DEKRA Testing and Certification, S.A.U.
Parque Tecnológico de Andalucía
c/ Severo Ochoa nº 2 - 29590 Campanillas - Málaga - España
C.I.F. A29 507 456

Test report No:
NIE: 73217RCS.001

Security Evaluation Report
DEKRA Evaluation framework

Target of Evaluation (ToE) Identification of item tested	App Version: 4.0.3
Model and /or type reference	xPal
Other identification of the product	com.mess.engerx
Features	Secure Messenger
Manufacturer	XPAL.com Corporation
Test method requested	Security Evaluation based on limited set of evaluation procedures from OWASP Mobile Application Security Verification Standard established by Google.
Approved by (name / position & signature)	Juan Manuel Martinez Cybersecurity Engineer
Date of issue	2023/04/03
Report template No	FDT08_EN

Table of Contents

Competences and guarantees

DEKRA Testing and Certification guarantees the reliability of the data presented in this report, which is the result of the measurements and the tests performed to the item under test on the date and under the conditions stated on the report and, it is based on the knowledge and technical facilities available at DEKRA Testing and Certification at the time of performance of the test.

DEKRA Testing and Certification is liable to the client for the maintenance of the confidentiality of all information related to the item under test and the results of the test.

The results presented in this Test Report apply only to the particular item under test established in this document.

IMPORTANT: No parts of this report may be reproduced or quoted out of context, in any form or by any means, except in full, without the previous written permission of DEKRA Testing and Certification.

General conditions

1. This report is only referred to the item that has undergone the test.
2. This report does not constitute or imply on its own an approval of the product by the Certification Bodies or competent Authorities.
3. This document is only valid if complete; no partial reproduction can be made without previous written permission of DEKRA Testing and Certification.
4. This test report cannot be used partially or in full for publicity and/or promotional purposes without previous written permission of DEKRA Testing and Certification and the Accreditation Bodies.

Document history

Report Number	Date	Description
73217RCS.001	2023/04/03	Emitted Evaluation Report 001

Remarks and Comments

Limited set of testing procedures from OWASP MASVS selected by Google

Authorizations

NDA signed with Google

Testing verdicts

PASS	P
FAIL	F
NA	NA
INCONCLUSIVE	INC

Mobile Security Testing Guide

Data Storage and Privacy Requirements	VERDICT			
	P	F	NA	INC
1 System credential storage facilities used to store sensitive data.	X			
2 No sensitive data should be stored outside of the app container.	X			
3 No sensitive data is written to application logs.	X			
5 The keyboard cache is disabled on sensitive data inputs.	X			
7 No sensitive data is exposed through the user interface.	X			
12 Educate the user about the types of personally identifiable information processed.	X			

Cryptography Requirements	VERDICT			
	P	F	NA	INC
1 App does not rely on symmetric cryptography with hardcoded keys.	X			
2 Proven implementations of cryptographic primitives.	X			

3 App uses cryptographic primitives that are appropriate for the particular use-case.	X			
4 No deprecated cryptographic protocols or algorithms.	X			
5 No re-use the same cryptographic key for multiple purposes.	X			
6 Random values are generated using a sufficientrly secure random number generator.	X			

Authentication and Session Management Requirements	VERDICT			
	P	F	NA	INC
1 Authentication for remote services.	X			
2 Randomly generated session identifiers.	X			
3 Stateless token-based authentication are signed.	X			
4 Remote endpoint terminates the existing session when the user logs out.	X			
5 Password policy exists and is enforced at the remote endpoint.	X			
6 Brute force mitigations.	X			
7 Sessions are invalidated at the remote endpoint after a predefined period of inactivity.	X			

Network Communication Requirements	VERDICT			
	P	F	NA	INC
1 Data is encrypted on the network using TLS.	X			
2 The TLS settings are in line with current best practices.	X			
3 The app verifies the X.509 certificate of the remote endpoint.	X			

Platform Interaction Requirements	VERDICT			
	P	F	NA	INC
1 Requests the minimum set of permissions.	X			
2 Inputs from external sources and the user are validated.	X			
3 App does not export sensitive functionality via custom URL schemes.	X			
4 App does not export sensitive functionality through IPC facilities.	X			

Code Quality and Build Setting Requirements	VERDICT			
	P	F	NA	INC
1 App is signed and provisioned with a valid certificate.	X			
2 App has been built in release mode.	X			
3 Debugging symbols have been removed from native binaries.	X			
4 Debugging code and developer assistance code have been removed.	X			
5 Third party components are checked for known vulnerabilities.	X			
9 Security features offered by the toolchain are activated.	X			

Appendix A: Evaluation Results

1. Categories, Security Features and Categories Summary

Security Evaluation of the ToE has been divided into different categories,

Security Analysis of each category is structured in different security features. In the same way, each security feature can be composed of several tests.

The following table shows the security features defined per each category and the number of tests of each security feature.

Category	Security Features	Nº TESTS
1. Mobile Security Testing Guide	1.1 Data Storage and Privacy Requirements	6
	1.2 Cryptography Requirements	6
	1.3 Authentication and Session Management Requirements	7
	1.4 Network Communication Requirements	3
	1.5 Platform Interaction Requirements	4
	1.6 Code Quality and Build Setting Requirements	6

2. Detailed Results

Complete results of the evaluation procedures carried on each category can be seen in the following attached documents:

Number	Appendix	Document Name
1	A.1	Mobile Security Testing Guide Evaluation Report