NGI REVIEW FACILITY.EU

Name: NGI Emergency Tech Review Facility

Contract nr: LC-01499045

Date of signature: 30-04-2020

Name of the deliverable: Deliverable 3.7 –
High-level assessment Base45Decoder of the EU Digital COVID Certificate App Core for Android

Authors: Tim Hummel, Marcus Bointon (Radically Open Security)

Level of distribution: Confidential, only for members of the facility
(including the Commission Services)

Confidential: Yes

Radically Open Security

EU Digital COVID Certificate App Core For Android Base45 Decoder Check

European Commission -
Directorate General CONNECT

V 1.0
Amsterdam, December 15th, 2021
Confidential

Document Properties

Client	European Commission - Directorate General CONNECT
Title	EU Digital COVID Certificate App Core for Android base45 decoder Check
Targets	The Base45Decoder after a patch in the EU Digital COVID Certificate App Core for Android: https://github.com/eu-digital-green-certificates/dgca-app-core-android/pull/67/commits/a55cf03c8edbe44562efa095fc4bb1b446558b1b
Version	1.0
Pentester	Tim Hummel
Authors	Tim Hummel, Marcus Bointon
Reviewed by	Marcus Bointon
Approved by	Melanie Rieback

Version control

Version	Date	Author	Description
0.1	December 14th, 2021	Tim Hummel	Initial draft
1.0	December 15th, 2021	Marcus Bointon	Review

Contact

For more information about this document and its contents please contact Radically Open Security B.V.

Name	Melanie Rieback
Address	Science Park 608 1098 XH Amsterdam The Netherlands
Phone	+31 (0)20 2621 255
Email	info@radicallyopensecurity.com

Radically Open Security B.V. is registered at the trade register of the Dutch chamber of commerce under number 60628081.

Table of Contents

1 Executive Summary

1.1 Introduction

Between December 6, 2021 and December 8, 2021, Radically Open Security B.V. carried out a quick check of the robustness of a Base45Decoder for the European Commission - Directorate General CONNECT.

1.2 Scope of Work

The scope of this evaluation was ONLY the `Base45Decoder.kt` file in the following repository and commit:

https://github.com/eu-digital-green-certificates/dgca-app-core-android/blob/a55cf03c8edbe44562efa095fc4bb1b446558b1b/decoder/src/main/java/dgca/verifier/app/decoder/base45/Base45Decoder.kt

Other files were OUT OF SCOPE and were only looked at for context.

1.3 Project objectives

The objective was to check the robustness of the patched base45 decoder implementation, and to check if it adheres to the standard https://datatracker.ietf.org/doc/html/draft-faltstrom-base45-07#section-6. The reason is to prevent further issues similar to https://github.com/eu-digital-green-certificates/dgca-app-core-android/issues/57 that triggered the release of the patch.

1.4 Timeline

The quick check took place between December 6, 2021 and December 8, 2021.

1.5 Conclusion

We did not discover any issues with the base45 decoder after the patch. It implements all security recommendations from the standard and covers the edge cases. We make some non-essential recommendations in our analysis below.

2 Analysis

We first read the source code and verified that it covers the edge cases. It takes the security considerations of the standard document into account. We then ran the patched base45 decoder ourselves and verified that it successfully discovered the different types of malformed input.

The project's test cases test at a high level. Additional lower level test cases would be desirable, even if surrounding code might prevent invalid input ever reaching the base45 decoder. The test cases actually contain only one malformed base45 test case https://github.com/eu-digital-green-certificates/dgc-testdata/blob/de140226ccfe1faebd376b504fe82907083ba0f9/common/2DCode/raw/B1.json.

The code is written in a compact way. While this is a sign of a skilled developer, longer but possibly simpler code is easier to understand and maintain. The base45 decoder in the corresponding iOS core https://github.com/eu-digital-green-certificates/dgca-app-core-ios/blob/main/Sources/Extensions/String%2BBase45.swift is much easier to understand. We confirmed visually that the iOS base45 decoder also takes the security considerations from the standard into account. We did not run test cases against it as it is not within the scope of this quick check.

Front page image by dougwoods (https://www.flickr.com/photos/deerwooduk/682390157/), "Cat on laptop", Image styling by Patricia Piolon, https://creativecommons.org/licenses/by-sa/2.0/legalcode.