IOS STATIC ANALYSIS REPORT

Grüner Pass (2.3.2)

File Name:	Grüner Pass.ipa
Identifier:	at.gv.brz.wallet
Scan Date:	May 7, 2022, 12:50 p.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	⚠ WARNING	ℹ INFO	✓ SECURE
2	2	1	1

FILE INFORMATION

File Name: Grüner Pass.ipa
Size: 2.47MB
MD5: 73e60b126cf2937014a253f1eacedd66
SHA1: 0f8eea018b11cc38d6bb1976948b921306d3cfa9
SHA256: a1e7ebb36a80fadb7cc9b49de5ef47c9f3e7a5d6fdfad904761470a9c677111c

APP INFORMATION

App Name: Grüner Pass
App Type: Swift
Identifier: at.gv.brz.wallet
SDK Name: iphoneos15.2
Version: 2.3.2
Build: 79
Platform Version: 15.2
Min OS Version: 13.0
Supported Platforms: iPhoneOS,

BINARY INFORMATION

Arch: ARM64
Sub Arch: CPU_SUBTYPE_ARM64_ALL
Bit: 64-bit
Endian: <

APPLICATION PERMISSIONS

PERMISSIONS	STATUS	DESCRIPTION	REASON IN MANIFEST
NSCameraUsageDescription	dangerous	Access the Camera.	Der Kamerazugriff wird benötigt, um QR-Codes zu scannen

IPA BINARY CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION
1	Binary makes use of insecure API(s)	high	**CWE:** CWE-676: Use of Potentially Dangerous Function **OWASP Top 10:** M7: Client Code Quality **OWASP MASVS:** MSTG-CODE-8	The binary may contain the following insecure API(s) _fopen , _sscanf , _memcpy , _strlen
2	Binary makes use of Logging function	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	The binary may use _NSLog function for logging.

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION
3	Binary makes use of malloc function	high	**CWE:** CWE-789: Uncontrolled Memory Allocation **OWASP Top 10:** M7: Client Code Quality **OWASP MASVS:** MSTG-CODE-8	The binary may use _malloc function instead of calloc

IPA BINARY ANALYSIS

PROTECTION	STATUS	SEVERITY	DESCRIPTION
NX	True	info	The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.
PIE	True	info	The binary is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.
STACK CANARY	True	info	This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.
ARC	True	info	The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.
RPATH	True	warning	The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.
CODE SIGNATURE	True	info	This binary has a code signature.

PROTECTION	STATUS	SEVERITY	DESCRIPTION
ENCRYPTED	False	warning	This binary is not encrypted.
SYMBOLS STRIPPED	False	warning	Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
opensource.org	ok	**IP:** 172.67.197.41 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.gruenerpass.gv.at	ok	**IP:** 194.48.236.195 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gruenerpass.gv.at	ok	**IP:** 194.48.236.195 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
www.apple.com	ok	**IP:** 23.199.248.211 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
crl.apple.com	ok	**IP:** 17.253.39.206 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
crl.thawte.com	ok	**IP:** 93.184.220.29 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dgc-trust.qr.gv.at	ok	**IP:** 95.131.199.105 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
ocsp.thawte.com0	ok	No Geolocation information available.
crl.verisign.com	ok	**IP:** 93.184.220.29 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
unlicense.org	ok	**IP:** 188.114.97.5 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
itunes.apple.com	ok	**IP:** 184.50.200.24 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.sitemaps.org	ok	**IP:** 20.40.202.27 **Country:** United States of America **Region:** Iowa **City:** Des Moines **Latitude:** 41.600540 **Longitude:** -93.609108 **View:** Google Map
d.symcb.com	ok	**IP:** 13.56.82.130 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
sc.symcd.com0	ok	No Geolocation information available.
www.brz.gv.at	ok	**IP:** 194.37.73.140 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
ocsp.verisign.com0	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ocsp.apple.com	ok	**IP:** 17.253.39.204 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
www.adobe.com	ok	**IP:** 81.198.165.233 **Country:** Latvia **Region:** Riga **City:** Riga **Latitude:** 56.945999 **Longitude:** 24.105890 **View:** Google Map
www.symauth.com	ok	**IP:** 13.56.82.130 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
ts-ocsp.ws.symantec.com07	ok	No Geolocation information available.
sc.symcb.com	ok	**IP:** 93.184.220.29 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
scripts.sil.org	ok	**IP:** 172.67.29.248 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
semver.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.bit.admin.ch	ok	**IP:** 162.23.129.87 **Country:** Switzerland **Region:** Bern **City:** Bern **Latitude:** 46.948090 **Longitude:** 7.447440 **View:** Google Map
www.w3.org	ok	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.gnu.org	ok	**IP:** 209.51.188.116 **Country:** United States of America **Region:** Massachusetts **City:** Boston **Latitude:** 42.358429 **Longitude:** -71.059769 **View:** Google Map
dgc-trusttest.qr.gv.at	ok	**IP:** 95.131.199.104 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
ec.europa.eu	ok	**IP:** 147.67.34.30 **Country:** Luxembourg **Region:** Luxembourg **City:** Luxembourg **Latitude:** 49.611671 **Longitude:** 6.130000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dgc.a-sit.at	ok	**IP:** 129.27.142.8 **Country:** Austria **Region:** Steiermark **City:** Graz **Latitude:** 47.066669 **Longitude:** 15.450000 **View:** Google Map
ts-aia.ws.symantec.com	ok	**IP:** 93.184.220.29 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
id.uvci.eu	ok	No Geolocation information available.
ts-crl.ws.symantec.com	ok	**IP:** 93.184.220.29 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
json-schema.org	ok	**IP:** 104.21.8.16 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
de7@gg.ǭgn	CovidCertificateWallet.app/CovidCertificateWallet

HARDCODED SECRETS

POSSIBLE SECRETS
WALLET_APP_SDK_API_TOKEN : aknZGsFD9qCNmCm4NzFYfcK7WWbBeTFF

APP STORE INFORMATION

Title: Grüner Pass

Score: 4.85938 **Features: Price:** 0.0 **Category:** Health & Fitness,
App Store URL: at.gv.brz.wallet

Developer: BRZ GmbH
Developer ID: 581870568
Developer Website: https://www.gruenerpass.gv.at/app
Developer URL: https://apps.apple.com/us/developer/brz-gmbh/id581870568?uo=4
Supported Devices iPhone5s-iPhone5s, iPadAir-iPadAir, iPadAirCellular-iPadAirCellular, iPadMiniRetina-iPadMiniRetina, iPadMiniRetinaCellular-iPadMiniRetinaCellular, iPhone6-iPhone6, iPhone6Plus-iPhone6Plus, iPadAir2-iPadAir2, iPadAir2Cellular-iPadAir2Cellular, iPadMini3-iPadMini3, iPadMini3Cellular-iPadMini3Cellular, iPodTouchSixthGen-iPodTouchSixthGen, iPhone6s-iPhone6s, iPhone6sPlus-iPhone6sPlus, iPadMini4-iPadMini4, iPadMini4Cellular-iPadMini4Cellular, iPadPro-iPadPro, iPadProCellular-iPadProCellular, iPadPro97-iPadPro97, iPadPro97Cellular-iPadPro97Cellular, iPhoneSE-iPhoneSE, iPhone7-iPhone7, iPhone7Plus-iPhone7Plus, iPad611-iPad611, iPad612-iPad612, iPad71-iPad71, iPad72-iPad72, iPad73-iPad73, iPad74-iPad74, iPhone8-iPhone8, iPhone8Plus-iPhone8Plus, iPhoneX-iPhoneX, iPad75-iPad75, iPad76-iPad76, iPhoneXS-iPhoneXS, iPhoneXSMax-iPhoneXSMax, iPhoneXR-iPhoneXR, iPad812-iPad812, iPad834-iPad834, iPad856-iPad856, iPad878-iPad878, iPadMini5-iPadMini5, iPadMini5Cellular-iPadMini5Cellular, iPadAir3-iPadAir3, iPadAir3Cellular-iPadAir3Cellular, iPodTouchSeventhGen-iPodTouchSeventhGen, iPhone11-iPhone11,

iPhone11Pro-iPhone11Pro, iPadSeventhGen-iPadSeventhGen, iPadSeventhGenCellular-iPadSeventhGenCellular, iPhone11ProMax-iPhone11ProMax, iPhoneSESecondGen-iPhoneSESecondGen, iPadProSecondGen-iPadProSecondGen, iPadProSecondGenCellular-iPadProSecondGenCellular, iPadProFourthGen-iPadProFourthGen, iPadProFourthGenCellular-iPadProFourthGenCellular, iPhone12Mini-iPhone12Mini, iPhone12-iPhone12, iPhone12Pro-iPhone12Pro, iPhone12ProMax-iPhone12ProMax, iPadAir4-iPadAir4, iPadAir4Cellular-iPadAir4Cellular, iPadEighthGen-iPadEighthGen, iPadEighthGenCellular-iPadEighthGenCellular, iPadProThirdGen-iPadProThirdGen, iPadProThirdGenCellular-iPadProThirdGenCellular, iPadProFifthGen-iPadProFifthGen, iPadProFifthGenCellular-iPadProFifthGenCellular, iPhone13Pro-iPhone13Pro, iPhone13ProMax-iPhone13ProMax, iPhone13Mini-iPhone13Mini, iPhone13-iPhone13, iPadMiniSixthGen-iPadMiniSixthGen, iPadMiniSixthGenCellular-iPadMiniSixthGenCellular, iPadNinthGen-iPadNinthGen, iPadNinthGenCellular-iPadNinthGenCellular, iPhoneSEThirdGen-iPhoneSEThirdGen, iPadAirFifthGen-iPadAirFifthGen, iPadAirFifthGenCellular-iPadAirFifthGenCellular,

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 ein 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.