 4-Augen-Prinzips mit ein. Eine entsprechende Statusinformation wird dazu geführt. Nach Ablauf der Gültigkeit wird die Information des privaten CA Signaturschlüssel unwiderruflich physisch gelöscht.

Die Erzeugung der Schlüssel für Zertifikatsinhaber („Subject“) erfolgt sicher, d. h. der verwendete Algorithmus und die entsprechende Länge des Schlüssel folgen dem gängigen Industriestandard und die Geheimhaltung des privaten Schlüssels des Zertifikatsinhabers wird, wie in der *Spezifikation Atos Trusted CA* beschrieben, während der Erzeugung und vor der Auslieferung sichergestellt. Die Gewährleistung der Vertraulichkeit und Integrität ist ebenfalls in der Dokumentation *Spezifikation Atos Trusted CA* geregelt.

3.3 Public key infrastructure: Certificate management lifecycle [7.3]

Zur Identifizierung eines Teilnehmers („Subscriber“) und eines Zertifikatinhabers („Subject“) werden geeignete Prüfungen durchgeführt und entsprechende Nachweise geführt. Die Arbeitsanweisung *Zertifikatserstellung* regelt u. a. die Überprüfung der Korrektheit der jeweiligen Namen und der dazugehörigen Daten. Diese Prüfaktivitäten sind Teil des definierten CA-Services, die u. a. an Hand von Nachweisen aus geeigneten und zugelassenen (externen) Quellen verifizieren, dass Zertifikatsanträge richtig, autorisiert und vollständig gemäß der vorliegenden Dokumentation gestellt sind. Die Zertifikatinhaber („Subjects“) können physische Einzelpersonen, Einzelpersonen zu einer Organisation gehörend, eine organisatorische Legal-Einheit oder ein Gerät oder System, welches von einer organisatorischen Legal-Einheit betrieben wird, sein. Die geprüften Nachweise werden für die Dauer der Gültigkeit von Zertifikaten revisionssicher aufbewahrt.

Zertifikatsanträge von Zertifikatsinhabern („Subject“), die zuvor bei derselben CA registriert wurden, werden auf Vollständigkeit, Korrektheit und Ordnungsmäßigkeit der Autorisierung geprüft. Dies bezieht sich auf Zertifikatsverlängerungen, erneute Schlüsselgenerierung („Rekey“) nach Sperrung oder vor Ablauf der Gültigkeit oder Aktualisierung(„Update“) auf Grund von Attributsänderungen des Zertifikatsinhabers („Subject“).

Die Ausgabe der Zertifikate erfolgt sicher und gewährleistet die Aufrechterhaltung der Authentizität. Die Zertifikate enthalten gem. den Regelungen X.509[2] u. a. die Identifikation der CA, Name von Zertifikatsinhabern („Subject“), spezifische Attribute der Signatur, öffentlicher Teil des Schlüsselpaares, Seriennummer des Zertifikats, elektronische Unterschrift der herausgebenden Stelle und Begrenzung des Gültigkeitsbereiches oder Transaktionswertes. Geeignete Maßnahmen zum Schutz vor Zertifikatsfälschung werden getroffen.

Allgemeine Geschäftsbedingungen, anzuwendende Policies und weitere Rahmenbedingungen (z. B. Technologie, Mitwirkungspflichten, Gültigkeitszeitraum) werden den Teilnehmer („Subscriber“) und vertrauenden Instanzen („Relying parties“) zur Verfügung gestellt. Regelungen dazu werden im *Betriebshandbuch Webservice* getroffen.

Zertifikate werden an Teilnehmer („Subscriber“), Zertifikatsinhaber („Subject“) und vertrauende Instanzen („Relying parties“) im erforderlichen Umfang verteilt und zur Verfügung gestellt. Die Rückverfolgbarkeit von Zertifikaten wird an 7 Tagen pro Kalenderwoche für 24 Stunden pro Tag (7 x 24) gewährleistet.

Die zeitnahe Sperrung von Zertifikaten, die auf Grund von autorisierten und überprüften Sperranfragen beantragt wird, wird in Prozessen und Verfahren geregelt und kann innerhalb von 24 Stunden durchgeführt werden. Der Empfang von Sperranfragen und die Durchführung der Sperrungen werden bestätigt und aufgezeichnet. Der Zertifikatsstatus ändert sich in „gesperrt“ oder ggf. in „suspendiert“ und in einer „CRL: Certificate Revocation List“ geführt, die alle 24 Stunden aktualisiert wird.

[2] ISO/IEC 9594-8/ITU-T Recommendation X.509:
"Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks”

3.4 CA management and operation [7.4]

Prozesse zum Security Management sind in das Informationssicherheitsmanagementsystem (ISMS) so eingebunden, dass die identifizierten Schutzziele zu schützender Unternehmenswerte (z. B. Objekten und Informationen), wie in der IS-Policy dargelegt, erreicht werden. Die zu schützenden Unternehmenswerte wurden identifiziert und gemäß ihrem Schutzbedarf klassifiziert. Aus potentiellen Schwachstellen und Bedrohungen wurden Risiken abgeleitet und bezüglich ihrer Eintrittswahrscheinlichkeit und Auswirkung bewertet. Zu deren Minderung wurden geeignete Maßnahmen abgleitet (IS-Controls des ISMS). Das ISMS nach ISO/IEC 27001 ist mit einem Qualitätssicherheitsmanagementsystem nach ISO 9001 zusammen in das Business Management System des Unternehmens integriert und wird zyklisch extern zertifiziert. Im ISMS werden auch IS-Controls beschrieben, die Vorgaben zur IS-bezogenen Infrastruktur (z. B. Zugriffsüberwachung, Berechtigungskonzept, Handhabung von IS-Incidents) machen. Die IS-Controls und CA-Prozesse berücksichtigen Einrichtungen, Systeme und Informationen (zu schützende Unternehmenswerte) der CA und sind dokumentiert, eingeführt und werden aufrechterhalten.

Personelle Anforderungen an internes und externes Personal vor, während und nach der Beschäftigung in der CA-Organisation sind im Rahmen des ISMS festgelegt. Dabei werden Personalkapazität, Fachwissen, Erfahrung und Qualifikation berücksichtigt. Für IS-Verstöße sind im Rahmen der Handhabung von IS-Incidents mögliche disziplinarische Maßnahmen definiert. IS-Rollen und -Verantwortlichkeiten, einschließlich der Berechtigungen für Zutritt, Zugang und Zugriff zu Informationen und Systemen werden in den Rollenbeschreibungen für Security Officer, System Administrator, System Operator und System Auditor beschrieben und in der Zugriffsberechtigungsüberwachung eingepflegt.

Der physische Zugriff auf kritische Dienste unterliegt einer Zugriffsüberwachung und physische Risiken der zu schützenden Unternehmenswerte werden durch IS-Controls minimiert. Berechtigungen für Zugriff, Zugang und Zugriff werden nach dem „Need-to-Know-Prinzip“ vergeben. IS-Controls zum Schutz vor Verlust, Beschädigung oder Beeinträchtigung zu schützender Unternehmenswerte und der Geschäftskontinuität. Dies berücksichtigt auch die Vermeidung der Beeinträchtigung oder des Diebstahls von Informationen und IT-Systemen. Die Erzeugung und Rücknahme von Zertifikaten finden in einer sicheren physischen Umgebung statt, die über Sicherheitsperimeter (z. B. Schutz der Gebäudeaußenhülle, Personenvereinzelungsanlagen), Zutrittsüberwachung, Brandschutz, Stromausfall und Disaster Recovery Maßnahmen verfügt.

CA-Systeme werden sicher und ordnungsgemäß betrieben um das Ausfallrisiko zu minimieren. Dies geschieht u. a. durch die Wahrung der Integrität von Daten, Informationen und Systemen (z. B. Schutz vor schadhafter oder unberechtigter Software), die Minimierung der Auswirkung von Security Incidents durch ein systematisches und zügiges Auswerte- und Meldeverfahren und die sichere Handhabung mobiler und stationärer Speichermedien (Schutz vor Verfall oder Beschädigung der Daten). Informationen werden nach ihrer Klassifizierung gem. Schutzbedarf gehandhabt. Die Anforderungen an Kapazität und Rechenleistung der CA-Systeme werden geplant, überwacht (u. a. durch kontinuierliches Monitoring mit Schwellwerten, eingebettet in Audittools zur Systemüberwachung) und durch geeignete Maßnahmen (z. B. Initiierung von Changes) erfüllt. IS-Maßnahmen umfassen operative IS-Prozesse und -Verantwortlichkeiten, die Planung und Freigabe von CA-Systemen, den Schutz vor schadhafter Software, die Organisation, das Netzwerkmanagement, die aktive Überwachung der Auditjournale, die Ereignisanalyse und Nachverfolgung signifikanter Ereignisse, die Handhabung und Statusüberwachung mobiler und stationärer Medien und den Austausch von Daten und Software.

Der Zugriff auf CA-Systeme ist auf ordnungsgemäß berechtigte Personen beschränkt. Das interne CA-Netzwerk ist durch geeignete IS-Controls (z. B. Firewall, Router, Intrusion Detection System) gegen den Zugriff durch externe Domains geschützt. Sensible Daten (z. B. Registrierungsinformationen) werden bei Übermittlung in unsicheren Netzten gegen unberechtigten Zugriff oder Änderung mittels Verschlüsselung geschützt. Das Berechtigungskonzept ist rollenbasiert und ermöglicht ein systematisches Account Management, das dem „Need-to-Know-Prinzip“ folgt. Zugriffe werden aufgezeichnet und Versuche des unberechtigten Zugriffs werden ausgewertet, bzw. lösen fallweise entsprechende Alarmmeldungen aus, die wiederrum zu weiteren Schutzmaßnahmen führen (z. B. Forced logout, re-login mit Notfall-User).

Es werden vertrauenswürdige Systeme und Produkte verwendet, die vor Veränderungen und Manipulationen mittels gehärteter Systeme geschützt sind, d. h. IS-Controls sind in das Betriebssystem fest „eingebaut“ und schützen die Erstellung und Speicherung der Private Keys. Das eingesetzte HSM ist nach *FIPS PUB 140-2 le-*

vel 3 des NIST[3] zertifiziert. Releases, Anpassungen oder Notfall-SW-Fixes durchlaufen einen Change Management Prozess mit entsprechenden Prüf- und Freigabeschritten.

Disaster Recovery Management Prozesse stellen für den Fall einer Katastrophe, einschließlich der Kompromittierung des privaten CA Signaturschlüssels, den Betrieb so schnell wie möglich wieder her. Dazu liegen Disaster Recovery Pläne vor, die aktualisiert und getestet werden. Diese schließen u. a. Verfahren zur Datensicherung (Backup mit externer Aufbewahrung der Sicherungsmedien und Fallback-Prozedur) und ein Business Continuity Plan im Falle tatsächlicher oder vermuteter Kompromittierung des privaten CA Signaturschlüssels (Information aller Teilnehmer („Subscriber“) und vertrauenden Instanzen („Relying parties“); gilt auch bei kompromittiertem Algorithmus) ein.

Für den Fall der Einstellung des Betriebes der CA werden potenzielle Beeinträchtigungen der Teilnehmer („Subscriber“) und vertrauenden Instanzen („Relying parties“) durch eine zeitgerechte und vollständige Information und der Übertragung der Verpflichtungen zur Aufrechterhaltung der Zertifikate an Dritte, bzw. die aktive Handhabung der Zertifikatsrücknahme minimiert. Somit wird u. a. der Fortbestand an Aufzeichnungen gewährleistet, der zum Nachweis in gerichtlichen Verfahren benötigt werden könnte.

Die Einhaltung gesetzlicher Anforderungen wird im Rahmen des Datenschutzes, um u. a. Verlust, Zerstörung oder Verfälschung vorzubeugen, durch geeignete technische und organisatorische Maßnahmen (IS-Controls nach §9 Anlage 1 BDSG) gewährleistet.

Alle relevanten Informationen über ein Zertifikat werden für einen angemessenen Zeitraum (gem. Geschäftsbedingungen) aufgezeichnet, so dass sie zum Zwecke des Nachweises der Zertifizierung in gerichtlichen Verfahren benutzt werden können. Die Aufbewahrung der Daten umfasst den gesamten Lebenszyklus des Schlüssels und der Zertifikate, erfolgt vollständig und ist vor unbefugten Änderungen durch ein geeignetes Verfahren zur Datensicherung geschützt. Die Übermittlung von Lebenszyklus-Daten wird protokolliert.

3.5 Organizational [7.5]

Die Zuverlässigkeit der CA-Organisation wird u. a. durch nichtdiskriminierende Policies und Prozesse, juristisch einwandfreie Legaleinheiten, Haftungsregelungen, finanzielle Stabilität, Verfahren zum Umgang mit Kundenbeschwerden und -streitigkeiten und vorhandene vertragliche Regelungen mit benötigten internen und externen Lieferanten und Providern sichergestellt.

[3] National Institute of Standards and Technology (NIST) als Herausgeber der FIPS 140 Publication Serie zur Koordination der Anforderungen und Normen für Hard- und Softwarekomponenten kryptographischer Module

4 Weitere Stärken und Verbesserungspotentiale

Auflistung der Stärken, wie im Schlussgespräch erläutert

- Die Bedeutung des Trustcenters konnte gehalten und weiter ausgebaut werden.
- Alle an dem Audit beteiligten Mitarbeiter hatten ein gutes Wissen zu den Themen. Alle relevanten Policies waren bekannt und konnten nachgewiesen werden.
- Das Trustcenter bedient alle Atos Mitarbeiter weltweit.
- Einführung eines „Officer on Duty“ im Rotationsverfahren.
- Einsatz der Root CA für die gematik.
- Das Trustcenter ist durch Microsoft und Mozilla anerkannt.
- Die Forderungen des CA/Browser Forums nach den Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.0 werden unterstützt.
- Im diesjährigen Audit wurden neben den ETSI und Browserforumsanforderungen auch die Umsetzung zur ISO 27001:2013 mit einem auf das Trustcenter angepassten Anwendungsbereich, sowie eine Zertifizierung nach TR3145 des BSI

Auflistung der Potentiale, wie im Schlussgespräch erläutert

- Keine siehe ISO 27001 Report

4.1 Im Visier der Weiterentwicklung

- Umzug ins neue Rechenzentrum nach Nürnberg
- Verbesserungspotentiale analysieren und geeignete Maßnahmen ableiten
- Weitere Prüfung der CPS-Dokumentation hinsichtlich einer möglichen Vereinfachung
- Weitere Vermarktung der Atos Trustcenter Services auch außerhalb der Atos Organisation

5 Ergebnisse der Begutachtung

5.1 ETSI TS 102 042 V2.4.1 (2013-02)

Geltungsbereich der Zertifizierung (Scope): Atos TrustedRoot CA	Atos TrustedRoot CA (ATC) für drei CAs: Atos TrustedRoot Server CA, Atos TrustedRoot Client CA und Atos TrustedRoot CodeSigning CA Angewendete Certificate Policy: Normalized Certificate Policy (NCP)
Das Certificate Practice Statement (CPS) wurde begutachtet. Es wurde Konformität mit den anzuwendenden Regelwerksanforderungen festgestellt.	Aktuelle Version des CPS: 1.7.1 ☒ ja ☐ nein Bemerkungen: Inhaltsverzeichnis CPS ist beigefügt
Das Managementsystem ist wirksam und erfüllt die Forderungen.	☒ ja ☐ nur teilweise - siehe Maßnahmenpläne ☐ nein - siehe Maßnahmenpläne
Anzahl der Abweichungen:	Hauptabweichungen: 0, Nebenabweichung: 0
Vor-Ort-Verifizierung der Abweichungen, erforderlich durch Nachbegutachtung:	☐ ja ☒ nein
Die Korrekturmaßnahmen aus der vorangegangenen Begutachtung sind	☐ wirksam umgesetzt ☐ nicht wirksam umgesetzt ☒ nicht anwendbar
Das derzeit gültige Zertifikat wurde geprüft. Es ist noch angemessen. Ablauf der Gültigkeit:	☒ ja ☐ nein
Die Nutzung des registrierten Firmensymbols in Verbindung mit dem/den Akkreditierungslogo(s) ist angemessen.	☒ ja ☐ nein Bemerkungen: Re-Zertifizierung
Die fortlaufende wirksame Umsetzung des Managementsystems wurde im vergangenen Zertifizierungszyklus aufgezeigt *(zwei Kriterien der Bewertung)*	☒ ja, die Aufzeichnungen zum Managementreview zeigen die Erreichung der festgelegten Ziele und die ständige Verbesserung auf. ☒ ja, die Trends der dokumentierten Korrekturmaßnahmen zeigen Effektivität und kontinuierliche Verbesserung. ☐ nein, s. Bemerkungen und Maßnahmenpläne Bemerkungen: ./.
Interne Audits und die Aufzeichnungen zu den Korrekturmaßnahmen zeigen die ununterbrochene Konformität des Managementsystems zum ausgewählten Regelwerk auf	☒ ja ☐ nein, s. Bemerkungen Bemerkungen: ./.
In der vergangenen Zertifizierungsperiode wurden vergleichbare Abweichungen wiederkehrend identifiziert	☐ ja, s. Bemerkungen ☒ nein Bemerkungen: ./.
In der vergangenen Zertifizierungsperiode wurden Zertifikate unter Auflagen erteilt, ausgesetzt oder es wurden außerordentliche Begutachtungen zu bestimmten Mängeln durchgeführt	☐ ja, s. Bemerkungen ☒ nein Bemerkungen: ./.

6 Auftragsdaten und Angaben zum Begutachtungsprozess

6.1 Auftragsdaten

Name des Unternehmens:	Atos Information Technology GmbH
Hauptadresse:	
	Luxemburger Straße 3
	45131 Essen
Aktenzeichen:	334220
Auftragsnummer:	A 271250
Datum des Audits:	23.-24.06.2015
Anzahl der Personentage (PT) gesamt:	2,0
SIC / IAF / EA / NACE Code: (Haupt)	33
Ausschlüsse, falls anwendbar	☒ keine

6.2 Oberste Leitung und Ansprechpartner

Chief Executive Officer / Oberste Leitung:	Winfried Holz
Telefon:	+49 89 636 44800
E-Mail:	winfried.holz@atos.net
Managementbeauftragter (Trustcenter):	Matthias Mönter
Telefon:	+49 211 399 36097
E-Mail:	armin.klimmek@atos.net
Leitender Auditor:	Jens Nicolaysen
Telefon:	+49 (4102) 7779000
E-Mail:	Jens.Nicolaysen@jnc.de
DQS-Kundenbetreuung	Benjamin Junginger
Telefon:	069-95427-0
E-Mail:	Benjamin.Junginger@dqs.de

6.3 Auditdaten

	Personenzahl	davon interviewt	%
Führungskräfte	2	2	100
andere Mitarbeiter	11	3	27
Gesamt	13	5	38

Stichprobenbasis Interviewpartner

Remote Locations und zusätzliche Standorte: nicht relevant

Zeitplan an Kunden versendet am: 25.05.2015

Ablauf der Begutachtung:
☒ Der Auditzeitplan wurde eingehalten
☐ Der Auditzeitplan wurde wie folgt geändert:

Abschlussbesprechung:

Eine Abschlussbesprechung mit dem Leiter der relevanten Abteilung wurde durchgeführt. Die Begutachtungsergebnisse wurden vorgestellt, erläutert und - soweit erforderlich - diskutiert. Korrekturmaßnahmen und Maßnahmenpläne wurden, soweit erforderlich, mit den jeweils Verantwortlichen vereinbart.

7 Nächste Schritte

7.1 Maßnahmen des Kunden

Korrekturmaßnahmen:

☒ Korrekturmaßnahmen waren nicht erforderlich

☐ Die geplanten Korrekturmaßnahmen werden wie vereinbart umgesetzt und bis zum TT.MM.JJJJ auf Wirksamkeit geprüft.

Verbesserungspotentiale:

Die identifizierten Verbesserungspotentiale werden intern bewertet und fließen ggf. in den kontinuierlichen Verbesserungsprozess ein, soweit dies als hilfreich angesehen wird.

Abweichungen die während des Audits festgestellt wurden, müssen nachweislich und wirksam innerhalb des festgesetzten Zeitrahmens geschlossen werden. Ansonsten kann es zur Aussetzung oder zum Entzug des Zertifikates kommen.

7.2 Maßnahmen der DQS

Art der nächsten Begutachtung:

☐ Begutachtung zur Systemförderung

☒ Wiederholungsbegutachtung

☐ Andere Begutachtung

Daten der nächsten Begutachtung:
(unverbindlich abgeschätzter Aufwand)

Geplanter Zeitpunkt für die nächste Begutachtung: Juni 2017
(ggf. KW oder Monat)

mit 3 Personentag(en)

durch Auditor(en)

Voraussichtliche Themenschwerpunkte: ./.

Kunde wünscht:

☐ Informationen über

☐ Angebot über

☐ Telefonanruf durch Kundenbetreuer

Weitere Bemerkungen: ./.

7.3 Identifizierter Änderungsbedarf

Basisdaten geändert ? ☐ ja ☒ nein

8 Anlagen zum Bericht

☐ Maßnahmenpläne — Anzahl: 0

Für den internen Gebrauch:

☐ Basisdaten — Anzahl:

☐ Basisdaten – für Regelwerk(e) [sofern anwendbar] — Anzahl:

☐ Feststellungen

☒ Weitere Dokumente für Regelwerk(e)
[sofern anwendbar für Medizin, Automotive . . . .

☐ Teilnehmerliste(n) Abschlussgespräch

☐ Geprüfte Zertifikatentwürfe [sofern anwendbar] — Anzahl:

☐ Sonstiges

Bericht erstellt am 01.06.2016

Auditleiter Jens Nicolaysen
Regelwerk ETSI TS 102 042 V2.4.1 (2013-02)

1.Juli 2016

Reinhard Witzke

Datum

fachliche Prüfung der DQS

Vertraulichkeit

Der Inhalt dieses Berichts und alle im Zusammenhang der Begutachtung erhaltenen Informationen über das begutachtete Unternehmen werden von den Mitgliedern des Auditteams und von der DQS vereinbarungsgemäß vertraulich behandelt.

Verteiler:

DQS
Atos Information Technology GmbH