National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Wickr Enterprise Client 6.10

Report Number: CCEVS-VR-VID11320-2023
Dated: April 7, 2023
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Jerome Myers

Marybeth Panock

Mike Quintos

Dale Schroeder

The Aerospace Corporation

Common Criteria Testing Laboratory

Allen Sant

Armin Najafabadi

Anthony Apted

Greg Beaver

Josh J. Marciante

Pascal Patin

Leidos Inc.

Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Wickr Enterprise Client 6.10 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in April 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the following document:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021

The Target of Evaluation (TOE) is the Wickr Enterprise Client 6.10.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the Security Target. Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Wickr Enterprise Client 6.10 Security Target, Version 1.0, 07 March 2023 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST): the unique identification of the document describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluated Product	Wickr Enterprise Client 6.10
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Wickr Enterprise Client 6.10. The platform-specific versions of the TOE include: 1. Wickr Enterprise Client for Windows 6.10.2 Evaluated on Microsoft Windows 10. 2. Wickr Enterprise Client for macOS 6.10.2 Evaluated on macOS 12.4 Monterey. 3. Wickr Enterprise Client for iOS 6.10.0 Evaluated on iOS 15.5. 4. Wickr Enterprise Client for Android 6.10.0 Evaluated on Android 12.
Protection Profile	Protection Profile for Application Software, Version 1.4, 7 October 2021
Security Target	Wickr Enterprise Client 6.10 Security Target, Version 1.0, 07 March 2023
Evaluation Technical Report	Evaluation Technical Report for Wickr Enterprise Client 6.10, Version 1.1, 5 April 2023.

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
Sponsor & Developer	Wickr LLC W 31st Street New York, NY 10001
Common Criteria Testing Lab (CCTL)	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	April 2023
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	*Protection Profile for Application Software*, Version 1.4, 7 October 2021
Evaluation Personnel	Allen Sant, Leidos Inc Armin Najafabadi, Leidos Inc Anthony Apted, Leidos Inc Greg Beaver, Leidos Inc Josh J. Marciante, Leidos Inc Pascal Patin, Leidos Inc
Validation Personnel	Jerome Myers: Senior Validator, The Aerospace Corporation Marybeth Panock: Lead Validator, The Aerospace Corporation Mike Quintos: ECR Team, The Aerospace Corporation Dale Schroeder: ECR Team, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following document:

Protection Profile for Application Software, Version 1.4, 7 October 2021

That information has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the PP_APP_v1.4 as described for this TOE in the Security Target.

As stated, the ST references PP_APP_v1.4 to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent, or hostile, and administers the software in compliance with the applied enterprise security policy.

Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

3.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following document:
  - *Protection Profile for Application Software*, Version 1.4, 7 October 2021
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Wickr Enterprise Client 6.10 Security Target, Version 1.0, 07 March 2023. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The TOE must be installed, configured, and managed as described in the documentation referenced in Section 6 of this this report.

4 Architectural Information

4.1 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The Wickr Client TOE is a software application that runs on the following platforms:

- Windows
- macOS
- iOS
- Android.

The product architecture is depicted in the following figure. The Wickr Client application (the TOE) is indicated by the red box. The other items are implemented on the Wickr Servers and other systems that are part of the TOE's Operational Environment.

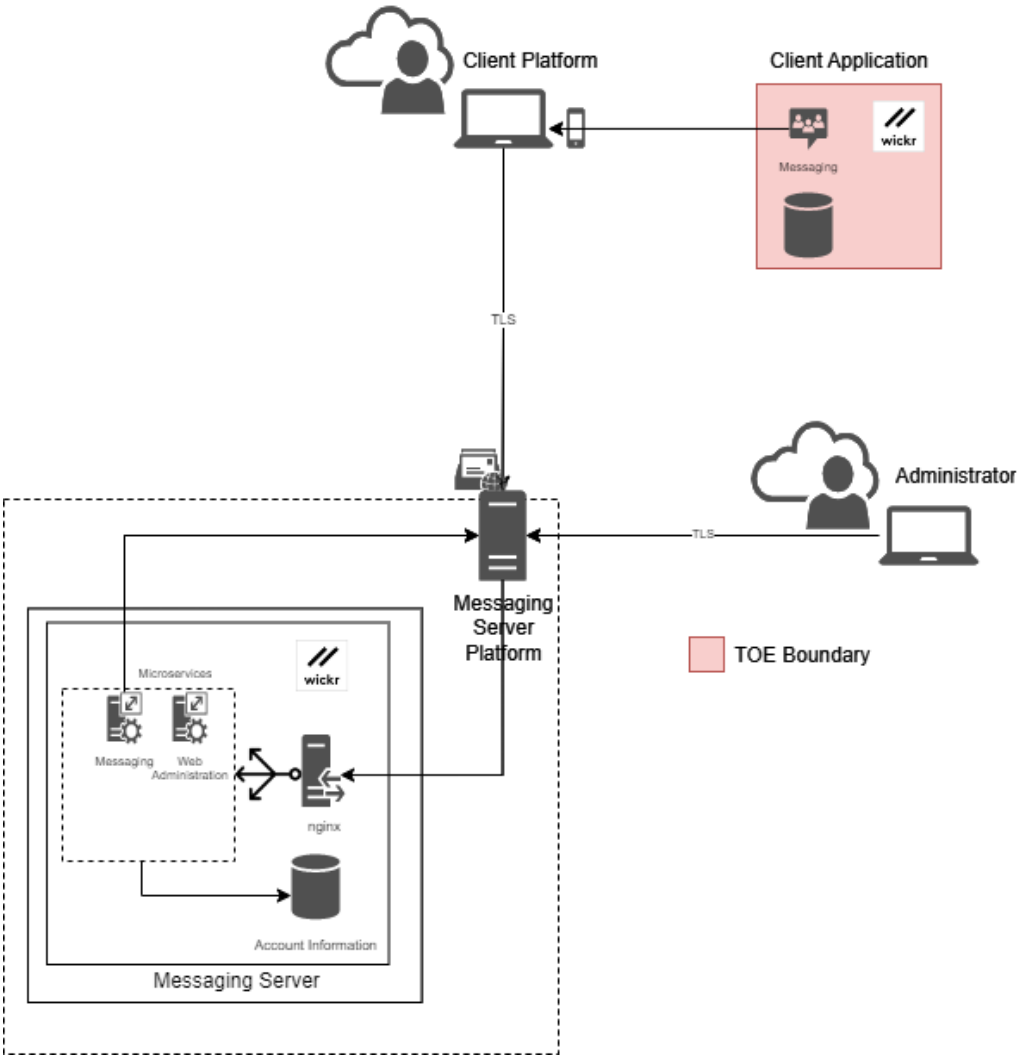


Figure 1: Wickr Architecture

The figure depicts initial communication setup for a call. The direction of the arrows indicates which system initiates communication. Communication is bi-directional once a connection is established. The Wickr Client relies on the cryptographic functions of its host platform for data in transit.

4.2 Physical Boundaries

The TOE consists of the Wickr Client application. For this evaluation, the TOE is evaluated on the following specific platforms:

- Windows:
  - Microsoft Surface Laptop 4
  - Intel i5-1145G7 (Tiger Lake) processor
  - Windows 10 64-bit OS
- macOS:
  - MacBook Pro
  - Intel i7-9750H (Coffee Lake) processor
  - macOS Monterey 12.4 OS
- iOS:
  - iPhone 12
  - Apple A14 Bionic (ARMv8) processor
  - iOS 15.5 OS
- Android:
  - Samsung Galaxy S20 FE
  - Qualcomm Snapdragon 865 (ARMv8) processor
  - Android 12 OS

In addition to the platforms identified above, the TOE's operational environment includes the following:

- A Wickr Server installed for messaging
- One or more remote Wickr Client instances to establish connections with
- A Workstation with a browser to access the Wickr Server's Admin Console (Wickr Clients receive configuration information from a Wickr Server)
- An Update server (public download site).

5 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

5.1 Cryptographic Support

The TOE uses NIST-validated cryptographic algorithms to secure messaging data in transit. The cryptographic functions for this are supplied by the host platform. All platform versions of the TOE also implement their own NIST-validated cryptographic algorithms through OpenSSL to support the protection of credential data at rest. The TOE relies on platform-provided entropy for random number generator seeding.

The TOE uses cryptographic functionality to protect stored credential data. This is done through a combination of TSF-provided cryptography and platform cryptography for all platform versions.

5.2 User Data Protection

The TOE provides cryptographic functionality and also leverages functionality provided by its underlying OS platforms to secure sensitive data at rest. The TOE uses network resources provided by the underlying platforms. All platform services are invoked at the direction of the user.

The TOE uses network connectivity to interact with a Wickr Server to establish connections with other Wickr Clients. The TOE or its platform, depending on platform version, check for updates from an update server.

5.3 Identification and Authentication

The TOE relies on platform-provided functionality to validate X.509 certificates used to authenticate TLS servers when establishing trusted communications except in the case where the desktop platform versions of the TOE (macOS, Windows) are responsible for validating the crlsign bit on any certificate used to sign a CRL. Certificate validation is performed in accordance with RFC 5280 and CRLs are used for revocation checking in all cases except for iOS, which uses OCSP.

5.4 Security Management

Wickr Client configuration data is stored locally using mechanisms that are recommended by the respective platform vendors. The TOE is not installed with default credentials. The Wickr Client applies configuration settings it obtains from the Wickr Server.

5.5 Privacy

The TOE does not process any personally identifiable information (PII). No transmission of PII occurs that is not in direct response to user activity.

5.6 Protection of the TSF

The TOE includes measures to integrate securely with its underlying OS platform. The TOE does not perform explicit memory mapping, nor does it allocate any memory region with both write and execute permissions. Similarly, the TOE does not write user-modifiable data to directories that contain executable files. The TOE is compatible with its supported host OS platform when configured in a secure manner. All platform versions of the TOE are compiled with stack overflow protection.

The TOE uses a well-defined set of platform APIs and third-party libraries.

The TOE provides the ability for a user to check its version. The TOE platform is used to apply updates. Updates are delivered in a format that is appropriate for the TOE's platform. Updates to the TOE are digitally signed, and the signature is validated prior to installation. The TOE does not modify its own code. Removal of the application removes all executable code associated with the TOE.

5.7 Trusted Path/Channels

The TOE uses trusted channels to secure data in transit between itself and external entities. The TOE communicates with the Wickr Server for messaging services and authentication using platform provided TLS.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Wickr Enterprise Client Common Criteria Evaluated Configuration Guide (CCECG)*, Version 1.0, 06 March 2023
- *Wickr Enterprise NIAP Version Installation and Maintenance*, Version 1.30.0
- *Wickr Enterprise Administrator Guide*, Version 426151b
- *Wickr Enterprise Desktop User Guide*, Version 6.10

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Wickr Enterprise Client Version 6.10 Common Criteria Test Report and Procedures, Version 1.1, 5 April 2023.*

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Wickr Enterprise Client 6.10*, Version 1.0, 5 April 2023

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specification:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

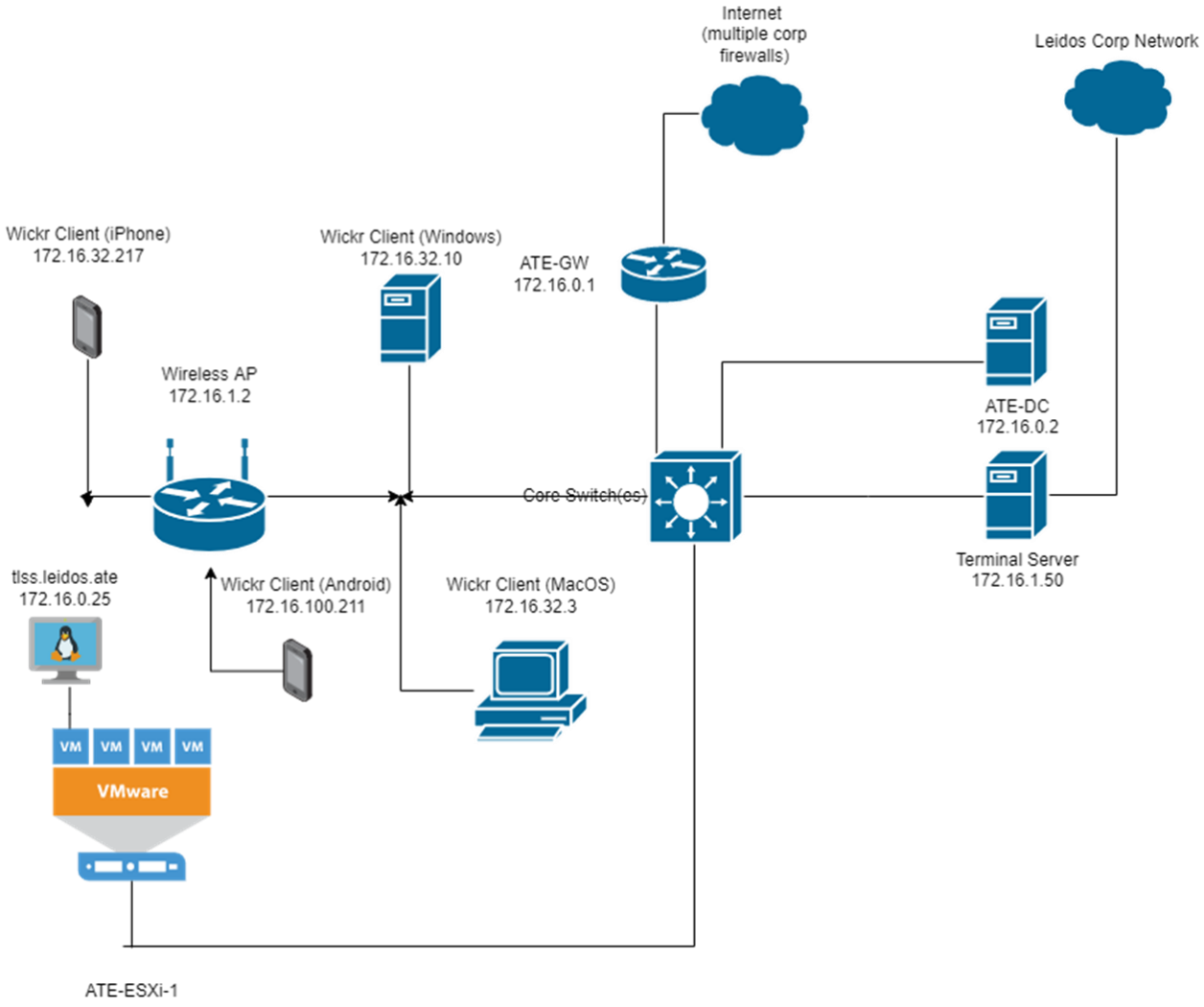
The evaluation team devised a test plan based on the test activities specified in the PP. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report listed above. Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from November 2022 to April 2023.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the team test plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Application Software* were fulfilled.

7.3 Test Configuration

This section identifies the devices used for testing the TOE and describes the test configuration. The test configuration is described below:



The following components were used to create the test configurations:

TOE Instances
- Wickr Windows Client 6.10.2
  - IP: 172.16.32.10
  - Microsoft Surface Laptop 4
  - Intel i5-1145G7 (Tiger Lake) processor
  - Windows 10 64-bit
- Wickr MacOS Client 6.10.2
  - IP: 172.16.32.3
  - MacBook Pro
  - Intel i7-9750H processor
  - macOS Monterey 12.4
- Wickr iOS Client 6.10.0
  - IP: 172.16.32.217
  - iPhone 12
  - Apple A14 Bionic (ArmV8) processor

- iOS 15
- Wickr Android Client 6.10.0
  - IP: 172.16.100.211
  - Samsung Galaxy S20 FE
  - Qualcomm Snapdragon 865 (ARMv8) processor
  - Android 12 OS

Additional Environment Devices

- ATE-GW (Physical)
  - Purpose: Main router/gateway
  - IP/MASK/MAC: 172.16.0.1 / 16 / ac:1f:6b:95:0c:1d
  - OS: PfSense 2.4.4-RELEASE-p2
- ATE-DC (Physical)
  - Purpose: Main Domain Controller (DC) for Test environment/DNS server
  - IP/MASK/MAC: 172.16.0.2 / 16 / 00:22:19:58:EB:8D
  - OS: Windows Server 2016 version 1607
  - Protocols used: RDP, NTP, LDAP, DNS
- ATE-ESXi-1 (Physical)
  - Purpose: Virtualization server
  - IP/MASK/MAC: 172.16.1.62 / 16 / 10:7b:44:92:77:bf
  - OS: VMware ESXi, 6.5.0, 5969303
- Terminal Server
  - Purpose: Provide tester access to the Test Environment from corporate network.
  - IP/MASK/MAC: 172.16.1.50 / 16 / D4:BE:D9:B4:FE:66
  - OS: Windows server 2016 version 1607
  - Protocols used: RDP, NTP, LDAP, DNS, SSH
- TLSS.leidos.ate (VM)
  - Purpose: Hosts TLS Test Tools
  - IP/MASK/MAC: 172.16.0.25 / 16 / 00:50:56:b1:66:0b
  - OS: Ubuntu 18.04.5
  - Protocols Used: SSH, TLS, NTP, DNS
  - Relevant Software:
    - Proprietary Python TLS test tools
    - OpenSSL 1.1.1
    - Wireshark 2.6.10
- Wireless Access Point
  - Purpose: Provides wifi access to test network for mobile devices
  - IP: 172.16.1.2
- Wickr Messenger Server (VM)
  - Purpose: Endpoint for Wickr connections
  - IP: 172.16.32.3
  - Running Wickr Enterprise 1.29.0

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is the Wickr Enterprise Client 6.10. The platform-specific versions of the TOE include:

1. Wickr Enterprise Client for Windows 6.10.2

   Evaluated on Microsoft Windows 10.

2. Wickr Enterprise Client for macOS 6.10.2

   Evaluated on macOS 12.4 Monterey.

3. Wickr Enterprise Client for iOS 6.10.0

   Evaluated on iOS 15.5.

4. Wickr Enterprise Client for Android 6.10.0

   Evaluated on Android 12.

The TOE is a third-party application that is installed onto a general-purpose operating system or mobile device. Wickr Enterprise Client is an on-premise application providing communication with remote peers.

Wickr Enterprise Client is part of a client-server distribution. The TOE is the client portion of this distribution. It interacts with the Wickr Enterprise Server application in its operational environment. Collectively, they make up the Wickr Enterprise solution. Wickr Enterprise is an end-to-end encrypted service that provides communication services for client devices in a closed-loop, zero-trust environment. The Wickr Client uses the Wickr Server to broker communications with other Wickr Clients for messaging rooms. The Wickr Client uses platform-provided TLS for security of data in transit.

8.2 Excluded Functionality

Excluded Functionality	Description
Voice and Video Services (Conferencing Server)	The TOE includes the base text messaging services only.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Wickr Enterprise Client 6.10 The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 and CEM version 3.1, revision 5, and the specific evaluation activities specified in:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 .

The evaluation determined the TOE satisfies the conformance claims made in the Wickr Enterprise Client 6.10 Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the PP listed above.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA evaluation activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the National Vulnerability Database (https://nvd.nist.gov/).

Searches were performed on 4/5/2023, using the following search terms:

- Wickr
- Encrypted Service
- zero trust
- OpenSSL 1.0.2zg
- OpenSSL 2.0.16
- symcrypt
- Apple coreCrypto Module
- BoringSSL
- Third Party Libraries identified in Section A.2 of the Security Target

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Wickr Enterprise Client Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, 06 March 2023. No versions of the TOE and software, either earlier or later were evaluated.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness. The Voice and Video Services (Conferencing Server) functionality is excluded from the evaluation. The TOE includes the base text messaging services only. This is specified in Section 8.2.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is *Wickr Enterprise Client 6.10 Security Target*, Version 1.0, 07 March 2023.

13 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

14 Bibliography

The validation team used the following documents to produce this VR:

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

[2] Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] Protection Profile for Application Software, Version 1.4, 07 October 2021.

[6] Wickr Enterprise Client 6.10 Security Target, Version 1.0, 07 March 2023.

[7] Wickr Enterprise Client Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, 06 March 2023.

[8] Wickr Enterprise NIAP Version Installation and Maintenance, Version 1.30.0

[9] Wickr Enterprise Administrator Guide, Version 426151b

[10] Wickr Enterprise Desktop User Guide, Version 6.10

[11] Evaluation Technical Report for Wickr Enterprise Client 6.10, Version 1.1, 5 April 2023.

[12] Assurance Activities Report for Wickr Enterprise Client 6.10, Version 1.0, 5 April 2023.

[13] Wickr Enterprise Client Version 6.10 Common Criteria Test Report and Procedures, Version 1.1, 5 April 2023.