Federal Office
for Information Security

BSI NESAS Certification Report

BSI-DSZ-NESAS-0016-2026

for

Converged Telephony Application Server (CTAS), Version R11.1

from

Mavenir Systems Inc

Document Version 1.0, 2026-07-27

Document History

Version	*Date*	*Author*	*Changes*
V1.0	2026-07-27	BSI	• Initial version

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Phone: +49 22899 9582 - 0 Infoline: + 49(0)800 2741 000
Email: nesas@bsi.bund.de
Internet: https://www.bsi.bund.de
© Federal Office for Information Security 2026

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-NESAS-0016-2026 (*)

Converged Telephony Application Server (CTAS), Version R11.1
5G network functions: IMS (only Application Server (AS) function)

from **Mavenir Systems Inc**

The IT product (Converged Telephony Application Server (CTAS)) identified in this certificate has been evaluated by a recognised evaluation facility in accordance with the requirements and regulations of the BSI's own product certification programme "Network Equipment Security Assurance Scheme - BSI NESAS Implementation" (BSI NESAS). The conclusions of the evaluation facility contained in the evaluation report are consistent with the evidence provided. The certification process was carried out in accordance with the requirements and regulations of BSI's own BSI NESAS programme.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report chapter 1.5.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 2026-08-05
Federal Office for Information Security

By order of

Fabian Hodouschek Head of Certification	L.S.	Sandro Amendola Director General

Contents

1 Certification Overview 6
1.1 Preliminary Remarks 6
1.2 Specifications of the Certification Procedure 6
1.3 Recognition agreements 7
1.4 Audit, Evaluation and Certification Procedure 7
1.5 Validity of the Certification Result 7
1.6 Publication 8
2 Certification Results 9
2.1 Executive Summary 9
2.2 Product Identification and Deliverables 9
2.3 Architectural Information 10
2.4 Results of Evaluation 11
2.5 Recommendations for upcoming recertifications 12
2.6 Missing information and discrepancies 12
2.7 Obligations for and information on using the product 12
2.7.1 Specific Conditions for the Vendor 12
2.7.2 Specific Conditions for the User 12
3 Definitions 13
3.1 Acronyms 13
3.2 Bibliography 14
4 Annexes 16
4.1 Minor updates to the evaluated configuration 16

1 Certification Overview

1.1 Preliminary Remarks

Under the BSI Act – BSIG (Federal Office for Information Security Act) [1], the Federal Office for Information Security (BSI) is responsible for testing and evaluating the security of information technology (IT) systems or components, and for issuing security certificates.

A product is certified at the instigation of the vendor, sponsor or distributor of IT products, hereinafter referred to as the applicant.

For IT product certification according to the "Network Equipment Security Assurance Scheme – BSI-NESAS Implementation" (BSI NESAS), part of the procedure is the assessment (audit) of the vendor's development and product lifecycle processes as well as the technical evaluation of the product in accordance with the security criteria published by the BSI or generally recognised security criteria.

The audit is generally carried out by an audit team contracted by the BSI or by the BSI itself. The evaluation is generally carried out by an Information Technology Security Evaluation Facility (ITSEF) recognized by the BSI or by the BSI itself.

The result of the certification procedure is this certification report. This includes, among others: the security certificate (summary assessment) and the detailed certification results.

The certification report contains the technical security description of the certified product, the details of the evaluation and information for the user.

1.2 Specifications of the Certification Procedure

The certification body (CB) carries out the procedure in accordance with the following specifications:

- Act on the Federal Office for Information Security (BSI Act - BSIG) [1];
- BSI Certification and Recognition Regulation (courtesy translation) (BSIZertV) [2];
- Special Regulation on BMI Fees (BMIBGebV) (courtesy translation) (BMIBGebV) [3];
- Special decrees of the Federal Ministry of the Interior (BMI);
- DIN EN ISO/IEC 17065 standard [4];
- Product Certification: Network Equipment Security Assurance Scheme (NESAS) – BSI NESAS Implementation (courtesy translation) (NESAS-Produkte) [5];
- Requirements for the selection of NESAS auditors (courtesy translation) (NESAS-Auditoren) [6];
- Recognition of evaluation facilities: Scheme for recognition as an evaluation facility for NESAS (courtesy translation) (NESAS-Prüfstellen) [7];
- Application Notes and Interpretations of the scheme (courtesy translation) (AIS-N) [8], [9];
- NESAS Specifications [10], [11], [12];
- Security Assurance Specifications (SCAS):
  - 3GPP TS 33.117 (General) [13];
  - 3GPP TS 33.226 (IMS) [14]

1.3 Recognition agreements

Currently, there are no agreements with regards to the recognition of BSI NESAS certificates.

1.4 Audit, Evaluation and Certification Procedure

The CB monitors each individual process assessment (audit) and evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The vendor's development and product lifecycle processes have the process ID Mavenir Integrated Management System.

A valid audit of the vendor’s development and product lifecycle processes with the process ID Mavenir Integrated Management System already existed at the time the certificate was applied for. Therefore, no audit of the vendor’s development and product lifecycle processes has been performed as part of the certification procedure.

The audit ID is BSI-AUD-NESAS-0007-2026. The audit results are recorded in the Audit Report [15] and Audit Summary Report [16].

The product Converged Telephony Application Server (CTAS), version R11.1 has been subject to the BSI certification procedure.

The technical evaluation of the product Converged Telephony Application Server (CTAS) was performed by atsec information security AB, which is recognised by the BSI as an ITSEF in the program BSI NESAS.

The evaluation was completed on 25 June 2026.

For this certification procedure the applicant is Mavenir Systems Inc.

The product Converged Telephony Application Server (CTAS) was developed by Mavenir Systems Inc.

The certification is concluded with the BSI confirming the compliance with the criteria and compiling this certification report.

1.5 Validity of the Certification Result

This certification report applies exclusively to the specified version of the product. The result of the certification only applies if the product is operated under the following conditions:

- All the requirements regarding the generation, configuration and use of the product set out in this report are observed;
- The product is operated under the assumptions described in this report.

The certificate confirms the assurance of the product specified by the NESAS security requirements for vendor development and product lifecycle processes as well as the applicable SCAS documents.

As attack methods evolve over time, it is essential to ensure that the resilience of the product is evaluated regularly. Vendors should therefore have the certified product monitored as part of the BSI's Assurance Continuity Program (e. g. through assessment of minor updates or re-certification).

This certificate was issued on 2026-08-05 and is valid until 2028-08-04. Validity can be renewed by recertification.

The security certificate is issued, in accordance with Section 22, Paragraph 1 of the BSIZertV [2], under the reservation of complete or partial revocation.

The holder of the certificate is obliged:

1. To refer to the certification report and comply with the BSI trademark regulations when advertising the certificate or the fact of product certification;
2. To provide each user of the product with the Certification Report and the referenced user documentation necessary for the deployment or use of the certified product;
3. Maintain the contact address security@mavenir.com;
4. promptly investigate and document any reports of potential product vulnerabilities, especially those reported via the contact address security@mavenir.com;
5. To maintain compliance with the NESAS development and lifecycle process requirements whenever changes are made to the audited processes related to the product for which the certificate is issued;
6. To inform the BSI's Market Surveillance (marktaufsicht@bsi.bund.de) without undue delay of any vulnerabilities identified in the product after certification, whether by you or by third parties;
7. Promptly provide users, free of charge, with a patch and, upon request, with supplemental information regarding the impact of the vulnerability.

If changes are applied to the product, the validity of the certificate may be extended to new versions. The condition for this is that the applicant shall apply for assurance continuity in accordance with the relevant rules and that the evaluation does not reveal any security deficiencies or deviations from the audited vendor's development and product lifecycle processes.

1.6 Publication

The product Converged Telephony Application Server (CTAS), version R11.1 has been included in the BSI list of certified products, which is published regularly (see also website: https://www.bsi.bund.de/nesas). Additional copies of this certification report can be requested from the applicant. The certification report may also be downloaded in electronic form from the website address specified above.

2 Certification Results

2.1 Executive Summary

The certification report is a summary of the vendor's security requirements for the product, the relevant evaluation results from the ITSEF and additional information and requirements of the CB

The product is Converged Telephony Application Server (CTAS), version R11.1. It supports parts of the network function IMS. The Application Server (AS) functionality as part of the IMS network function were evaluated during the evaluation. The product was developed and built in accordance with the audited vendor's product development and life cycle processes with the process ID Mavenir Integrated Management System.

The product, called Converged Telephony Application Server (CTAS) or Mavenir Converged Telephony Application Server (CTAS), implements parts of the IP Multimedia Subsystem (IMS) 3GPP Release 17, specifically the Application Server (AS). The AS in IMS provides the actual multimedia telephony service, supplementary services and features, such as call forwarding, conferencing, and messaging functions for IMS registered subscribers. Furthermore the AS implements the service logic, while IMS handles signalling and session control. More details are presented in the product description [17] section 6.

Not all threats defined in TR 33.926 [18] section 5 are comprehensively mitigated by the product, so that corresponding mitigation measures should be provided via the operational environment (operating system, platform or similar) of the product. Furthermore, some threats defined in TR 33.926 [18] section 5 were found to not apply to the product. Details regarding which threats require mitigation via the operational environment and which are not applicable can be found in section 2.3 of this document.

This certificate is only valid for the specified version of the product in the evaluated configuration and with the complete certification report. This certificate is not an endorsement of the IT Product by the BSI or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2.2 Product Identification and Deliverables

The product is called: Converged Telephony Application Server (CTAS), version R11.1. This release identifier applies at an overall product level but does not represent a single, unified version in the traditional sense. Instead, versioning is applied at the level of individual components that collectively deliver the overall functionality. The core functional capability of the product resides primarily within the Mobile Telephony Application Server (MTAS), deployed as the main pod. Supporting functions, including signalling, routing, load balancing, and service orchestration, are handled by a set of auxiliary components such as Routing Engines (RE), the Virtual Load Balancer Forward Engine (VLBFE), and the Service Manager (SM). These components operate cohesively but are versioned and maintained separately.

The following table outlines the product deliverables:

No	*Type*	*Identifier*	*Version*	*Form of Delivery*
1	SW	Mobile Telephony Application Server (MTAS)	MTAS-R_11_1_42_0EC	Pod, Provided by the vendor to customers.
2	SW	Routing Engine - SIP (RESIP)	RESIP-R_2_0_66_0E	Pod, Provided by the vendor to customers.
3	SW	Routing Engine - Diameter (REDIAM)	REDIAM-R_2_0_67_0E	Pod, Provided by the vendor to customers.

No	*Type*	*Identifier*	*Version*	*Form of Delivery*
4	SW	Routing Engine - General Traffic (REGT)	REGT-R_2_0_71_0C	Pod, Provided by the vendor to customers.
5	SW	Virtual Load Balancer Forward Engine (VLBFE)	VLBFE-V-R_1_0_53_1	Pod, Provided by the vendor to customers.
6	SW	Service Manager (SM)	SM-R_2_0_15_1A	Pod, Provided by the vendor to customers.
7	SW	Routing Engine - SS7 (RESS7)	RESS7-R_2_0_43_0C	Pod, Provided by the vendor to customers.
8	DOC	Mavenir CTAS Product description Guide R11 (11.1, 11.2) [17]	Version 78	Provided by the vendor to customers.
9	DOC	Mavenir TAS Security Guide [19]	Version 8	Provided by the vendor to customers.

Table 1: Deliverables of the product

The version of each software deliverable can be verified by executing the command

cat /etc/mav-image-rel

within the corresponding pod. More information can be found in the ETR [20] section 2.2.

The documentation listed in Table 1 above will be submitted along with the product. Product users shall observe the additional notes and requirements for secure use of the product contained in section 2.7 of this report.

2.3 Architectural Information

A high-level description of the IT product and its major components can be found in the product description [17] section 5.1.2.2 and 6.1.

The product supports the Application Server (AS) as part of the 5G Core Network Function IMS, Release 17.

The product supports Virtualized Network Function (VNF) based deployment and Containerized Network Function (CNF) based deployment. The product that is in scope of the certification is deployed on Kubernetes as CNF.

Assets and threats specific to a network function or applicable for more than one network function and protected by the product are defined in the Technical Report TR 33.926 [18]. The SCAS tests verify the implementation and behavioural conformity of network functions against security requirements derived from the 3GPP Security Architecture for 5G systems (TS 33.501 [21]) and the threat analyses in TRs, with the aim of achieving a standardised security assurance level.

Due to the design of the product, the following threats defined in TR 33.926 [18] section 5 are not comprehensively mitigated by the product, so that corresponding mitigation measures should be provided via the operational environment (operating system, platform or similar) of the product:

Threat name	*Section in TR 33.926*
Spoofing identity	5.3.3
Default Accounts	5.3.3.1
Weak Password Policies	5.3.3.2
Password peek	5.3.3.3
IP Spoofing	5.3.3.5
Malware	5.3.3.6

Threat name	*Section in TR 33.926*
Log Tampering	5.3.4.4
Lack of User Activity Trace	5.3.5.1
Information disclosure	5.3.6
Insecure Data Storage	5.3.6.4
Unnecessary Services	5.3.6.11
Log Disclosure	5.3.6.12
Denial of service	5.3.7
Implementation Flaw	5.3.7.2
Misuse by authorized users	5.3.8.1
Over-Privileged Processes/Services	5.3.8.2
Folder Write Permission Abuse	5.3.8.3
Insecure Network Services	5.3.8.6
Elevation of Privilege via Unnecessary Network Services	5.3.8.7
Incorrect validation of client credentials assertion	6.3.4.1

Table 2: Threats that are not comprehensively mitigated within the product

Furthermore, the following threats defined in TR 33.926 [18] section 5 were found to be not applicable to the product:

Threat name	*Section in TR 33.926*
External Device Boot	5.3.4.3
User Session Tampering	5.3.4.7
Weak cryptographic algorithms	5.3.6.3
File/Directory Read Permissions Misuse	5.3.6.9
Elevation of privilege via incorrect verification of access tokens	6.3.3.1

Table 3: Threats that are not applicable to the product

Details can be found in the Evaluation Technical Report (ETR) [20] section 9.1.

2.4 Results of Evaluation

The results of the evaluation are documented in the ETR [20].

All tests were carried out at the test centre provided by Mavenir (Brno, Czech Republic). The requirements specified in document NESAS-Prüfstellen [7] were taken into account by ITSEF. Individual tests were supervised by the certification body.

At the beginning of the evaluation, the tests specified in TS 33.117 [13] were analysed regarding their relation to the threats from TR 33.926 [18] section 5. Those tests addressing a threat from TR 33.926 [18] section 5 that is considered be not applicable to the product were categorised as non-applicable and were not performed during the evaluation. Tests addressing a threat from TR 33 926 [18] section 5 that, due to the design of the product, were found to require mitigation via the operational environment of the product were also categorised as non-applicable and were not performed during the evaluation. In total, 56 tests were categorised as non-applicable. All non-applicable test cases and corresponding justifications are listed in the ETR [20] section 9.1.

Compliance with the audited processes for the evaluated product were based on the ‘Compliance Evidences to be provided for Network Product and Evidence Evaluation’ for each security requirement, as required by the audit report [15]. The technical evaluation of the product was based on the SCAS documents listed in section 1.2 of this report.

The final verdict of the ITSEF is pass. The provided compliance evidence was found sufficient to demonstrate compliance with the audited processes. The product passed all applicable SCAS tests.The ITSEF has specified any requirements for the vendor or user.

2.5 Recommendations for upcoming recertifications

none

2.6 Missing information and discrepancies

none

2.7 Obligations for and information on using the product

The product must be deployed and operated in accordance with the guidance provided for test execution for Mavenir IMS (TAS): [17], [19], maintaining conditions necessary to preserve the evaluated security posture. Only required network interfaces should be exposed, with network access controls, firewalls, and certificates configured as indicated in the [19] guidance. RBAC, authentication, and logging must be enabled, and credentials managed securely. The product must be maintained within a controlled and monitored environment, preventing unauthorized access, modification, or connections to untrusted systems. External dependencies, including the Kubernetes platform, operating system, and network infrastructure, must be configured and maintained to a security level consistent with the evaluated component.

The user of the product shall include the results of this certification in their risk management process. A time interval should be defined during which a re-assessment of the product is required and requested by the holder of this certificate to take into account the further development of attack methods and techniques.

2.7.1 Specific Conditions for the Vendor

The specific conditions in the Table 4 shall be fulfilled in order to use the product in accordance with the conditions specified in the certification.

Identifier	*Description*
-	-

Table 4: Specific Conditions for the Vendor

2.7.2 Specific Conditions for the User

The specific conditions in the Table 5 shall be fulfilled in order to use the product in accordance with the conditions specified in the certification.

Identifier	*Description*
-	-

Table 5: Specific Conditions for the User

3 Definitions

3.1 Acronyms

AIS ..... Application Notes and Interpretations of the Scheme

AS ..... Application Server

BMI ..... Bundesministerium des Innern (Federal Ministry of the Interior)

BMIBGebV .. Besondere Gebührenverordnung BMI

BSI ..... Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)

BSIG ..... Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (Act on the Federal Office for Information Security)

CB ..... Certification Body

CNS ..... Containerized Network Function

CTAS ..... Converged Telephony Application Server

DIN ..... Deutsche Institut für Normung e. V.

EN ..... Europäische Norm (European Norm)

ETR ..... Evaluation Technical Report

HW ..... Hardware

IEC ..... International Electrotechnical Commission

IMS ..... IP Multimedia Subsystem

ISO ..... International Organization for Standardization

IT ..... Information Technology

ITSEF ..... Information Technology Security Evaluation Facility

MTAS ..... Mobile Telephony Application Server

RE ..... Routing Engines

SCAS ..... Security Assurance Specifications

SM ..... Service Manager

SW ..... Software

TR ..... Technical Report

TS ..... Technical Specification

VLBFE ..... Virtual Load Balancer Forward Engine

VNF ..... Virtualized Network Function

3.2 Bibliography

[1] "Act on the Federal Office for Information Security (BSI-Gesetz - BSIG)," in *Bundesgesetzblatt 2025 I Nr. 301*, 2025, p. p. 2.

[2] "Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV)," in *Bundesgesetzblatt I, no. 61*, 2014, p. 2231.

[3] "Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Sec. 7 (BSI-Gesetz)," in *Bundesgesetzblatt I*, 2019, p. 1365.

[4] *DIN EN ISO/IEC 17065:2013-01: Conformity assessment - Requirements for bodies certifying products, processes and services (ISO/IEC 17065:2012); German and English version EN ISO/IEC 17065:2012,* International Organization for Standardization (ISO), 2013.

[5] „Produktzertifizierung: Programm Network Equipment Security Assurance Scheme (NESAS) – BSI-NESAS Implementierung - NESAS-Produkte Version 2.0," Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 01.07.2025.

[6] Anforderungen für die Auswahl von NESAS-Auditoren - NESAS-Auditoren Version 2.0, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 01.07.2025.

[7] Anerkennung von Prüfstellen: Programm zur Anerkennung als Prüfstelle im Bereich NESAS - - NESAS-Prüfstellen Version 2.0, Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 01.07.2025.

[8] „Anwendungshinweise und Interpretationen zum Schema (AIS) - AIS-N1 - Auditmethodologie BSI NESAS - Version 2.0," Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 01.07.2025.

[9] „Anwendungshinweise und Interpretationen zum Schema (AIS) - AIS-N2 - Anforderungen an die Evaluierung eines Netzwerkproduktes für das Zertifizierungsschema BSI NESAS - Version 2.1," Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 15.02.2026.

[10] „FS.13: NESAS – Framework - Version 3.0," GSM Association, London, 2025.

[11] „FS.14: NESAS – Requirements for NESAS Auditing Organisations, NESAS Security Test Laboratories and Associated Personnel Accreditation - - Version 3.0," GSM Association, London, 2025.

[12] „FS.47: NESAS – Methodology for Product and Evidence Evaluation - Version 3.0," GSM Association, London, 2025.

[13] „TS 33.117 Version 19.2.0: Catalogue of general security assurance requirements," 3rd Generation Partnership Project - Technical Specification Group Services and System Aspects, Valbonne, 2026-01.

[14] „TS 33.226 Version 19.0.0: Security assurance for IP Multimedia Subsystem (IMS)," 3rd Generation Partnership Project - Technical Specification Group Services and System Aspects, Valbonne, 2025-10.

[15] „Audit Report BSI-AUD-NESAS-0007-2026, Version 1.1," Federal Office for Information Security, (confidential document), 2025-12-10.

[16] „Audit Summary Report," Federal Office for Information Security.

[17] „Mavenir CTAS Product Description Guide; Release: R11 (11.1, 11.2); Document Version: 78.0," Mavenir, (confidential document), 2026-03-24.

[18] „TR 33.926 Version 19.3.0: SCAS threats and critical assets in 3GPP network product classes," 3rd Generation Partnership Project - Technical Specification Group Services and System Aspects, Valbonne, 2025-01.

[19] „Mavenir TAS Security Guide, Document Version 8," Mavenir, (confidential document), 2026-04-21.

[20] „Evaluation Technical Report (ETR), Version 3.0," atsec information security AB, Svärdvägen 23, SE-182 33 Danderyd, Sweden, (confidential document), 2026-06-24.

[21] „TS 33.501 Version 19.4.0: Security architecture and procedures for 5G system," 3rd Generation Partnership Project - Technical Specification Group Services and System Aspects, Valbonne, 2025-09.

4 Annexes

4.1 Minor updates to the evaluated configuration

Minor updates listed in Table 6 have been subsequently added to this certification report.

Date Minor Update	*Identifier*	*Release*	*Changes compared to last Release*
-	-	-	-

Table 6: Minor updates to the evaluated configuration

Note: End of report