National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 14 - Spring

Report Number: CCEVS-VR-VID11444-2024
Dated: May 6, 2024
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Fernando Guzman
Patrick Mallett
Jerome Myers
Dave Thompson

The Aerospace Corporation

Farid Ahmed
Kurt Bahnsen

Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

James Arnold
Tammy Compton
Rizheng Sun
Nick Van

Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of *Samsung Galaxy Devices on Android 14 - Spring* solution provided by Samsung Electronics Co., Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in May 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended compliant, and meets the assurance requirements of the following Protection Profiles and Functional Packages (collectively referred to in this document as the CRITERIA):

- Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.3, (PP_MDF_V3.3)
- PP-Module: PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, (MOD_VPNC_V2.4)
- PP-Module: PP-Module for Bluetooth, Version 1.0, (MOD_BT_V1.0)
- PP-Module for WLAN Client, Version 1.0 (MOD_WLANC_V1.0)
- PP-Module: collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module], Version 1.1, September 12, 2022 (MOD_CPP_BIO_V1.1)
- Functional Package: Functional Package for Transport Layer Security (TLS), Version 1.1, (PKG_TLS_V1.1)

The Target of Evaluation (TOE) is the *Samsung Galaxy Devices on Android 14 - Spring*.

The TOE has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). The validation team concludes that the testing laboratory's

findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 14 - Spring Security Target, Version 0.5, April 24, 2024 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Samsung Galaxy Devices on Android 14 - Spring (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Mobile Device Fundamentals, Biometric enrollment and verification – for unlocking the device, Bluetooth, Virtual Private Network (VPN) Clients, and WLAN Clients, Version 1.0, 24 October 2022 (CFG_MDF-BIO-BT-VPNC-WLANC_V1.0) which includes the Base PP: Mobile Device Fundamentals, Version 3.3, 12 September 2022 (MDF33) with the collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module], Version 1.1, 12 September 2022 (BIO11); the PP-Module for Bluetooth, Version 1.0, 15 April 2021 (BT10); the PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24); the PP-Module

Item	Identifier
	for WLAN Clients, Version 1.0, 31 March 2022 (WLANC10); plus the Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 (PKGTLS11)
ST	Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 14 - Spring Security Target, Version 0.5, April 24, 2024
Evaluation Technical Report	Evaluation Technical Report for Samsung Galaxy Devices on Android 14 - Spring, Version 1.0, May 6, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
Sponsor	Samsung Electronics Co., Ltd.
Developer	Samsung Electronics Co., Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Fernando Guzman, Patrick Mallett, Jerome Myers, and Dave Thompson of The Aerospace Corporation and Farid Ahmed and Kurt Bahnsen of Johns Hopkins University Applied Physics Lab.

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is the *Samsung Galaxy Devices on Android 14 - Spring*.

3.1 TOE Description

The TOE is a mobile device based on Android 14 with a built-in IPsec VPN client and modifications made to increase the level of security provided to end users and enterprises. The TOE is intended for use as part of an enterprise mobility solution providing mobile staff with enterprise connectivity.

The TOE includes a Common Criteria mode (or "CC mode") that an administrator can invoke using a Mobile Device Management (MDM) solution. The TOE must meet the following prerequisites in order for an administrator to transition the TOE to and remain in the CC configuration.

- Require a boot and device lock password (swipe, PIN, pattern, or accessibility (direction). (Screen locks are not allowed)). Acceptable biometrics vary with the device.
- The maximum password failure retry policy should be less than or equal to 30.
- A screen lock password is required to decrypt data during boot.
- Revocation checking must be enabled.

- Security and audit logging must be enabled.
- External storage must be encrypted.
- Developer debugging must be disabled.

When CC mode has been enabled, the TOE behaves as follows:

- The TOE sets the system wide Android CC mode property to be enabled.
- The TOE prevents loading of custom firmware/kernels and requires that all updates occur through FOTA.
- The TOE utilizes ACVP/CAVP approved cryptographic ciphers for TLS.

The TOE includes the ability to create separate profiles as part of the Knox Platform. A profile provides a way to segment applications and data into separate areas on the device, such as a personal area and a work area, each with its own separate apps, data and security policies. For this effort, the TOE was evaluated both with and without profiles. Thus, the evaluation includes several Knox-specific claims that apply when these profiles are created. The TOE also requires loaded applications to be implemented utilizing the NIAPSEC library.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The TOE supports the use of an MDM solution, which enables the Enterprise to watch, control and administer all deployed mobile devices, across multiple mobile service providers as well as facilitate secure communications through a VPN. However, this evaluation did not include an MDM agent nor server. The combination of the TOE and an MDM provides a secure mobile environment that can be managed and controlled by the environment and reduces the risks inherent in any mobile deployment.

Data on the TOE is protected through the implementation of Samsung File-Based Encryption (FBE) that utilizes ACVP/CAVP certified cryptographic algorithms to encrypt device storage. This functionality is combined with a number of on-device policies including local wipe, remote wipe, password complexity, automatic lock and privileged access to security configurations to prevent unauthorized access to the device and stored data.

The Knox Platform for Enterprise provides a set of flexible deployment options for work environments. With Knox Platform for Enterprise, it is possible to segment the device into two separate areas, by convention called the personal profile and the work profile. In creating a work profile, the Enterprise establishes a completely separate workspace, with its own authentication, applications and services, and ensure they are kept separate from anything the user may do in the personal profile. Another mechanism for deployment is Knox Separated Apps, a folder where the Enterprise can isolate a group of applications from the rest of the device, restricting access to shared information, while maintaining seamless access to the isolated applications for the user.

The Samsung Knox Software Development Kit (SDK) builds on top of the existing Android security model by expanding the current set of security configuration options to more than 600 configurable policies and including additional security functionality such as application allow and block listing.

3.4 Physical Boundaries

The TOE is a multi-user capable mobile device based on Android 14 that incorporates the Samsung Knox SDK. 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 includes an IPsec VPN client integrated into the firmware (as opposed to a downloadable application). Within an Enterprise environment, the Enterprise can manage the configuration of the mobile device, including the VPN client, through a compliant device management solution.

The TOE communicates and interacts with 802.11-2012 Access Points and mobile data networks to establish network connectivity, and through that connectivity interacts with MDM servers that allow administrative control of the TOE.

4 Security Policy

This section summaries the security functionality of the TOE:

4.1 Security audit

The TOE generates logs for a range of security relevant events. The TOE stores the logs locally so they can be accessed by an administrator or they can be exported to an MDM.

4.2 Cryptographic support

The TOE includes multiple cryptographic libraries with ACVP certified algorithms for a wide range of cryptographic functions including the following: asymmetric key generation and establishment, symmetric key generation, encryption/decryption, cryptographic hashing and keyed-hash message authentication. 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, EAP-TLS, IPsec, and HTTPS and to encrypt the media (including the generation and protection of data and key encryption keys) used by the TOE. Many of these cryptographic functions are also accessible as services to applications running on the TOE.

4.3 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. The functionality provided by work profiles and Knox Separated Apps enhance the security of

user data by providing an additional layer of separation between different categories of apps and data while the device is in use. The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

4.4 Identification and authentication

The TOE supports a number of features related to identification and authentication. From a user perspective, except for making phone calls to an emergency number, a password or Biometric Authentication Factor (BAF) must be correctly entered to unlock the TOE. In addition, even when the TOE is unlocked the password must be re-entered to change the password or re-enroll the biometric template. 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 will be wiped to protect its contents. Passwords can be constructed using upper and lower case characters, numbers, and special characters and passwords between 4 and 16 characters are supported. The TOE can also be configured to utilize a fingerprint biometric authentication factor, to unlock the device (Note: This only works after the primary authentication method, password, has been entered after the device powers on).

The TOE can also serve as an 802.1X supplicant and can use X.509v3 and validate certificates for EAP-TLS, TLS and IPsec exchanges. The TOE can also act as a client or server in an authenticated Bluetooth pairing.

4.5 Security management

The TOE provides all the interfaces necessary to manage the security functions (including the VPN client) identified in the 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 removes all MDM policies and disables CC mode.

4.6 Protection of the TSF

The TOE implements self-protection mechanisms 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 (e.g., for log accountability). It 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 isolating the address spaces of applications from one another, to protect those applications.

The TOE includes functions to perform self-tests and software/firmware integrity checking so that it might detect when it is failing or may be corrupt. If any self-tests fail, the TOE will not go into an operational mode. It also 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.

4.7 TOE access

The TOE can be locked, obscuring its display, by the user or after a configured interval of inactivity. The TOE also has the capability to display an advisory message (banner) when users unlock the TOE for use.

The TOE is also able to attempt to connect to wireless networks, when so configured.

4.8 Trusted path/channels

The TOE supports the use of 802.11-2012, 802.1X, EAP-TLS, TLS, HTTPS and IPsec to secure communications channels between itself and other trusted network devices.

5 Assumptions & Clarification of Scope

Assumptions
The Security Problem Definition, including the assumptions, may be found in the following documents:

- Mobile Device Fundamentals, Version 3.3, 12 September 2022 (MDF33)
- collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module], Version 1.1, 12 September 2022 (BIO11)
- PP-Module for Bluetooth, Version 1.0, 15 April 2021 (BT10)
- PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24)
- PP-Module for WLAN Clients, Version 1.0, 31 March 2022 (WLANC10)
- Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 (PKGTLS11)

That information has not been reproduced here and should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the CRITERIA as described for this TOE in the Security Target and in Section 1 of this document. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope
All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the CRITERIA and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Mobile Device models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the CRITERIA and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Samsung Android 14 on Galaxy Devices Administrator Guide, Version 9.0.3, April 24, 2024
- Samsung Knox VPN JSON Message Definition (https://docs.samsungknox.com/dev/knox-sdk/features/mdm-providers/vpn/knox-vpn-json-message-definition/),
- Android Developers references from the AGD
    - setSecurityLoggingEnabled (https://developer.android.com/reference/android/app/admin/DevicePolicyManager#setSecurityLoggingEnabled(android.content.ComponentName,%20boolean),
    - onSecurityLogsAvailable (https://developer.android.com/reference/android/app/admin/DeviceAdminReceiver.html#onSecurityLogsAvailable(android.content.Context,%20android.content.Intent)),
    - retrieveSecurityLogs (https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html#retrieveSecurityLogs(android.content.ComponentName))
    - VpnService (https://developer.android.com/reference/android/net/VpnService)
    - All of the references in AGD Section 6.1, Table 15

- References in AGD Sections 6.2 Bluetooth APIs, 6.3 TLS/HTTPS APIs, 6.4 Certificate Pinning, 6.5 IPsec VPN APIs, 6.7 Secure Development Practices,
- NIST Special Publication 8090-63B, Section 5.1.1, Memorized Passwords, https://pages.nist.gov/800-63-3/sp800-63b.html#memsecret, which is referenced in the AGD.

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Samsung Galaxy Devices on Android 14 - Spring, Version 0.2, April 24, 2024 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the CRITERIA, including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The model numbers of the mobile devices used during evaluation testing are as follows:

Device Name	Chipset Vendor	SoC	Arch	Kernel	Build Number
Galaxy S24 Ultra 5G	Qualcomm	Snapdragon 8 Gen 3	ARMv8	6.1	UP1A.231005.007
Galaxy S24 5G	Samsung	Exynos 2400	ARMv8	6.1	UP1A.231005.007
Galaxy S23 Ultra 5G	Qualcomm	Snapdragon 8 Gen 2 Mobile Platform	ARMv8	5.15	UP1A.231005.007
Galaxy S22 Ultra 5G	Samsung	Exynos 2200	ARMv8	5.10	UP1A.231005.007
Galaxy S22 5G	Qualcomm	Snapdragon 8 Gen 1 Mobile Platform	ARMv8	5.10	UP1A.231005.007
Galaxy S21 Ultra 5G	Samsung	Exynos 2100	ARMv8	5.4	UP1A.231005.007
Galaxy S21 Ultra 5G	Qualcomm	Snapdragon 888	ARMv8	5.4	UP1A.231005.007

Device Name	Chipset Vendor	SoC	Arch	Kernel	Build Number
Galaxy XCover6 Pro	Qualcomm	Snapdragon 778G	ARMv8	5.4	UP1A.231005.007
Galaxy Tab Active5	Samsung	Exynos 1380	ARMv8	5.15	UP1A.231005.007

Evaluated Devices

In addition to the evaluated devices, the following are claimed as equivalent:

Evaluated Device	SoC	Equivalent Devices	Differences
Galaxy S24 Ultra 5G	Snapdragon 8 Gen 3	Galaxy S24+ 5G	S24 Ultra > S24+ > S24 in terms of display size
		Galaxy S24 5G	
Galaxy S24 5G	Exynos 2300	Galaxy S24+ 5G	S24 Ultra > S24+ > S24 in terms of display size
Galaxy S23 Ultra 5G	Snapdragon 8 Gen 2	Galaxy S23+ 5G	S23 Ultra > S23+ > S23 in terms of display size
		Galaxy S23 5G	
		Galaxy Z Fold5 5G	Z Fold5 5G & Z Flip5 5G have power button fingerprint sensor
		Galaxy Z Flip5 5G	
		Galaxy Tab S9 Ultra	Tab S9 devices are tablets (no voice calling) with S Pen
		Galaxy Tab S9+	Tab S9 Ultra > Tab S9+ > Tab S9 in terms of display size
		Galaxy Tab S9	Tab S9 Ultra & Tab S9+ have under screen image fingerprint sensor Tab S9 has power button fingerprint sensor
		Galaxy S23 5G	
Galaxy S22 Ultra 5G	Exynos 2200	Galaxy S22+ 5G	S22 Ultra > S22+ > S22 in terms of display size
		Galaxy S22 5G	S22+ & S22 devices have S21 Ultra 5G Wi-Fi chip
		Galaxy S23 FE	
		Galaxy S22 5G	S22+ & S22 devices have S21 Ultra 5G Wi-Fi chip
Galaxy S22 5G	Snapdragon 8 Gen 1	Galaxy S22 Ultra 5G	S22 Ultra > S22+ > S22 in terms of display size
		Galaxy S22+ 5G	S22+ & S22 devices have S21 Ultra 5G Wi-Fi chip
		Galaxy Tab S8 Ultra	Tab S8 devices are tablets (no voice calling) with S Pen
		Galaxy Tab S8+	Tab S8 Ultra > Tab S8+ > Tab S8 in terms of display size
		Galaxy Tab S8	Tab S8 Ultra & Tab S8+ have under screen image fingerprint sensor Tab S8 has power button fingerprint sensor
		Galaxy Z Flip4 5G	Z Flip4 & Z Fold4 have 2 displays & folding display
		Galaxy Z Fold4 5G	Z Flip4 & Z Fold4 have power button fingerprint sensor
		Galaxy S23 FE	
		Galaxy S22+ 5G	S22+ & S22 devices have S21 Ultra 5G Wi-Fi chip
		Galaxy Tab S8 Ultra	Tab S8 devices are tablets (no voice calling) with S Pen
		Galaxy Tab S8+	Tab S8 Ultra > Tab S8+ > Tab S7 in terms of display size
		Galaxy Tab S8	Tab S8 Ultra & Tab S8+ have under screen image fingerprint sensor Tab S8 has power button fingerprint sensor
		Galaxy Z Flip4 5G	Z Flip4 & Z Fold4 have 2 displays & folding display
		Galaxy Z Fold4 5G	Z Fold4 > Z Flip4 in terms of display size

Evaluated Device	SoC	Equivalent Devices	Differences
Galaxy S21 Ultra 5G	Exynos 2100	Galaxy S21+ 5G	S21 Ultra > S21+ > S21 > S21 FE in terms of display size
		Galaxy S21 5G	S21+ & S21 devices have S20+ 5G Wi-Fi chip
Galaxy S21 Ultra 5G	Snapdragon 888	Galaxy S21+ 5G	S21 Ultra > S21+ > S21 > S21 FE in terms of display size
		Galaxy S21 5G	S21+ & S21 devices have S20+ 5G Wi-Fi chip
		Galaxy S21 5G FE	Z Fold3 5G & Z Flip3 5G have 2 displays & folding display
		Galaxy Z Fold3 5G	Z Fold3 5G & Z Flip3 5G have power button fingerprint sensor
		Galaxy Z Flip3 5G	Z Fold3 & Z Flip3 have S22 Ultra Wi-Fi chip
Galaxy XCover6 Pro	Snapdragon 778G	Galaxy Tab Active4 Pro	Tab Active4 Pro is tablet and have bigger screen size
Galaxy Tab Active5	Exynos 1380	N/A	

Equivalent Devices

The Evaluated Configuration is the above hardware and software when configured in accordance with the guidance provided in the Documentation section of this report.

9 Results of the Evaluation

The results of executing required assurance actions are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined that the Samsung Galaxy Devices on Android 14 - Spring TOE is CC Part 2 Extended compliant and meets the Security Assurance Requirements (SARs) contained in the CRITERIA.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Samsung Galaxy Devices on Android 14 - Spring products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides

the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the CRITERIA related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the CRITERIA and recorded the results in a Test Report, summarized in the AAR.

The validator reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes

a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 24 Apr 2024 with the following search terms: “Galaxy S24”, “Galaxy S24+”, “SM-S928”, “SM-S926”, “SM-S921”, “Galaxy S23”, “Galaxy S23+”, “SM-S918”, “SM-S916”, “SM-S911”, “SM-S711”, “Galaxy S22”, “Galaxy S22+”, “SM-G908”, “SM-G906”, “SM-G901”, “Galaxy S21”, “Galaxy S21+”, “SM-G998”, “SM-G996”, “SM-G991”, “SM-G990”, “Galaxy XCover6 Pro”, “SM-G736”, “Galaxy Tab Active5”, “SM-X300”, “SM-X306”, “SM-X308”, “Galaxy Z Fold5”, “SM-F946”, “Galaxy Z Flip5”, “SM-F731”, “Galaxy Tab S9”, “SM-X916”, “SM-X910”, “SM-X716”, “SM-X710”, “Galaxy Tab S9+”, “SM-X818”, “SM-X816”, “SM-X810”, “Galaxy Tab S8”, “SM-X900”, “SM-X708”, “SM-X706”, “SM-X700”, “Galaxy Tab S8+”, “SM-X808”, “SM-X806”, “SM-X800”, “Galaxy Z Flip4”, “SM-F721”, “Galaxy Z Fold4”, “SM-F936”, “Galaxy Z Fold3”, “SM-F926”, “Galaxy Z Flip3”, “SM-F711”, “Galaxy Tab Active4”, “SM-T636”, “SM-T638”, “SM-T630”, “Knox”, “BoringSSL”, “strongswan”, “charon”, “Android”, "SCrypto", "Samsung Crypto", "Samsung Kernel Crypto", "Exynos", and "Qualcomm Snapdragon".

The validator reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

All validator comments and recommendations are adequately addressed in the Assumptions and Clarification of Scope section.

11 Security Target

The Security Target is identified as: *Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 14 - Spring Security Target, Version 0.5, April 24, 2024*.

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Mobile Device Fundamentals, Version 3.3, 12 September 2022 (MDF33).

[5] collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module], Version 1.1, 12 September 2022 (BIO11).

[6] PP-Module for Bluetooth, Version 1.0, 15 April 2021 (BT10).

[7] PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24).

[8] PP-Module for WLAN Clients, Version 1.0, 31 March 2022 (WLANC10).

[9] Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 (PKGTLS11).

[10] Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 14 - Spring Security Target, Version 0.5, April 24, 2024 (ST).

[11] Assurance Activity Report for Samsung Galaxy Devices on Android 14 - Spring, Version 0.2, April 24, 2024 (AAR).

[12] Detailed Test Report for Samsung Galaxy Devices on Android 14 - Spring, Version 0.2, April 24, 2024 (DTR).

[13] Evaluation Technical Report for Samsung Galaxy Devices on Android 14 - Spring, Version 0.2, April 24, 2024 (ETR).

[14] Samsung Android 14 on Galaxy Devices Administrator Guide, Version 9.0.3, April 24, 2024 (AGD). Includes online references and embedded documents.