

Certification Report

BSI-DSZ-CC-S-0323-2025

for

**Ardentec Corporation, Talent site (T Site),
Keystone site (K Site) and data centers of Glory
site (G Site) and Prosperity site (P Site)**

of

Ardentec Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111



Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches



IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-S-0323-2025

Test Center

**Ardentec Corporation, Talent site (T Site), Keystone site (K Site)
and data centers of Glory site (G Site) and Prosperity site (P Site)**



of Ardentec Corporation

Life cycle phase: Wafer Testing and WLCSP

Assurance (*): Common Criteria Part 3 conformant
- ALC_CMC.5, ALC_CMS.5, ALC_DVS.2,
ALC_LCD.1
- ALC_DEL.1, ALC_TAT.3

valid until: 7 February 2028

The site identified in this certificate has been evaluated by an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 extended by BSI Scheme procedures including the Supporting Document Guidance CCDB-2007-11-001 for conformance to the Common Criteria for IT Security Evaluation (CC), CC:2022.

This certificate applies only to the specific site as indicated above and in conjunction with the complete content of the Certification Report and the Site Security Target.

(*) For information on the evaluated scope of the certified site and the application of the assurance components listed above and their relevance and applicability for the certified site see the Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the site by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the site 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, 2 October 2025

For the Federal Office for Information Security

Fabian Hodouschek
Head of Certification

L.S.

Sandro Amendola
Director-General Directorate General S

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 87 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn

Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A Certification..... 6

1 Preliminary Remarks..... 6

2 Specifications of the Certification Procedure..... 6

3 Recognition Agreements..... 7

4 Performance of Evaluation and Certification..... 7

5 Validity of the certification result..... 8

6 Publication..... 8

B Certification Results..... 10

1 Identification of the Site..... 10

2 Life cycle phase..... 10

3 Technical scope..... 10

4 Assumptions and Clarification of Scope..... 11

5 Documentation..... 11

6 Results of the Evaluation..... 12

7 Obligations and notes for the usage of the site..... 13

8 Site Security Target..... 13

9 Definitions..... 13

9.1 Acronyms..... 13

9.2 Glossary..... 14

10 Bibliography..... 15

A Certification

1 Preliminary Remarks

Under the Act on the Federal Office for Information Security (BSIG)¹, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products as well as for development and production sites for information technology products.

The results from a site certification can be re-used for product certifications. For products which have been certified using a site certificate an individual certificate will be issued.

Certification of a site is carried out on the instigation of the operator of the site. A part of the procedure is the technical examination (evaluation) of the site according to the security criteria published by the BSI or generally recognised security criteria. The evaluation is carried out by an evaluation facility recognised by the BSI or by BSI itself. The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the description of the site, the activities for which the site is responsible within a product life cycle, the details of the evaluation (strengths and weaknesses) and instructions for the client of the site.

2 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security (BSIG)¹
- BSI Certification and Approval Ordinance²
- BMI Regulations on Ex-parte Costs³
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3], including CC Site Certification
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

¹ Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821
Current version see website: http://www.gesetze-im-internet.de/bsig_2009/index.html

² Ordinance on the Procedure for Issuance of Security Certificates and Approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231
Current version see website: http://www.gesetze-im-internet.de/bsizertv_2014/index.html

³ BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365
Current version see website: <https://www.bsi.bund.de/Gebuehrenverordnung>

- Common Criteria for IT Security Evaluation (CC), CC:2022⁴ [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation, CC:2022 [2] also published as ISO/IEC 18045
- Supporting Document Guidance Site Certification [5]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Internal procedure for the issuance of a site certificate

3 Recognition Agreements

Currently the Recognition Agreements in place (SOGIS-MRA and CCRA) do not cover the recognition of Site Certificates. However, the evaluation process performed was outlined according to the rules of the agreements and by using the agreed supporting document on Site Certification [5].

Therefore, the results of this evaluation and certification procedure can be re-used in a subsequent product evaluation and certification procedure by the product certificate issuing scheme depending on its scheme policy.

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level up to and including Common Criteria (CC) Evaluation Assurance Levels EAL 4, and in addition at higher recognition levels for IT-Products related to certain technical domains only. Details on recognition, technical domains and the agreement itself can be found at <https://www.sogis.eu>.

The international Common Criteria Recognition Arrangement (CCRA) became effective in September 2014 in its current version. It defines the recognition of certificates for IT-Products at a basic recognition level up to and including Common Criteria (CC) Evaluation Assurance Levels EAL 2. Details on recognition, signatory nations and the agreement itself can be found at <https://www.commoncriteriaportal.org>.

4 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The site Ardentec Corporation, Talent site (T Site), Keystone site (K Site) and data centers of Glory site (G Site) and Prosperity site (P Site) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-S-0238-2023.

The evaluation of the site Ardentec Corporation, Talent site (T Site), Keystone site (K Site) and data centers of Glory site (G Site) and Prosperity site (P Site) was conducted by Deutsche Telekom Security GmbH (Bonn). The evaluation was completed on 1 October 2025. The Deutsche Telekom Security GmbH (Bonn) is an evaluation facility (ITSEF) recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Ardentec Corporation.

The operator of the site is: Ardentec Corporation.

⁴ Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5 Validity of the certification result

This Certification Report only applies to the site and its evaluated scope as indicated. The confirmed assurance package is only valid on the condition that all assumptions and preconditions required by the site, as given in the following report and the Site Security Target [7], are observed.

For the meaning of the assurance components please refer to Supporting Document [5] for the definition of the security assurance requirements AST and to CC [1] Part 3 for the definition of the security assurance components for the class ALC Life-cycle support, for the class AVA Vulnerability assessment and for the cross reference of Evaluation Assurance Levels (EALs) and assurance components.

In case of changes to the certified site, the validity can be extended to the changed site, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified site, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

The owner of the certificate is obliged:

- When advertising the certificate or the fact of the site's certification, to refer to the Certification Report.
- To provide the Certification Report, the Site Security Target and the guidance documentation for the usage of the site mentioned herein (if applicable) to any client of the site and to related evaluation and certification/approval entities for re-use of certification results, e.g. in product evaluation procedures.
- To uphold and apply the assurance measures as evaluated for the full validity period of this certificate.
- To inform the Certification Body at BSI immediately in the case security relevant changes at the site will be made as well as to inform the Certification Body at BSI immediately about vulnerabilities at the site that have been identified by the operator of the site or any third party.
- To inform the Certification Body at BSI immediately in the case that confidentiality of documentation and information related to the site or resulting from the evaluation and certification process is not given any longer.

As long as assurance measures that are within the scope of this certificate have not been changed and no vulnerabilities have been detected, the validity of the certificate ends as outlined on the certificate.

This certificate has been issued with respect to production for the markets covered by the SOGIS MRA.

6 Publication

The site Ardentec Corporation, Talent site (T Site), Keystone site (K Site) and data centers of Glory site (G Site) and Prosperity site (P Site) has been included in the BSI list of certified sites, which is published regularly (see also Internet: <https://www.bsi.bund.de> and

[6]). The Certification Report and the Site Security Target [7] can be obtained in electronic form at the internet address stated above.

B Certification Results

The following results represent a summary of

- the Site Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Identification of the Site

The evaluated site is Ardentec Corporation, Hsinchu, Taiwan, ARDT site which consists of Talent site (T Site), Keystone site (K Site) and data centers of Glory site (G Site) and Prosperity site (P Site). They are located at:

Ardentec Corporation, Talent site (T-site): No. 3, Gongye 3rd Rd., Hsin-Chu Industrial Park, Hukou Township, Hsinchu County 303036, Taiwan, R.O.C., of which the 2nd floor of building P1 (TSP1) is used for the testing of security products, and the basement and 1st floor house supporting services, and the 1st floor of building P2 (TSP2) houses supporting services.

Ardentec Corporation, Keystone site (K-site): No. 24, Wenhua Rd., Hsin-Chu Industrial Park, Hukou Township, Hsinchu County, 303035, Taiwan, R.O.C., of which the 5th floor is used for the testing of security products and WLCSP, and the 2nd floor houses the Fault Analysis Lab and, together with the 1st floor, other supporting services.

Ardentec Corporation, Glory site (G-site): No. 9, Renyi Rd., Hukou Township, Hsinchu County 303035, Taiwan, R.O.C., used for supporting services.

Ardentec Corporation, Prosperity site (P-site): No. 12, Guangfu N. Rd. Hukou Township, Hsinchu County 303036, Taiwan, R.O.C., used for supporting services.

2 Life cycle phase

The certification of the site covers the following life cycle phase: Parts of life cycle phase 3 and 4 of Security IC's as described in Security IC Platform Protection Profile [9] for the IC manufacturing. The Ardentec Corporation Ting-Sing site (T Site) and Kaiyuan site (K Site) provide services for wafer testing and IC pre-personalisation. If the ICs on the wafers are locked after testing by the test program provided by the client, Ardentec T Site changes the lifecycle phase of the ICs from phase 3 to phase 4. Additionally, the site provides semiconductor testing services (wafer test and Failure Analysis), as well as semiconductor packaging services (WLCSP Process).

3 Technical scope

The Ardentec Corporation, ARDT site provides services for wafer testing, final test of smart card ICs on wafers, fault analysis, and some WLCSP packaging services. The wafers are tested to the requirements of the clients. Ardentec Corporation does not develop any test programs for security products. The finished wafers are tested based on test programs provided by the client. The services offered by the evaluated site comprise also steps in the test flow of the wafers including pre-personalisation and life-cycle transition. That means, if the ICs on the wafers are locked after testing by the test program which is provided by the client, the lifecycle phase of the ICs change from phase 3 to phase 4. In

addition, Ardentec Corporation, ARDT site provide secure destruction procedures for wafers and dies. For more details please refer to the Site Security Target [7], chapter 2.2.

The full version of the Site Security Target [7] is the basis for this certification.

The certification of the site covers the following life cycle phase: Parts of the life cycle phase 3 and 4 related to the testing and WLCSP processes with Security ICs. If the ICs on the wafers are locked after testing by the test program, Ardentec Corporation, ARDT site changes the lifecycle of ICs from phase 3 to phase 4.

The Security Problem Definition for this site comprises security problems derived from threats against relevant assets and for the type of TOE considered as well as security problems derived from the configuration management requirements. The assets, assumptions, threats and organisational security policies are defined in the document Site Security Target [7], chapter 4.1 - 4.4. They are derived from the Security IC Platform Protection Profile [9]. Only aspects that are applicable to the life cycle phase 3 and 4 are considered here.

The security objectives for the site are derived from these threats and organisational security policies as stated in the Site Security Target [7], chapter 4.

The Site Security Target claimed the following Common Criteria Part 3 life cycle security assurance components to be part of the evaluation:

- CM capabilities - ALC_CMC.5
- CM scope - ALC_CMS.5
- Delivery - ALC_DEL.1
- Development security - ALC_DVS.2
- Life-cycle definition - ALC_LCD.1
- Tools and techniques - ALC_TAT.3

The specific scope of these components relevant at this site is explained in the Site Security Target [7], chapter 7. As outlined in the Site Security Target, the activities of the site are not related to TOE Delivery ALC_DEL and Tools and techniques ALC_TAT. However, the components have been claimed in order to ensure the assessment of related items during the evaluation process and therefore to support the reuse of the evaluation results in a product evaluation accordingly.

For the assessment of the security measures attackers with high attack potential are assumed. This allows an evaluation of products using this site according to the assurance component AVA_VAN.5.

4 Assumptions and Clarification of Scope

The assumptions defined in the Site Security Target are not covered by the site itself. These aspects have to be followed by a client of the site. The list of assumptions which have to be followed by the client of the site can be found in the Site Security Target [7], chapter 4.4.

5 Documentation

There is no evaluated documentation being provided to the client of the site. The client has to follow the requirements as stated in the Assumptions in the Site Security Target [7], chapter 4.4.

6 Results of the Evaluation

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the site.

Specifically the Supporting Document Guidance CCDB-2007-11-001 Site Certification [5], AIS 47 "Regelungen zu Site Certification" [4] and AIS 1 including the JIL Documents were used.

For smart card IC specific methodology the CC supporting document "The Application of CC to Integrated Circuits" (see [4] AIS 25) was used.

All assurance components claimed in the Site Security Target [7], chapter 7 are confirmed to be Common Criteria Part 3 conformant.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components applicable to the site:

- CM capabilities - ALC_CMC.5
- CM scope - ALC_CMS.5
- Development security - ALC_DVS.2
- Life-cycle definition - ALC_LCD.1

The following assurance components have been covered by the evaluation, but the evaluation concluded that the site does not provide contributions to the security objectives and therefore these components are not applicable to the site:

- Delivery - ALC_DEL.1
- Tools and techniques - ALC_TAT.3

For reusing the evaluation results in product evaluations, the specific scope of the assurance components as relevant at this site and outlined in the Site Security Target has to be assessed if it fits into the product life cycle considered.

As the assurance components assessed are derived from the assurance level EAL6 of the CC assurance class "Life-cycle Support", this site certificate supports product evaluations up to the assurance level EAL6.

For the assessment of the security measures attackers with high attack potential have been assumed. This supports an evaluation of products using this site according to the assurance component AVA_VAN.5.

The evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-S-0238-2023. The focus of this re-evaluation was on covering the constant site security evolution and maintaining the certified status of the site.

The evaluation has confirmed for the type of product considered that the phases of the development and production life cycle and the related processes as stated in the SST are covered by the site.

The certification results only apply to the site as indicated in the certificate, the scope as defined in the Site Security Target and on the condition that all the stipulations are kept as detailed in this Certification Report.

This certificate is not an endorsement of the site by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate,

and no warranty of the site by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

The audit has been performed as a regular on-site audit according to the BSI Scheme requirements and according to the rules defined in the SOGIS-MRA. Therefore, the results of this certification can be reused for 30 months from the audit date. The validity of this certificate has been defined accordingly.

For this site certificate there is a Site Technical Audit Report (STAR) available [10]. The purpose of that document is to provide guidance for unified Site audit results reporting across all SOGIS CBs and in light of the MSSR as well as to fulfil the requirements of a CC evaluation and certification in the event of ALC reuse of Site audit results for product certification. The distribution of this Site Technical Audit Report (STAR) [10] is restricted to a 'Need to Know' basis between the Developer/Sponsor of the Site, the Evaluation Labs, and the Certification Bodies.

7 Obligations and notes for the usage of the site

The relevant information for using the evaluated scope of the site within product evaluations is given in the Site Security Target [7]. During a product evaluation the evidence for the fulfilment of the Assumptions given in section 4.4 of the Site Security Target shall be examined by the evaluator of the product when re-using the results of this site evaluation. Note that the sponsor of a potential product evaluation has to ensure that all information required by the Assumptions is made available.

The specific scope of the ALC assurance components as evaluated and as outlined in the Site Security Target has to be assessed if it fits into the product life cycle considered.

The assets assessed, any limitations in covering confidentiality or integrity aspects and the resistance level (AVA_VAN) applied have to be considered according to the Site Security Target when re-using the evaluation results in a product evaluation.

8 Site Security Target

For the purpose of publishing, the Site Security Target is provided within a separate document as an annex of this report. It is a sanitised version of the complete Site Security Target [7] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

9 Definitions

9.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MSSR	Minimum Site Security Requirements
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SST	Site Security Target
ST	Security Target
STAR	Site Technical Audit Report
TOE	Target of Evaluation
TSF	TOE Security Functionality

9.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Client - The term "client" is used to describe the subcontracting relationship between the developer/manufacturer of the product and the site providing a specific manufacturing step described in the SST. The term is used to prevent confusion regarding the words "customer" and "consumer" that are reserved in CC for the recipient (addressee) of the finished product.

Extension - The addition to an SST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in Part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Life cycle phase – part of a life cycle of a product.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Site Security Target - A statement of security needs for a specific identified development or production site.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Site - A part or the whole of an existing or anticipated TOE development environment. A site may consist of one geographical location, be a part of one location, or may span (parts of) multiple locations. A site may consist of one organisational unit, be part of an organisational unit, or may span (parts of) multiple organisational units.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

10 Bibliography

- [1] Common Criteria for Information Technology Security Evaluation/CC
 ISO-Version:
 ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
 - Part 1: Introduction and general model
 - Part 2: Security functional components
 - Part 3: Security assurance components
 - Part 4: Framework for the specification of evaluation methods and activities
 - Part 5: Pre-defined packages of security requirements_
<https://www.iso.org/standard/72891.html>
<https://www.iso.org/standard/72892.html>
<https://www.iso.org/standard/72906.html>
<https://www.iso.org/standard/72913.html>
<https://www.iso.org/standard/72917.html>
 CCRA-Version:
 CC:2022 R1, Common Criteria for Information Technology Security Evaluation
 - Part 1: Introduction and general model
 - Part 2: Security functional components
 - Part 3: Security assurance components
 - Part 4: Framework for the specification of evaluation methods and activities
 - Part 5: Pre-defined packages of security requirement
<https://www.commoncriteriaportal.org>
- [2] Common Methodology for Information Technology Security Evaluation (CEM),
 Evaluation Methodology
 ISO-Version:
 ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
<https://www.iso.org/standard/72889.html>
 CCRA-Version:
 CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
<https://www.commoncriteriaportal.org>
- [3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), <https://www.bsi.bund.de/zertifizierung>
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE⁵
<https://www.bsi.bund.de/AIS>.

⁵specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers - including JIL Document
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen - including JIL Document and CC Supporting Document

- [5] Supporting Document Guidance CCDB-2007-11-001 Site Certification, October 2007, Version 1.0, Revision 1
- [6] German IT Security Certificates, periodically updated list published also on the BSI Website: <https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten>:
- [7] Site Security Target Ardentec Corporation, ARDT site, AG0065, BSI-DSZ-CC-S-0323, Rev. 16, 08.9.2025, Ardentec Corporation (confidential document) and Site Security Target Lite Ardentec Corporation, ARDT site, AG0066, BSI-DSZ-CC-S-0323, Rev. 11, 26.9.2025, Ardentec Corporation (sanitised public document)
- [8] Evaluation Technical Report, Ardentec Corporation, Talent site (T Site), Keystone site (K Site) and data centers of Glory site (G Site) and Prosperity site (P Site), Version 5.0, 26.09.2025, Deutsche Telekom Security GmbH (confidential document)
- [9] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014
- [10] Site Technical Audit Report (STAR) Ardentec ARDT site BSI-DSZ-CC-S-0323, Version 4.1, 26.9.2025, Deutsche Telekom Security GmbH (confidential document)

Note: End of report

- AIS 32, Version 7, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) - including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results
- AIS 47, Version 1.1, Regelungen zu Site Certification