bugshell

Letter of Attestation

Confirmation of a performed penetration test for

SCS - Secure Communication Services Limited
Dubai (UAE)
Baywater Bay by Omniyat

Executive Summary

Scope

A gray box penetration test for SCS was conducted in order to assess its risk posture and identify security issues that could affect data, systems or reputation of SCS. The assessment of the CRYPE application was conducted by one pentester between 27. Oct. 2025 and 31. Oct. 2025.

The auditor was not provided with any detailed information about the application in scope. No user accounts and no information about the underlying architecture were given to the auditors beforehand. The auditors used the self-registration on the staging environment to register users for testing purposes.

Audit Goal

It was the goal of the audit to find any kinds of vulnerabilities and reveal common configuration issues in the CRYPE application. This penetration test was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities such as those catalogued in the OWASP Top 10. The assessment also included a spot check review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters leveraged tools to facilitate their work; however, the majority of the assessment involves manual analysis.

Detailed attention was paid to the following questions:

- Is an attacker able to access data of other customers (horizontal privilege escalation)?
- Is an attacker able to obtain administrative access to services (vertical privilege escalation)?
- Can an attacker inject malicious code?
- Are the services configured according to the minimal principle?
- Can the authentication be bypassed?
- Does the application store message content, calls metadata or media on any server beyond sender and receiver?

Results

The pentester identified altogether 5 findings: 0 Critical, 0 High, 1 Medium, and 4 Low risk vulnerabilities. The root of these vulnerabilities is based on the following problems:

- Insecure configuration of services
- Missing anti automation
- Weak password checks

The application uses WebRTC for real-time communication, establishing peer-to-peer (P2P) connections directly between clients or, when necessary, routing traffic through a TURN server. When using a TURN Server, only metadata is transferred to central servers that are necessary for maintaining the service.

A review of the WebRTC implementation and configuration found no security vulnerabilities or misconfigurations. Encryption, connection setup, and signaling were handled securely.

Key Findings

Based on the observations made during the gray-box penetration test and the identified and retested issues, BugShell GmbH can state the following:

- End-to-End Data Confidentiality: User communications, including text messages, voice, and video, were exchanged exclusively between the communication partners. All traffic captured during the assessment was exchanged solely between the communication endpoints, and no evidence was found of content exposure to third-party servers, intermediaries, or the service provider itself.

- State-of-the-Art Encryption: Communication data in transit were protected using modern encryption protocols (including but not limited to AES-256 and ECDH key exchange). Encryption keys were generated and managed on-device, ensuring that only the sender and receiver could decrypt messages.
- No Significant Vulnerabilities: At the time of testing and following retests, no critical or high-severity security vulnerabilities were identified. The application successfully resisted the attack vectors attempted during the assessment, including eavesdropping, man-in-the-middle (MitM), injection, and privilege-escalation attempts.
- Privacy by Design: The CRYPE application did not send message content, call metadata, or media to any server beyond what is strictly necessary for delivery. Once delivered, all communication content remained solely on the devices of the participants.
- Alignment with Security Best Practices: The implementation adheres to current security best practices and relevant data protection principles, including those outlined in OWASP Top 10 and the ASVS (Application Security Verification Standard).

BugShell GmbH concludes that, based on the scope and methods of the gray-box penetration test performed, the application demonstrates strong security characteristics and behaves in accordance with its stated privacy and confidentiality objectives. The above conclusions are derived from observable system behavior during testing and do not constitute verification of internal implementation details. A penetration test generally reveals the presence of vulnerabilities but does not provide proof of their absence.

Berlin, November 28, 2025

Volker Haupt

Managing director