EPI-USE LABS
value through innovation

J&S Soft

enmeshed penetration test report executive summary

Version: 1.1

Date: 23 June 2023

Executive summary

The enmeshed ecosystem was developed to facilitate complex end-to-end encrypted communication workflows. Critical enmeshed components were open-sourced by j&s-soft to promote transparency. An assessment of the enmeshed ecosystem was conducted by EPI-USE from October 2022 to April 2023 to assess the security and privacy of the solution, identify architectural problems, identify software-development-related problems, and identify security problems.

The scope of the assessment included:

- The open-source enmeshed libraries and j&s-soft libraries used by the enmeshed ecosystem;
- The mobile application;
- The enmeshed Connector;
- The enmeshed Backbone.

The enmeshed testing project consisted of four predefined phases, namely:

- Technology review;
- Source code review;
- Container vulnerability review;
- Penetration tests.

A centralised architecture is implemented within the enmeshed ecosystem (as opposed to a decentralised architecture). Within the domain in which enmeshed operates, a centralised architecture may provide various benefits, such as simplicity, accountability and efficiency.

The enmeshed ecosystem is well-designed, and it is evident that a lot of thought went into design decisions made. In addition, the enmeshed source code is clean and of good quality. During the assessment, no critical or high-risk vulnerabilities were identified. A few lower-risk vulnerabilities were identified and documented in a risk register for tracking purposes. The team has demonstrated their commitment to security by evaluating and responding to all pentest findings, and the majority of findings have already been addressed.

It was also confirmed that the end-to-end encryption mechanisms are working as expected and it was verified that the enmeshed Backbone does not have the ability to intercept, read or modify end-to-end encrypted messages. It was also verified that cryptographic techniques were applied appropriately to ensure that the origin of specific messages can be traced back cryptographically to a specific identity (thereby exhibiting non-repudiation properties).

As a result of testing performed, we believe the enmeshed ecosystem does not contain any critical security issues. We also believe that enmeshed will be able to provide services to businesses systems and consumers securely, provided that enmeshed components deployed by clients (such as the Connector, application) are kept up to date, dependencies are properly configured and patched, and that the operational environment is hardened according to enmeshed recommendations.