IOS STATIC ANALYSIS REPORT

Covid Cert (4.1.0)

File Name:	Covid Cert.ipa
Identifier:	ch.admin.bag.covidcertificate.wallet
Scan Date:	May 7, 2022, 12:42 p.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	WARNING	INFO	SECURE
2	2	0	1

FILE INFORMATION

File Name: Covid Cert.ipa
Size: 10.11MB
MD5: 7b514e46d95dc76f56d9cf253e2548b3
SHA1: 7a59466a5dafac1deed4aacc2204ceab054f3a6c
SHA256: 78e0f8a7a365af010fc8e174a1bc7a4c2d7c0b4636c6f13316376378147b28ec

APP INFORMATION

App Name: Covid Cert
App Type: Swift
Identifier: ch.admin.bag.covidcertificate.wallet
SDK Name: iphoneos15.2
Version: 4.1.0
Build: 220429.1021.99279
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: <

#CUSTOM URL SCHEMES

URL NAME	SCHEMES
ch.admin.bag.covidcertificate.wallet Editor	hcert covidcert

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

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 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.

PROTECTION	STATUS	SEVERITY	DESCRIPTION
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.
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
www.cc-a.bit.admin.ch	ok	**IP:** 108.156.22.76 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
opensource.org	ok	**IP:** 104.21.84.214 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.gl.ch	ok	**IP:** 193.135.58.32 **Country:** Switzerland **Region:** Thurgau **City:** Frauenfeld **Latitude:** 47.558159 **Longitude:** 8.898540 **View:** Google Map
www.lu.ch	ok	**IP:** 194.40.144.142 **Country:** Switzerland **Region:** Luzern **City:** Luzern **Latitude:** 47.050480 **Longitude:** 8.306350 **View:** Google Map
www.pki.admin.ch	ok	**IP:** 162.23.43.114 **Country:** Switzerland **Region:** Bern **City:** Bern **Latitude:** 46.948090 **Longitude:** 7.447440 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
covid19-vac-check.ch	ok	**IP:** 185.48.147.44 **Country:** Switzerland **Region:** Vaud **City:** Bussigny **Latitude:** 46.551102 **Longitude:** 6.555970 **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:** 81.198.165.227 **Country:** Latvia **Region:** Riga **City:** Riga **Latitude:** 56.945999 **Longitude:** 24.105890 **View:** Google Map
bag-coronavirus.ch	ok	**IP:** 34.65.60.252 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.ar.ch	ok	**IP:** 185.17.69.20 **Country:** Switzerland **Region:** Luzern **City:** Luzern **Latitude:** 47.050480 **Longitude:** 8.306350 **View:** Google Map
www.whocc.no	ok	**IP:** 194.63.250.90 **Country:** Norway **Region:** Oslo **City:** Oslo **Latitude:** 59.912731 **Longitude:** 10.746090 **View:** Google Map
www.jura.ch	ok	**IP:** 193.246.28.145 **Country:** Switzerland **Region:** Jura **City:** Delemont **Latitude:** 47.364929 **Longitude:** 7.344530 **View:** Google Map
www.cc.bit.admin.ch	ok	**IP:** 108.156.22.6 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.sz.ch	ok	**IP:** 193.135.58.23 **Country:** Switzerland **Region:** Thurgau **City:** Frauenfeld **Latitude:** 47.558159 **Longitude:** 8.898540 **View:** Google Map
unlicense.org	ok	**IP:** 188.114.96.5 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
www.coronaimpfzentrumbasel.chxfriburgo	ok	No Geolocation information available.
www.ge.ch	ok	**IP:** 160.53.252.106 **Country:** Switzerland **Region:** Geneve **City:** Geneva **Latitude:** 46.202221 **Longitude:** 6.145690 **View:** Google Map
covid-19-diagnostics.jrc.ec.europa.eu	ok	**IP:** 139.191.221.12 **Country:** Italy **Region:** Lombardia **City:** Milan **Latitude:** 45.464272 **Longitude:** 9.189510 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gesundheit.tg.ch	ok	**IP:** 161.78.13.64 **Country:** Switzerland **Region:** Thurgau **City:** Frauenfeld **Latitude:** 47.558159 **Longitude:** 8.898540 **View:** Google Map
www.zh.ch	ok	**IP:** 194.247.8.174 **Country:** Switzerland **Region:** Zurich **City:** Aussersihl **Latitude:** 47.377522 **Longitude:** 8.521270 **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
www.gsi.be.ch	ok	**IP:** 159.144.56.20 **Country:** Switzerland **Region:** Bern **City:** Bern **Latitude:** 46.948090 **Longitude:** 7.447440 **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
ofsp-coronavirus.ch	ok	**IP:** 34.65.60.252 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.baselland.ch	ok	**IP:** 193.47.168.16 **Country:** Switzerland **Region:** Basel-Landschaft **City:** Liestal **Latitude:** 47.484550 **Longitude:** 7.734460 **View:** Google Map
loinc.org	ok	**IP:** 3.92.153.161 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
covidcertificate-form-a.admin.ch	ok	**IP:** 162.23.147.236 **Country:** Switzerland **Region:** Bern **City:** Bern **Latitude:** 46.948090 **Longitude:** 7.447440 **View:** Google Map
ocsp.apple.com	ok	**IP:** 17.253.39.202 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
www.be.ch	ok	**IP:** 159.144.56.20 **Country:** Switzerland **Region:** Bern **City:** Bern **Latitude:** 46.948090 **Longitude:** 7.447440 **View:** Google Map
ufsp-coronavirus.ch	ok	**IP:** 34.65.60.252 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.corona-impfung-zug.ch	ok	**IP:** 3.69.136.55 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
www.coronaimpfzentrumbasel.chxfreiburg	ok	No Geolocation information available.
www.ubique.ch	ok	**IP:** 149.126.4.43 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map
sh.ch	ok	**IP:** 178.250.24.196 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.coronaimpfzentrumbasel.chwfriburg	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.ai.ch	ok	**IP:** 159.100.250.129 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
www.coronaimpfzentrumbasel.ch	ok	**IP:** 34.249.235.125 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
foph-coronavirus.ch	ok	**IP:** 34.65.60.252 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
covidcertificate-app.bit.admin.ch	ok	**IP:** 162.23.132.114 **Country:** Switzerland **Region:** Bern **City:** Bern **Latitude:** 46.948090 **Longitude:** 7.447440 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.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
www.bl.ch	ok	**IP:** 193.47.168.16 **Country:** Switzerland **Region:** Basel-Landschaft **City:** Liestal **Latitude:** 47.484550 **Longitude:** 7.734460 **View:** Google Map
www.ow.ch	ok	**IP:** 195.65.10.20 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **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

DOMAIN	STATUS	GEOLOCATION
reopen.europa.eu	ok	**IP:** 139.191.221.32 **Country:** Italy **Region:** Lombardia **City:** Milan **Latitude:** 45.464272 **Longitude:** 9.189510 **View:** Google Map
spor.ema.europa.eu	ok	**IP:** 195.144.18.87 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
youtu.be	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
www.ur.ch	ok	**IP:** 195.65.10.20 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.fr.ch	ok	**IP:** 52.29.81.245 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
www.coronaimpfzentrumbasel.chxfribourg	ok	No Geolocation information available.
www.bag.admin.ch	ok	**IP:** 108.156.22.42 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **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
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

DOMAIN	STATUS	GEOLOCATION
www.vs.ch	ok	**IP:** 193.247.117.21 **Country:** Switzerland **Region:** Valais **City:** Sion **Latitude:** 46.229080 **Longitude:** 7.359420 **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
snomed.info	ok	**IP:** 3.225.65.37 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
covid19.impf-check.ch	ok	**IP:** 185.48.147.42 **Country:** Switzerland **Region:** Vaud **City:** Bussigny **Latitude:** 46.551102 **Longitude:** 6.555970 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.ag.ch	ok	**IP:** 193.47.122.80 **Country:** Switzerland **Region:** Aargau **City:** Aarau **Latitude:** 47.392540 **Longitude:** 8.044220 **View:** Google Map
www.nw.ch	ok	**IP:** 195.65.10.26 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.cc-d.bit.admin.ch	ok	**IP:** 108.156.22.41 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.ti.ch	ok	**IP:** 193.246.181.24 **Country:** Switzerland **Region:** Ticino **City:** Bellinzona **Latitude:** 46.192780 **Longitude:** 9.017030 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.gr.ch	ok	**IP:** 193.247.16.45 **Country:** Switzerland **Region:** Graubunden **City:** Chur **Latitude:** 46.849861 **Longitude:** 9.532870 **View:** Google Map
vd.ch	ok	**IP:** 145.232.192.197 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
ec.europa.eu	ok	**IP:** 147.67.210.30 **Country:** Luxembourg **Region:** Luxembourg **City:** Luxembourg **Latitude:** 49.611671 **Longitude:** 6.130000 **View:** Google Map
www.ne.ch	ok	**IP:** 148.196.30.27 **Country:** Switzerland **Region:** Neuchatel **City:** Neuchatel **Latitude:** 46.991791 **Longitude:** 6.931000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.sg.ch	ok	**IP:** 193.238.142.3 **Country:** Switzerland **Region:** Sankt Gallen **City:** Wil **Latitude:** 47.461521 **Longitude:** 9.045520 **View:** Google Map
so.ch	ok	**IP:** 193.135.80.188 **Country:** Switzerland **Region:** Solothurn **City:** Solothurn **Latitude:** 47.207909 **Longitude:** 7.537140 **View:** Google Map

✉ EMAILS

EMAIL	FILE
ekeweeeeeeef5f@fe.nulluni004	CovidCertificateWallet.app/Impressum/fonts/Inter-Light.otf
3@q.sg	CovidCertificateWallet.app/Impressum/fonts/Inter-Bold.woff

APP STORE INFORMATION

Title: COVID Certificate

Score: 3.39216 **Features: Price:** 0.0 **Category:** Health & Fitness, Utilities,
App Store URL: ch.admin.bag.covidcertificate.wallet

Developer: Bundesamt für Gesundheit BAG
Developer ID: 557143322
Developer Website: https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/covid-zertifikat.html
Developer URL: https://apps.apple.com/us/developer/bundesamt-f%C3%BCr-gesundheit-bag/id557143322?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:

Keep Swiss COVID certificates easily and securely on your mobile phone COVID Certificate is the official app for storing and presenting Swiss COVID certificates. It is developed by the Federal Office of Information Technology, Systems and Telecommunication FOITT on behalf of the Federal Office of Public Health. In Switzerland, people who have been vaccinated, or who have tested negative or recovered from COVID can apply for a COVID certificate. COVID certificates are issued in hard copy or electronic format serve as proof of: 1. Vaccination against COVID-19 2. Recovery from Sars-CoV-2 infection 3. A negative result following Sars-CoV-2 test analysis How the app works When the app is first launched after installation on the mobile device, a brief introduction provides information on how to use it and how to scan a hard-copy COVID certificate. In the app, the required COVID certificate can be selected, and presented if desired. The app shows whether, from when and for how long the COVID certificate is valid. All data contained in a certificate's QR code can also be displayed. It is possible to store several COVID certificates in the app, e.g. for family members, or several COVID test certificates. Use of the COVID Certificate app is voluntary and free of charge. Data protection is a top priority COVID certificate data is stored solely on the mobile device. COVID certificates are protected by a digital seal (signature) and are thus forgery-proof. COVID certificates are generated by the FOITT, but are not stored in a central system. That is why it is not possible to obtain a copy of an issued certificate. The use of the app is limited to Switzerland and is subject to Swiss law.

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.