Certification Report

EAL 4+ (ALC_FLR.3) Evaluation of

ORDULU TEKNOLOJİ A.Ş

ULAK.IM Secure Instant Messenger v.2.0

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-90

TABLE OF CONTENTS

Document Information

Date of Issue	**27.12.2023**
Approval Date	**28.12.2023**
Certification Report Number	**21.0.03/23-007**
Sponsor and Developer	**Ordulu Teknoloji A.Ş**
Evaluation Facility	**STM ITSEF**
TOE Name	**ULAK.IM Secure Instant Messenger v.2.0**
Pages	**18**

Prepared by *(Common Criteria Expert)*	**Mehmet Kürşad ÜNAL**
Prepared by (Common Criteria Candidate Expert)	**Almıla Beyza KARAKAPICI** a.ikizoglu
Reviewed by *(Reviewer)*	**Göktuğ İLISU**

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	**27.12.2023**	**All**	**First Release**

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 5, using Common Methodology for IT Products Evaluation, version 3.1, revision 5. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCTL is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCTL has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by STM ITSEF, which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for ULAK.IM Secure Instant Messenger v.2.0 whose evaluation was completed on 26.12.2023 and whose evaluation technical report was drawn up by STM ITSEF (as CCTL), and with the Security Target document with version no 1.9 of the relevant product.

The certification report, certificate of product evaluation and security target lite document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL2. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: ULAK.IM Secure Instant Messenger v.2.0

IT Product version: 2.0

Developer's Name: Ordulu Teknoloji A.Ş

Name of CCTL: STM ITSEF

Assurance Package: EAL 4+ (ALC_FLR.3)

Completion date of evaluation: 26.12.2023

1.1 Brief Description

The Target of Evaluation (TOE) is a secure module which belongs a communication service that consists of two main components, namely the ULAK.IM Server and the ULAK.IM Client App. While ULAK.IM Server is an integration management server designed to manage both desktop and mobile communication process, ULAK.IM Client App is an application that provide secure messaging platform. The TOE can be categorized as "Network and Network-Related Devices and Systems" in accordance with the categories identified on the Common Criteria Portal that lists all certified products.

1.2 Major Security Features

The TOE provides the following security services;

- **Security audit:** The TOE generates audit records with a reliable time stamp for security events like logins and user management activity. The administrators have the ability to view the audit trail.
- **Identification and authentication:** All users are required to identify or authenticate with the TOE prior to any user action or information flow being permitted. In order to login to Admin Panel, administrators authenticate themselves by username and password. When using the mobile application, the user performs initial authentication via passcode.
- **Secure communications:** Users communicate over the encryption key. (AES-256-bit encryption is created for each mutual message exchange of users, using asymmetric cryptography with the key referred to as the encryption key). Users who create public keys using Diffie-Hellman transfer data in an encrypted manner. Communication with the server uses TLS 1.3 protocol. The server certificate is signed using the SHA2

hash algorithm and uses the RSA 2048-bit asymmetric key. Key exchange X25519 and asymmetric keys formed from double elliptic curve are used in end-to-end encryption. Messages are encrypted using AES-256 with 256-bit keys. Each user has temporary and permanent asymmetric keys. When two users start talking for the first time, a common symmetric encryption key is created using key exchange permanent and temporary keys. This common encryption key changes in mutual messages as long as the two users continue to talk to each other.

- **User data protection:** TOE users in user role can send/receive messages. They can reply, forward, revoke, download and delete messages. TOE users in administrator role can configure system settings for the secure messaging service, search and remove users, and perform other management operations from Admin Panel. The administrator in the organization sets a permission level which determines the message operations users are allowed to perform. However, they cannot perform operations on individual messages as users. TOE has also a functionality called disappearing message. Once enabled, new messages sent in the individual or group chat will disappear after a period of time.
- **Security management:** The administrators of the TOE platform have access to the TOE configuration files. The administrators can manage the configuration files locally or remotely. The followings are the actions that administrators can consider;
    - Configuration of system settings
    - Configuration of trusted Identity Providers (IDPs)
    - User and account management (add/remove/update)
    - Bot management
    - Application update

1.3 Threats

The threats are;

- **T.EAVESDROP:** An attacker tries to eavesdrop on messages or management data when they are transmitted between the TOE and user's web browser.
- **T.MODIFY:** An attacker tries to modify with messages or management data (i.e. replacing or modifying the content) when they are transmitted between the TOE and user's browser, without being detected.
- **T.UNAUTHORISED_ACCESS:** A user may gain unauthorized access to the TOE and residing data by sending impermissible information through the TOE resulting the exploitation of protected resources such as IDP.
- **T.MASQUERADE:** An attacker pretends to be an authorized user or a non-administrative user pretends to be another user at login time. An attacker or a non-administrative user may also pretend to be an

administrator. This includes the case where the user/attacker tries to fake or modify the user identity provided by an IDP

aikiz

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-90
TOE Name and Version	ULAK.IM Secure Instant Messenger v.2.0
Security Target Document Title, Version and Date	ULAK.IM Secure Instant Messenger v2.0 Security Target, 1.9, 21.12.2023
Security Target Lite Title, Version and Date	Security Target Lite ULAK.IM Secure Instant Messenger v2.0, 1.9, 27.12.2023
Assurance Level	EAL 4 + (ALC_FLR.3)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	None
Sponsor and Developer	Ordulu Teknoloji A.Ş
Evaluation Facility	STM ITSEF
Certification Scheme	TSE CCCS

2.2 Security Policy

The organizational security policies are;

- **P.NETWORK:** There should be an appropriate network layer protection, that there is a firewall in place that only permits access through required ports for users to access the web-server.
- **P.MANAGEMENT:** The TOE and the operational environment shall provide administrators with secure means to manage the TSFs.
- **P.TRUSTED_IDP:** The TOE shall ensure that only trusted IDPs are used for user identification and authentication.
- **P.LOGGING:** Message operations performed by users and management operations performed by administrators shall be logged. Message subjects and contents shall not be logged.
- **P.ERASURE:** Messages in an account shall be permanently deleted upon request from an authorized user and when the account is removed. Additionally, The TOE shall permanently delete messages after a time period, if configured.

2.3 Assumptions and Clarification of Scope

Assumptions for the operational environment of the TOE are;

- **A.ADMIN:** The Administrator is not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by administrator documentation.
- **A.PLATFORM:** It is assumed that the underlying operating system and the hardware platform on which the TOE is installed work correctly and have no undocumented security critical side effects on the security functions of the TOE.
- **A.TIMESTAMP:** The underlying operating system will have a reliable time source that the TOE can utilize for generating audit log timestamps.
- **A.IDP:** It is assumed that one or more trusted IDPs are available and they meet the necessary authentication requirements.
- **A.UPDATE:** The underlying platform on which the TOE operates will be regularly updated with the latest security patches and fixes to ensure data stored on the platform remains protected and secure.
- **A.PHYSICAL:** It is assumed that the TOE (server) is located in a physically secure environment, no unauthorized persons have physical access to the TOE and its underlying system.

aikiz

2.4 Architectural Information

TOE includes both client and server's components. The Client component is referred to here for both mobile and desktop client application. The TOE components can be seen in Figure 1 and were inserted into red dotted boxes.

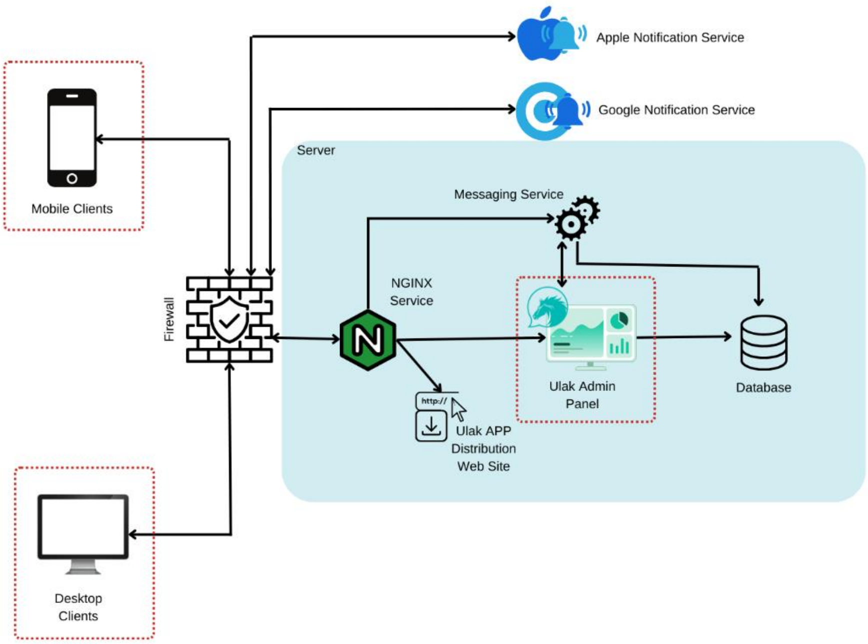

Figure 1. Physical Boundaries of TOE

- **ULAK.IM Client:** ULAK.IM client is on mobile (Android, iOS) and desktop platform. The client is able to establish encrypted calls and live chats with clients on other devices using message server. Any mobile device is initialized with phone number and signature via Admin Panel or mobile phone. ULAK.IM Client Application is the TOE.
- **ULAK.IM Server-Admin Panel:** The management functionalities are performed using the Admin Panel. The functionalities mean verifying users, configuring settings as well as account management. The admin panel offers a web interface that is accessible using a web browser from the administrator's local machine.

The operational environment of the TOE must ensure:

- the proper functioning of the underlying operating system and hardware platform on which the product is installed, and it should ensure there are no critical undocumented security implications on the security functions of the product

aikiz

- the availability of one or more trusted IDPs and meet authentication requirements
- the product is physically located in a secure environment under the organization's control
- a firewall that allows access to the web server from external users only through necessary ports

The necessary configurations to operate the product safely within the scope of certification are as follows:

- ULAK.IM Server
  - 8 core CPU, 8 GB RAM, 500 MB HDD,
  - Nginx 1.16.1
  - PostgreSQL 9.5-9.6
  - Redis 3.2.12
  - Docker 19.03.4
  - Node 12.13.0
- ULAK.IM Client Application
  - iOS 13, Android 7.0 and newer versions (for mobile app)
  - Windows 10+, Mac 10+, Ubuntu 18 and newer versions (for desktop app)

2.5 Documentation

Documents below are provided to the customer by the developer alongside the TOE;

Name of Document	Version Number	Date
Security Target Lite ULAK.IM Secure Instant Messenger v2.0	V.1.4	27.12.2023
ULAK.IM Secure Instant Messenger v2.0 Kurulum Kılavuzu	v.1.0	06.12.2023
ULAK.IM Secure Instant Messenger v2.0 Kullanım Kılavuzu	v.1.2	06.12.2023

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report (ETR) of ULAK.IM Secure Instant Messenger v.2.0.

It is concluded that the TOE supports EAL 4+ (ALC_FLR.3). There are 25 assurance families which are all evaluated with the methods detailed in the ETR.

2.6.1 Developer Testing

Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE Design documentation which includes TSF subsystems and its interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 13 functional tests in total.

2.6.2 Evaluator Testing

- **Functional and Independent Testing:** Evaluator re-executed all developer tests. Additionally, evaluator prepared 5 independent tests. TOE has passed all 18 functional tests to demonstrate that its security functions work as it is defined in the ST.
- **Penetration Testing:** TOE was tested against common threats and other threats surfaced by vulnerability analysis. 15 penetration tests were conducted. In a result of penetration testing, the TOE is resistant to attackers who have Enhanced-Basic potential.

2.7 Evaluated Configuration

The necessary configurations to operate the product safely within the scope of certification are as follows:

- ULAK.IM Server
  - 8 core CPU, 8 GB RAM, 500 MB HDD,
  - Nginx 1.16.1
  - PostgreSQL 9.5-9.6
  - Redis 3.2.12
  - Docker 19.03.4
  - Node 12.13.0
- ULAK.IM Client Application
  - iOS 13, Android 7.0 and newer versions (for mobile app)
  - Windows 10+, Mac 10+, Ubuntu 18 and newer versions (for desktop app)
- Guidance documents

2.8 Results of the Evaluation

The table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.3

Assurance Class	**Component**	**Component Title**
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-Defined Development Tools
	ALC_FLR.3	Systematic Flaw Remediation

Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent testing - sample
Vulnerability Analysis	AVA_VAN.3	Focused Vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (ALC_FLR.3) assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE “ULAK.IM Secure Instant Messenger v.2.0”, the results of the assessment of all evaluation tasks are “Pass”.

2.9 Evaluator Comments / Recommendations

It is recommended that all guidance outlined in the Guidance Documents be followed and all assumptions are fulfilled in order to the secure usage of the TOE.

3 SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:

Title: ULAK.IM Secure Instant Messenger v2.0 Security Target
Version: v1.9
Date of Document: 21.12.2023

The vendor preferred to publish Security Target Lite document rather than this ST document. The ST Lite document is identified by the following terminology:

Title: Security Target Lite ULAK.IM Secure Instant Messenger v2.0
Version: v1.4
Date of Document: 27.12.2023

aikiz

4 GLOSSARY

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

IDP: Identity Provider

ITCD: Information Technologies Test and Certification Department

EAL : Evaluation Assurance Level

OSP : Organisational Security Policy

PP : Protection Profile

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017,

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017,

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017,

[4] Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017,

[5] STM-03-ETR-v1.0 ULAK.IM Evaluation Technical Report, 26 December 2023,

[6] Secure Messages Protection Profile v.1.1, 26 November 2018

6 ANNEXES

6.1 TOE SPECIFICATIONS

TOE: ULAK.IM Secure Instant Messenger v.2.0

TOE Hash (MD5): e3106688e0b822ce90d1e24b50c90514