ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Samsung Electronics Co., Ltd. Samsung Galaxy S6 SOCOM (MDFPP20)

Maintenance Update of Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 6 (MDFPP20)

Maintenance Report Number: CCEVS-VR-VID10726-2016

Date of Activity: 12 October 2016

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;

Impact Analysis Report for Samsung Electronics Co., Ltd. Samsung Galaxy S6 SOCOM (MDFPP20), Version 1.0, September 29, 2016

Documentation reported as being updated:

- https://www2.samsungknox.com/knoxportal/files/Galaxy%20S6%20LTE%28G920T%29%20Application%20List_0.pdf

Assurance Continuity Maintenance Report:

Gossamer Security Solutions, on behalf of Samsung Electronics Co., Ltd., submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 3 October 2016. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

The IAR identifies the changes to the TOE, which include support for USB On-The-Go (OTG) and charging for SOCOM-provided USB hub, additional network drivers and support for additional USB network connectivity, blocking of SIM card removed notifications, and the removal of a specific set of pre-installed apps as well as the installation of the Device Protection Manager and the Knox License Activation Tool. In addition, patches for software updates for vulnerabilities are prepared as required by various policies and MDF requirements, which constitute the only security-related changes to the TOE. Because this device is not intended to use a SIM card, the updates are provided directly from the vendor and is not impacted by carrier delays to deploy patches. The rest of the features listed above are new non-security features that were considered to be outside the scope of the MDF evaluation.

Only the application list in the website listed above was new and added, as well as the IAR.

Note that Samsung continually tracks bugs, vulnerabilities, and other defects reported in the public domain and at the time of this report there are no known outstanding security-related vulnerabilities in the TOE.

Changes to TOE:

The specific device in question is a new variation of the T-Mobile S6 device (SM-G920T) specifically for SOCOM use. The device is identical hardware but with a modified system image. No documentation updates were made for the new device except for the addition of the Application List in the website above. In general, the addition of network support for USB Network Interface Cards (NICs) and the removal and addition of pre-installed apps were the only two major areas where changes were made to the device. The changes and effects of additional features and support are summarized below.

1. USB support and notifications

Security Consideration	Assessment
Support for USB OTG and Charging for SOCOM-provided USB hub (based on USB ID). When this type of USB hub is plugged in (as noted by the USB ID), charging and USB port access will be simultaneously enabled.	This is not security relevant because the claimed and tested MDF functionality remains the same.
• Additional Network Drivers and support for additional USB network connectivity o Multiple, concurrent Ethernet connection support and APIs to control them o Support for PPPD including in all added components o Support for CDC ECM, ASIX and RNDIS_Host modes	The addition of driver support does not affect the security functionality of the device as the claimed and tested MDF functionality remains the same.
SIM card removed notification is blocked (i.e. the device will not show the message when no SIM is inserted)	This is not security relevant because the claimed and tested MDF functionality remains the same.

2. Pre-installed apps

Security Consideration	Assessment
List of pre-installed apps from the G920T device removed	Pre-installed apps are provided by device manufacturers, OS developers, and mobile carriers. They provide capabilities outside of scope and do not provide security functionality mandated by the MDF PP.

	Therefore, the removal of these pre-installed apps does not affect the original assurance of the product.
Installation of Device Protection Manager app -- an MDM Agent providing the API access for the additional functionality requested related to networking	MDM Agents are outside the scope of an MDF PP evaluation and are evaluated separately. Original assurance is maintained.
Knox License Activation Tool – a licensing tool for offline activation of the licenses required for the features required by SOCOM	The Knox License Activation Tool is a pre-installed app. Pre-installed apps are provided by device manufacturers, OS developers, and mobile carriers. They provide capabilities outside of scope and do not provide security functionality mandated by the MDF PP. Because AVA_VAN.1 limits the scope of vulnerability search activities, the original assurance of the product is not affected.

3. General Security Updates

Security Consideration	Assessment
The devices (both the existing devices and the SOCOM device) receive regular updates to maintain the overall security of the system as expected under a Common Criteria evaluation. Samsung works with Google to create update packages on a monthly basis for deployment (this is the SMR listed below). Samsung reviews the CVE database and prepares patches for applicable vulnerabilities on a regular basis and adds these into the SMRs for deployment during these updates.	This is consistent with all applicable NIAP policies and MDF requirements related to vulnerabilities. Because a SIM card is not utilized and carrier delays do not impact the deployment of these updates (the updates are direct from the vendor), original assurance is maintained.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found them all to be minor.

In addition, the mobile device vendor reported having conducted a vulnerability search update that located no new vulnerabilities up to the end of the previous month as reflected by update newsletters by the platform and mobile device vendors. Further, it was also reported that the

Vendor did regression testing and that the changes, collectively, had no security impact on the TOE.

Therefore, CCEVS agrees that the original assurance is maintained for the product.