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: 83620RCS.001

Security Evaluation Report
DEKRA Evaluation framework

(*) Identification of item tested	App version: 5.3.0
(*) Trademark	xPal
(*) Model and /or type reference tested	xPal
Other identification of the product	com.mess.engerx (*) SHA256 Hash: ae8c942770bdd406b3c06018d8772bcf64f950f9ec459a0c55f2540b63d82ff3
(*) Features	Secure Messenger
Manufacturer	XPAL.com Corporation
Test method requested, standard	Security Evaluation based on limited set of evaluation procedures from OWASP Mobile Application Security Verification Standard established by ADA, following PECS020_02 Google MASA Cybersecurity Testing Procedure.
Summary	IN COMPLIANCE
Approved by (name / position & signature)	Alvaro Ortega Chamorro, Laboratory Manager  27/06/2025
Date of issue	27/06/2025
Report template No	FCS316_00 (*) "Data provided by the client"

Index

Competences and guarantees

DEKRA Testing and Certification S.A.U. is a testing laboratory accredited by A2LA (The American Association for Laboratory Accreditation) to perform the test indicated in the Certificate 7071.01.

In order to assure the traceability to other national and international laboratories, DEKRA Testing and Certification S.A.U. has a calibration and maintenance program for its measurement equipment.

DEKRA Testing and Certification S.A.U. 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 S.A.U. 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.

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 S.A.U.
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 S.A.U. and the Accreditation Bodies.

Data provided by the client

The following data has been provided by the client:

1. Information relating to the description of the sample ("Identification of the item tested", "Trademark", "Model and/or type reference tested".

2. Information relating to the development version of the sample ("HW version", "FW version").

DEKRA Testing and Certification S.A.U. declines any responsibility with respect to the information provided by the client and that may affect the validity of results.

Usage of samples

Samples undergoing test have been selected by: Google LLC

Sample M/01 is composed of the following elements:

Control Nº	Description	Model	Serial Nº	Date of reception
83620	xPal	xPal	N/A	2025-06-11

Test sample description

Sample Components ..... :	**Software**
	xPal. Version: 5.3.0

Identification of the client

Company	XPAL.com Inc.
Address	1030 E. El Camino Real Suite 210 Sunnyvale, CA 94087

Testing period and place

Name	DEKRA Testing and Certification, S.A.U.
Test Location	Parque Tecnológico de Andalucía - c/ Severo Ochoa nº 2 - 29590 Campanillas - Málaga - España
Date (start)	2025/06/23
Date (finish)	2025/06/26

Document history

Report number	Date	Description
83620RCS.001	**2025/06/27**	**Emitted Evaluation Report 001**

Remarks and Comments

- Limited set of testing procedures from OWASP MASVS selected by ADA.
- The following table includes the name, position and signature of the person/s that participate in the evaluation:

Name	Position	Signature
Juan Manuel Martínez Hernández	Project Manager	
José María Santos López	Evaluator	

Testing verdicts

PASS	P
FAIL	F
NA	NA
INCONCLUSIVE	INC

Summary: Mobile Profile Evaluation

Storage-1: The app securely stores sensitive data in external storage	P	F	NA	INC
1 The app shall securely store sensitive data in external storage	X			

Storage-2: The app prevents leakage of sensitive data	P	F	NA	INC
1 The Keyboard Cache Is Disabled for sensitive data inputs	X			
2 No sensitive data is stored in system logs	X			

Crypto-1: The app employs current strong cryptography and uses it according to industry best practices	P	F	NA	INC
1 No insecure random number generators shall be utilized for any security sensitive context	X			
2 No insecure operations shall be used for symmetric cryptography	X			
3 Strong cryptography shall be implemented according to industry best practices	X			

Crypto-2: The app performs key management according to industry best practices	P	F	NA	INC
1 Cryptographic keys shall only be used for their defined purpose	X			
2 Cryptographic key management shall be implemented properly	X			

Auth-1: The app uses secure authentication and authorization protocols and follows the relevant best practices	P	F	NA	INC
1 If using OAuth 2.0 for authorization, or if using OpenID Connect for authentication, Proof Key for Code Exchange (PKCE) shall be implemented to protect the code grant			X	

Network-1: The app secures all network traffic according to the current best practices	P	F	NA	INC
1 Network connections shall be encrypted	X			
2 TLS configuration of network connections shall adhere to industry best practices	X			
3 Endpoint identity shall be verified on network connections	X			

Platform-1: The app uses IPC mechanisms securely	P	F	NA	INC

1 The app shall limit content provider exposure and harden queries against injection attacks	X			
2 The app shall use verified links and sanitize all link input data	X			
3 Any sensitive functionality exposed via IPC shall be intentional and at the minimum required level	X			
4 All Pending Intents shall be immutable or otherwise justified for mutability	X			

Platform-2: The app uses WebViews securely	P	F	NA	INC
1 WebViews shall securely execute JavaScript	X			
2 WebView shall be configured to allow the minimum set of protocol handlers required while disabling potentially dangerous handlers	X			

Platform-3: The app uses the user interface securely	P	F	NA	INC
1 The app shall by default mask data in the User Interface when it is known to be sensitive	X			

Code-1: The app requires an up-to-date platform version	P	F	NA	INC
1 The app shall set the targetSdkVersion to an up-to-date platform version	X			

Code-2: The app only uses software components without known vulnerabilities	P	F	NA	INC
1 The app only uses software components without known vulnerabilities	X			

Code-3: The app validates and sanitizes all untrusted inputs	P	F	NA	INC
1 Compiler security features shall be enabled	X			
2 The App shall Mitigate Against Injection Flaws in Content Providers	X			
3 Arbitrary URL redirects shall not be included in the app's webviews	X			
4 Any use of implicit intents shall be appropriate for the app's functionality and any return data shall be handled securely	X			

Resilience-1: The app implements anti-tampering mechanisms	P	F	NA	INC
1 The app shall be properly signed	X			

Resilience-2: The app implements anti-static analysis mechanisms	P	F	NA	INC
1 The app shall disable all debugging symbols in the production version	X			

Resilience-3: The app implements anti-dynamic analysis mechanisms	P	F	NA	INC
1 The app shall not be debuggable if installed from outside of commercial app stores	X			

Privacy-1: The app minimizes access to sensitive data and resources	P	F	NA	INC

1 The app shall minimize access to sensitive data and resources provided by the platform	X			

Privacy-2: The app is transparent about data collection and usage	P	F	NA	INC
1 The app shall be transparent about data collection and usage	X			

Privacy-3: The app offers user control over their data	P	F	NA	INC
1 Users shall have the ability to request their data to be deleted via an in-app mechanism	X			

Appendix A: Test 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 Profile Evaluation	1.1 Storage-1: The app securely stores sensitive data in external storage	1
	1.2 Storage-2: The app prevents leakage of sensitive data	2
	1.3 Crypto-1: The app employs current strong cryptography and uses it according to industry best practices	3
	1.4 Crypto-2: The app performs key management according to industry best practices	2
	1.5 Auth-1: The app uses secure authentication and authorization protocols and follows the relevant best practices	1
	1.6 Network-1: The app secures all network traffic according to the current best practices	3
	1.7 Platform-1: The app uses IPC mechanisms securely	4
	1.8 Platform-2: The app uses WebViews securely	2
	1.9 Platform-3: The app uses the user interface securely	1
	1.10 Code-1: The app requires an up-to-date platform version	1
	1.11 Code-2: The app only uses software components without known vulnerabilities	1
	1.12 Code-3: The app validates and sanitizes all untrusted inputs	4
	1.13 Resilience-1: The app implements anti-tampering mechanisms	1
	1.14 Resilience-2: The app implements anti-static analysis mechanisms	1
	1.15 Resilience-3: The app implements anti-dynamic analysis mechanisms	1
	1.16 Privacy-1: The app minimizes access to sensitive data and resources	1
	1.17 Privacy-2: The app is transparent about data collection and usage	1
	1.18 Privacy-3: The app offers user control over their data	1

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 Profile Evaluation Report