



**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**  
**ASSURANCE CONTINUITY MAINTENANCE REPORT FOR**

---

**BlackBerry SecuSUITE Client v4.0 and CACI SteelBox v4.0 (ASPP13/PKGTLS11/VVoIPASEP10)**  
**Maintenance Report Number:** CCEVS-VR-VID10993-2021

**Date of Activity:** 10 February 2021

**References:**

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 3.0, September 12, 2016

NIAP Policy #12 “Acceptance Requirements of a product for NIAP Evaluation.” March 20, 2013

Common Criteria document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements” Version 1, February 2004

Protection Profile for Application Software, Version 1.3, 1 March 2019 (ASPP13)

Impact Analysis Report for BlackBerry SecuSUITE Client v4.0 Revision 1.1 February 4, 2021

SecuSUITE Client (ASPP13/PKGTLS11/VVoIPASEP10) Security Target Version 0.7 January 30, 2021

Common Criteria Configuration Guide BlackBerry SecuSUITE 4.0 Version 1.3 January 30, 2020

**Affected Evidence:**

BlackBerry SecuSUITE Client v4.0 and CACI SteelBox v4.0 (ASPP13/PKGTLS11/VVoIPASEP10) Security Target Version 0.9 February 4, 2021

Common Criteria Configuration Guide BlackBerry SecuSUITE 4.0 CACI SteelBox 4.0 Version 1.5 January 26, 2021

**Updated Developer Evidence:**

The TOE has been revised to add a rebranded client named CACI Steelbox 4.0 client. The original application remains unchanged except for a security patch. The code with the security patch was used as a base for the Steelbox client

### Description of ASE Changes:

The CACI Steelbox client was developed by BlackBerry. There is no contribution from CACI the development and build process of the application binaries (aside that they have provided the splash screen graphics). The resulting binaries get the same release numbers that are coming out of the same BlackBerry development and build process and CACI does not have any access to the BlackBerry code base. CACI is a partner and distribution channel for BlackBerry.

### Changes to TOE:

SteelBox client releases are build based on the same code base and at the same time as the SecuSUITE client releases. There are only a few adaptations in place that take care of the different text and graphical assets that are used and that introduce the unavoidable differences mentioned below to make it a different/separate product.

### Assurance Continuity Maintenance Report:

Gossamer submitted an Impact Analysis Report (IAR) on behalf of BlackBerry Limited to add a rebranded client named CACI Steelbox 4.0 client. The original application remains unchanged except for a security patch. The code with the security patch was used as a base for the Steelbox client.

The changes are summarized in the tables below.

1. There are several new features that are somewhat related to the SFRs but no not directly impact the requirements.

New Feature Description	Assessment
Product specific Package/Bundle ID - Steelbox clients use their own unique package id/ bundle ID	As the Steelbox client is deployed as a separate product distributed by CACI, the Android and iOS clients need their own package/bundle ID to which they are associated in the Apple App Store and Google Play. The package/bundle ID is related to the publishing process only and has no functional impact to the clients. It could be seen as impacting the ASPP13: FPT_TUD_EXT.2.1. This requires applications to be packaged as required by the platform. In this case, the rebranded application is packaged as an APK or IPA as required by the platforms. No security features are impacted as the rebranded product is bundled in the same manner as the original TOE.
Client signature - Steelbox clients are signed with separate CACI specific developer signing keys	As the Android/iOS Steelbox clients are deployed as separate products distributed by CACI as developer of the apps, the app publishing processes require separate developer specific signing keys. The application signing follows the same processes as for the SecuSUITE Android and iOS clients. This could be seen as impacting ASPP13: FPT_TUD_EXT.1.4 which requires applications to be signed. In this case, the platform vendors require signatures and the standard is the same for all applications. Hence, the rebranded applications meets the same standard as the original application.

2. Several non-security features have been added. See the following table for an analysis of each.

New Feature Description	Assessment
Splash Screen - Splash Screen has been replaced in rebranded client	This has no impact on the requirements. It simply projects the new client name to the user.
Few text assets replaced to adapt the client to the Steelbox product branding such as <ul style="list-style-type: none"> <li>• Product name replaced</li> <li>• EULA text replaced</li> <li>• CACI/Steelbox branded “About screen”</li> </ul>	This has no impact on the requirements. It is just client name related information and not related to any product function (security or non-security).
Graphical assets have been replaced such as <ul style="list-style-type: none"> <li>• Application icon</li> <li>• Status bar icons (connected/not connected)</li> </ul>	This has no impact on the requirements. It is just client name related information and not related to any product function (security or non-security).
Push notifications - Configuration changes related to the Push notification Services (Apple Push Notification Service, Google Firebase Cloud Messaging). Related configurations had to be adapted to the separate product flavors (use of separate push IDs and push tokens etc.).	Push notification services are associated to specific clients and hence the related configs had to be adapted to match the updated product configuration. Push notification services are used through the related platform APIs in the same way the services are used by the BlackBerry SecuSUITE client. The client already requested notification access so this remains unchanged. This does not impact any product function (security or non-security).

**Description of Regression Testing:**

BlackBerry has performed regression testing on the SteelBox client.

Since BlackBerry is responsible for the developing the SteelBox client, all client testing that is performed for SecuSUITE clients applies also to the SteelBox client. For regression, all SecuSUITE and Steelbox client releases are tested in parallel with the BlackBerry test-automation system. This is a (self-developed) system that executes automatically a number of functional, security, stability and duration tests (Client enrollment, Call set-up and tear down). That way BlackBerry is able to execute hundreds (and if needed thousands) of client enrollment and call tests overnight even with daily builds.

Additionally, release candidates of the SecuSUITE and Steelbox clients are used in beta testing program by BlackBerry staff to find any defects in the daily use of the solution.

**Vulnerability Assessment:**

Gossamer searched the Internet for potential vulnerabilities in the TOE using the two web sites listed below.

- National Vulnerability Database (NVD, <https://nvd.nist.gov/>)

- Vulnerability Notes Database (<http://www.kb.cert.org/vuls/>)

Gossamer selected the 24 search key words based upon the vendor name, the product name, and key platform features the product leverages. The search terms used were:

- webrtc
- Boost
- ZLIB
- BZip2
- Openssl 1.0.2
- pjproject
- PocoCpp
- libphonenumber
- opus
- silk
- libsrtp
- secusmart
- secusuite
- joda
- spongycastle
- androidannotations
- firebase
- androidx.appcompat
- zxing
- kotlin
- androidx.biometric
- CACI
- Steelbox
- CACI SteelBox

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. This search was performed on January 25, 2021; vendor name terms were searched on February 3, 2021. No vulnerabilities applicable to the TOE were found.

**Vendor Conclusion:**

The 'Description of Changes' section (Chapter 2) of the IAR indicates that BlackBerry SecuSUITE Client v4.0, the TOE, has been revised to add a rebranded client named CACI Steelbox 4.0 client. This change allows a third party to resell the same product and as indicated above none change the security claims in the evaluated ST.

The evaluation evidence consists of the Security Target, administrative guidance, and test evidence. The Guidance was updated to address the rebranded client and other non-security relevant features.

Note that BlackBerry 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.

Based on this and other information from within this IAR document, the assurance impact of these changes is minor.

**Validation Team Conclusion:**

The validation team reviewed the changes and concur the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Neither the Security Target nor the Common Criteria Guide were changed. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.