Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1173-2021

for

Zoom Application Version 5.6.6

from

Zoom Video Communications, Inc.

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-1173-2021 (*)

Video Communications Client

Zoom Application
Version 5.6.6

from	Zoom Video Communications, Inc.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 part A chapter 5.

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.

Common Criteria
Recognition Arrangement

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, 21 December 2021

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - 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

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally 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 technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

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[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- 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]
- 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

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

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

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certifications of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

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 and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

This certificate is recognized under CCRA-2014 for all assurance components selected.

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 product Zoom Application, Version 5.6.6 has undergone the certification procedure at BSI.

The evaluation of the product Zoom Application, Version 5.6.6 was conducted by secuvera. The evaluation was completed on 17 December 2021. secuvera is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Zoom Video Communications, Inc.

The product was developed by: Zoom Video Communications, Inc.

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 applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 21 December 2021 is valid until 20 December 2026. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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

6. Publication

The product Zoom Application, Version 5.6.6 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Zoom Video Communications, Inc.
San Jose Headquarters 55 Almaden Boulevard
6th Floor San Jose, CA 95113

B. Certification Results

The following results represent a summary of

- the 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. Executive Summary

The Target of Evaluation (TOE) is a multi-platform software client application used to host, run and organize enterprise web video communications (web meetings) using a cloud platform (Zoom Backend) for video and audio conferencing, collaboration, chat across mobile devices and desktops. The Zoom Backend is not part of the TOE, but of its environment.

Web meetings are primarily used to offer audio and video conferencing as well as desktop sharing. Additionally, during web meetings a user can share files and text messages with the other participants.

The TOE also offers an out-of-meeting instant messaging service called Zoom Chat, which can be used to share text, audio and video messages with one or more TOE users outside of web meetings. It is also possible share files with other users outside of web meetings by uploading them to Zoom Chat.

The TOEs main security features are:

- Secure user authentication,
- Protection of confidentiality and integrity of all data transferred during Zoom Meetings,
- Enforcing access control rules during Zoom Meetings, e.g. prohibiting users from unmuting their microphone,
- Enforcing of user controls, e.g. making sure no audio data is transferred if a user mutes his microphone during a Zoom Meeting,
- Protection of integrity and confidentiality of all data exchanged during Zoom Chats, including protection from Zoom itself by offering optional end-to-end encryption for Zoom Chats,
- Protection of Zoom Chat data (e.g. chat messages, voice notes) stored on the user's device.

The TOE has been evaluated and certified in form of the following client versions:

- Windows-Client (64-Bit),
- macOS-Client (Intel architecture),
- Android-Client,
- iOS/iPadOS-Client.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter "SECURITY REQUIREMENTS". They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
User identification and authentication	The TOE identifies and authenticates all user before granting them access to any TSF functionality.
Meeting authentication	Authentication to a meeting is password based.
User and security controls	During a meeting, users are able to access controls like muting and unmuting their microphone or starting and stopping screen sharing.
Secure data transfer	All data transferred between the TOE and Zoom backend is protected by either a TLS channel or Zoom's meeting encryption.
Zoom Chat	Zoom Chat generally uses the same TLS channel as the rest of the TOE functionality. Additionally, the TOE stores Zoom Chat data in a database that is encrypted and integrity protected.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter "TOE SUMMARY SPECIFICATION".

The assets to be protected by the TOE are defined in the Security Target [6], chapter "SECURITY PROBLEM DEFINITION". Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter "SECURITY PROBLEM DEFINITION".

This certification covers the configurations of the TOE as outlined in chapter 8 of this document.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product 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 IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Zoom Application, Version 5.6.6

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Zoom Application for Microsoft Windows Client	5.6.6	Secure download via TLS 1.2 https://zoom.us/download
2	SW	Zoom Application for Apple macOS Client	5.6.6	Secure download via TLS 1.2 https://zoom.us/download

No	Type	Identifier	Release	Form of Delivery
3	SW	Zoom Application for Apple iOS/iPadOS Client	5.6.6	Download via Apple app store (https://apps.apple.com/us/app/id546505307)
4	SW	Zoom Application for Android Client	5.6.6	Secure download via TLS 1.2 https://zoom.us/download or Google Play (https://play.google.com/store/apps/details?id=us.zoom.videomeetings)
5	DOC	Zoom Application – Guidance Documentation [9] SHA256: df06eb4bc252b5a143f5f6d1f203249bba8a207469545b1cf36575e777a20b02	1.5	Secure download via TLS 1.2 https://explore.zoom.us/en/common-criteria/

Table 2: Deliverables of the TOE

The scope of the TOE includes the main functionality of the product which is updated on a regular basis. The certified version may not be publicly available anymore if it has been superseded by a newer version. Therefore the delivery of the client is not described especially for the certified version but for the client versions independent of the version number.

Table 2 outlines the general delivery of the Zoom client Application and its documentation. In general the TOE or the latest product version for the different client versions is available via download from the Zoom webpage or from the app stores of Google and Apple. The guidance documentation [9] is available via download from the Zoom webpage.

The user is able to verify the authenticity and integrity of the delivered TOE. The procedure is described in detail in the guidance documentation [9] chapter 2.3.

The TOE verification is performed with the digital signature of the TOE. The SHA-256 fingerprint can be compared with the information given in the guidance documentation [9]. If the fingerprints are matching, the TOE client version is verified correctly. For Apple iOS/iPadOS the TOE client is only available via the iOS app store and thereby protected via its security mechanisms.

The details for each of the four platforms are as follows:

Windows: Right click on the downloaded installer file, click on *“Properties”* and navigate to the *“Digital Signatures”* tab in the Properties window. Click on one of the signatures in the list and then click on the *“Details”* button. In the new window, Windows will show whether the digital signature is OK or not. The signature of the installed application can be checked in the same way by right clicking on the *Zoom.exe* file. Alternatively, the *SignTool* of the Microsoft Windows SDK can be used to verify the signature.

The SHA-256 fingerprint of the certificate used to sign the Windows installer of version 5.6.6 is `6ba9ef6eb60103b1912b9e79f3eef4c6f662c4f7`. It can be viewed by first navigating to the *“Details”* section as described above and then clicking on *“Show certificate”*. A new window will open and the fingerprint is contained in the *“Details”* tab of this window.

macOS: Double click on the downloaded *Zoom.pkg* file to open a window that guides the user through the installation process. In the top right corner of this window, a small padlock icon is shown. Click on this padlock icon to show the details of the used certificate and to verify the signature of the package.

The SHA-256 fingerprint of the certificate used to sign the macOS installer of version 5.6.6 is `36 AF C6 B4 4F F0 68 FD 67 40 AC D2 80 F6 6E B7 82 D1 08 E8 15 22 EC 3B 2F 57 6E BA 90 AC 62 BC`. It can be viewed by clicking on the padlock icon as described above and then opening the details section of the certificate issued by Zoom.

Note that Windows and macOS in their default configurations also check the signatures of the apps on first run.

Android (via Zoom Download Center): The file's digital signature needs to be verified as described under *https://developer.android.com/studio/command-line/apksigner*.

The SHA-256 digest of the certificate used to sign the the APK file of version 5.6.6 published by Zoom is `60b75724b34686e52bde944969de120f16bd6d959788d54384494caedd4e445d`. It can be viewed by using the command `apksigner verify --print-certs zoom.apk`, where "`zoom.apk`" is the filename of the APK.

Android (via Google Play Store) and iOS/iPadOS: If the mobile app was downloaded and installed using the official app stores there is no need to verify the app since it is protected by the stores' security mechanisms.

In case signature verification of the downloaded installer files (on desktop or Android) fails, the installer must not be used.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The TOE implements policies pertaining to the following security functional classes:

- User identification and authentication
- Meeting authentication
- User and security controls
- Secure data transfer
- Zoom Chat

Specific details concerning the above mentioned security policies can be found in the Security Target [6], chapter "TOE SUMMARY SPECIFICATION".

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The topics listed in the ST [6] chapter "ASSUMPTIONS" are of relevance.

Namely they are:

- A.Meeting_Key: The Zoom backend generates SA.Meeting_Key and provides at least 120 bit security.
- A.User_Credentials: Any user of the TOE does not disclose their authentication or meeting credentials to any individual not authorized for access to the TOE or meeting.
- A.Rate_Limiting: The Zoom backend implements rate limiting on brute-force-attacks for meeting password and user authentication.
- A.Secure_Backend: The Zoom backend is trusted. Data sent from the Zoom backend is assumed to be with integrity.
- A.Host_Device: The TOE's host device of the TOE offers means to securely store and access cryptographic keys, as well as provide a random number generator of appropriate strength to be used for cryptographic operations required by the TOE.
- A.Managed_Device: The TOE runs on a managed device. The device management controls which applications can be installed on the device, to ensure no malicious applications are installed which could harm the security of the TOE. For Android smartphones this means, the device has to support an enterprise container technology, and the TOE runs in a work profile or on an exclusive, managed enterprise device.
- A.Proper_User: The user of the application is not wilfully negligent or hostile and uses the TOE within compliance of the applied enterprise security policy.
- A.Non_Hostile_Platform: The platform on which the TOE is running on does not start any attacks on assets protected by the TOE.

5. Architectural Information

The TOE is a multi-platform software client application used to host, run and organize enterprise web video communications (web meetings) using a cloud platform (Zoom Backend) for video and audio conferencing, collaboration, chat across mobile devices and desktops. The Zoom Backend is not part of the TOE.

The architectural description on EAL2 level covers mainly a high-level overview of the main components. Their roles in a Zoom meeting communication are summarized in Figure 4 of the ST [6].

The TOEs main security features are:

- Secure user authentication,
- Protection of confidentiality and integrity of all data transferred during Zoom Meetings,
- Enforcing access control rules during Zoom Meetings, e.g. prohibiting users from unmuting their microphone,
- Enforcing of user controls, e.g. making sure no audio data is transferred if a user mutes his microphone during a Zoom Meeting,
- Protection of integrity and confidentiality of all data exchanged during Zoom Chats, including protection from Zoom itself by offering optional end-to-end encryption for Zoom Chats,
- Protection of Zoom Chat data (e.g. chat messages, voice notes) stored on the user's device.

The TOE can be executed on all platforms that are specified in the ST [6], table 2.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

Developer Testing

The developer used the tool *Testrail*, a management tool for testing. In *Testrail* different test cases are described, performed and tracked. The tests are allocated to a tester who performs the tests. The tester describes the test result and sets a rating (*pass, fail*) to each test. The ratings for all tests are visible in *Testrail* and further information can be examined.

The QA test team has access to new TOE / product releases and performs the testing on every software built.

By using a regression testing strategy each prior tested function will be tested in a new TOE release. Thereby the TOE features are examined if they still perform as specified and expected. The usage of *Testrail* for managing the testing supports the regression testing strategy. Older test results are visible and can easily be compared. The tests are manually performed by a Zoom tester of the QA team with the described testing procedure in *Testrail*. As the testing is performed via the graphical interface of the TOE on the four platforms “Windows”, “macOS”, “iOS/iPadOS” and “Android” a human tester can efficiently recognize inconsistencies with the expected results or the behaviour on the different platforms.

All functional and non-functional tests cover the graphical user interface of the TOE which is the defined TSFI of the TOE.

Zoom conducts tests on real environments, i.e. on all above mentioned platforms and OS versions. If a specific OS version of the ST [6], table 2 has not been covered by the test configuration of the developer, either a convincing justification has been provided by the evaluator why it can still be included into the evaluated scope or the independent evaluator tests covered that OS version.

The tests for each platform were performed on physical machines and devices.

For the testing of the TOE Client for Android, the *Google Pixel 4XL* was used amongst other devices.

The test results of the testing performed by Zoom are described in a test document. All tests show the expected result “pass” and thereby the TOE clients behave as expected.

Independent Evaluator Tests

The testing was divided in the parts along the main operations of the TOE, i.e. “Installation & Login”, “Meeting”, “Chat”. The operation “Failure Handling” tested the behaviour of the TOE without a network connection. The tests were performed via the graphical user interface of the TOE, which is the identified TSFI and the only available interface for a user.

During the operations “Meeting” and “Chat” not only the functionality was tested but also the configuration of the TOE by the TOE settings. During the operation “Installation & Login” it was investigated how the TOE achieves its known state.

All tests were performed for the certified TOE version and on all TOE platforms that are listed in the security target [6].

During the testing the following HW and SW configurations were used:

- Microsoft Windows: Windows 10 Pro and Dell Precision Tower 3420.
- Apple macOS: macOS 11.2.1 (Big Sur) and MacBook Air Apple.
- iOS/iPadOS: iOS 14.2 and iPhone SE.
- Android: Android 10 and Xiaomi Mi 10T Pro.

The TOE was tested in a real productive environment and on real hardware. That means, the TOE was installed on the platforms and used in the same way a user will install and use it. The real Zoom backend was used. No virtualisation of the Zoom backend or of other parts of the environment was used.

The TOE was installed on the different platforms by executing the installation according to the guidance documentation [9] in chapter 2.4, “Installation”.

The security objective for the TOE environment *OE.Managed_Device* was not implemented in the test environment. That means on the different platforms there was no client management used and the devices were not managed, however, that security objective was still kept in mind during the whole testing period and within the test assessment.

The test results of the independent testing showed the expected result “pass” and thereby the TOE clients behave as expected.

Penetration Testing

Penetration testing of the TOE was conducted by using the same test configuration and machines as described above in the independent evaluator test subchapter. The TOE was tested on the different platforms in a productive environment. That means, the TOE was installed on the real platforms and used like a user will install and use it. No virtualisation of the Zoom backend or of other parts of the environment was used.

The penetration testing was divided in different threat paths, i.e. the delivery process, exploiting over a network, login process, data stored on the device, operation/meeting and operation/chat. The penetration testing was performed by triggering functionality in the graphical user interface and analyse the behaviour of the TOE, the TSFI, and the communication with the Zoom Backend.

A CVE analysis was performed. All CVEs that are publicly known for the Zoom client and its components were analysed and evaluated. Furthermore the public domain was searched for information on additional vulnerabilities and attack paths. By that investigation no vulnerabilities or failures of the TOE were identified that could be exploited in the intended configuration and environment of the TOE according to the ST [6] and guidance [9].

To verify the behaviour of TLS in the client the *Achelos TLS Client Inspector* was used. During the performed checks no behaviour was identified which was not expected.

During the penetration testing, no vulnerability was identified that can be exploited by an attacker with basic attack potential.

8. Evaluated Configuration

The TOE is the Zoom Application in version 5.6.6 and has been evaluated on the following platforms

- Microsoft Windows (64-Bit): Windows 10 Home, 10 Pro and 10 Enterprise
- Apple macOS: macOS 10.13 (Sierra), 10.14 (Mojave), 10.15 (Catalina), 11 (Big Sur)
- Apple iOS/iPadOS: iOS 12, 13 and 14, iPadOS 13 and 14
- Android: Android 8.1, 9, 10 and 11

and on the above mentioned hardware devices.

Note that a Linux version of the TOE is also available. However, this version is not in scope for the certification.

The complete TOE deliverables in terms of the Common Criteria include:

- the software application, in form of an executable program,
- an operational manual [9], available as a secure download from Zoom's website in form of a PDF file.

The TOE only includes the Zoom Meeting and Zoom Chat functionality of the Zoom client application. The Zoom backend is not part of the TOE.

Admin management is not part of the Zoom application and therefore not TOE functionality.

The certified version of the TOE needs to be operated with a paid license. The binary of the Zoom application is the same for all licensing models, the only technical difference in terms of security is that users with a free license cannot initiate end-to-end encrypted Zoom Chats, they can however still participate in end-to-end encrypted chats if a user with a paid license initiated the chat.

The TOE needs to run on either a computer running Windows or macOS or a mobile device running Android or iOS/iPadOS.

All devices the Zoom application is installed on need to be part of a managed client infrastructure that controls which applications can be installed on the device. The TOE also requires the Zoom backend to operate.

For Android devices it is required that the TOE runs in a managed environment (i.e. the device supports an enterprise container technology and the TOE is only used in a managed work profile, or the TOE is executed on an exclusive, managed enterprise device) and that the device makes use of an embedded security module.

The TOE was tested on the following Android mobile devices: *Xiaomi Mi 10T Pro,Google Pixel 4XL*.

The evaluated and certified configuration was tested on the above listed hardware models and OS versions, however the commercial product is designed to run on a wider range of hardware and OS versions that exceeds the scope of the certification.

The TOE has to be configured, and is limited to the restrictions as stated in the Security Target [6] and Guidance [9]. The TOE has to be configured following the TOE guidance [9]. The components of the TOE are defined by the TOE configuration list [8].

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] 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 TOE.

The Evaluation Methodology CEM [2] was used.

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

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target, Common Criteria Part 2, extended
- for the Assurance: Common Criteria Part 3 conformant, EAL 2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Meeting encryption	AES in GCM mode	FIPS 197, NIST SP800-38D	|k| = 256	Yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
2	Key Agreement	ECDH with SHA-256	NIST SP 800-56A Rev. 3, FIPS 180-4	Key sizes corresponding to the used elliptic curve P-521	Yes	
3	Zoom Chat encryption	AES in CBC mode	FIPS 197, NIST SP800-38A	|k| = 256	Yes	
4	Database encryption	AES in CBC mode	FIPS 197, NIST SP800-38A	|k| = 256	Yes	
5	Database integrity protection	HMAC-SHA512	RFC 2104 NIST FIPS 180-4	|k| = 256	Yes	
6	TLS 1.2 - AES 256	TLS v1.2 with the following Cipher Suites: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	RFC 5246, RFC 5288, RFC 5289	|k| = 256	Yes	
7	TLS 1.2 - AES 128	TLS v1.2 with the following Cipher Suites: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	RFC 5246, RFC 5288, RFC 5289	|k| = 128	Yes	
8	TLS 1.2 - ChaCha20	TLS v1.2 with the following Cipher Suites: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	RFC 5246, RFC 7905	|k| = 256	Not rated	No rating of the security level has been performed.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
9	TLS 1.3 - AES 256	TLS v1.3 with the following Cipher Suite: TLS_AES_256_GCM_SHA384	RFC 8446	|k| = 256	Yes	
10	TLS 1.3 - AES 128	TLS v1.3 with the following Cipher Suite: TLS_AES_128_GCM_SHA256	RFC 8446	|k| = 128	Yes	
11	TLS 1.3 - ChaCha20	TLS v1.3 with the following Cipher Suite: TLS_CHACHA20_POLY1305_SHA256	RFC 8446	|k| = 256	Not rated	No rating of the security level has been performed.
12	Key generation	ECC key generation with curve P-521	FIPS 186-4, B.4 and D.1.2.5	Key sizes corresponding to the used elliptic curve P-521	Yes	
13	Symmetric key generation	Random bit input from OE.RNG.	N/A	|k| = 256	Yes	

Table 3: TOE cryptographic functionality

Reference details for table 3:

***NIST SP800-38A**: NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation – Methods and Techniques, 2001*

***NIST SP 800-38D**: NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007*

***NIST SP 800-56A Rev. 3**: NIST Special Publication 800-56A Rev. 3, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, 2018*

***FIPS 180-4**: Federal Information Processing Standards Publication 186-4, Secure Hash Standard (SHS), August 2015*

***FIPS 186-4**: Federal Information Processing Standards Publication 186-4, Digital Signature Standard (DSS), July 2013*

***FIPS 197**: Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), 2001*

***RFC 2104**: RFC 2104 – HMAC: Keyed-Hashing for Message Authentication*

***RFC 5246**: RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2*

***RFC 5288**: RFC 5288 - AES Galois Counter Mode (GCM) Cipher Suites for TLS*

***RFC 5289**: RFC 5289 - TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

***RFC 7905**: RFC 7905 - ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)*

***RFC 8446**: RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3*

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

10. Obligations and Notes for the OE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

If available, certified updates of the TOE should be used.

The scope of the TOE includes the main functionality of the product which is updated on a regular basis. A risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security. In this context users may use the latest available (non-certified) version of the TOE and assess the risk to use the TOE within the user's information system or take additional measures in order to maintain system security, e.g. to implement additional policies on the managed client.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

The TOE needs to run on either a computer running Windows or macOS or a mobile device running Android or iOS/iPadOS as specified in the ST [6], table 2.

All devices the Zoom client application is installed on need to be part of a managed client infrastructure that controls which applications can be installed on the device

The TOE requires the Zoom backend to operate.

The *“link preview”* feature in the chat settings of the Zoom client needs to be disabled.

For Android devices it is required that the TOE is executed in a managed environment (i.e. the device supports an enterprise container technology and the TOE is only used in a managed work profile, or the TOE is executed on an exclusive, managed enterprise device) and that the device makes use of an embedded security module.

The TOE only includes the Zoom Meeting and Zoom Chat functionality of the Zoom client application. The Zoom backend is not part of the TOE.

Admin management is not part of the Zoom client application and therefore not TOE functionality.

Entropy that is required by the cryptographic operations of the TOE is obtained from a random number generator of appropriate strength located in the TOE’s environment. Users of the TOE are able to choose which platform they use. See also OE.RNG.

The developer must publish the secure product homepage

https://explore.zoom.us/en/common-criteria/

It has to be present throughout the validity of this certificate and include the relevant information and versions of the documents.

The user has to follow all instructions given in the ST [6] and guidance [9]. The Guidance contains necessary information about the secure administration, configuration, and usage

of the TOE and all security hints therein have to be considered. Chapter 5.1 of the Guidance [9] gives additional usage guidelines for the certified TOE version.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APK	Android Package
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
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie-Hellman
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
HMAC	Hash-based Message Authentication Code
HW	Hardware
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NIST	National Institute of Standards and Technology
OS	Operating System
PP	Protection Profile
RFC	Request for Comments
RSA	Rivest–Shamir–Adleman

SAR	Security Assurance Requirement
SDK	Software Development Kit
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
SW	Software
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

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

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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

Informal - Expressed in natural language.

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

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

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

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017

Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, 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 TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target – Zoom Application, BSI-DSZ-CC-1173-2021, Version 1.8, Date 15/12/2021, Zoom Video Communications, Inc.

[7] Evaluation Technical Report for Zoom Application from Zoom Video Communications, Inc., BSI-DSZ-CC-1173, Version 4, Date 17.12.2021, secuvera GmbH, (confidential document)

[8] Configuration item list for the Zoom Application in version 5.6.6, Date 15/12/2021, File name ‘CIs Zoom client 5.6.6 15-12-2021.xlsx’, Zoom Video Communications, Inc. (confidential document)

[9] Zoom Application - Guidance Documentation, Version 1.5, Date 12/06/2021, Zoom Video Communications, Inc.

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report