MOBSF

ANDROID STATIC ANALYSIS REPORT

Coronapas (1.4.6)

File Name:	dk.sum.ssicpas.apk
Package Name:	dk.sum.ssicpas
Scan Date:	May 9, 2022, 6:07 a.m.
App Security Score:	64/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	WARNING	INFO	SECURE
0	4	2	1

FILE INFORMATION

File Name: dk.sum.ssicpas.apk
Size: 17.3MB
MD5: 0fdb9c5186f115be54e5ff2fee9dbf6b
SHA1: 8a46aa32a955e56a6a8b5e5a06fcc4b5be7b6dba
SHA256: e5749f6a24247803117c817e2dc90d7594561f1497b75230271ec1799b9f4c01

APP INFORMATION

App Name: Coronapas
Package Name: dk.sum.ssicpas
Main Activity: crc645a23998331bf56a8.SplashActivity
Target SDK: 30
Min SDK: 21
Max SDK:
Android Version Name: 1.4.6
Android Version Code: 272

APP COMPONENTS

Activities: 8
Services: 1
Receivers: 5
Providers: 2
Exported Activities: 1
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-04-15 10:18:50+00:00
Valid To: 2051-04-15 10:18:50+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xb66a1dd760e32f22406d5196228b2a2a83e80804
Hash Algorithm: sha256
md5: 46bd07759ea8c56eda2ebcc4a4d2fbcc
sha1: 9cd98fd6f0e7445a4de9905325339d65d81a308b
sha256: d1d44decaa90565781d65c1f0175abfccb9ff2a9688b0f910103c69aadf844ea
sha512: 80b0e817ceea5bf1f691a94d92ab725f2b9263b7104234d3a1779c51d8df62f37e8a4111f88de94aa9fe9dada2e260d107a2370ad5adb335202b9830fb861679
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 186498adf75dbd9a8cbd28969991ee652779be2a270572a27bc10c2725fd17ca

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
com.honeywell.decode.permission.DECODE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check possible VM check
	FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
md52eac344ff43f7bff7f1301c3ba1d0d0c.AuthUrlSchemeInterceptorActivity	Schemes: dk.sum.ssicpas://, Paths: /oauth2redirect,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
2	Activity (md52eac344ff43f7bff7f1301c3ba1d0d0c.AuthUrlSchemeInterceptorActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/honeywell/aidc/BarcodeFailureEvent.java device/common/MsrResultCallback.java com/honeywell/aidc/BarcodeReader.java com/cipherlab/barcode/ReaderManager.java com/honeywell/aidc/BarcodeReadEvent.java com/airbnb/lottie/utils/LogcatLogger.java com/cipherlab/barcode/ReaderManagerAPI.java mono/android/incrementaldeployment/IncrementalClassLoader.java com/honeywell/aidc/TriggerStateChangeEvent.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/LottieAnimationView.java com/honeywell/aidc/AidcManager.java device/common/SerialPort.java
2	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	okio/Buffer.java
3	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	mono/android/content/ClipboardManager_OnPrimaryClipChangedListenerImplementor.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['camera', 'network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
7	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
9	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
10	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
11	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
12	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
13	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

PLAYSTORE INFORMATION

Title: Coronapas

Score: 1.6315789 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Medical **Play Store URL:** dk.sum.ssicpas

Developer Details: Sundhedsministeriet, Sundhedsministeriet, Sundhedsministeriet Holbergsgade 6, 1057 København K, Denmark, None, info@sundhed.dk,

Release Date: May 20, 2021 **Privacy Policy:** Privacy link

Description:

The Corona Passport App helping Denmark to reopen society When you go out or when you start travelling abroad again, you can easily with the app in hand show that you have tested negative for COVID-19, have been vaccinated, or that you are immune after recovery from COVID-19. Downloading and use of the app is voluntary. It is safe to use, and you do not show any personal information when you use the corona passport as your entrance ticket to city life in Denmark. You simply show that your corona passport is valid. When you use the app for trips abroad, you need to show a little more information. How does the app work? - You log on using your NemID - The Corona Passport app automatically retrieves data from the Danish Microbiology Database (MiBa) and The National Vaccine Registry, which supply test and vaccine data respectively - When your corona passport is valid, you will see the colour green as well as a QR code. The passport is valid if you are vaccinated, have a negative test result no older than 72 hours from the time of the test, or are immune after recovery from COVID-19 - Your data is secured – the app does not share information about negative test result, vaccination, or immunity - You may experience that controllers or other users of the app scan your QR code. They do this to ensure that your corona passport is in fact valid - The app will not register any additional information about you, and is based solely on data that is already registered in centralised health care databases - When traveling, select the particular display of your corona passport: International travel. Here, a controller can see more detailed information on why your corona passport is valid - ie. whether you have a negative test result, have been vaccinated or are immune after recovery from COVID-19. The work of developing the

app's functions is ongoing. When you download the Corona Passport app you accept Terms and conditions. You must consent once you have downloaded the app in order to use it. The Corona Passport has been developed by the Danish Ministry of Health, the Danish Health Data Authority, SSI, and the Danish Agency for Digitisation. Read more about the app at: www.coronasmitte.dk/coronapas

---

Report Generated by - MobSF v3.5.1 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.