Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 3/22

(Certification No.)

Prodotto: Huawei Mate 40 Pro (M40 pro) with EMUI 11.0

(Product)

Sviluppato da: Huawei Device Co., Ltd.

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

Conforme a: Protection Profile for Mobile Device Fundamentals, v3.1

(Conformant to)

(ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 20 gennaio 2022

Common Criteria

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Huawei Mate 40 Pro (M40 pro) with EMUI 11.0

OCSI/CERT/ATS/10/2020/RC

Version 1.0

20 January 2022

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	20/01/2022

2 Table of contents

3 Acronyms

AES Advanced Encryption Standard

API Application Programming Interface

BAF Biometric Authentication Factor

CAVP Cryptographic Algorithm Validation Program

CAVS Cryptographic Algorithm Validation System

CB Certification Body

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

CVE Common Vulnerabilities and Exposures

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

EAP Extensible Authentication Protocol

EMUI Emotion UI

EP Extended Package

ETR Evaluation Technical Report

HMAC Keyed-hash Message Authentication Code

HTTP HyperText Transfer Protocol

HTTPS HTTP over Secure Socket Layer

ISA Instruction Set Architecture

IT Information Technology

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

MDM Mobile Device Management

NIAP National Information Assurance Partnership

NIS	Nota Informativa dello Schema
NM	Nano Memory
OCSI	Organismo di Certificazione della Sicurezza Informatica
OS	Operating System
PMK	Pairwise Master Key
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
WLAN	Wireless Local Area Network

4 References

4.1 Criteria and regulations

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

4.2 Technical documents

[CCG] "Common Criteria Guide for Huawei (M40 pro) EMUI 11.0", v0.4, Huawei Device Co., Ltd., 3 September 2021

[ETR] Final Evaluation Technical Report "Huawei Mate 40 Pro (M40 pro) with EMUI 11.0", Version 1.0, atsec information security GmbH, 14 December 2021

[PPMDF] Protection Profile for Mobile Device Fundamentals, NIAP, Version 3.1, 16 June 2017

[PPWLANC] General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package (EP) - Wireless Local Area Network (WLAN) Clients, NIAP, Version 1.0, 8 February 2016

[ST] "Huawei Mate 40 Pro (M40 pro) Mobile Device with EMUI 11.0 (MDFPP31/WLANCEP10) Security Target", Version 1.0, Huawei Device Co., Ltd., 3 November 2021

5 Recognition of the certificate

5.1 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all declared assurance components included in EAL1.

6 Statement of certification

The Target of Evaluation (TOE) is the product “Huawei Mate 40 Pro (M40 pro) with EMUI 11.0”, developed by Huawei Device Co., Ltd.

The TOE is the Huawei Mate 40 Pro smartphone (M40 pro in short) with the EMUI 11.0.0.165 operating system, including kernel version 4.14. The TOE is intended to be used in enterprise environments that ensure that it is configured and operated in accordance to the specific Common Criteria mode as described by the guidance documentation.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance components included in the PP [PPMDF], according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “Huawei Mate 40 Pro (M40 pro) with EMUI 11.0” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Huawei Mate 40 Pro (M40 pro) with EMUI 11.0
Security Target	“Huawei Mate 40 Pro (M40 pro) Mobile Device with EMUI 11.0 (MDFPP31/WLANCEP10) Security Target”, Version 1.0 [ST]
Evaluation Assurance Level	Conformant to PP including the following assurance components: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, and AVA_VAN.1
Developer	Huawei Device Co., Ltd.
Sponsor	Huawei Device Co., Ltd.
LVS	atsec information security GmbH
CC version	3.1 Rev. 5
PP conformance claim	Protection Profile for Mobile Device Fundamentals v3.1 [PPMDF] with the following Extended Package: • GPOSPP EP - Wireless Local Area Network (WLAN) Clients v1.0 [PPWLANC]
Evaluation starting date	14 December 2020
Evaluation ending date	14 December 2021

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE is the Huawei Mate 40 Pro mobile device (M40 pro in short) running the EMUI 11.0.0.165 operating system with kernel version 4.14. The EMUI 11.0 is a smartphone operating system which can run upon several models of Huawei mobile phones and provides the security functionalities of the TOE.

The TOE is intended for use as part of an enterprise mobility solution providing mobile staff with enterprise connectivity. The TOE provides wireless connectivity and creates a runtime environment for applications designed for the mobile Android environment. The TOE also provides telephony and networking features.

Details on the M40 pro smartphone device are shown in Table 1.

Device name	Model number	Chipset vendor	CPU	Build arch. / ISA	OS version	Kernel version
Mate 40 Pro	NOH-AN00	Hisilicon	Kirin 9000	ARM 64	EMUI 11.0	4.14

Table 1 - TOE hardware and firmware reference

For a detailed description of the TOE, consult sect. 1.4 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE architecture

The TOE's physical boundary is the physical perimeter of its enclosure. The TOE does not include the user applications that run on top of the operating system, but does include controls that limit application behavior.

The TOE provides an Application Programming Interface to mobile applications and allows users installing an application to either approve or reject an application based upon the API access that the application requires.

The TOE also provides users with the ability to protect Data-at-Rest with AES encryption, including all user and mobile application data stored in the user's data partition. The TOE affords special protection to all user and application cryptographic keys stored in the TOE.

Finally, the TOE interacts with an MDM server to allow enterprise control of the configuration and operation of the device so as to ensure adherence to enterprise-wide policies.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 7 of the Security Target [ST]. The most significant aspects are summarized below:

- **Security Audit**: the TOE generates audit records for a wide array of security relevant events concerning TOE usage and configuration. The TOE stores all audit records in the log files and sets access permission of logs making them unavailable to applications, to prevent from any malicious modifications.

- **Cryptographic support**: the TOE includes cryptographic modules with CAVP validated algorithms that are used for cryptographic functions including: asymmetric key generation and establishment, symmetric key generation, encryption/decryption, cryptographic hashing and keyed-hash message authentication (HMAC). These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key and protected data destruction. These primitive cryptographic functions are used to implement security protocols such as TLS, and HTTPS and also to encrypt the media (including the generation and protection of data encryption keys and key encryption keys) used by the TOE.
  The TOE provides cryptographic services via the following three cryptographic modules:
  - The BoringSSL Cryptographic Module (User Space)
  - The Kernel Crypto Cryptographic Module (Kernel Space)
  - The CC engine Cryptographic Module (TEE and bootup)

- **User data protection**: the TOE controls access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE protects user and other sensitive data using encryption so that, even if a device is physically lost, the data remains protected.

- **Identification and authentication**: the TOE supports a number of features related to identification and authentication. From a user perspective, except for limited functions such as making phone calls to an emergency number and receiving notifications, a password or Biometric Authentication Factor (BAF) must be correctly entered to unlock the TOE. Also, even when the TOE is unlocked, the password must be re-entered to change the password. Passwords are obscured when entered, so they cannot be read from the TOE's display. The frequency of entering passwords is limited, and when a configured number of failures occurs, the TOE is wiped of user data. Also, the TOE can use X.509v3 certificates to perform certificate validation on EAP-TLS, TLS, and HTTPS exchanges.

- **Security management**: the TOE provides all the interfaces necessary to manage the security functions identified by the Security Target as well as other functions commonly found in mobile devices. Many of these functions are available to the users of the TOE while others are restricted to administrators operating through a Mobile Device Management solution once the TOE has been enrolled.

- **Protection of the TSF**: the TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as cryptographic keys so that they are not accessible or exportable. It also provides its own timing mechanism to ensure that reliable time information is available. It enforces read, write, and execute memory page protections, uses address space layout randomization, and uses stack-based buffer overflow protections to minimize the potential to exploit application flaws. It is

designed to protect itself from modification by applications as well as to isolate the address spaces of applications from one another to protect those applications.
The TOE also includes functions to perform self-tests and software/firmware integrity checking so that it can detect when it is failing or may be corrupt. If any self-test fails, the TOE does not go into an operational mode. It includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE. Digital signature checking also extends to verifying applications prior to their installation.

- **TOE access**: the TOE can be locked, obscuring its display, by a user or after a configured interval of inactivity. The TOE can also attempt to connect to wireless networks as configured.

- **Trusted path/channels**: the TOE supports the use of 802.11-2012, 802.1X, and EAP-TLS, to secure communications channels between itself and other trusted network devices.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.3 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims exact conformance to the following Protection Profile and Extended Package:

- Protection Profile for Mobile Device Fundamentals, version 3.1 [PPMDF]

- General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package (EP) - Wireless Local Area Network (WLAN) Clients, Version 1.0 [PPWLANC]

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected or derived by extension from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

Considering that the Security Target [ST] claims exact conformance to the Protection Profile for Mobile Device Fundamentals [PPMDF] and the Wireless Local Area Network (WLAN) Clients Extended Package [PPWLANC], all the SARs and SFRs from the PP and EP are included.

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM]. Furthermore, all specific assurance activities required by the Protection Profile for Mobile Device Fundamentals [PPMDF] and the Wireless Local Area Network (WLAN) Clients Extended Package [PPWLANC] have been carried out.

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) atsec information security GmbH.

The evaluation was completed on 14 December 2021 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 21 December 2021. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS atsec information security GmbH and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that the TOE "Huawei Mate 40 Pro (M40 pro) with EMUI 11.0" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level defined by the SARs included in the PP [PPMDF], with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 2 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level defined by the SARs included in the PP [PPMDF].

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives for the operational environment	ASE_OBJ.1	Pass
Stated security requirements	ASE_REQ.1	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Basic functional specification	ADV_FSP.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Labelling of the TOE	ALC_CMC.1	Pass
TOE CM coverage	ALC_CMS.1	Pass
Timely Security Updates	*ALC_TSU_EXT.1*	Pass
Tests	**Class ATE**	Pass
Independent testing - conformance	ATE_IND.1	Pass
Vulnerability assessment	**Class AVA**	Pass

Assurance classes and components		Verdict
Vulnerability survey	AVA_VAN.1	Pass

Table 2 - Final verdicts for assurance requirements

8.2 Additional assurance activities

The Protection Profile for Mobile Device Fundamentals [PPMDF] and the Wireless Local Area Network (WLAN) Clients Extended Package [PPWLANC] include additional assurance activities that are specific to the TOE technology type, and are required for exact conformance to the PP and EP.

The Evaluators used for the PP/EP assurance activities a notation similar to assurance components of existing CC assurance classes. The objective of these sub-activities is to determine whether the requirements of the assurance activities included in the PP/EP are met.

Table 3 summarizes the final verdict of the PP/EP assurance activities carried out by the LVS.

PP/EP assurance activities		Verdict
ASE: Security Target evaluation	ASE_MDFPP.1	Pass
	ASE_WLANEP.1	Pass
AGD: Guidance documents	AGD_MDFPP.1	Pass
	AGD_WLANEP.1	Pass
ALC: Life cycle support	ALC_MDFPP.1	Pass
ATE: Tests	ATE_MDFPP.1	Pass
	ATE_WLANEP.1	Pass
AVA: Vulnerability assessment	AVA_MDFPP.1	Pass

Table 3 - Final verdicts for PP/EP assurance activities

8.3 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product “Huawei Mate 40 Pro (M40 pro) with EMUI 11.0” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions and the Organizational Security

Policies described, respectively, in sect. 3.2 and 3.3 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([CCG]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

TOE hardware is delivered to retailers and users can buy the TOE from them.

When the user receives the device, the user needs to make sure that the package is intact, and the sealing label is not broken. Refer to sect. 12.1 (“Security Acceptance”) of the guidance documentation [CCG] for further details.

9.2 Identification of the TOE

Users need to check the hardware model number and the software version by accessing *Settings* > *About phone* on the TOE UI.

9.3 Installation, initialization and secure usage of the TOE

Users should refer to the following document for instructions on how to install, configure and update the TOE:

- “Common Criteria Guide for Huawei (M40 pro) EMUI 11.0”, v0.4, 3 September 2021 [CCG]

The guidance documentation [CCG] also provides information on TOE secure usage in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “Huawei Mate 40 Pro (M40 pro) with EMUI 11.0”, developed by Huawei Device Co., Ltd.

The evaluated configuration of the TOE includes the Huawei M40 Pro Mobile Device (Model Number: NOH-AN00, as described in Table 1) and the guidance documentation listed in section 9.3.

The software identification for the evaluated devices is as follows:

- Kernel Version: 4.14
- Build Number: 11.0.0.165

The TOE includes a Common Criteria mode (or “CC mode”) that an administrator can invoke by using a Mobile Device Management (MDM) system. When CC mode has been enabled, the TOE performs the following actions:

- The TOE sets the system wide Android CC mode property to be enabled.
- The TOE executes three cryptographic modules (Kernel Crypto, BoringSSL, CC engine) self-tests after system boot up, and records security audit log event.
- The security audit log events are stored in internal storage to prevent from losing them after a power cycle.
- The TOE wipes all of protected data after the number of unsuccessful authentication attempts reaches to the max number.
- Users are not allowed to use the NM (Nano Memory) card in CC mode.

10.1 TOE operational environment

The following non-TOE hardware/software is required in the operational environment to allow the correct functioning of the TOE (see sect. 1.4.2 of the Security Target [ST]):

- 802.11-2012 access point for WLAN connection.
- Authentication Server for EAP-TLS mutual authentication and establishment of pairwise master key (PMK).
- Mobile data networks for network connectivity.
- MDM server for administrative control of the TOE.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level defined by the SARs included in the PP [PPMDF], such activities do not require the execution of functional tests by the Developer, but only independent functional tests and penetration tests by the Evaluators.

11.1 Test configuration

The Evaluators received from the Developer a Huawei M40 Pro device for testing.

The Developer also provided development and testing environments for performing the test cases required by the PP [PPMDF] and EP [PPWLANC]. In particular, the Evaluators received developer version of the device (pre-commercial release, which is identical to the release version) and some Android applications to be installed on the device.

The Evaluators visited a development site in Germany to perform tests with the support from the Developer. The Evaluators configured the TOE and set up the test environment following the indications of the guidance documentation [CCG].

The Evaluators verified that the configured TOE and environment were consistent with the requirements of the Security Target [ST].

11.2 Functional and independent tests performed by the Evaluators

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly. They also verified that the test environment was properly set up.

The Evaluators performed tests to ensure that the TOE behaves as specified in the Security Target [ST] and the guidance documentation [CCG] as well as to perform all required tests described in the PP [PPMDF] and EP [PPWLANC], and in the applicable NIAP Technical Decisions listed in sect. 2 of the Security Target [ST].

The CAVS tests confirming the correct implementation of cryptographic mechanisms were run on a specially instrumented TOE version in the Developer's lab and observed by the Evaluators and the CB certifiers connected in a video conference. During that session, the Evaluators could confirm that the test machine ran the same build number 11.0.0.165 (executing the "adb device" command on the test machine). The Developer confirmed that the test machine was only modified to open up some internal interfaces required for the CAVS tests to the external test programs, but that the implementation of the cryptographic mechanisms themselves remained unchanged from the TOE version.

All Evaluator test cases, including CAVS tests, were completed successfully, i.e., all the actual test results were consistent to the expected test results.

11.3 Vulnerability analysis and penetration tests

The Evaluators performed a search of public domain sources to identify potential vulnerabilities in the TOE, including Common Vulnerabilities and Exposures (CVE), Exploit

Database, Packet Storm and SecurityFocus. The Evaluators also checked the Android Security Bulletins and security publications on the Developer's website.

The Evaluators used keywords for the public search, which were carefully chosen in such a way that they are wide enough to cover all subjects of interest and specific enough to eliminate unrelated items (for ex., "Huawei Mate 40 Pro", "M40 Pro", "EMUI 11.0", "Huawei Kirin 9000", and "Android 10.0").

Based on the collected information, the Evaluators compiled a list of potentially applicable vulnerabilities. The Evaluators performed an analysis of all found vulnerabilities and could not identify any potential vulnerabilities applicable to the TOE that were not appropriately mitigated by the Developer. Thus, the Evaluators identified no need for additional testing.

The Evaluators could then conclude that the TOE is resistant to an attack potential of Basic in its intended operational environment. No exploitable or residual vulnerabilities have been identified.