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)

Firmato digitalmente
da Eva Spina
Data: 2022.01.20
09:40:44 +01'00'

Roma, 20 gennaio 2022

Common Criteria

Questa pagina è lasciata intenzionalmente vuota

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

Rapporto di Certificazione

Huawei Mate 40 Pro (M40 pro) with EMUI 11.0

OCSI/CERT/ATS/10/2020/RC

Versione 1.0

20 gennaio 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	20/01/2022

2 Indice

3 Elenco degli acronimi

AES	Advanced Encryption Standard
API	Application Programming Interface
BAF	Biometric Authentication Factor
CAVP	Cryptographic Algorithm Validation Program
CAVS	Cryptographic Algorithm Validation System
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
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
ODV	Oggetto della Valutazione
PMK	Pairwise Master Key
PP	Protection Profile
RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SO	Sistema Operativo
ST	Security Target
TDS	Traguardo di Sicurezza
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 Riferimenti

4.1 Criteri e normative

[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 Documenti tecnici

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

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

[TDS] "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 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia dichiarati inclusi nel livello EAL1.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Huawei Mate 40 Pro (M40 pro) with EMUI 11.0", sviluppato da Huawei Device Co., Ltd.

L'ODV comprende il modello di *smartphone* Huawei Mate 40 Pro (abbreviato in M40 pro), dotato di sistema operativo EMUI 11.0.0.165 con *kernel* versione 4.14. L'ODV è destinato all'uso in ambienti aziendali che garantiscano che i dispositivi siano configurati e gestiti in conformità alla specifica modalità Common Criteria descritta nella documentazione di guida.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti e/o utilizzatori. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per i componenti di garanzia inclusi nel PP [PPMDF], in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "Huawei Mate 40 Pro (M40 pro) with EMUI 11.0" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	Huawei Mate 40 Pro (M40 pro) with EMUI 11.0
Traguardo di Sicurezza	"Huawei Mate 40 Pro (M40 pro) Mobile Device with EMUI 11.0 (MDFPP31/WLANCEP10) Security Target", Version 1.0 [TDS]
Livello di garanzia	Conforme a PP con i seguenti componenti di garanzia: 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 e AVA_VAN.1
Fornitore	Huawei Device Co., Ltd.
Committente	Huawei Device Co., Ltd.
LVS	atsec information security GmbH
Versione dei CC	3.1 Rev. 5
Conformità a PP	Protection Profile for Mobile Device Fundamentals v3.1 [PPMDF] col seguente Extended Package: • GPOSPP EP - Wireless Local Area Network (WLAN) Clients v1.0 [PPWLANC]
Data di inizio della valutazione	14 dicembre 2020
Data di fine della valutazione	14 dicembre 2021

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV è costituito dal dispositivo mobile Huawei Mate 40 Pro (abbreviato in M40 pro) su cui è installato il sistema operativo EMUI 11.0.0.165 con *kernel* versione 4.14. EMUI 11.0 è un sistema operativo per *smartphon*e che può essere eseguito su diversi modelli di telefoni cellulari Huawei e fornisce le funzionalità di sicurezza dell'ODV.

L'ODV è destinato ad essere utilizzato come parte di una soluzione di mobilità aziendale che fornisce accesso alla rete aziendale al personale in mobilità. L'ODV fornisce connettività wireless e realizza un ambiente di *runtime* per le applicazioni progettate per la piattaforma mobile Android. L'ODV fornisce anche funzionalità di telefonia e di rete.

La Tabella 1 fornisce i dettagli del dispositivo M40 pro.

Nome del dispositivo	**Numero modello**	**Produttore del chipset**	**CPU**	**Architettura (ISA)**	**Versione SO**	**Versione *kernel***
Mate 40 Pro	NOH-AN00	Hisilicon	Kirin 9000	ARM 64	EMUI 11.0	4.14

Tabella 1 - Elenco dei componenti hardware e firmware dell'ODV

Per una descrizione dettagliata dell'ODV, si consulti il par. 1.4 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

Il confine fisico dell'ODV coincide con il perimetro fisico del dispositivo mobile. L'ODV non include le applicazioni utente che vengono eseguite sul sistema operativo, ma include i controlli che limitano il comportamento delle applicazioni.

L'ODV fornisce un'interfaccia di programmazione (API) alle applicazioni mobili e consente agli utenti che installano un'applicazione di approvarne o rifiutarne l'installazione in base alle API a cui l'applicazione richiede l'accesso.

L'ODV offre inoltre agli utenti la possibilità di proteggere i dati a riposo, inclusi tutti i dati d'utente e delle applicazioni mobili archiviati nella partizione dati dell'utente, mediante cifratura AES. L'ODV fornisce una protezione speciale a tutte le chiavi crittografiche dell'utente e delle applicazioni memorizzate nell'ODV stesso.

Infine, L'ODV è in grado di interagire con un server MDM al fine di consentire il controllo a livello aziendale della configurazione e del funzionamento del dispositivo, in modo da garantire l'aderenza alle policy aziendali.

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nel cap. 3 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il cap. 7 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Audit di sicurezza**: l'ODV genera record di audit per un'ampia gamma di eventi rilevanti per la sicurezza riguardanti il suo utilizzo e la sua configurazione. L'ODV memorizza tutti i record di audit in file di log e, per prevenirne eventuali modifiche malevole, imposta l'autorizzazione di accesso a tali file rendendoli non disponibili per le applicazioni.

- **Supporto crittografico**: l'ODV include moduli crittografici con algoritmi convalidati CAVP che vengono utilizzati per funzioni crittografiche tra cui: generazione e scambio di chiavi asimmetriche, generazione di chiavi simmetriche, cifratura/decifratura, *hash* crittografico e *keyed-hash message authentication* (HMAC). Queste funzioni sono supportate da opportune funzioni di generazione di bit casuali, derivazione di chiavi, generazione di *salt*, generazione di vettori di inizializzazione, archiviazione sicura delle chiavi e distruzione delle chiavi e dei dati protetti. Queste funzioni crittografiche primitive vengono utilizzate per implementare protocolli di sicurezza come TLS e HTTPS e anche per cifrare i supporti utilizzati dall'ODV (inclusi generazione e protezione delle chiavi per la cifratura dei dati e di altre chiavi).
  L'ODV fornisce i servizi crittografici mediante i seguenti tre moduli crittografici:
  - BoringSSL (spazio dell'utente)
  - Kernel Crypto (spazio del *kernel*)
  - CC engine (TEE e fase di avvio)

- **Protezione dei dati d'utente**: l'ODV controlla l'accesso ai servizi di sistema da parte delle applicazioni installate, inclusa la protezione del Trust Anchor Database. Inoltre, l'ODV applica la cifratura ai dati dell'utente e ad altri dati sensibili in modo che, anche in caso di perdita fisica del dispositivo, tali dati rimangano protetti.

- **Identificazione e autenticazione**: l'ODV supporta una serie di funzionalità relative all'identificazione e all'autenticazione. Ad esclusione di funzioni limitate come effettuare chiamate telefoniche a numeri di emergenza e ricevere notifiche, è necessario che l'utente sblocchi l'ODV immettendo correttamente una password o un fattore di autenticazione biometrico (BAF). Inoltre, anche quando l'ODV è sbloccato, la password deve essere reinserita per poterla modificare. Le password vengono oscurate durante l'inserimento e non possono essere lette sullo schermo dell'ODV. La frequenza di immissione delle password è limitata e, nel caso si verifichi un numero configurabile di errori di immissione, i dati dell'utente vengono cancellati dall'ODV. Inoltre, l'ODV supporta l'uso di certificati X.509v3 per eseguire la convalida dei certificati su connessioni EAP-TLS, TLS e HTTPS.

- **Gestione della sicurezza**: l'ODV fornisce tutte le interfacce necessarie per gestire le funzioni di sicurezza identificate dal TDS nonché altre funzioni comunemente presenti nei dispositivi mobili. Molte di queste funzioni sono disponibili per gli utenti dell'ODV, mentre altre sono limitate agli amministratori che operano tramite una soluzione di Mobile Device Management una volta che l'ODV è stato registrato nel sistema.

- **Protezione del TSF**: l'ODV implementa una serie di funzionalità progettate per proteggersi e garantire così l'affidabilità e l'integrità delle sue funzionalità di sicurezza. L'ODV protegge i dati particolarmente sensibili come le chiavi crittografiche in modo che non siano accessibili o esportabili; fornisce un proprio meccanismo di temporizzazione per garantire la disponibilità di informazioni affidabili sull'orario; impone la protezione in lettura, scrittura ed esecuzione delle pagine di memoria; utilizza la randomizzazione dello spazio degli indirizzi e misure contro gli *overflow* del buffer basati su *stack* per ridurre al minimo il potenziale sfruttamento di difetti delle applicazioni. L'ODV è progettato per proteggersi da modifiche non autorizzate da parte delle applicazioni e per proteggere le applicazioni stesse isolando i rispettivi spazi di indirizzamento.
  L'ODV include anche funzioni di autotest e di controllo dell'integrità del software/firmware in modo da rilevare malfunzionamenti o danneggiamenti. Se un test automatico fallisce, l'ODV non entra in modalità operativa. L'ODV include meccanismi (ovvero la verifica della firma digitale di ogni nuova immagine) che gli consentono di venire aggiornato garantendo al contempo che gli aggiornamenti non introducano modifiche impreviste o malevole nell'ODV. Il controllo della firma digitale si estende anche alla verifica delle applicazioni prima della loro installazione.

- **Accesso all'ODV**: l'ODV può essere bloccato, con oscuramento dello schermo, dall'utente o dopo un periodo di inattività configurabile. In base alla configurazione, l'ODV può anche tentare di connettersi automaticamente alle reti wireless.

- **Percorsi e canali attendibili**: l'ODV supporta i protocolli standard 802.11-2012, 802.1X e EAP-TLS per proteggere i canali di comunicazione tra l'ODV stesso e altri dispositivi di rete attendibili.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] dichiara conformità *exact* ai seguenti Profili di Protezione e pacchetti estesi:

- 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 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati o ricavati per estensione dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2].

Considerando che il TDS dichiara conformità *exact* al Protection Profile for Mobile Device Fundamentals [PPMDF] e al Wireless Local Area Network (WLAN) Clients Extended Package [PPWLANC], sono inclusi tutti i SAR e gli SFR definiti in questo PP e nel relativo EP.

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, gli SFR e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM]. Inoltre, sono state eseguite tutte le attività di garanzia specifiche richieste dal Protection Profile for Mobile Device Fundamentals [PPMDF] e dal Wireless Local Area Network (WLAN) Clients Extended Package [PPWLANC].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS atsec information security GmbH.

L'attività di valutazione è terminata in data 14 dicembre 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 21 dicembre 2021. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS atsec information security GmbH e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "Huawei Mate 40 Pro (M40 pro) with EMUI 11.0" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia definito dai SAR inclusi nel PP [PPMDF], in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 2 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia definito dai SAR inclusi nel PP [PPMDF].

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

Classi e componenti di garanzia		Verdetto
Vulnerability survey	AVA_VAN.1	Positivo

Tabella 2 - Verdetti finali per i requisiti di garanzia

8.2 Attività di garanzia aggiuntive

Il Protection Profile for Mobile Device Fundamentals [PPMDF] e il Wireless Local Area Network (WLAN) Clients Extended Package [PPWLANC] includono attività di garanzia aggiuntive che sono specifiche per il tipo di tecnologia dell'ODV e sono richieste per la conformità *exact* al PP e all'EP.

I Valutatori hanno utilizzato per le attività di garanzia del PP/EP una notazione simile a quella dei componenti delle classi di garanzia CC esistenti. L'obiettivo di queste sotto-attività è quello di determinare se sono soddisfatti tutti i requisiti delle attività di garanzia incluse nel PP/EP.

La Tabella 3 riassume i verdetti finali di ciascuna attività di garanzia del PP/EP svolta dall'LVS.

Attività di garanzia del PP/EP		Verdetto
ASE: Security Target evaluation	ASE_MDFPP.1	Positivo
	ASE_WLANEP.1	Positivo
AGD: Guidance documents	AGD_MDFPP.1	Positivo
	AGD_WLANEP.1	Positivo
ALC: Life cycle support	ALC_MDFPP.1	Positivo
ATE: Tests	ATE_MDFPP.1	Positivo
	ATE_WLANEP.1	Positivo
AVA: Vulnerability assessment	AVA_MDFPP.1	Positivo

Tabella 3 - Verdetti finali per le attività di garanzia del PP/EP

8.3 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "Huawei Mate 40 Pro (M40 pro) with EMUI 11.0" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le ipotesi e le Politiche di

Sicurezza dell'Organizzazione descritte rispettivamente nel par. 3.2 e nel par. 3.3 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella sua configurazione valutata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'inizializzazione, all'installazione e all'utilizzo sicuro del prodotto, in accordo con la documentazione di guida fornita con l'ODV ([CCG]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

L'hardware dell'ODV viene consegnato ai rivenditori dai quali può essere acquistato dagli utenti.

Quando l'utente riceve il dispositivo, deve assicurarsi che la confezione sia intatta e che l'etichetta di chiusura non sia rotta. Per ulteriori dettagli si faccia riferimento al par. 12.1 ("Security Acceptance") della documentazione di guida [CCG].

9.2 Identificazione dell'ODV

Gli utenti devono controllare il numero del modello hardware e la versione software accedendo a *Impostazioni* > *Info telefono* nell'interfaccia utente (UI) dell'ODV.

9.3 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'aggiornamento dell'ODV devono essere eseguiti dagli utenti secondo le istruzioni riportate nel seguente documento:

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

La documentazione di guida [CCG] fornisce informazioni sull'utilizzo sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS].

10 Appendice B – Configurazione valutata

L'oggetto di valutazione (ODV) è il prodotto "Huawei Mate 40 Pro (M40 pro) with EMUI 11.0", sviluppato dalla società Huawei Device Co., Ltd.

La configurazione valutata dell'ODV comprende il dispositivo mobile Huawei M40 Pro (Numero di modello: NOH-AN00, come riportato in Tabella 1) e la documentazione di guida elencata nel par. 9.3.

I dati identificativi del software per i dispositivi valutati sono i seguenti:

- Versione *kernel*: 4.14
- Numero di *build*: 11.0.0.165

L'ODV include una modalità Common Criteria (o "CC Mode") che un amministratore può attivare mediante un sistema di Mobile Device Management (MDM). Quando la modalità CC viene abilitata, l'ODV esegue le seguenti azioni:

- L'ODV abilita la proprietà "CC Mode" a livello di sistema Android.
- L'ODV esegue gli autotest dei tre moduli crittografici (Kernel Crypto, BoringSSL, CC engine) dopo l'avvio del sistema e registra gli eventi di sicurezza nei log di audit.
- I log di audit degli eventi di sicurezza vengono archiviati nella memoria interna per evitare di perderli a seguito di un ciclo di alimentazione.
- L'ODV cancella tutti i dati protetti nel caso in cui si raggiunga il numero massimo di tentativi di autenticazione falliti.
- Gli utenti non possono utilizzare la scheda NM (Nano Memory) in modalità CC.

10.1 Ambiente operativo dell'ODV

I seguenti componenti hardware/software non-ODV sono richiesti nell'ambiente operativo per consentire il corretto funzionamento dell'ODV (si veda il par. 1.4.2 del Traguardo di Sicurezza [TDS]):

- Access point 802.11-2012 per connessione WLAN.
- Server per l'autenticazione reciproca EAP-TLS e la generazione della Pairwise Master Key (PMK).
- Reti dati mobili per la connettività di rete.
- Server MDM per il controllo amministrativo dell'ODV.

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia definito dai SAR inclusi nel PP [PPMDF], tali attività non prevedono l'esecuzione di test funzionali da parte del Fornitore, ma soltanto test funzionali indipendenti e test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

Per le attività di test, i Valutatori hanno ricevuto dal Fornitore un dispositivo Huawei M40 Pro.

Il Fornitore ha anche messo a disposizione ambienti di sviluppo e di test per eseguire i casi di test richiesti dal PP [PPMDF] e dall'EP [PPWLANC]. In particolare, i Valutatori hanno ricevuto una versione per sviluppatori del dispositivo (versione pre-commerciale, identica alla versione di rilascio) e alcune applicazioni Android da installare sul dispositivo.

I Valutatori hanno visitato un sito di sviluppo in Germania per eseguire test con il supporto del Fornitore. I Valutatori hanno configurato l'ODV e predisposto l'ambiente di test seguendo le indicazioni fornite nella documentazione di guida [CCG].

I Valutatori hanno verificato che l'ODV e l'ambiente così configurati fossero coerenti con i requisiti del Traguardo di Sicurezza [TDS].

11.2 Test funzionali ed indipendenti svolti dai Valutatori

Prima di iniziare l'attività di test, i Valutatori hanno verificato che l'ambiente di test fosse stato predisposto in maniera appropriata e che l'ODV fosse configurato correttamente.

I Valutatori hanno eseguito test per verificare che il comportamento dell'ODV fosse coerente con quanto specificato nel Traguardo di Sicurezza [TDS] e nella documentazione di guida [CCG]. I Valutatori hanno altresì eseguito tutti i test richiesti descritti nei PP [PPMDF], nell'EP [PPWLANC] e nelle Technical Decision del NIAP applicabili elencate nel cap. 2 del Traguardo di Sicurezza [TDS].

I test CAVS per la conferma della corretta implementazione dei meccanismi crittografici sono stati eseguiti su una versione dell'ODV appositamente predisposta nel laboratorio del Fornitore e osservati dai Valutatori e dai certificatori dell'OCSI collegati in videoconferenza. Durante questa sessione di test, i Valutatori hanno verificato che sul dispositivo di test fosse installato il sistema con lo stesso numero di *build* 11.0.0.165 (eseguendo il comando "adb device" sul dispositivo). Il Fornitore ha confermato che il dispositivo di test è stato modificato unicamente per consentire l'accesso ad alcune interfacce interne ai programmi esterni utilizzati per i test CAVS, mentre l'implementazione dei meccanismi crittografici è rimasta invariata rispetto alla versione dell'ODV.

Tutti i test eseguiti dai valutatori, inclusi i test CAVS, sono stati completati con successo, ovvero hanno fornito risultati coerenti con i risultati attesi.

11.3 Analisi delle vulnerabilità e test di intrusione

I Valutatori hanno consultato fonti di informazioni di dominio pubblico, tra cui Common Vulnerabilities and Exposures (CVE), Exploit Database, Packet Storm e SecurityFocus, per identificare potenziali vulnerabilità note dell'ODV. I Valutatori hanno anche controllato i bollettini sulla sicurezza di Android e le pubblicazioni sulla sicurezza sul sito Web del Fornitore.

I Valutatori hanno utilizzato per la ricerca parole chiave scelte con cura, in modo tale da essere sufficientemente generiche da coprire tutti gli argomenti di interesse e sufficientemente specifiche da eliminare elementi non correlati (ad es., "Huawei Mate 40 Pro", "M40 Pro", "EMUI 11.0", "Huawei Kirin 9000", and "Android 10.0").

Sulla base delle informazioni raccolte, i Valutatori hanno compilato un elenco di vulnerabilità potenzialmente applicabili all'ODV. I Valutatori hanno eseguito un'analisi di tutte le vulnerabilità elencate e non sono stati in grado di identificare potenziali vulnerabilità applicabili all'ODV che non fossero già state adeguatamente mitigate dal Fornitore. Pertanto, i Valutatori non hanno riscontrato la necessità di ulteriori test.

I Valutatori hanno quindi concluso che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state identificate vulnerabilità sfruttabili o residue.