BlackBerry | Cybersecurity Services

SKY ECC Mobile Application Assessment

Application Assessment

IT Health Check (ITHC)

Performed Between The

8th October 2018 and 11th October 2018

By

BlackBerry Cybersecurity Services

BlackBerry UK Limited
Ground Floor, The Pearce Building
West Street
Maidenhead
Berkshire
United Kingdom
SL6 1RL
+44 (0)330 100 2345

BlackBerry | Cybersecurity Services

Contents

BlackBerry | Cybersecurity Services

1 Management Summary

This report details the findings of an information systems security review conducted on the Sky ECC Android mobile application undertaken by BlackBerry Cybersecurity Services between the 8th and the 11th of October 2018 on behalf of Sky Global.

The purpose of the review was to identify any vulnerabilities present within the Sky Global ECC Mobile Application that could be exploited by an attacker and which may adversely affect the confidentiality, integrity or availability of the mobile device or data contained within the application itself. The review was conducted according to a white-box methodology, whereby the devices and credentials were provided.

The application was subjected to manual and automated testing techniques which aimed to cover both static and dynamic analysis of the mobile application in order to enumerate any vulnerabilities or attack vectors; any issues discovered were then further scrutinised by the tester to assess their validity and potential impact. The mobile application was tested from the provided devices (BlackBerry KeyOne and Google Pixel 2) and from a stand alone Android PacKage (APK) perspective. The ECC mobile application's Android file was also reviewed for any security related issues and vulnerabilities.

Testing identified a number of Android permissions required by the application. Upon review and investigation into the permissions and the fact the application is installed on mobile-device-management (MDM) devices, there was no risk found by the required permissions.

The application's development and configuration was found to be following current industry best practices surrounding user input handling, authentication, authorisation and segregation. Further to this, a review of the secure communications service was carried out to ascertain the level of confidentiality surrounding application data in transit, such as chat messages; the results from this review identified that the service has been configured following industry best practices.

A number of provided test cases were assessed against to provide Sky Global assurance regarding the confidentiality, integrity and availability of the application. All test cases were assessed against, and the application was found to be secure and correctly prevented unauthorised and unauthenticated access to the application, user data and the service. BlackBerry Cybersecurity Services have therefore assessed the overall risk posed to Sky Global by the ECC Android mobile application to be:

Risk Level: **Low**

BlackBerry | Cybersecurity Services

2 Overview of Vulnerabilities

In total 0 vulnerability groups have been identified and documented.

Vulnerability Category	Total	Risk Rating			
		Critical	High	Medium	Low
All Categories	-	-	-	-	-
Application Software	-	-	-	-	-
Database Configuration	-	-	-	-	-
Host Configuration	-	-	-	-	-
Infrastructure Design	-	-	-	-	-
Password Policy	-	-	-	-	-
Security Management	-	-	-	-	-
Patch Management	-	-	-	-	-

All security issues are presented with recommendations for mitigating the risks posed. Each recommendation or fix has been assigned an effort rating which estimates how much remedial work will be required to address the item, this is summarised in the following table:

Remediation Effort	Total	Risk Rating			
		Critical	High	Medium	Low
Total	-	-	-	-	-
High Effort	-	-	-	-	-
Medium Effort	-	-	-	-	-
Low Effort	-	-	-	-	-

Low: up to 1 day of effort

Medium: up to 10 days of effort

High: over 10 days of effort

3 Key Findings

The following list summarises the key findings during the assessment.

- Overall, the static analysis of the mobile application demonstrated a good security policy, with suitable error handling and directory access controls in place throughout, limiting the threat surface available to an attacker. A full source code review is recommended to provide continuity of testing with this assessment.

- The testing devices used were running either Android 8.1.0 (Oreo) or 9.0 (Pie) as well as device end-point management, demonstrating that the application utilises leading third-party protection and built-in Android protections to mitigate Man-in-the-Middle attacks.

- Test case assessments against the application and devices identified that it is not possible to bypass the application's authentication and authorisation processes. Therefore, BlackBerry can confirm it is not possible to access the chat messages, contact lists, or protected data from the devices without following the application's authentication process.

- Attempts were made, both over typical wireless networks and in a testing lab environment, to intercept chat communications between clients. These attempts failed due to the end-to-end encryption and device protections in place.

- Brute force protection was found to be in place to prevent automated brute forcing of the ECC password prompt required to access the application. After four incorrect password attempts the application requires the user to pass a CAPTCHA test, providing further security measures against brute force attempts. After 5 incorrect attempts, ECC access is revoked from the device. Regaining access to the application requires the ECC ID and activation code.

BlackBerry | Cybersecurity Services

4 Presentation of Issues and Findings

Issues are presented in a common format to aid readability and assist the client in prioritising issues and, importantly, prioritising remedial action where necessary. The common presentation format contains a number of fields describing the nature of the issue, risk and recommendation as follows:

TITLE	Short form title summarising the security issue.
IMPACT RATING	A rating of the likely impact resulting from a successful attack or exploitation of the issue. Ratings run Informational, Low, Medium, High, Critical.
LIKELIHOOD RATING	A rating of the likelihood of a successful attack, this incorporates parameters such as availability of exploit code, complexity of attack and compensating controls/mitigating factors. Ratings run Informational, Low, Medium, High, Critical.
RISK	An overall rating of the 'technical risk' posed by the issue. This is generally decided by both the impact and the likelihood, although it is subject to modification based on other factors considered by the security assessor. Ratings run Informational, Low, Medium, High, Critical.
FIX EFFORT	A rating of the anticipated effort required to successfully perform remediation work, generally based on the recommendations made for a specific issue. This rating is highly subjective, but is based on the security assessor's experience of similar issues and organisations. Ratings run Informational, Low, Medium and High. This can loosely be translated to days as follows: • Low: up to 1 day of effort • Medium: up to 10 days of effort • High: over 10 days of effort
SUMMARY / RISK DESCRIPTION	A description of the security issue.
AFFECTED COMPONENTS	Where applicable this will detail the systems, applications or other components affected by the issue. Where an issue is prevalent throughout a large population of components this may simply state that the issue is widespread.
RECOMMENDATION	A recommendation or set of recommendations for remediation or otherwise mitigating the risks posed by the issue.
NOTES	Any observations, references or other notes relating to the issue.

5 Tool List

The test team utilise a wide ranging tool set that often includes bespoke tools and code created for specific purposes during testing.

It is important to emphasise that tools represent one aspect of the penetration testing methodology and approach. The effective use of the tools and their output is a very important aspect of the penetration testing methodology. The primary function of the tools is to provide information to the testing consultants so that the information gathering phase is reduced in time.

During the testing the primary tool set used by the testers included:

Burp Suite 2.0.09	Web application testing proxy tool
Postman 5.3.2	API testing tool
MobSF v1.0.1	Mobile security framework
Wireshark 2.6.2	Network packet inspector
Mobile Device	Google Pixel 2 and BlackBerry KeyOne

BlackBerry | Cybersecurity Services

6 Scope of Work

Application Assessment	
IN-DEPTH PENETRATION TESTING OF WEB SITE	A full test on the nominated website (including OWASP most common vulnerabilities), with attempted exploitation of any potential vulnerability found. This will be followed by an in-depth analysis and report, highlighting risk, effect and effort to fix. Where appropriate, a full resolution to the vulnerability will be given.
Mobile Application in Scope	Sky Global ECC Android Mobile Application
Out of Scope	Any other asset or service not already identified above
WHAT	WHAT BlackBerry Cybersecurity Services TEST
Remote Scan	To ascertain any potential vulnerabilities and ”open” doors. This will also identify links to other sites. Those sites that are identified and require examination will be added to the scope once authority to do so is given.
In-Depth Exploitation	A senior security consultant will use the output from the above, as well as other methods, to target areas that appear to be vulnerable. These areas will then be exploited to ascertain what an attacker could achieve.
Information Gathering	Fingerprinting the application using bespoke and COTS tools to identify every system asset.
Configuration Management Testing	Including database management systems, infrastructure, secure communication protocols, file type handling etc.
Business Logic Testing	Creating functional tests to understand how the application works and then applying incorrect functional flow to assess how the application reacts.
Authentication Testing	Assessing the security of any authentication mechanisms, such as CAPTCHA, multiple-factor authentication, brute-force testing, predictable username and password combinations etc.
Authorisation Testing	Testing for privilege escalation, authorisation bypass issues etc.

Session Management	Testing for cookie implementation, linear regression testing of cookie value randomness, session management schema, session fixation, session variable theft and exposure and cross-site request forgery.
Data Validation	A thorough series of automated and manual tests will be undertaken to verify that all user-supplied data sent to the application is correctly sanitised. Testing seeks to identify, but is not limited to, cross-site scripting, DOM-based issues, SQL, LDAP, ORM, XML, SSI and Xpath injections, as well as vector-based overflows etc.
Denial of Service	Testing activity will be undertaken to actively seek out functions which may be abused to create a denial-of-service condition within the application.
Web Services	Where present, web services, such as SOAP, will be tested using the same methodology as detailed above.

BlackBerry | Cybersecurity Services

7 Summary of Vulnerabilities

Ref.	Title	Impact	Risk	Likelihood	Fix Effort
7.1 - Static Analysis					
7.1.1	Android APK Review	Informational	Informational	Informational	Informational
7.2 - Dynamic Analysis					
7.2.1	Overview	Informational	Informational	Informational	Informational

Colour Coding

	Critical
	High
	Medium
	Low
	Informational

8 Vulnerability Findings and Full Technical Details

The following section details vulnerabilities listed in section 9 above but also includes the following information.

Impact
Risk
Likelihood
Fix Effort
Summary
Risk Description
Affected Components
Recommendation
Notes

Results are presented as detailed in section 6 of this report and may also refer to appendices for logs and / or screen shots where appropriate. Where possible the method of discovery of the issue is detailed along with any tools and / or logs to support the findings.

8.1 Static Analysis

8.1.1 Android APK Review

Impact: **Informational**
Risk: **Informational**
Likelihood: **Informational**
Fix Effort: **Informational**

Summary

The static analysis of the Sky ECC mobile application consisted of passively analysing an Android mobile application .APK file. This was performed using a combination of automated and manual testing techniques, with a view to further scrutiny by the tester to assess the validity and potential impact of any issues identified.

Risk Description

Static program analysis is the analysis of software which can be installed and run on a computer, laptop or mobile platform, such as a tablet or phone. Static analysis is performed without actually executing the program or application itself, in contrast with dynamic analysis, which is analysis performed on a program or application while it is executing its intended functions. In most cases the analysis is performed on a version of the source code, and in the other cases, some form of the object code.

The Sky ECC mobile application APK (app-prod-release-obfuscation.apk) was independently provided by Sky Global.

From here the consultant was able to extract the Sky ECC APK file and use various methods and open source tooling to conduct static analysis on the target APK file. The static analysis identified that the application conforms to security best practices, with restrictions in place and only permissions requested that are required for the functionality of the application.

The results of the static analysis can be found below and have been divided into specific section headers.

BlackBerry | Cybersecurity Services

Signer Certificate

[
[
Version: V3
Subject: CN=Sky, OU=Sky, O=Sky, L=Sky, ST=Sky, C=01
Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key:
Validity: [*From: Thu Feb 01 17:39:47 UTC 2018,*
To: Mon Jan 26 17:39:47 UTC 2043]
Issuer: CN=Sky, OU=Sky, O=Sky, L=Sky, ST=Sky, C=01
SerialNumber: [*0d13904d*]

Certificate Extensions: 1
[*1*]*: ObjectId: 2.5.29.14 Criticality=false*
SubjectKeyIdentifier [
KeyIdentifier [
0000: 2D 49 9E A2 DE 74 1B 9D E3 E6 F1 28 29 CE 22 02 -I...t.....().".
0010: DB 98 12 D4 ....
]
]

]
Algorithm: [*SHA256withRSA*]
Signature:
0000: 1D 4B 6D BE B2 06 49 8D B3 91 67 F3 4A CF 1D CE .Km...I...g.J...
0010: F0 92 98 BD 1A E7 3A 46 E3 FF D9 E5 69 E7 D3 B6 ......:F....i...
*0020: A8 3C 2D 76 BA BD 16 00 F8 E8 55 E4 0C E7 DE 2A .<-v.....U....**
0030: 6C 78 92 83 58 57 21 EA 6E BB D3 96 49 45 8F A8 lx..XW!.n...IE..
0040: 52 3B 16 E0 B2 8F D7 55 44 BE E1 27 53 75 9B CA R;.....UD..'Su..
0050: 5E 8C C3 7E 18 38 FC 1A 23 E9 2E 8A 45 69 5A AA ^....8..#...EiZ.
0060: 49 EC 1C 91 4E C1 4F 9C 7B F1 74 72 11 A4 53 B0 I...N.O...tr..S.
0070: 52 0F 72 3F A0 C1 79 51 E4 12 1C C9 A5 57 B7 03 R.r?..yQ.....W..
0080: FD 42 C9 94 D4 E6 7F 43 89 41 91 0E E6 66 BF 32 .B.....C.A...f.2
0090: D8 3E 27 0A AB 50 6F 11 76 1B A9 4B 33 85 36 B7 .>'..Po.v..K3.6.
00A0: B9 1D F9 B7 FB 89 09 38 73 D8 0F 1C AE FF 1E AD .....8s.....
00B0: F4 39 79 60 29 39 6A B4 60 F0 4D B7 DF CF 78 3A .9y')9j.'.M...x:

BlackBerry | Cybersecurity Services

00C0: EE 62 8D 16 8D 17 E5 17 77 E8 AF 78 DA EA DB 97 .b.....w..x....
00D0: DD 95 09 BF E2 52 48 A7 BF 10 45 E5 AA 89 6C A0 .....RH...E...l.
00E0: 41 C0 95 CA DF EE 3D CD ED 5E A0 4D F3 3D 4D DB A.....=..^.M.=M.
00F0: 1C 31 56 60 8F 69 AB 87 32 68 29 0C 78 5E B8 76 .1V‘.i..2h).x^.v

]

Android Permissions

Android Permissions

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	dangerous	Unknown permission from android reference	Unknown permission from android reference
se.skyglobal.app.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.

DEX Malware Analysis

BlackBerry | Cybersecurity Services

ANTI-VM	COMPILER	OBFUSCATOR	PACKER	DROPPER	MANIPULATOR	ANTI-ASSEMBLY	ABNORMAL PATTERN
Anti-VM Code Found Build.FINGERPRINT check	Compiler Found dx	No Obfuscator Found	No Packer Found	No Dropper Found	No Manipulator Found	No Anti-Disassembly Code	No Abnormal Pattern Found

APKiD: 1.0.0

Broadcast Receivers

com.google.firebase.iid.FirebaseInstanceIdReceiver

Content Providers

com.google.firebase.provider.FirebaseInitProvider
android.arch.lifecycle.ProcessLifecycleOwnerInitializer

Activities

se.skyglobal.app.ui.SplashActivity
se.skyglobal.app.ui.activation.ActivationActivity
se.skyglobal.app.ui.LoginActivity
se.skyglobal.app.ui.activation.GenerateSecureKeyActivity
se.skyglobal.app.ui.profile.GenerateSecureKeyActivitySetting
se.skyglobal.app.ui.activation.DefineAppPasswordActivity
se.skyglobal.app.ui.profile.DefineAppPasswordActivitySetting
se.skyglobal.app.ui.activation.SetupProfileActivity
se.skyglobal.app.ui.activation.ChangeProfilePictureActivity
se.skyglobal.app.ui.profile.ChangeProfilePictureActivitySetting
se.skyglobal.app.ui.camera.CameraActivity
se.skyglobal.app.ui.activation.CameraActivityForActivation
se.skyglobal.app.ui.activation.ConfirmProfilePhotoActivity
se.skyglobal.app.ui.profile.ConfirmProfilePhotoActivitySetting
se.skyglobal.app.ui.activation.GeneratePublicPrivateKeyActivity
se.skyglobal.app.ui.AppActivity

se.skyglobal.app.ui.chats.ChatActivity
se.skyglobal.app.ui.chats.ChatInformationActivity
se.skyglobal.app.ui.chats.NewChatActivity
se.skyglobal.app.ui.chats.ViewAndDownloadAttachmentActivity
se.skyglobal.app.ui.chats.ViewSavedForwardingChatActivity
se.skyglobal.app.ui.vault.ViewAndEditVaultNotesActivity
se.skyglobal.app.ui.vault.VaultActivity
se.skyglobal.app.ui.vault.AddVaultPhotoActivity
se.skyglobal.app.ui.chats.NameGroupChatActivity
se.skyglobal.app.ui.contacts.AddCategoryActivity
se.skyglobal.app.ui.vault.VaultAddNoteActivity
se.skyglobal.app.ui.vault.EditImageFromVaultActivity
se.skyglobal.app.ui.vault.DefineVaultPasswordActivity
se.skyglobal.app.ui.contacts.AddContactActivity
se.skyglobal.app.ui.contacts.ShareContactActivity
se.skyglobal.app.ui.profile.BlockListActivity
se.skyglobal.app.ui.profile.RenewSubscriptionActivity
se.skyglobal.app.ui.profile.AddFundsActivity
se.skyglobal.app.ui.contacts.AddCategoryWithIconActivity
se.skyglobal.app.ui.profile.CollectFromCreditCardActivity
se.skyglobal.app.ui.profile.BitCoinQRCodeScannerActivity
se.skyglobal.app.ui.contacts.AddGroupMemberActivity
se.skyglobal.app.ui.profile.RenewalActivity
se.skyglobal.app.ui.profile.StealthModeCalculator
se.skyglobal.app.ui.profile.ProfileSettingsActivity
se.skyglobal.app.ui.DuressActivity
se.skyglobal.app.ui.ToSActivity
com.google.android.gms.common.api.GoogleApiActivity

Services Identified

se.skyglobal.app.firebase.MessagingService
se.skyglobal.app.firebase.TokenService
com.google.firebase.messaging.FirebaseMessagingService
com.google.firebase.components.ComponentDiscoveryService
com.google.firebase.iid.FirebaseInstanceIdService

Files Identified

AndroidManifest.xml
META-INF/CERT.RSA
META-INF/CERT.SF
META-INF/MANIFEST.MF
META-INF/android.arch.core_runtime.version
META-INF/android.arch.lifecycle_extensions.version
META-INF/android.arch.lifecycle_livedata-core.version
META-INF/android.arch.lifecycle_livedata.version
META-INF/android.arch.lifecycle_runtime.version
META-INF/android.arch.lifecycle_viewmodel.version
META-INF/app_prodRelease.kotlin_module
META-INF/com.android.support_animated-vector-drawable.version
META-INF/com.android.support_appcompat-v7.version
META-INF/com.android.support_cardview-v7.version
META-INF/com.android.support_design.version
META-INF/com.android.support_recyclerview-v7.version
META-INF/com.android.support_support-compat.version
META-INF/com.android.support_support-core-ui.version
META-INF/com.android.support_support-core-utils.version
META-INF/com.android.support_support-fragment.version
META-INF/com.android.support_support-media-compat.version
META-INF/com.android.support_support-v4.version

Note: A full list of files can be found in the appendices section of the report.

Affected Components

Sky ECC Mobile Application

Recommendation

None. This finding is for informational purposes.

Notes

https://developer.android.com/guide/topics/permissions/overview
https://developer.android.com/studio/command-line/adb
https://www.sitepoint.com/how-to-implement-javas-hashcode-correctly/

8.2 Dynamic Analysis

8.2.1 Overview

Impact: Informational
Risk: Informational
Likelihood: Informational
Fix Effort: Informational

Summary

Dynamic analysis of the Sky ECC mobile application was attempted from both the Android APK file and the provided testing devices. Testing was attempted using a combination of automated and manual testing techniques, with a view to further scrutiny by the tester to assess the validity and potential impact of any issues identified.

Risk Description

Dynamic analysis, unlike static analysis, is analysis performed on a program or application while it is executing its intended functions while being run on a computer, laptop or mobile platform such as a tablet or phone. Using the data gathered from the static analysis phase the consultant identified areas which they would like to investigate further.

The consultant attempted to employ various methods which would allow the consultant to use their computer to act as a proxy between the test devices and the internet, therefore intercepting any traffic to and from the devices and consequently the SKY ECC application. These proxy attempts were unsuccessful, preventing further in-depth testing interactions with the application and any traffic it generated.

The SKY ECC application refused to establish connections to endpoints which presented custom certificates. This behaviour is indicative of TLS/SSL certificate pinning, in which a certificate known to be used by the server is hard-coded into the mobile application. The app can then ignore the device's trust store and rely on its own, and allow only TLS/SSL connections to hosts signed with certificates stored inside the application.

To bypass proper certificate pinning, an attacker would need physical access to the targeted mobile device. From there, the attacker would need to root or jailbreak the device and modify the functions performing

certificate pinning during runtime. A number of tools exist that can perform these steps; however, due to the implemented device restrictions, this attack vector would not be possible.

Test case assessments against the application and devices identified that it is not possible to bypass the application's authentication and authorisation processes. Therefore, BlackBerry can confirm it is not possible to access the chat messages, contact lists, or protected data from the devices or Sky server without providing valid authorisation credentials to the ECC application.

Brute force protection was found to be in place to prevent automated brute forcing of the ECC password prompt required to access the application. After four incorrect password attempts the application requires the user to pass a CAPTCHA test, providing further security measures against brute force attempts. After 5 incorrect attempts, ECC access is revoked from the device. Regaining access to the application requires the ECC ID and activation code.

Affected Components

Sky ECC Mobile Application

Recommendation

None. This finding is for informational purposes.

Notes

None.