MOBSF

ANDROID STATIC ANALYSIS REPORT

GreenPass (2.0.1)

File Name:	com.italinnovation.green_pass.apk
Package Name:	com.italinnovation.green_pass
Scan Date:	May 9, 2022, 6:13 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/428

FINDINGS SEVERITY

HIGH	WARNING	INFO	SECURE
2	13	2	2

FILE INFORMATION

File Name: com.italinnovation.green_pass.apk
Size: 23.99MB
MD5: a64ffc5ac6b3e20f92cb1ea396aebd25
SHA1: 52669de61fafcbe49b21dbd6d27128054b83312f
SHA256: 73c3c1ee343073ee05af700ea0e83339a8198acbceb43317ab1d28057db04e2f

APP INFORMATION

App Name: GreenPass
Package Name: com.italinnovation.green_pass
Main Activity: com.italinnovation.green_pass.MainActivity
Target SDK: 31
Min SDK: 24
Max SDK:
Android Version Name: 2.0.1

Android Version Code: 29

APP COMPONENTS

Activities: 8
Services: 14
Receivers: 11
Providers: 8
Exported Activities: 0
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: False
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: 2021-07-28 13:49:29+00:00
Valid To: 2051-07-28 13:49:29+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x1fe5cc2e2983b65098f0446a05955c3c1a6eb633
Hash Algorithm: sha256
md5: e334144bd39cd5947572951f19fe6f78
sha1: eef93457a27a6d60c23cf12c39b0ab3d700d0ab9
sha256: e0dca4e34c112aeff3c94666c4b96fcb5cbab1d3aa0096e23f83c6a3990700c2
sha512: 8213c2320413bfe9cd18f2c1744de14b1971343852c5b77fcea20f9e11815719036d9f1050e1ec521d90d5b780fd9ab0a87e418bdb8154015b7fd897153e53a2
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 064d0a308c7c467431d1580842558cff648e196364b498240b96a34b0318ecd8

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.QUERY_ALL_PACKAGES	normal		Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
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.

APKID ANALYSIS

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

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.
3	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d/a/a/o.java d/a/a/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d/b/b/b/e/r/wp0.java io/flutter/plugins/urllauncher/b.java d/b/b/b/e/n/dt.java d/b/b/b/e/m/fc.java d/b/b/b/e/i/co0.java d/b/b/b/e/m/pa.java c/e/f/f.java d/b/b/b/e/r/cs0.java com/yalantis/ucrop/UCropActivity.java d/c/g/j.java d/b/b/b/e/i/lo0.java d/b/b/b/e/n/xu.java c/e/f/g.java d/b/b/b/e/i/im0.java d/b/b/b/e/r/sr0.java d/b/g/s/a/d.java d/b/g/s/a/n/b/a.java com/yalantis/ucrop/view/b.java d/b/b/b/e/x/re.java io/flutter/plugins/googlemobileads/p.java d/b/b/b/e/c/m.java d/b/b/b/e/r/lw.java io/flutter/plugins/firebase/messaging/p.jav a c/e/m/u.java d/b/b/b/e/i/qp.java d/b/b/c/a/b/f.java c/e/e/a.java d/b/b/b/e/i/zq.java c/e/m/c0.java io/flutter/plugins/imagepicker/b.java c/a/k/a/a.java d/b/b/b/e/n/ht.java d/b/b/b/b/a.java d/b/b/b/e/i/oq.java d/b/e/a/c/b.java c/e/l/a.java d/b/b/b/c/r.java io/flutter/plugins/googlemobileads/u.java d/b/e/d/e/k.java d/b/b/c/a/b/d0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d/b/b/b/e/i/jo0.java io/flutter/plugins/c/h.java d/b/b/b/e/z/vc.java d/b/b/b/e/m/kc.java d/b/b/b/e/i/vo0.java d/b/b/b/e/r/rs0.java c/e/e/e/f.java com/yalantis/ucrop/m/a.java c/e/m/g.java d/b/b/b/e/m/ec.java c/e/e/e/a.java com/journeyapps/barcodescanner/x/p.java com/journeyapps/barcodescanner/x/e.java d/b/b/b/c/y.java d/b/b/b/e/i/po0.java d/a/a/n.java c/e/m/x.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/googlemobileads/w.java d/b/b/b/e/i/eo0.java d/b/b/b/e/r/xr0.java d/b/b/b/e/x/ge.java d/b/b/b/e/r/ir0.java f/a/b.java d/b/b/b/e/m/ta.java d/b/b/b/c/s.java io/flutter/plugins/googlemobileads/g0.java d/b/b/b/e/i/ko0.java com/journeyapps/barcodescanner/x/m.java d/b/b/b/e/z/oc.java d/b/b/b/e/r/is0.java d/b/b/b/c/d.java d/b/g/s/a/f.java c/e/m/v.java d/b/b/b/e/c/l.java io/flutter/plugins/firebase/messaging/t.java io/flutter/plugins/firebase/messaging/o.java

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	d/b/b/b/e/i/ml0.java d/b/b/b/e/z/rc.java io/flutter/plugins/googlemobileads/d.java d/b/b/b/e/w/o2.java d/b/b/b/e/r/bv.java c/e/f/k.java d/b/b/b/e/n/g6.java c/h/a/a.java d/b/b/b/e/i/vn0.java d/b/b/b/e/r/qv.java d/b/b/b/e/i/mm0.java com/journeyapps/barcodescanner/x/f.java com/yalantis/ucrop/n/c.java d/b/b/b/c/h.java com/journeyapps/barcodescanner/x/g.java c/n/a.java d/b/b/b/e/m/qc.java d/b/b/b/e/r/cw.java d/b/b/b/e/r/pq0.java d/b/b/b/e/n/ou.java d/b/g/s/a/n/a.java d/b/b/a/i/v/a.java c/e/f/j.java d/b/b/b/e/i/bn0.java c/m/a/c.java d/b/b/b/e/u/i0.java d/b/b/b/e/m/ka.java d/b/b/b/e/c/c.java d/b/b/b/e/r/zv.java com/yalantis/ucrop/n/f.java io/flutter/plugins/imagepicker/g.java d/b/b/b/e/r/zr0.java com/yalantis/ucrop/n/a.java d/b/b/b/e/z/ke.java d/c/g/g.java d/b/b/b/e/c/k.java d/b/b/b/c/u.java d/b/b/b/e/r/cr0.java d/b/b/b/e/n/dv.java d/b/b/b/i/a.java d/b/b/b/e/c/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d/b/b/b/e/i/io0.java c/a/h/g.java d/b/b/b/e/h/q9.java d/b/b/b/e/l/b.java com/journeyapps/barcodescanner/i.java d/b/b/b/e/n/yu.java c/o/i0.java d/b/b/b/e/c/w5.java io/flutter/plugins/googlemobileads/c0.java d/b/b/b/e/r/zo0.java d/b/b/b/e/z/qe.java io/flutter/plugins/urllauncher/c.java d/b/b/b/e/i/tq.java d/a/a/p.java d/b/b/b/e/i/qq.java d/b/b/b/c/a0.java io/flutter/plugins/googlemobileads/k.java d/b/b/b/e/i/eq.java d/b/b/b/e/z/fe.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java c/e/i/e.java d/b/e/d/h/e/a/k.java d/b/b/b/e/i/dp0.java d/b/b/b/e/x/pc.java d/b/e/a/c/q/c.java d/b/b/b/e/x/fe.java com/journeyapps/barcodescanner/n.java d/b/b/b/c/x.java d/b/b/b/e/c/m5.java d/b/b/b/e/z/yd.java io/flutter/plugins/urllauncher/a.java d/b/b/b/e/r/yr0.java e/a/a/d.java d/b/b/b/e/g/g0.java d/b/b/b/e/z/ee.java d/b/b/b/h/b/a.java io/flutter/plugins/googlemobileads/d0.java c/e/f/e.java d/b/b/b/e/i/pn0.java d/b/b/b/e/x/le.iava

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c/o/y.java org/tensorflow/lite/NativeInterpreterWrapper.java d/b/b/b/e/n/jv.java com/journeyapps/barcodescanner/x/k.java d/b/b/b/e/n/lt.java d/b/b/b/e/n/nu.java d/b/b/b/e/x/sc.java c/e/m/b.java com/journeyapps/barcodescanner/j.java com/yalantis/ucrop/m/b.java d/b/b/b/e/r/qr0.java d/b/b/b/e/i/so.java c/e/e/e/b.java d/b/b/b/e/m/xb.java d/b/b/b/e/r/ag0.java c/e/m/i.java c/p/a/a/h.java d/b/b/b/e/r/wr0.java c/l/a/a.java d/b/b/b/e/g/m0.java d/b/b/b/e/x/wc.java d/b/b/b/e/x/zd.java d/b/b/b/c/b.java d/b/b/b/e/r/fw.java d/b/b/b/e/g/h.java d/b/b/b/e/c/a6.java c/e/m/e0/b.java c/e/f/c.java c/k/a/b.java d/c/g/f.java
2	SHA-1 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	d/b/b/b/e/i/yk0.java d/b/b/b/e/r/mo0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	d/b/b/b/e/r/zs0.java d/b/b/b/e/r/bt0.java c/e/e/a.java io/flutter/plugins/c/h.java d/b/b/b/e/i/lp0.java c/e/e/b.java d/b/b/b/e/i/np0.java l/a/a/a/a/a.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	d/b/b/b/e/m/pa.java d/b/b/b/e/x/re.java d/b/b/b/e/n/ht.java h/z/d/a.java d/b/b/b/e/i/ml0.java d/b/b/b/e/z/rc.java d/b/b/b/e/r/p0.java d/b/b/b/e/m/qc.java h/z/b.java d/b/b/b/e/i/b1.java d/b/b/b/e/r/zo0.java d/b/b/b/e/z/qe.java d/b/b/b/e/g/g0.java d/b/b/b/e/n/jv.java d/b/b/b/e/x/sc.java h/z/a.java
5	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/platform/f.java io/flutter/plugin/editing/b.java
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	d/b/b/b/e/r/cs0.java d/b/b/c/a/b/t.java d/b/b/b/e/i/po0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	d/b/b/b/e/r/yp0.java d/b/b/b/e/i/km0.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	j/e0/c.java
9	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	d/b/b/a/i/x/j/r.java c/m/a/g/a.java d/b/b/a/i/x/j/h0.java d/b/b/a/i/x/j/f0.java
10	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	io/flutter/plugins/imagepicker/e.java c/h/a/a.java l/a/a/a/a/a.java io/flutter/plugins/imagepicker/c.java com/journeyapps/barcodescanner/j.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['camera', 'network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	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.
8	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.
9	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	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.
13	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.
14	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
15	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
16	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	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.
18	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
firebaseremoteconfig.googleapis.com	ok	**IP:** 142.250.74.74 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 216.58.211.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebaseinstallations.googleapis.com	ok	**IP:** 172.217.21.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
journeyapps.com	ok	**IP:** 108.156.22.6 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.74.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyB-zzv9D68rjuDPiV1H2VIR1EFyGXpuUFs"
"google_crash_reporting_api_key" : "AIzaSyB-zzv9D68rjuDPiV1H2VIR1EFyGXpuUFs"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

PLAYSTORE INFORMATION

Title: Green Pass Italia

Score: 4.78 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** 7.0 and up **Category:** Tools **Play Store URL:** com.italinnovation.green_pass

Developer Details: Ital Innovation SRL, 4762002820116830536, None, https://iisrl.it, info@italinnovationsrl.it,

Release Date: Aug 2, 2021 **Privacy Policy:** Privacy link

Description:

In this application you will be able to save all the GreenPasses that you need to have always at hand, whether they are yours or your family members'. You'll be able to scan the QRcode and save it so that you can easily use it whenever you are asked. With the new regulations it will be compulsory to show it at the entrance of some activities open to the public and with this application you won't have to worry about looking for it among thousands of other images. The data of your GreenPass will be saved only inside your phone and will not be accessible to us or anyone else. This is to ensure the respect of your privacy and for more data security. Our company deals with the creation of digital products, for more information contact us at info@iisrl.it

---