



## ANDROID STATIC ANALYSIS REPORT



 Green Pass (2.3.2)

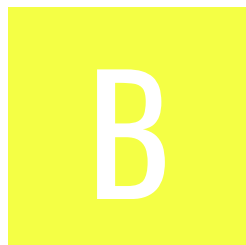
File Name: at.gv.brz.wallet.apk

Package Name: at.gv.brz.wallet





Scan Date: May 7, 2022, 1:22 p.m.

App Security Score: 58/100 (MEDIUM RISK)

Grade:



## FINDINGS SEVERITY

 HIGH	 WARNING	 INFO	 SECURE
1	8	2	2

## FILE INFORMATION

**File Name:** at.gv.brz.wallet.apk

**Size:** 11.39MB

**MD5:** 8a1103f2f305f290111314dbd95cf017

**SHA1:** 3b8ba3720fdefeb23b0a29350f3dce052844af6f

**SHA256:** 83b3ed3941a0fd0bd55ba391470d851240a0413b40fa35d268255843fc2bce11

## APP INFORMATION

**App Name:** Green Pass

**Package Name:** at.gv.brz.wallet

**Main Activity:** at.gv.brz.wallet.MainActivity

**Target SDK:** 30

**Min SDK:** 23

**Max SDK:**

**Android Version Name:** 2.3.2

**Android Version Code:** 76

## APP COMPONENTS

Activities: 5

Services: 6

Receivers: 8

Providers: 2

Exported Activities: 0

Exported Services: 2

Exported Receivers: 1

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: 2021-06-30 09:50:03+00:00

Valid To: 2051-06-30 09:50:03+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x54acb57165fd26b38789cc2bd2946881a961073a

Hash Algorithm: sha256

md5: 53ab93cff285bc460df059c75e5d4695

sha1: fe38df75e954989e30e4f9acb75ccfab2dd0625b

sha256: bd29d6e453ceda343b2850da862e828292573168dda611c71f1d2555ccae71a2

sha512: f01efc32e9ae2f0fa5b81e9068a94f260de439099cabdf0dfcb376ee6dc3b92d0eccb569afbfb3d9638bfebb1f72cce466907ae1910118afc1f94ad1c34c2f88

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 82e356f5f87969a413b79ffe84b2f44f7ad3719bbb777220ea393f3cc5b8d5d8

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.INTERNET	normal	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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check
	Compiler	r8
classes2.dex	FINDINGS	DETAILS
	Compiler	r8
classes3.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)
classes4.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)

# NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

## MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
2	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.
3	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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	<p>Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.DUMP [android:exported=true]</p>	warning	<p>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.</p>

## </> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	<p>CWE: CWE-312: Cleartext Storage of Sensitive Information</p> <p>OWASP Top 10: M9: Reverse Engineering</p> <p>OWASP MASVS: MSTG-STORAGE-14</p>	<p>io/jsonwebtoken/JwsHeader.java</p> <p>at/gv/brz/wallet/data/NotificationSecureStorage.java</p> <p>dgca/verifier/app/engine/DefaultCertLogicEngine.java</p>
2	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	<p>CWE: CWE-532: Insertion of Sensitive Information into Log File</p> <p>OWASP MASVS: MSTG-STORAGE-3</p>	<p>at/gv/brz/wallet/settings/SettingsFragment.java</p> <p>com/github/jaiimageio/impl/plugins/tiff/TIFFLZWDecompressor.java</p> <p>COSE/ASN1.java</p> <p>at/gv/brz/eval/net/ToByteConvertFactory.java</p> <p>io/github/aakira/napier/DebugAntilog.java</p>



NO	ISSUE	SEVERITY	STANDARDS	FILES
3	<a href="#">The App uses an insecure Random Number Generator.</a>	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	j\$/util/concurrent/ThreadLocalRandom.java
4	<a href="#">This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.</a>	secure	OWASP MASVS: MSTG-NETWORK-4	at/gv/brz/eval/CovidCertificateSdk.java at/gv/brz/common/net/ConfigRepository.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	net/i2p/crypto/eddsa/EdDSASecurityProvider.java
6	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/lyft/kronos/AndroidClockFactory.java
7	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	at/gv/brz/wallet/pdf/PdfViewModel\$importPdf\$1.java

## NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	<a href="#">FCS_RBG_EXT.1.1</a>	Security Functional Requirements	Random Bit Generation Services	The application implement 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 leverage platform-provided 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	<a href="#">FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2</a>	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	<a href="#">FCS_CKM.1.1(1)</a>	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	<a href="#">FCS_CKM.1.1(3),FCS_CKM.1.2(3)</a>	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm..
13	<a href="#">FCS_COP.1.1(1)</a>	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
14	<a href="#">FCS_COP.1.1(2)</a>	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
15	<a href="#">FCS_COP.1.1(3)</a>	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
16	<a href="#">FCS_HTTPS_EXT.1.2</a>	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	<a href="#">FCS_HTTPS_EXT.1.3</a>	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.
18	<a href="#">FIA_X509_EXT.1.1</a>	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The application validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates', 'The application validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 2560 or a Certificate Revocation List (CRL) as specified in RFC 5759 or an OCSP TLS Status Request Extension (i.e., OCSP stapling) as specified in RFC 6066', 'The certificate path must terminate with a trusted CA certificate'].
19	<a href="#">FIA_X509_EXT.1.2</a>	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.
20	<a href="#">FIA_X509_EXT.2.1</a>	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.
21	<a href="#">FIA_X509_EXT.2.2</a>	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate ,or not accept the certificate.
22	<a href="#">FPT_TUD_EXT.2.1</a>	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
23	<a href="#">FCS_CKM.1.1(2)</a>	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

## DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
gruenerpass.gv.at	ok	<b>IP:</b> 194.48.236.195 <b>Country:</b> Austria <b>Region:</b> Wien <b>City:</b> Vienna <b>Latitude:</b> 48.208488 <b>Longitude:</b> 16.372080 <b>View:</b> <a href="#">Google Map</a>
pwall.net	ok	<b>IP:</b> 92.243.0.172 <b>Country:</b> France <b>Region:</b> Ile-de-France <b>City:</b> Paris <b>Latitude:</b> 48.853409 <b>Longitude:</b> 2.348800 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	<b>IP:</b> 128.30.52.100 <b>Country:</b> United States of America <b>Region:</b> Massachusetts <b>City:</b> Cambridge <b>Latitude:</b> 42.365078 <b>Longitude:</b> -71.104523 <b>View:</b> <a href="#">Google Map</a>
javax.xml.xmlconstants	ok	No Geolocation information available.
java.sun.com	ok	<b>IP:</b> 96.16.49.213 <b>Country:</b> United States of America <b>Region:</b> Louisiana <b>City:</b> New Orleans <b>Latitude:</b> 29.954651 <b>Longitude:</b> -90.075073 <b>View:</b> <a href="#">Google Map</a>
apache.org	ok	<b>IP:</b> 151.101.2.132 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
itunes.apple.com	ok	<b>IP:</b> 184.50.200.24 <b>Country:</b> Japan <b>Region:</b> Tokyo <b>City:</b> Tokyo <b>Latitude:</b> 35.689507 <b>Longitude:</b> 139.691696 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
github.com	ok	<b>IP:</b> 140.82.121.4 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
tools.ietf.org	ok	<b>IP:</b> 4.31.198.62 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Jose <b>Latitude:</b> 37.339390 <b>Longitude:</b> -121.894958 <b>View:</b> <a href="#">Google Map</a>
dgc-trust.qr.gv.at	ok	<b>IP:</b> 95.131.199.105 <b>Country:</b> Austria <b>Region:</b> Wien <b>City:</b> Vienna <b>Latitude:</b> 48.208488 <b>Longitude:</b> 16.372080 <b>View:</b> <a href="#">Google Map</a>
json-schema.org	ok	<b>IP:</b> 172.67.130.91 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>

POSSIBLE SECRETS
"language_key" : "en"
"wallet_add_certificate" : "Add"
"language_key" : "de"
"wallet_add_certificate" : "Hinzufügen"

## PLAYSTORE INFORMATION

**Title:** Grüner Pass

**Score:** 5 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Health & Fitness **Play Store URL:** [at.gv.brz.wallet](https://play.google.com/store/apps/details?id=at.gv.brz.wallet)

**Developer Details:** BRZ GmbH, BRZ+GmbH, None, <https://www.sozialministerium.at/Informationen-zum-Coronavirus/Coronavirus---Haeufig-gestellte-Fragen/FAQ-Gruener-Pass.html>, [walletapp@brz.gv.at](mailto:walletapp@brz.gv.at),

**Release Date:** Jan 14, 2022 **Privacy Policy:** [Privacy link](#)

### Description:

Die österreichische App zum Grünen Pass ermöglicht die sichere Speicherung von EU-konformen SARS-CoV-2 Zertifikaten aus Österreich am Mobiltelefon und erleichtert das Vorweisen bei einer Kontrolle von 3-G-Nachweisen und im internationalen Reiseverkehr. Das österreichische Bundesrechenzentrum (BRZ) betreibt die App im Auftrag des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK). Das Covid-19 Zertifikat in Österreich: SARS-CoV-2 Zertifikate werden in Österreich in Papierform oder elektronischer Form (PDF) ausgestellt und dienen als 3-G-Nachweis (Geimpft, Genesen, Getestet). Wie Sie Ihr SARS-CoV-2-Zertifikat erhalten erfahren Sie unter <https://www.gruenerpass.gv.at/>. Um ein SARS-CoV-2-Zertifikat zur Grünen-Pass-App hinzuzufügen, benötigen Sie das Ihnen ausgestellte Originalzertifikat auf Papier oder als PDF-Dokument. In wenigen Schritten zum Grünen Pass auf Ihrem Smartphone: - Scannen Sie den QR-Code auf Ihrem SARS-CoV-2-Zertifikat oder - fügen Sie das SARS-CoV-2-Zertifikat als PDF direkt in der App hinzu. - Verwahren Sie so Ihre Zertifikate für den 3-G-Nachweis digital und sicher - Nutzen Sie die App zum Vorzeigen des Zertifikats (QR-Code) bei einer Überprüfung - Auch mehrere Zertifikate (z. B. für Familienmitglieder) können in dieser App aufbewahrt werden. Datenschutz ist uns wichtig: - Sämtliche Daten bleiben in der App und werden zu keinem Zeitpunkt auf fremde Server hochgeladen - Ihre Zertifikate sind nur lokal auf



Ihrem Smartphone hinterlegt. Die Daten in Ihrer App werden in keinem zentralen System gespeichert. - Die Zertifikate werden durch eine digitale Signatur geschützt und dadurch fälschungssicher. - Zur Überprüfung des Zertifikats ist neben dem QR-Code auch ein Lichtbildausweis erforderlich. Die Nutzung der App „Grüner Pass“ ist freiwillig und kostenlos. Alle Informationen zum Grünen Pass in Österreich und den verschiedenen SARS-CoV-2-Zertifikaten bzw. Möglichkeiten des 3-G-Nachweises erhalten Sie auf <https://www.gruenerpass.gv.at>. Credits: Die App „Grüner Pass“ basiert auf der vom Bundesamt für Informatik und Telekommunikation (BIT) im Auftrag des Bundesamts für Gesundheit in der Schweiz entwickelten Open-Source-App „COVID Certificate“ und wurde vom Bundesrechenzentrum für die Verwendung in Österreich weiterentwickelt.

---

## 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.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).