Reference: 2025-3-INF-4661- v1
Target: Limitada al expediente
Date: 26.01.2026

Created by: CERT16
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2025-3**
TOE	**KATIM X3M on KATIM OS 13**
Applicant	**CN-2891037 - KATIM L.L.C.**

References

[EXT-9413] 2025-03 KATIM_X3M on KATIM OS 13

[EXT-9847] 2025-09-24_2025-03_ETR_v1

Certification report of the product KATIM X3M on KATIM OS 13, as requested in [EXT-9413] dated 09/01/2025, and evaluated by Layakk Seguridad Informatica S.L., as detailed in the Evaluation Technical Report [EXT-9847] received on 24/09/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product KATIM X3M on KATIM OS 13.

The Target of Evaluation (TOE) is KATIM X3M mobile device running KATIM OS 13.

Developer/manufacturer: KATIM L.L.C.

Sponsor: KATIM L.L.C..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Layakk Seguridad Informatica S.L.

Protection Profile:

The ST and the TOE claims exact conformance to PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients, Version 1.0, 11 October 2022 (CFG_MDF-BT-WLANC_V1.0).

The PP-Configuration includes the following components:

- Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.3, 12 September 2022 (PP_MDF_V3.3)
- PP-Module: PP-Module for Bluetooth, Version 1.0, 15 April 2021 (MOD_BT_V1.0)
- PP-Module: PP-Module for WLAN Clients, Version 1.0, 31 March 2022 (MOD_WLANC_V1.0)

Evaluation Level: Common Criteria CC:2022 R1

Evaluation end date: 15/09/2025

Expiration Date[1]: 22/11/2030

All the assurance components required by the evaluation level of [CFG_MDF-BT-WLANC_V1.0] have been assigned a "PASS" verdict. Consequently, the laboratory Layakk Seguridad Informatica S.L. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the [CFG_MDF-BT-WLANC_V1.0], as defined by the Common Criteria CC:2022 R1, CEM CC:2022 R1 and [CFG_MDF-BT-WLANC_V1.0].

Considering the obtained evidences during the instruction of the certification request of the product KATIM X3M on KATIM OS 13, a positive resolution is proposed.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

TOE SUMMARY

The Target of Evaluation (TOE) provides standard telecommunication functionalities, such as initiating and receiving voice calls, and sending and receiving SMS messages, in addition to comprehensive network connectivity capabilities, supporting both 802.11ax Wi-Fi and multi-generation cellular technologies (3G WCDMA, 4G TDD & FDD LTE, 5G NR Sub 6 GHz NSA/SA).

Furthermore, the TOE facilitates secure network access by supporting client certificate-based authentication for connecting to WPA2/WPA3 networks via 802.1ax/EAP-TLS protocols, and also establishes connectivity with cellular base stations for mobile data communication.

Additionally, the TOE exposes an Application Programming Interface (API) that integrates with the KATIM OS framework, enabling OS services for mobile applications, and also providing mobile device management (MDM) capability for MDM agents to perform device management operations via the KATIM OS MDM API.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level of [CFG_MDF-BT-WLANC_V1.0] according to Common Criteria CC:2022 R1

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_FSP.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.1
	ALC_CMS.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.1
	ASE_REQ.1
	ASE_TSS.1
ATE	ATE_IND.1
AVA	AVA_VAN.1

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria version 2022:

SECURITY FUNCTIONAL REQUIREMENTS
FAU_GEN.1

FAU_GEN.1/BT
FAU_GEN.1/WLAN
FAU_SAR.1
FAU_STG.1
FAU_STG.4
FCS_CKM.1
FCS_CKM.1/WPA
FCS_CKM.2/UNLOCKED
FCS_CKM.2/LOCKED
FCS_CKM.2/WLAN
FCS_CKM_EXT.1
FCS_CKM_EXT.2
FCS_CKM_EXT.3
FCS_CKM_EXT.4
FCS_CKM_EXT.5
FCS_CKM_EXT.6
FCS_CKM_EXT.8
FCS_COP.1/ENCRYPT
FCS_COP.1/HASH
FCS_COP.1/SIGN
FCS_COP.1/KEYHMAC
FCS_COP.1/CONDITION
FCS_HTTPS_EXT.1
FCS_IV_EXT.1
FCS_RBG_EXT.1
FCS_SRV_EXT.1

FCS_STG_EXT.1
FCS_STG_EXT.2
FCS_STG_EXT.3
FCS_TLS_EXT.1
FCS_TLSC_EXT.1
FCS_TLSC_EXT.2
FCS_TLSC_EXT.1/WLAN
FCS_TLSC_EXT.2/WLAN
FCS_TLSC_EXT.4
FCS_TLSC_EXT.5
FCS_WPA_EXT.1
FDP_ACF_EXT.1
FDP_ACF_EXT.2
FDP_DAR_EXT.1
FDP_DAR_EXT.2
FDP_IFC_EXT.1
FDP_STG_EXT.1
FDP_UPC_EXT.1/APPS
FDP_UPC_EXT.1/BLUETOOTH
FIA_AFL_EXT.1
FIA_BLT_EXT.1
FIA_BLT_EXT.2
FIA_BLT_EXT.3
FIA_BLT_EXT.4
FIA_BLT_EXT.6
FIA_BLT_EXT.7

FIA_PAE_EXT.1
FIA_PMG_EXT.1
FIA_TRT_EXT.1
FIA_UAU.5
FIA_UAU.6/CREDENTIAL
FIA_UAU.6/LOCKED
FIA_UAU.7
FIA_UAU_EXT.1
FIA_UAU_EXT.2
FIA_X509_EXT.1
FIA_X509_EXT.1/WLAN
FIA_X509_EXT.2
FIA_X509_EXT.2/WLAN
FIA_X509_EXT.3
FIA_X509_EXT.6
FMT_MOF_EXT.1
FMT_SMF.1
FMT_SMF_EXT.1/BT
FMT_SMF.1/WLAN
FMT_SMF_EXT.2
FPT_AEX_EXT.1
FPT_AEX_EXT.2
FPT_AEX_EXT.3
FPT_AEX_EXT.4
FPT_JTA_EXT.1
FPT_KST_EXT.1

FPT_KST_EXT.2
FPT_KST_EXT.3
FPT_NOT_EXT.1
FPT_STM.1
FPT_TST_EXT.1
FPT_TST_EXT.2/PREKERNEL
FPT_TST_EXT.3/WLAN
FPT_TUD_EXT.1
FPT_TUD_EXT.2
FPT_TUD_EXT.3
FTA_SSL_EXT.1
FTA_TAB.1
FTA_WSE_EXT.1
FTP_BLT_EXT.1
FTP_BLT_EXT.2
FTP_BLT_EXT.3/BR
FTP_BLT_EXT.3/LE
FTP_ITC_EXT.1
FTP_ITC.1/WLAN

IDENTIFICATION

Product: KATIM X3M on KATIM OS 13

Security Target: KATIM X3M on KATIM OS 13 – Security Target, 15/09/2025.

Protection Profile:

The ST and the TOE claims exact conformance to PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients, Version 1.0, 11 October 2022 (CFG_MDF-BT-WLANC_V1.0).

The PP-Configuration includes the following components:

- Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.3, 12 September 2022 (PP_MDF_V3.3)
- PP-Module: PP-Module for Bluetooth, Version 1.0, 15 April 2021 (MOD_BT_V1.0)
- PP-Module: PP-Module for WLAN Clients, Version 1.0, 31 March 2022 (MOD_WLANC_V1.0)

Evaluation Level: Common Criteria CC:2022 R1 (assurance packages according to [CFG_MDF-BT-WLANC_V1.0].

SECURITY POLICIES

The use of the product KATIM X3M on KATIM OS 13 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.3 (“Organizational Security Policies”).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.2 (“Assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product KATIM X3M on KATIM OS 13, although the agents implementing attacks have the attack potential according to the Basic level of AVA_VAN.1 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.1 (“Threats”).

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 (“Security Objectives for the operational Environment”).

ARCHITECTURE

LOGICAL ARCHITECTURE

The logical scope of the TOE is defined by the following security functions provided by the TOE:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

Security Audit

The TOE implements two primary logging mechanisms, SecurityLog and Logcat, which store logs in circular memory buffers within KATIM OS. These logs can be accessed and retrieved by an MDM agent for further processing, such as storing the log data in non- volatile memory or transmitting it to an MDM server.

Cryptographic Support

The TOE incorporates several cryptographic libraries, to support a wide array of cryptographic operations, including asymmetric key generation and key agreement, symmetric key generation, encryption and decryption, cryptographic hashing, and keyed-hash message authentication. These cryptographic operations are backed by compliant random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and secure destruction of keys and protected data.

User Data Protection

The TOE regulates access to system services for hosted applications, ensuring the protection of critical resources such as the Trust Anchor Database. In addition, the TOE employs encryption to safeguard user and other sensitive data, ensuring the data remains secure even in the event of device loss. The root encryption key derivation process depends on both the SoC of the TOE as well as the independent secure element to prevent single points of failure.

Identification and Authentication

The TOE includes several identification and authentication features. From the user's perspective, a Password Authentication Factor is required to unlock the device, with the exception of FCC-mandated functions, such as emergency calls, or non-sensitive actions like selecting a keyboard input method or taking screenshots. Even after the device is unlocked, the TOE mandates re-entering the password to modify the password itself. To enhance security, passwords are masked during input and are restricted by a configurable limit on failed attempts, after which the device will wipe its contents to safeguard data. Passwords can be composed of upper and lower-case letters, numbers, and special characters, with support for up to 16-character passwords. The TOE also functions as an 802.1X supplicant, supporting the use and validation of X.509v3 certificates for secure exchanges via EAP-TLS, TLS, and HTTPS protocols.

Security Management

The TOE offers all necessary interfaces for managing the security functions outlined in this Security Target, along with additional functionalities commonly found in mobile devices. While many features are accessible to the end users, certain security and management functions are restricted to administrators who manage the device through a MDM solution once the TOE is enrolled. Upon unenrollment from the MDM, the TOE will automatically remove all Enterprise applications and clear MDM policies, ensuring the device returns to its original state.

Protection of the TFS

The TOE incorporates a range of mechanisms to safeguard its reliability and the integrity of its security features. It ensures that sensitive data, such as cryptographic keys, remain protected by preventing their access or export via the application processor’s hardware. The TOE includes self-test and integrity-checking functions for both software and firmware, enabling it to detect any failures or potential corruption. If a self-test fails, the TOE will not enter an operational state. The TOE also verifies the digital signatures of all new software or firmware images before installation, ensuring that updates do not introduce malicious or unintended changes.

TOE Access

The TOE can be locked either manually by the user or automatically after a configured period of inactivity, both causing the display of the device to be obscured. Additionally, the TOE has the capability to display an administrator-defined advisory message banner

upon the first unlock following a reboot, which can be configured using the MDM API of the TOE. The TOE is also capable of attempting to connect to wireless networks according to the configured settings.

Trusted Path/Channels

The TOE supports secure communication channels with trusted network devices through the use of IEEE 802.11-2012, 802.1X, EAP-TLS, TLS, and HTTPS protocols.

PHYSICAL ARCHITECTURE

The physical boundary of the TOE is defined by the outer perimeter of its hardware enclosure (smartphone). The TOE includes the KATIM operating system (OS) preinstalled in the device. It does not encompass, however, the user applications that run on top of the KATIM OS.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

DOCUMENT	VERSION	UNIQUE IDENTIFIER (SHA256)
Security Target Lite	1.0	319783f09eaccb7bbc0c723a9b77f07a32900314f0efc7b0c2a18930d5fb0e3f
End User Guide	1.1	a33ba6d55b2d332b38d364dbdc1cc9b0601083cd1fb45683776a8f10db2f488a
Administrative Guide	1.3	09599bf86a6872e3108fc0b8037798d87205738919f44ece05bdbd1bfbc2b35d

PRODUCT TESTING

The TOE declares exact conformance to PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients, Version 1.0, 11 October 2022 (CFG_MDF-BT-WLANC_V1.0), which includes the following components:

- Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.3, 12 September 2022 (PP_MDF_V3.3)
- PP-Module: PP-Module for Bluetooth, Version 1.0, 15 April 2021 (MOD_BT_V1.0)
- PP-Module: PP-Module for WLAN Clients, Version 1.0, 31 March 2022 (MOD_WLANC_V1.0)

The PP-Configuration defines the whole set of tests that the Laboratory must perform in the evaluation. The coverage of all security functions is guaranteed by the PP-Configuration.

The Laboratory prepared and executed a test plan covering all (100%) of those required tests and verified that the obtained results obtained were equal to the expected results.

The PP-Configuration also defines the type and depth of vulnerability analysis that the Laboratory must perform in the evaluation.

The Laboratory conducted the required vulnerability analysis, including a survey of open sources to discover what vulnerabilities had been discovered that might apply to the TOE and an analysis of the likelihood of these vulnerabilities affecting the TOE. No vulnerabilities were identified in the TOE in its evaluated configuration.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product KATIM X3M on KATIM OS 13 it is necessary the disposition of the following software components:

In order to ensure compliance with the evaluated security configuration, the following settings must be enforced via the KATIM OS Management API:

- Enforce lock screen password
- Disable Smart Lock
- Encryption for Wi-Fi and Bluetooth credentials must be activated using the NIAP mode DPM API
- Installation of applications from unknown sources must be prohibited
- Security logging must be enabled
- Administrator-installed, connectivity-enabled applications must use NIAPSEC library for Sensitive Data Protection, Hostname Checking, Revocation Checking, and TLS Cipher-suite restriction

Adherence to these settings ensures that the device meets the Protection Profile for Mobile Device Fundamentals (PP_MDF_V3.3) requirements. Please refer to the Administrative Guide on how to configure the above settings

EVALUATION RESULTS

The product KATIM X3M on KATIM OS 13 has been evaluated against the Security Target KATIM X3M on KATIM OS 13 – Security Target, 15/09/2025.

All the assurance components required by the evaluation level of [CFG_MDF-BT-WLANC_V1.0] have been assigned a “PASS” verdict. Consequently, the laboratory Layakk Seguridad Informatica S.L. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the [CFG_MDF-BT-WLANC_V1.0], as defined by the Common Criteria CC:2022 R1, CEM CC:2022 R1 and [CFG_MDF-BT-WLANC_V1.0].

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

Since all evaluation assurance activities performed during the evaluation, including the tests and the vulnerability analysis yielded positive results, the Laboratory recommends the use of the TOE in its evaluated configuration.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product KATIM X3M on KATIM OS 13, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, November 2022, CC:2022, Revision 1

[CC_P2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, November 2022, CC:2022, Revision 1

[CC_P3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, November 2022, CC:2022, Revision 1

[CC_P4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, November 2022, CC:2022, Revision 1

[CC_P5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022, Revision 1

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, November 2022, CC:2022, Revision 1

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- KATIM X3M on KATIM OS 13 – Security Target, 15/09/2025.

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- KATIM X3M on KATIM OS 13 – Security Target Lite, 25/09/2025.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components selected.