Swedish Certification Body for IT Security

Certification Report - OPPO Find X5 Pro

Issue: 1.0, 2022-Mar-31

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is OPPO Find X5 Pro, running on ColorOS 12.1. The TOE is a mobile phone, and is intended both for personal and for enterprise use.

The TOE is

device name:	OPPO Find X5 Pro
model number:	CPH2305
chipset vendor:	Qualcomm
CPU:	Snapdragon 8 Gen 1
OS version:	ColorOS 12.1 (based on Android 12)
kernel version:	Linux kernel 5.10
build number:	CPH2305_11_A.11

The TOE does not include the user applications that run on top of the operating system, but includes controls that limit application behaviour. Furthermore, the TOE provides support for downloadable Mobile Device Management (MDM) agents to be installed to limit or permit various functionality in the device. No MDM agents are pre-installed in the TOE and the evaluated configuration does not contain any MDM agents. However, the MDM interface is used for setting up the TOE in its evaluated configuration.

The TOE communicates and interacts with 802.11-2012 access points and mobile data networks to establish network connectivity, and through that connectivity the TOE may interact with MDM servers that allow administrative control over the TOE.

The TOE is delivered to the users via retailers, including necessary guidance for the secure usage of the phone, including verification of the TOE after delivery.

The ST claims exact conformance to PP-Configuration for Mobile Device Fundamentals and Bluetooth v1.0 [CFG], comprised of Protection Profile for Mobile Device Fundamentals v3.2 [MDFPP], including the WLAN extension package [WLAN], the Functional Package for TLS v1.1 [PKG], and the PP-Module for Bluetooth v1.0 [BTPPM].

The evaluation has been performed by atsec information security AB, mainly in their premises in Danderyd, Sweden, and to a minor extent in the developer's premises in PRC (Peoples Republic of China).

The evaluation was completed on the 23rd of March 2022.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL 1, augmented by ASE_SPD.1 and ALC_TSU_EXT.1, and in accordance with the evaluation activities implied by the PP-Configuration for Mobile Device Fundamentals and Bluetooth v1.0 [CFG].

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:
EAL 1 + ASE_SPD.1 + ALC_TSU_EXT.1 and in accordance with the evaluation activities implied by the PP-Configuration for Mobile Device Fundamentals and Bluetooth v1.0 [CFG].

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2021007
Name and version of the certified IT product	OPPO Find X5 Pro, including ColorOS 12.1, and Qualcomm Snapdragon® 8 Gen 1 Mobile Platform
Security Target Identification	OPPO Find X5 Pro on ColorOS 12.1 Security Target, document version 1.4
EAL	EAL 1 augmented with ASE_SPD.1 and ALC_TSU_EXT.1
PP claim	PP-Configuration for Mobile Device Fundamentals and Bluetooth v1.0 [CFG], comprised of the Protection Profile for Mobile Device Fundamentals v3.2 [MDFPP], including the WLAN extension package [WLAN] and the Functional Package for TLS v1.1 [PKG], and the PP-Module for Bluetooth v1.0 [BTPPM]
Sponsor	Guangdong OPPO Mobile Telecommunications Corporation Ltd.
Developer	Guangdong OPPO Mobile Telecommunications Corporation Ltd.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.1.1
Scheme Notes Release	18.0
Recognition Scope	CCRA, SOGIS, and EA/MLA
Certification date	2022-03-31

3 Security Policy

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

3.1 Security Audit

The TOE implements a security log and logcat that are each stored in a circular memory buffer. An MDM agent can read/fetch the security logs, can retrieve logcat logs, and then handle appropriately (potentially storing the log to Flash or transmitting its contents to the MDM server).

3.2 Cryptographic support

The TOE provides cryptographic services via the following two cryptographic modules:

- BoringSSL ae2bb641735447496bed334c495e4868b981fe32
- Application Processor

BoringSSL is a fork of OpenSSL which is built into shared libraries of ColorOS. The cryptographic functions provided by BoringSSL include symmetric key generation, encryption and decryption, asymmetric key generation and key establishment, cryptographic hashing, and keyed-hash message authentication. The TOE also provides below functions which are used to implement security protocols and the encryption of data-at-rest:

- Random number generation
- Data encryption and decryption
- Signature generation/verification
- Message digest
- Message authentication
- Key generation
- Key wrapping

Application Processor provides a set of FIPS 140-2 certified hardware cryptographic modules, the cryptographic functions provided by Application Processor include symmetric key generation, encryption and decryption, cryptographic hashing, and keyed-hash message authentication. The TOE also provides below functions which are used to implement security protocols and the encryption of data-at-rest:

- Random number generation
- Data encryption and decryption
- Message digest
- Message authentication
- Key generation
- Key derivation

3.3 User data protection

The TOE controls access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, User data in files is protected using cryptographic functions, ensuring this data remains protected even if the device gets lost or is stolen. Data is protected such that only the app that owns the data can access it. The TOE's evaluated configuration supports Android Enterprise profiles to provide additional separation between application and application data belonging to the Enterprise profile. Please see the Admin Guide for additional details regarding how to set up and use Enterprise profiles.

3.4 Identification and authentication

Except for answering calls, making emergency calls, using the cameras, using the flashlight, using the quick settings, and checking notifications, users need to authenticate using a passcode or a biometric (fingerprint / face). The user is required to use the passcode authentication mechanism under the following conditions.

- Turn on or restart the device
- Unlock the device for the first time after reboot
- Update software
- Erase the device
- View or change passcode settings
- Install enterprise profiles

The passcode can be configured for a minimum length, for dedicated passcode policies, and for a maximum lifetime. When entered, passcodes are obscured and the frequency of entering passcodes is limited as well as the number of consecutive failed attempts of entering the passcode.

The TOE also enters a locked state after a (configurable) time of user inactivity, and the user is required to either enter his passcode or use biometric authentication (fingerprint) to unlock the TOE.

External entities connecting to the TOE via a secure protocol (Extensible Authentication Protocol Transport Layer Security (EAPTLS), Transport Layer Security (TLS)) can be authenticated using X.509 certificates.

3.5 Security management

The TOE provides all the interfaces necessary to manage the security functions identified throughout this Security Target as well as other functions commonly found in mobile devices. Many of the available functions are available to users of the TOE while many are restricted to administrators operating through a Mobile Device Management solution once the TOE has been enrolled.

Once the TOE has been enrolled and then un-enrolled, it will remove Enterprise applications and remove MDM policies

3.6 Protection of the TSF

Some of the functions the TOE implements to protect the TSF and TSF data are as follows:

- Protection of cryptographic keys - they are not accessible or exportable using the application processor's hardware.

- Protection of REKs - The TOE disallows all read access to the Root Encryption Key and retains all keys derived from the REK within its the Trusted Execution Environment (TEE). Application software can only use keys derived from the REK by reference and receive the result.
- The TOE enforces read, write, and execute memory page protections, uses address space layout randomization, and stack-based buffer overflow protections to minimize the potential to exploit application flaws. It also protects itself from modification by applications as well as to isolate the address spaces of applications from one another to protect those applications.
- Digital signature protection of the TSF image - all updates to the TSF need to be digitally signed.
- Software/firmware integrity self-test upon start-up - the TOE will not go operational when this test fails.
- Digital signature verification for apps.
- Access to defined TSF data and TSF services only when the TOE is unlocked.
- The TOE provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

3.7 TOE access

The TSF provides functions to lock the TOE upon request by user or after an administrator configurable time of inactivity.

The TOE also has the capability to display an administrator specified (using the TOE’s MDM API) advisory message (banner) when the user unlocks the TOE for the first use after reboot.

The TOE is also able to attempt to connect to wireless networks as configured

3.8 Trusted path/channels

The TOE supports the use of the following communication and cryptographic protocols that define a trusted channel between itself and another

trusted IT product.

- IEEE 802.11-2012
- IEEE 802.11ac-2013 (a.k.a. Wi-Fi 5)
- IEEE 802.11ax (a.k.a. Wi-Fi 6)
- IEEE 802.1X
- EAP-TLS (1.0, 1.1, 1.2)
- TLS (1.1, 1.2)
- HTTPS
- Bluetooth (5.0)

4 Assumptions and Clarification of Scope

4.1 Environmental Assumptions

The Security Target [ST] makes six assumptions on the usage and the operational environment of the TOE.

A.CONFIG (MDFPP)

It is assumed that the TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

A.NOTIFY (MDFPP)

It is assumed that the mobile user will immediately notify the administrator if the Mobile Device is lost or stolen.

A.PRECAUTION (MDFPP)

It is assumed that the mobile user exercises precautions to reduce the risk of loss or theft of the Mobile Device.

A.PROPER_USER (MDFPP)

Mobile Device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

A.NO_TOE_BYPASS (WLAN)

Information cannot flow between the wireless client and the internal wired network without passing through the TOE.

A.TRUSTED_ADMIN (WLAN)

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner

4.2 Clarification of Scope

The Security Target contains eight threats, which have been considered during the evaluation.

T.NETWORK_EAVESDROP (MDFPP)

An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the Mobile Device and other endpoints.

T.NETWORK_ATTACK (MDFPP)

An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may initiate communications with the Mobile Device or alter communications between the Mobile Device and other endpoints in order to compromise the Mobile Device. These attacks include malicious software update of any applications or system software on the device. These attacks also include malicious web pages or email attachments, which are usually delivered to devices over the network.

T.PHYSICAL_ACCESS (MDFPP)

An attacker, with physical access, may attempt to access user data on the Mobile Device including credentials. These physical access threats may involve attacks, which attempt to access the device through external hardware ports, impersonate the user authentication mechanisms, through its user interface, and also through direct and possibly destructive access to its storage media. Note: Defending against device re-use after physical compromise is out of scope for this Protection Profile.

T.MALICIOUS_APP (MDFPP)

Applications loaded onto the Mobile Device may include malicious or exploitable code. This code could be included intentionally or unknowingly by the developer, perhaps as part of a software library. Malicious apps may attempt to exfiltrate data to which they have access. They may also conduct attacks against the platform’s system software, which will provide them with additional privileges and the ability to conduct further malicious activities. Malicious applications may be able to control the device's sensors (GPS, camera, microphone) to gather intelligence about the user's surroundings even when those activities do not involve data resident or transmitted from the device. Flawed applications may give an attacker access to perform network-based or physical attacks that otherwise would have been prevented.

T.PERSISTENT_PRESENCE (MDFPP)

Persistent presence on a device by an attacker implies that the device has lost integrity and cannot regain it. The device has likely lost this integrity due to some other threat vector, yet the continued access by an attacker constitutes an on-going threat in itself. In this case, the device and its data may be controlled by an adversary as well as by its legitimate owner.

T.TSF_FAILURE (WLAN)

Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.

T.UNAUTHORIZED ACCESS (WLAN)

A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

T.UNDETECTED_ACTIONS (WLAN)

Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

The Security Target does not contain any Organisational Security Policies (OSPs).

5 Architectural Information

The TOE OS manages the device hardware and provides the technologies with a rich API set required to implement native applications, it also provides the capability to approve or reject an application based upon the API access that the application requires (or to grant applications access at runtime).

The TOE provides a built-in Mobile Device Management (MDM) framework API, giving management features that may be utilized by external MDM solutions (not part of this evaluation), allowing enterprises to use profiles to control some of the device settings. Security management capabilities are also provided to users via the user interface of the device and to administrators through the installation of Configuration Profiles on the device by using MDM solutions.

The TOE provides cryptographic services for the encryption of data-at-rest within the TOE, for secure communication channels, for protection of Configuration Profiles, and for use by apps. These cryptographic services can also be used to establish a trusted channel to other IT entities.

User data protection is provided by encrypting all of the user and mobile application data stored in the user’s data partition, restricting access by apps and by restricting access until the user has been successfully authenticated.

User identification and authentication is provided by a user defined passphrase (and supplemented by biometric technologies) where the minimum length of the passphrase, passphrase rules, and the maximum number of consecutive failed authentication attempts can be configured by an administrator. Any kind of Smart Lock mechanism shall be disabled in the CC configuration of the TOE.

The TOE protects itself by having its own code and data protected from unauthorized access (using hardware provided memory protection features), by encrypting internal user and TOE Security Functionality (TSF) data using TSF protected keys and encryption/decryption functions, by self-tests, by ensuring the integrity and authenticity of TSF updates and downloaded apps, and by locking the TOE upon user request or after a defined time of user inactivity.

6 Documentation

The following guidance document is part of the TOE:

OPPO Find X5 Pro on ColorOS 12.1 Administrator Guidance v1.1

7 IT Product Testing

7.1 Evaluator Testing

In January and February 2022, the evaluators performed all applicable tests required by the PP/EP/Modules claimed in the ST. The evaluated version of the TOE is:

device name:	OPPO Find X5 Pro
model number:	CPH2305
chipset vendor:	Qualcomm
CPU:	Snapdragon 8 Gen 1
OS version:	ColorOS 12.1 (based on Android 12)
kernel version:	Linux kernel 5.10
build number:	CPH2305_11_A.11.

The testing of cryptographic algorithms was performed against NIST CAVP by the developer, using test vectors generated by the evaluators. The evaluators also verified the test results of the CAVP tests. The measurements of electro-magnetic emanations were performed by the evaluators in the developer's premises. All other testing was performed by the evaluators in their premises in Danderyd, Sweden.

All tests were successful.

7.2 Penetration Testing

No potential vulnerabilities were found to be applicable to the TOE in its operational environment. Thus the evaluators did not see any need for penetration testing.

8 Evaluated Configuration

The guidance documentation provides the following instructions for activation of CC mode (the evaluated configuration):

1. WiFi keys and Bluetooth keys are encrypted by default and can never be disabled.
2. Require a lock-screen password
3. Disable Smart Lock
4. Disable Debugging Features (Developer options)
5. Disable installation of applications from unknown sources
6. Enable Audit Logging
7. Disable USB Debugging function

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The evaluators also performed all evaluation activities required by the Protection Profile for the Mobile Device Fundamentals [MDFPP], the Bluetooth PP-Module [BTPPM], the WLAN package [WLAN], and the TLS package [PKG].

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC], and the PP-Configuration for Mobile Device Fundamentals and Blue-tooth [CFG].

The evaluators' overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Functional Specification	ADV_FSP.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Evaluation Activities for MDFPP	AGD_MDFPP.1	PASS
Assurance activities for BTPPM	AGD_BTPPM.1	PASS
Assurance activities for WLAN package	AGD_WLANEP.1	PASS
Assurance activities for TLS package	AGD_TLSPKG.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.1	PASS
CM Scope	ALC_CMS.1	PASS
Timely Security Updates	ALC_TSU_EXT.1	PASS
Evaluation Activities for MDFPP	ALC_MDFPP.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.1	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.1	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Evaluation Activities for MDFPP	ASE_MDFPP.1	PASS
Assurance activities for BTPPM	ASE_BTPPM.1	PASS
Assurance activities for WLAN package	ASE_WLANEP.1	PASS
Assurance activities for TLS package	ASE_TLSPKG.1	PASS

Tests	ATE	PASS
Independent Testing	ATE_IND.1	PASS
Evaluation Activities for MDFPP	ATE_MDFPP.1	PASS
Assurance activities for BTPPM	ATE_BTPPM.1	PASS
Assurance activities for WLAN package	ATE_WLANEP.1	PASS
Assurance activities for TLS package	ATE_TLSPKG.1	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.1	PASS
Evaluation Activities for MDFPP	AVA_MDFPP.1	PASS

10 Bibliography

ST OPPO Find X5 Pro on ColorOS 12.1 Security Target, Guangdong OPPO Mobile Telecommunications Corporation Ltd, 2022-03-16, document version 1.4

ADM Guide OPPO Find X5 Pro on ColorOS 12.1 Administrator Guidance, Guangdong OPPO Mobile Telecommunications Corporation Ltd, 2022-02-11, document version 1.1

CFG PP-Configuration for Mobile Device Fundamentals and Blue-tooth, NIAP, 2021-04-15, document version 1.0

MDFPP Protection Profile for Mobile Device Fundamentals, NIAP, 2021-04-15, document version 3.2

BTPPM PP-Module for Bluetooth, NIAP, 2021-04-15, version 1.0

WLAN Wireless Local Area Network (WLAN) Clients, NIAP, 2016-02-08, document version 1.0

PKG Functional Package for TLS, NIAP, 2019-02-12, version 1.1

CCpart1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001

CCpart2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002

CCpart3 Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1, revision 5, April 2017, CCMB-2017-04-003

CC CCpart1 + CCPart2 + CCPart3

CEM Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was entered into the registry 2021-10-01:

QMS 1.25 valid from 2021-06-17

QMS 2.0 valid from 2021-11-24

QMS 2.1 valid from 2022-01-18

QMS 2.1.1 valid from 2022-02-25

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in:

“Ändringslista CSEC QMS 2.1”.

The certifier concluded that, from QMS 1.25 to the current QMS 2.1.1, there are no changes with impact on the result of the certification

A.2 Scheme Notes

The following Scheme Notes has been considered during the evaluation:

Scheme Note 18 Highlighted requirements on the Security Target v3.0

Clarifications concerning requirements on the Security Target.

Scheme Note 21 NIAP PP Certifications v3.0

All evaluation activities required in the supporting document of the PP shall be reported (in AAR or in SERs).

Scheme Note 22 Vulnerability assessment v3.0

Clarifications regarding the vulnerability assessment.

Mandatory update of the vulnerability database search, if older than 30 days, at the end of the evaluation.

Scheme Note 23 Evaluation reports for NIAP PPs and cPPs v1.0

Both evaluation activities and work units shall be covered in the evaluation reports.