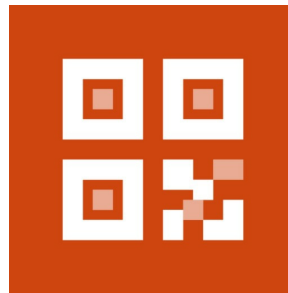




IOS STATIC ANALYSIS REPORT



🍏 Covid19Verify (1.3.10)

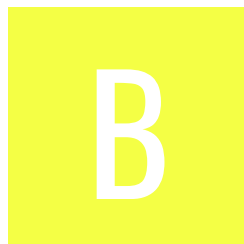
File Name: Covid19Verify.ipa

Identifier: lv.verification.dgc





Scan Date: May 7, 2022, 11:30 a.m.

App Security Score: 44/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 WARNING	 INFO	 SECURE
2	2	0	1

FILE INFORMATION

File Name: Covid19Verify.ipa

Size: 3.32MB

MD5: 5189fa7ee3558d828bba32db5dcf8e6

SHA1: 0d8970c81705302419b01469953c457a13f226c5

SHA256: 0a339eb1515fce66c4a33f155adbd19a1a163d2776581d359a20bae25cfc9bf6

APP INFORMATION

App Name: Covid19Verify

App Type: Swift

Identifier: lv.verification.dgc

SDK Name: iphoneos15.2

Version: 1.3.10

Build: 4

Platform Version: 15.2

Min OS Version: 13.0

Supported Platforms: iPhoneOS,

APPLICATION PERMISSIONS

PERMISSIONS	STATUS	DESCRIPTION	REASON IN MANIFEST
NSCameraUsageDescription	dangerous	Access the Camera.	To be able to scan QR codes

APP TRANSPORT SECURITY (ATS)

NO	ISSUE	SEVERITY	DESCRIPTION
1	App Transport Security AllowsArbitraryLoads is allowed	high	App Transport Security restrictions are disabled for all network connections. Disabling ATS means that unsecured HTTP connections are allowed. HTTPS connections are also allowed, and are still subject to default server trust evaluation. However, extended security checks like requiring a minimum Transport Layer Security (TLS) protocol version—are disabled. This setting is not applicable to domains listed in NSExceptionDomains.

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	False	high	This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.

PROTECTION	STATUS	SEVERITY	DESCRIPTION
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.
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
mths.be	ok	IP: 83.137.145.144 Country: Netherlands Region: Groningen City: Groningen Latitude: 53.219170 Longitude: 6.566670 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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: 17.253.107.202 Country: Denmark Region: Hovedstaden City: Ballerup Latitude: 55.731651 Longitude: 12.363280 View: Google Map
cordova.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
momentjs.com	ok	IP: 104.17.93.38 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
mozilla.github.io	ok	IP: 185.199.108.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
feross.org	ok	IP: 50.116.11.184 Country: United States of America Region: California City: Fremont Latitude: 37.548271 Longitude: -121.988571 View: Google Map
stuartk.com	ok	IP: 75.2.60.5 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
www-cs-students.stanford.edu	ok	IP: 171.64.66.201 Country: United States of America Region: California City: Stanford Latitude: 37.421261 Longitude: -122.163948 View: Google Map

DOMAIN	STATUS	GEOLOCATION
apps.apple.com	ok	IP: 184.50.200.24 Country: Japan Region: Tokyo City: Tokyo Latitude: 35.689507 Longitude: 139.691696 View: Google Map
ocsp.apple.com	ok	IP: 17.253.107.202 Country: Denmark Region: Hovedstaden City: Ballerup Latitude: 55.731651 Longitude: 12.363280 View: Google Map
reactjs.org	ok	IP: 76.76.21.21 Country: United States of America Region: California City: Walnut Latitude: 34.015400 Longitude: -117.858223 View: Google Map
stuk.github.io	ok	IP: 185.199.108.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.covid19sertifikats.lv	ok	IP: 212.70.163.133 Country: Latvia Region: Riga City: Riga Latitude: 56.945999 Longitude: 24.105890 View: Google Map
raw.github.com	ok	IP: 185.199.109.133 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
localforage.github.io	ok	IP: 185.199.108.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
covid19sertifikats.lv	ok	IP: 104.21.8.55 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 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.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
example.com	ok	IP: 93.184.216.34 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
material-ui.com	ok	IP: 159.65.118.56 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map

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
fb.me	ok	IP: 185.60.216.35 Country: United States of America Region: California City: Menlo Park Latitude: 37.453831 Longitude: -122.182190 View: Google Map

EMAILS

EMAIL	FILE
u@jvbph3.`qa	App.app/public/static/media/montserrat-200.af7f01cb.woff
feross@feross.org	App.app/public/static/js/4.27f0ce06.chunk.js.LICENSE.txt

APP STORE INFORMATION

Title: Covid19Verify

Score: 0 **Features:** iosUniversal, **Price:** 0.0 **Category:** Medical, Health & Fitness,

App Store URL: [lv.verification.dgc](https://apps.apple.com/lt/app/covid19verify/id1513573143)

Developer: SPKC

Developer ID: 1513573143

Developer Website: <http://www.vmnvd.gov.lv/>

Developer URL: <https://apps.apple.com/us/developer/spkc/id1513573143?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:

Covid19Verify lietotne sniedz iespēju pārbaudīt atbilstoši EU regulai izsniegto Covid-19 sertifikātu derīgumu un autentiskumu, ievērojot Latvijā pieņemtos noteikumus. Pārbaude tiek veikta skenējot personas uzrādītā sertifikāta QR kodu. Lietotne ļauj noteikt derīgumu šāda veida sertifikātiem – sertifikāts par veikto vakcināciju pret Covid-19, sertifikāts par Covid-19 laboratoriskās pārbaudes rezultātiem, sertifikāts par Covid-19 izslimošanas faktu. Lietotnes izmantošana - atverot lietotni, jāizmanto ierīcē iebūvētā foto kamera un jānoskenē QR kods. Lietotne uzrāda paziņojumu par to, vai noskenētais sertifikāts ir derīgs vai nav derīgs.

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](#).