First Round Security Test Anomaly Report of
(DYCE) Digi Yatra Central Ecosystem (iOS Version)

Report No: STQCITTvm /DYCE - iOS/AR(1)-ST / 1040922

STQC IT SERVICES
ERTL(S), STQC Directorate,
Ministry of Electronics & Information Technology
Govt. of India
Akkulam, Sreekariyam.
Thiruvananthapuram 695017
(TEL: 0471 2444896; FAX: 0471 2559943)
e-mail: ittvm@stqc.gov.in
Web: www.stqc.gov.in

Table of Contents

1.0	**Client Details**	
1.1	Name of Client	Digi Yatra Foundation
1.2	Address of Client	Digi Yatra Foundation, I.A.A Niamar T/Center IGI Airport New Delhi, 110037
2.0	**Details of the software Application under Test**	
2.1	Mobile Application Nomenclature	“Digi Yatra Central Ecosystem - DYCE(iOS Version) ”
2.2	Version Number	---
2.3	Date of Release	---
2.4	Software Product Description	The Digi Yatra Central Ecosystem manages Self Sovereign Identity of the passenger by maintaining a digital verifiable credential for any claim he/she wants to proof to the airport. This encompasses the implementation of a digital identity wallet for the user from which the airports can securely request passenger Identity, vaccination and Itinerary information prior to his travel and make his experience at the airport a seamless walk-in-park.
2.5	Applicable Specifications	Security Testing of “Digi Yatra Central Ecosystem -iOS version” as per the following specifications: • OWASP Mobile Application Security Verification Standard Version 1.4 • OWASP Top 10 – 2021 Top10 Critical Security Risks
2.6	Name of the Software Product Developing Organization	Dataevolve
2.7	Supplied Media	The details of deliverables provided by the client: 1. IPA (iOS) o App Name: DigiYatra o Size: 32.35MB o Identifier :org.reactjs.native.example.digiYatra o SDK Name : iphonesimulator15.4 o Version : 1.3 o Min OS version : 11.0 o SHA256 of IPA : c8da117375a7aa00329a07a7214f7f9e1e1c9af121c8dea42f5878cc79f6f667
2.8	Documents Supplied	1. DYCE Technical Implementation Overview

2.9	Date of Receipt of Product	22/08/2022
3.0	**Test Description**	
3.1	Name & Address of Testing Agency	STQC IT SERVICES, ERTL(S), STQC Directorate Ministry of Electronics and Information Technology, Govt. of India, Akkulam, Sreekaryam, Thiruvananthapuram, 695017
3.2	Location of Testing	Same as above
3.3	Scope of Testing	1. Security testing of the iOS Mobile app of DYCE which include the IPA provided by the client. This includes : a. Static Analysis of the mobile application (IPAs only) is performed for vulnerabilities as per OWASP Mobile Application Security Verification Standard Version 1.4 Level 1 verification requirements (MASVS v1.4 L1) 2. Functionality Testing of Critical Business flows to be done in Audit mode 3. Mobile Application Security Testing will be done on the release and debug version of the mobile application provided, and application loaded on the Test Server 4. Third party frameworks along with any other library internals used are not in the scope of testing
3.4	Test Methodology	• For Static Analysis product is verified and scanned for the vulnerabilities as per OWASP Mobile Application Security Verification Standard Version1.4, using the following Open Source tools o MobSF • Source Code Review is done using Fortify Static Code Analyzer 20.2.1.0010 • Manual Analysis was also performed for verification and identification of anomalies

3.5	Standards for Testing	The testing activities (Test Planning, Test Case designing, Defect Reporting & Test Reporting) are being carried out as per following standards: • IEC 29119 • OWASP Mobile Application Security Verification Standard Version 1.4 • OWASP Top 10 – 2021 Top10 Critical Security Risks
3.6	Test Data	▪ The test data used for testing was generated based on test Scenarios for both valid as well invalid cases. ▪ Test database supplied along with software application was also used.
3.7	Test Environment	The following hardware / software configurations have been used for conducting the testing.
	Hardware & Software Configuration (Lab)	Hardware: Laptop(Macbook): Processor: 2.3 GHz Dual-Core Intel Core i5 OS: macOS Catalina version 10.15.7 RAM:8 GB 2133 MHz LPDDR3 iOS Device: Processor: Apple A13 Bionic Operating System: iOS 15.1 Internal Memory: 238GB RAM: 4GB
	Hardware & Software Configuration (Client)	____
3.8	Details of Test Team	Bodda Suman Praveen P S Yash Raizada Sachin Upadhyay
3.9	Period of Testing	22/08/2022 to 21/09/2022

4.0 Anomaly Summary:

1. This test anomaly report documents the results of the first round security testing carried out on iOS version of Digi Yatra Central Ecosystem application.

2. The scope of testing is as stated at Sl. no 3.3

3. The Test Methodology is as specified at sl no 3.4.

   - Static Analysis was done on the IPA file

4. Security Testing was done on the iOS version of the Digi Yatra Central Ecosystem Mobile Application

   - Static Analysis was carried out as per OWASP Mobile Application Security Verification Standard Version 1.4 Level 1 verification requirements (MASVS v1.4 L1) on the IPA of the application provided by the client for iOS platform.
   - Third party frameworks along with any other library internals used are not in the scope of testing

5. Source Code Review of iOS version of the mobile application was performed using the tools mentioned at sl no 3.7

6. Correctness/Legal implication of information content has not been verified.

7. The MASVS Compliance Summary Details are given in Annexure A. The details of the anomalies are given in Annexure B having the following sections:
   - Static Analysis
   - Source Code Review
   - Dynamic Analysis

8. Permissions used by the application are given in Annexure C. Explanation is required from the developer as to whether these permissions are required by the app for its operation

9. Tool report for source code analysis is given as Annexure D.

5.0 Approvals

Approved & Released by

Reji Nair
Sr. Director/ Scientist G,
Head, STQC IT Centre,
Thiruvananthapuram.

Annexure A

Summary Report MASVS Compliance Summary

V1	Architecture, design and threat modelling		
1.1	MSTG-ARCH-1	All app components are identified and known to be needed.	The components identified during the analysis are mentioned in Annexure C. Explanation required from developer to verify whether they are all needed
1.2	MSTG-ARCH-2	Security controls are never enforced only on the client side, but on the respective remote endpoints.	Fail - Refer Annexure B for remote endpoint vulnerabilities.
1.3	MSTG-ARCH-3	A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	Pass - A high level architecture design was provided by the client.
1.4	MSTG-ARCH-4	Data considered sensitive in the context of the mobile app is clearly identified.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
1.12	MSTG-ARCH-12	The app should comply with privacy laws and regulations	Fail - Refer Annexure B II- 2
V2	Data Storage and Privacy		
2.1	MSTG-STORAGE-1	System credential storage facilities are used appropriately to store sensitive data, such as PII, user credentials or cryptographic keys.	Fail - Refer Annexure B II- 2
2.2	MSTG-STORAGE-2	No sensitive data should be stored outside of the app container or system credential storage facilities.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
2.3	MSTG-STORAGE-3	No sensitive data is written to application logs.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
2.4	MSTG-STORAGE-4	No sensitive data is shared with third parties unless it is a necessary part of the architecture.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
2.5	MSTG-STORAGE-5	The keyboard cache is disabled on text inputs that process sensitive data.	Pass – The keyboard cache is disabled for data entered in password field.
2.6	MSTG-STORAGE-6	No sensitive data is exposed via IPC mechanisms.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
2.7	MSTG-STORAGE-7	No sensitive data, such as passwords or pins, is exposed through the user interface.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
2.10	MSTG-STORAGE-10	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
2.12	MSTG-STORAGE-12	The app educates the user about the types of personally identifiable information processed, as well as security best practices the user should follow in using the app.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**

2.13	MASVS: MSTGSTORAGE-14	Files may Contain Hardcoded Sensitive Information like usernames, passwords, keys etc.	Fail Refer Annexure B II- 4, 12 for details.
V3	Cryptography		
3.1	MSTG-CRYPTO-1	The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
3.2	MSTG-CRYPTO-2	The app uses proven implementations of cryptographic primitives.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
3.3	MSTG-CRYPTO-3	The app uses cryptographic primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
3.4	MSTG-CRYPTO-4	The app does not use cryptographic protocols or algorithms that are widely considered deprecated for security purposes.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
3.5	MSTG-CRYPTO-5	The app doesn't re-use the same cryptographic key for multiple purposes.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
3.6	MSTG-CRYPTO-6	All random values are generated using a sufficiently secure random number generator.	Fail – . Refer Annexure B II- 3 for details.
V4	Authentication and Session Management		
4.1	MSTG-AUTH-1	If the app provides users access to a remote service, some form of authentication, such as username/password authentication, is performed at the remote endpoint.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
4.2	MSTG-AUTH-2	If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
4.3	MSTG-AUTH-3	If stateless token-based authentication is used, the server provides a token that has been signed using a secure algorithm.	Fail - Refer Annexure B II- 9 for details
4.4	MSTG-AUTH-4	The remote endpoint terminates the existing session when the user logs out.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
4.5	MSTG-AUTH-5	A password policy exists and is enforced at the remote endpoint.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
4.6	MSTG-AUTH-6	The remote endpoint implements a mechanism to protect against the submission of credentials an excessive number of times.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**

4.7	MSTG-AUTH-7	Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access tokens expire.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
4.12	MSTG-AUTH-12	Authorization models should be defined and enforced at the remote endpoint.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
V5	Network Communication		
5.1	MSTG-NETWORK-1	Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.	Fail - Refer Annexure B II- 1 , for details
5.2	MSTG-NETWORK-2	The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.	Fail - Refer Annexure B II- 1 , for details
5.3	MSTG-NETWORK-3	The app verifies the X.509 certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
5.4	MASVS: MSTGNETWORK-4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
V6	Platform Interaction		
6.1	MSTG-PLATFORM-1	The app only requests the minimum set of permissions necessary.	Fail - Refer Annexure B II- 5, 6, 7, 8
6.2	MSTG-PLATFORM-2	All inputs from external sources and the user are validated and if necessary sanitized. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.	Fail - Refer Annexure B II- 15
6.3	MSTG-PLATFORM-3	The app does not export sensitive functionality via custom URL schemes, unless these mechanisms are properly protected.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
6.4	MSTG-PLATFORM-4	The app does not export sensitive functionality through IPC facilities, unless these mechanisms are properly protected.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
6.5	MSTG-PLATFORM-5	JavaScript is disabled in WebViews unless explicitly required.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
6.6	MSTG-PLATFORM-6	WebViews are configured to allow only the minimum set of protocol handlers required (ideally, only https is supported). Potentially dangerous handlers, such as file, tel and app-id, are disabled.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
6.7	MSTG-PLATFORM-7	If native methods of the app are exposed to a WebView, verify that	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**

		the WebView only renders JavaScript contained within the app package.	
6.8	MSTG-PLATFORM-8	Object deserialization, if any, is implemented using safe serialization APIs.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
V7	Code Quality and Build Settings		
7.1	MSTG-CODE-1	The app is signed and provisioned with a valid certificate, of which the private key is properly protected.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
7.2	MSTG-CODE-2	The app has been built in release mode, with settings appropriate for a release build (e.g. non-debuggable).	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
7.3	MSTG-CODE-3	Debugging symbols have been removed from native binaries.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
7.4	MSTG-CODE-4	Debugging code has been removed, and the app does not log verbose errors or debugging messages.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
7.5	MSTG-CODE-5	All third party components used by the mobile app, such as libraries and frameworks, are identified, and checked for known vulnerabilities.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
7.6	MSTG-CODE-6	The app catches and handles possible exceptions.	Fail - Refer Annexure B Cl 13, 14 for details
7.7	MSTG-CODE-7	Error handling logic in security controls denies access by default.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
7.8	MSTG-CODE-8	In unmanaged code, memory is allocated, freed and used securely.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**
7.9	MSTG-CODE-9	Free security features offered by the toolchain, such as byte-code minification, stack protection, PIE support and automatic reference counting, are activated.	Refer Report No: **STQCITTvm /DYCE-Android /TR-ST / 1040822**

Annexure B

Anomaly Details

Sl. No.	Issue/Location	Description	Level
I	**Static Analysis Report**		
1.	App Transport Security AllowsArbitaryLoads is Allowed	App Transport Security restrictions are disabled for all network connections.Disabling ATS means that unsecured HTTP connections are allowed.HTTP connections are also allowed,and are still subject to default server trust evaluation.	High

II	Source Code Review		
1.	Insecure Transport: Disabled App Transport Security (Security Features, Configuration)	Disabling App Transport Security (ATS) partially or entirely may expose the application to network attacks.	High
2.	Privacy Violation: iOS Property List (Security Features, Configuration)	The data may represent private information in an unprotected iOS Property List file.	High
3.	Insecure Randomness (Security Features, Structural)	The random number generator implemented by random() cannot withstand a cryptographic attack.	High
4.	Password Management: Password in Configuration File (Environment, Configuration)	Storing a plain text password in a configuration file may result in a system compromise.	High
5.	Privilege Management: Android Camera (Security Features, Configuration)	e application declares the use of a permission that controls access to the device's camera on line 6 and 7 of AndroidManifest.xml.	High
6.	Privilege Management: Android Data Storage (Security Features, Configuration)	The program requests permission to write data to Android's external storage on line 9 and 10 of AndroidManifest.xml	High
7.	Privilege Management: Android Microphone (Security Features, Configuration)	The application declares the use of a permission that controls access to the device microphone on line 8 of AndroidManifest.xml.	High
8.	Privilege Management: Unnecessary Permission (Security Features, Configuration)	The application fails to adhere to the principle of least privilege, which greatly amplifies the risk posed by other vulnerabilities.	High
9.	Cross-Site Request Forgery (Encapsulation, Structural)	The HTTP request must contain a user-specific secret to prevent an attacker from making unauthorized requests	Low
10.	Insecure Storage: Android Backup Storage (Encapsulation, Configuration)	The program uses Android's backup service to save persistent application data to a remote cloud storage.	Low
11.	JavaScript Hijacking: Vulnerable Framework (Encapsulation, Structural)	Applications that use JavaScript notation to transport sensitive data can be vulnerable to JavaScript hijacking, which allows an unauthorized attacker to read confidential data from a vulnerable application.	Low
12.	Password Management: Password in Comment (Security Features, Structural)	Storing passwords or password details in plain text anywhere in the system or system code may compromise system security in a way that cannot be easily remedied.	Low
13.	Poor Error Handling: Overly Broad Catch (Errors, Structural)	The catch block at AgentModule.java line 203 and 264 handles a broad swath of exceptions, potentially trapping dissimilar issues or problems that should not be dealt with at this point in the program.	Low

14.	Poor Style: Value Never Read (Code Quality, Structural)	The method agentRequestMethod() in AgentModule.java never uses the value it assigns to the variable ResponsePayload on line 258.	Low
15.	SQL Injection (Input Validation and Representation, Structural)	The program invokes a SQL query built using input potentially coming from an untrusted source. This call could allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.	Low
16.	System Information Leak (Encapsulation, Semantic)	Function reveals system data or debug information by calling printStackTrace() on line. The information revealed by printStackTrace() could help an adversary form a plan of attack.	Low

Annexure C

Permissions

The following permissions have been observed in the mobile app. Explanation is required from the developer as to whether these permissions are required by the app for its operation

SI No	Permission	Info	Description
1.	NSCameraUsageDescription	Access the Camera	Please allow access to iPhone camera
2.	NSLocationWhenInUseUsageDescription	Access location information when app is in the foreground.	----
3.	NSPhotoLibraryUsageDescription	Access the user’s photo library	DigiYatra2 would like access to your photo gallery