Guidelines On Participation in the Fiji Quick Response Code Scheme

Reserve Bank of Fiji

19 May 2026

GUIDELINES ON PARTICIPATION IN THE FIJI QUICK RESPONSE CODE SCHEME (FJQR)[1]

1. Introduction

1.1. Purpose

This document sets out the guidelines for Payment Service Providers (PSPs) participating in the Fiji Quick Response (QR) Code Scheme ("the Scheme"). It outlines the obligations and expectations of PSPs with respect to the generation, issuance, management, and support of merchant-presented QR codes under a national interoperable standard.

The aim is to promote a unified, secure, and inclusive retail payment ecosystem, by ensuring QR code solutions are interoperable across PSPs and accessible to all merchants and consumers. In doing so, the Scheme supports the broader objectives of the National Payment System in improving payment system efficiency, enhancing user experience to drive adoption, ensuring the continued safety and security of the payments system, and establishing a future-ready system.

These Guidelines supplement the Fiji QR Code (FJQR) Technical Specification and must be read in conjunction with applicable regulatory instruments issued by the Reserve Bank of Fiji (RBF), alongside all other relevant laws, subsidiary legislation, directives, codes, and additional guidance that may be issued by the Government of Fiji from time to time. PSPs participating in the Scheme are expected to align with these Guidelines to ensure that the Scheme achieves its intended objectives.

1.2. Scope

These Guidelines apply to all PSPs participating in the FJQR Scheme by means of a static QR code,[2] and cover the following:

- Definitions of key stakeholders participating in the FJQR Scheme.
- Operational model underlying the FJQR Scheme.
- Eligibility and participation requirements for PSPs.
- Obligations of PSPs to merchants, including operational and technical support.
- QR code configuration and presentation requirements.
- Branding standards for QR Code Labels.

These Guidelines do not cover:

- Technical specifications and data structures, which are separately documented in the FJQR Technical Specification, aligned with the EMV® Merchant-Presented Mode (MPM) QR standard.[3]

[1] Interim name – to be decided by RBF.
[2] The FJQR Scheme does not currently, but is expected to, accept dynamic and customer-presented QR codes in the future. A separate Customer-Presented Mode (CPM) QR standard will be developed. The FJQR Scheme is not expected to cover peer-to-peer (P2P) QR payments.
[3] EMV® QR Code Specification for Payment Systems – Merchant-Presented Mode, EMVCo, Version 1.1.

2. Background

2.1. Background

A QR code is a two dimensional barcode that stores encoded data, which can be scanned by a mobile device to initiate electronic payments. A QR code functions as an overlay, and QR-initiated payments are processed through existing payment rails (e.g., fast payment systems, card payment schemes, and other proprietary platforms). In a merchant-presented model, the merchant displays their choice(s) of preferred QR code(s). From this array of QR code(s), the consumer then selects a QR code of their choice and scans it using a payment application. In addition to broader objectives stated above, the adoption of a standardised QR code across Fiji provides for the following:

- Streamlines roles and responsibilities for QR generation/management.
- Supports a secure customer experience by ensuring standard security processes; and
- Promotes the broader adoption of digital transactions across merchants and consumers.

The FJQR Scheme is built on the EMV® MPM QR specifications, version 1.1, to ensure a high level of interoperability and compatibility across different payment providers, and to provide a strong foundation for future efforts on cross-border interoperability. The EMV® MPM QR standard has been adopted internationally across Africa, Europe, Asia, and South America.

2.2. Definitions

For the purposes of these Guidelines:

- **Reserve Bank of Fiji (RBF)**: The national regulatory authority responsible for oversight of payment systems. The RBF is also the authority responsible for the implementation, management, and operation of the FJQR Scheme, which includes designating and enforcing technical, operational, and security standards for the FJQR Scheme.

- **Payment Service Providers (PSPs)**: Licensed or authorised financial entities that provide a payment service or operate a payment system.

- **Merchant Registry**: A database owned and operated by each participating PSP, that stores relevant merchant information deemed essential by the PSP. While the merchant information stored within a participating PSP's merchant registry remains their prerogative, PSPs are required to conduct due diligence prior to onboarding merchants, in alignment with obligations outlined in the RBF Payment Service Provider Supervision Policy Statement No. 1.

- **Certificate Authority (CA)**: A trusted entity operated by the RBF, that facilitates the use of cryptographic techniques to ensure the confidentiality, authenticity, and integrity of information in electronic form. Within the scope of these guidelines, the CA signs the public keys generated by participating PSPs for use within the FJQR Scheme with the CA's appropriate private key, which helps to secure the authenticity and integrity of QR codes issued under the FJQR Scheme.

- **Public-Private Key Pair**: A public-private key pair is generated by each participating PSP. The private key is used to cryptographically sign the content of a QR code, whilst the public key is used to verify the authenticity and integrity of a QR code. For each public-private key pair, the PSP will store and retain the private key used for the signing of generated QR codes, while the corresponding public key will be submitted to the CA for countersigning. In countersigning, the public key will form part of a Public Key Certificate (see next item).

- **Public Key Certificate (PKC)**: A unique Public Key Certificate is generated for each PSP when the CA signs each public key (submitted by participating PSPs) with the CA's own private key and returns the PKC to the relevant PSP. The PKC will then be used to verify the authenticity of QR codes issued under the FJQR Scheme.[4]

- **Merchant**: An individual or business that accepts payment in exchange for goods and services. Within the scope of these guidelines, a merchant is an individual or business that contracts with a payment service provider for accepting payment for goods and services, by means of a QR code.

- **Consumer**: An individual who makes payment to a merchant in exchange for goods and services. Within the scope of these guidelines, the consumer is an individual that uses a mobile application or device to scan a QR code and make a digital payment.

- **Merchant-Presented QR Code (MPM)**: A QR code displayed by the merchant for the consumer to scan.

- **Static QR Code**: A QR code with fixed merchant information, reused for multiple transactions. They usually contain basic merchant information, such as the merchant identifier (merchant ID), merchant "doing business as" name, merchant branch identifier, and PSP details. Upon scanning a static QR code, customers first verify the merchant "doing business as" name and (where applicable) retail branch, then manually enter the transaction amount before proceeding with the payment.

- **Dynamic QR Code**:[5] A QR code uniquely generated for each transaction and includes specific transaction details such as the amount, merchant information, and a unique transaction reference. This allows automatic processing, minimises manual input errors, and improves transaction traceability and reconciliation.

- **QR Code Label:** A physical or digital output label generated by merchants' acquiring PSPs for display, that includes elements such as the unique FJQR Code, Scheme logo, and PSP logo.

[4] During a payment transaction, a customer's payment application retrieves the PSP's PKC from the QR code. The application then validates the authenticity of the PKC by using the CA's public key. Once successful, the PKC itself is used to verify the authenticity of the QR code issued under the FJQR Scheme by the PSP. Further detail on the authentication process can be found in Section 3.3.

[5] The FJQR Scheme does not currently, but is expected to, accept dynamic QR codes in the future.

3. Operational Model

3.1. Overview

The operational architecture of the FJQR Scheme is defined by three core components:

- **Federated Merchant Registries** that allow participating PSPs to manage their own merchant registries, while enabling the RBF to maintain oversight of selected QR payment information for supervisory purposes through periodic reporting by PSPs.

- **Certificate Authority** to generate PKCs for use within the FJQR Scheme, which helps to secure the authenticity and integrity of signed FJQR Codes.

- **Display of Multiple QR Codes** to give merchants the option to present to consumers the QR Code Label(s) for any PSPs that they have an established relationship with.

Figure 1: Illustration of the Federated Merchant Registries

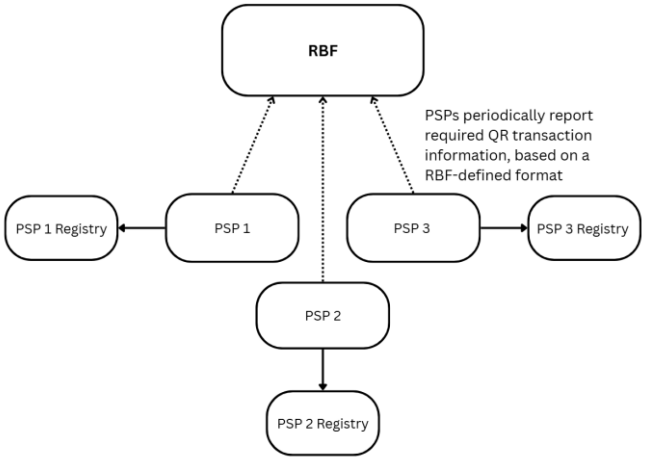
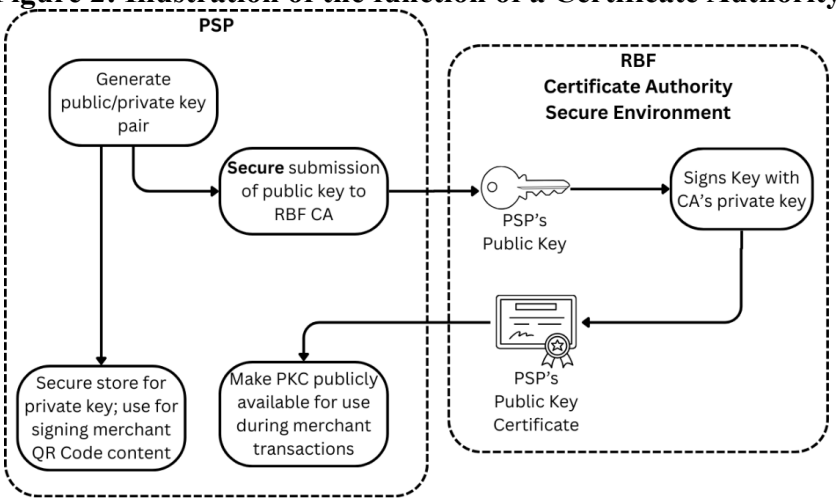


Figure 2: Illustration of the function of a Certificate Authority



This model aligns with the RBF's key objectives to improve transaction efficiency, enable regulatory oversight, and establish a future-ready payment system.

Federated Merchant Registries

The FJQR Scheme allows participating PSPs to manage their individual merchant registries, while ensure that the RBF maintains oversight over QR payments for supervisory purposes through periodic reporting of selected information by PSPs. Under this arrangement:

- Participating PSPs may, with the merchant's consent, store any merchant information that they deem essential for their commercial operations, and maintain their respective merchant registries in their desired data formats;
- Participating PSPs are required to conduct due diligence prior to onboarding merchants, in alignment with obligations outlined in the RBF Payment Service Provider Supervision Policy Statement No. 1;
- For supervisory purposes, participating PSPs are required to report on a monthly basis, to the RBF (in an RBF-defined format), in alignment with the National Payments System Act 2021 and Regulations 2022:
    - Total value and volume of QR payment transactions (both on-us and off-us) processed by the PSP;
    - Merchant business name;
    - Merchant ID;
    - Trading address(es);
    - Business registration number;
    - Principal owner(s);
    - Merchant trading name(s);
    - Merchant category code (MCC).
- In the event that merchants have been revoked by a participating PSP, the participating PSP is required to notify the RBF within 24 hours of its occurrence.

3.2. Certificate Authority

The FJQR Scheme will leverage the RBF's role as a CA to generate a unique PKC for each PSP. Under this arrangement:

- Each participating PSP generates their unique public-private key pair designated for use within the FJQR Scheme, and submits their public key to the RBF while securely storing and retaining the private key;
- The RBF, through its role as a CA, signs each participating PSP's public key with the CA's private key appropriate to the FJQR Scheme, to generate a unique PKC for the PSP.[6]

The above steps need to be undertaken by participating PSPs as a prerequisite to the issuing of a merchant-presented QR code. In addition:

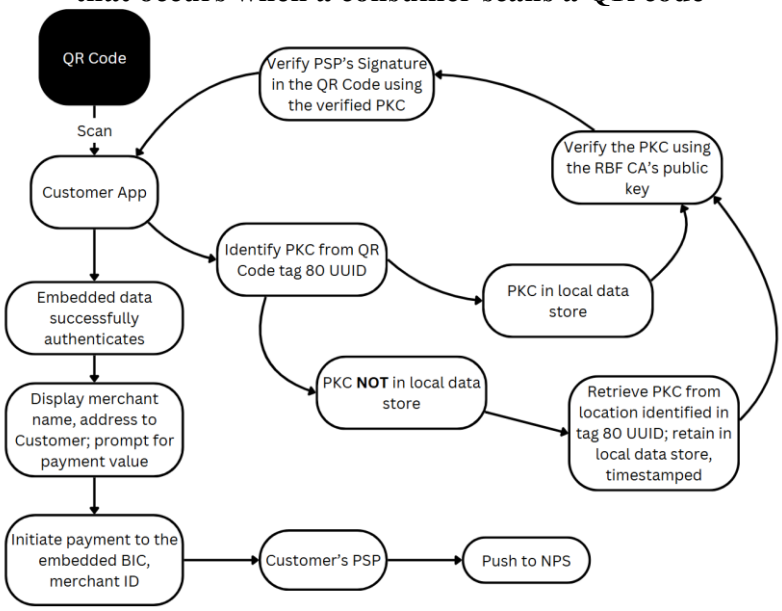
- Participating PSPs are required to sign all generated QR codes with their respective private keys before the issuance of QR codes to their acquired merchants. The act of signing ensures that each QR code is generated by a PSP participating in the FJQR Scheme, and that the QR codes have not been tampered with.

[6] The Certificate Authority also has a public-private key pair. The private key is used by the CA to sign PSPs' public keys, transforming them into public key certificates; and the public key is used to validate the PKCs.

When a consumer scans a signed QR code at the point of transaction, their consumer applications will (see Figure 3 below):

- Extract the QR code content to identify the issuing PSP via the embedded Business Identifier Code (BIC);
- Identify and fetch the issuing PSP's PKC via a reverse URL look-up process;
- Upon retrieval, validate the authenticity of the PKC against the CA's public key that is embedded within the PSP application. This step ensures that the PKC has been issued by a trusted CA;
- Verify the PSP's signature in the QR code content against the PSP's public key, which is located within the PKC. This step ensures that the QR code has been issued by a PSP participating in the FJQR Scheme.

Figure 3: Illustration of the QR code authentication process that occurs when a consumer scans a QR code



To ensure that consumer applications can successfully authenticate Scheme-issued QR codes:

- Participating PSPs are required to retrieve the CA's public key from the CA and embed it within their applications. Participating PSPs are also required to ensure that the embedded CA public key is updated within one month following notification of any change. The prior CA public key should remain valid within the application for one month to allow for an overlap in validity;

- Participating PSPs are required to maintain a local store of retrieved PKCs in their PSP applications for a month, with each entry indexed by BIC and accompanied by a timestamp. The use of a local store promotes transactional efficiency by minimising the need for the application to fetch PKCs repeatedly at each transaction;

- When the CA has added a compromised PKC to the key revocation list,[7] participating PSPs are required to remove the PKC in their local stores immediately upon notification, and replace the compromised PKC with an updated PKC from the relevant issuing PSP;
- Participating PSPs are required to regenerate their PKCs at a frequency to be defined by the CA, or immediately upon detection of compromise of their private keys.

3.3. Display of Multiple QR Codes

The FJQR Scheme will utilise a multiple QR code model that permits merchants to display multiple QR Code Labels (and per till, if needed). Under this arrangement:

- All participating PSPs will generate, sign, and issue a PSP-specific QR Code Label for their acquired merchants at onboarding;
- Merchants can choose to display whichever FJQR Code Label(s) (from any participating PSP they have established a relationship with) they wish to have the payments routed to;
- A merchant may have multiple merchant IDs, one with each PSP it is onboarded with.

4. Eligibility and Participation

4.1. PSP Eligibility

Participation in the Scheme is mandatory only for PSPs that issue merchant-presented QR codes in Fiji.[8] To be eligible, a PSP must:

- Be licensed or authorised to provide payment services under the National Payment System Act 2021 and Regulations 2022 in Fiji;
- Demonstrate operational capability to:
    - Onboard and train merchants to offer QR payments;
    - Provide ongoing merchant and customer support and technical assistance for QR payments;
    - Resolve QR payment-related disputes and incidents;
    - Ensure compliance with reporting requirements and update intervals outlined in Sections 3.2 and 3.3 respectively;
    - Ensure compliance with technical, data, and operational standards indicated in the Fiji QR Code (FJQR) Technical Specification;
    - Process QR payment transactions, including initiation, authentication, authorisation, and settlement that are compliant with FIJICLEAR's specifications.
- Maintain risk management practices including cybersecurity, operational resilience, and consumer protection in alignment with procedures laid out in the National Payments System Act 2021 and Regulations 2022 and the RBF Payment Service Provider Supervision Policy Statement No. 1. PSPs must notify the RBF of their intent to participate in the Scheme and submit a registration request.

[7] A key revocation list is a compilation of public key certificates that have been revoked by the CA prior to their original expiration date.

[8] PSPs that do not offer a merchant-presented static QR code as part of its payment services are not required to participate in the FJQR Scheme.

Obligations of PSPs to Merchants

4.2. Responsibilities of PSPs

PSPs must ensure that merchants receive effective support and that QR codes deployed at merchant locations are reliable, secure, and aligned with these Guidelines. PSPs must:

- Facilitate merchant onboarding processes and conduct due diligence (e.g., Know Your Business (KYB)/Know Your Customer (KYC) checks) in alignment with the RBF Payment Service Provider Supervision Policy Statement No. 1;
- Submit all transaction information required for reporting to the RBF (in alignment with the National Payment System Act 2021 and Regulations 2022), in compliance with the RBF-defined format and adhering to the reporting intervals outlined in Section 3.2;
- Ensure that generated QR Code Labels (i) meet the standards outlined in the FJQR Technical Specifications; and are (ii) digitally signed before distributing the QR Code Labels to merchants;
- Ensure that its PKC is refreshed in accordance with the timelines outlined in Section 3.3;
- Provide and distribute training and materials to merchants on how to use and display QR Code Labels;
- Ensure technical support channels are available for merchants to resolve QR-related complaints within twenty-one working days, in alignment with the Policy Statement on Minimum Requirements for Risk Management Frameworks of Licensed Payment Service Providers in Fiji;
- Provide mechanisms for consumer dispute resolution and fraud management related to QR payments, in alignment with national guidelines (such as the National Payment System Act 2021, National Payment System Act 2021 and Regulations 2022, and RBF Payment Service Provider Supervision Policy Statement No. 1).

4.2.1. Operational and technical support

PSPs must:

- Provide clear onboarding documentation to merchants;
- Generate, sign, and issue QR Code Labels that are accurate and compliant with the national QR specification;
- Regenerate, resign, and reissue QR Code Labels that are outdated, unreadable, or damaged in a timely manner;
- Maintain accessible communication channels for merchant support, including helpdesks or service portals;
- Process and respond to merchant complaints, including incidents relating to fraud, in alignment with the National Payment System Act 2021, National Payment System Act 2021 and Regulations 2022, and RBF Payment Service Provider Supervision Policy Statement No. 1.
-

4.2.2. Template Configuration

When issuing QR Code Labels to onboarded merchants, PSPs should observe the following presentation standards:

- **Print Quality**:
    - For printed/laminated QR Code Labels, use high-resolution printing on durable, weather-resistant materials to avoid degradation.
    - For digital QR Code Labels, use a high-resolution display to ensure clear rendering of QR Codes.

- **Minimum Size**: QR codes must be at least 3 cm x 3 cm in size to allow easy scanning from approximately 15-30 cm away.

- **Display Location**: Encourage merchants to display their QR Code Labels prominently (e.g., at the cashier counter) to facilitate fast and accurate consumer scanning.

- **Environmental Considerations**: Encourage merchants to place their QR Code Labels away from direct sunlight and reflective surfaces, where possible, to avoid scanning issues.

5. Branding Standards

5.1. Standardised Branding Elements

Figure 4: Preliminary mock-up of FJQR Code Label

Uniform branding enhances the visibility and credibility of the FJQR Scheme. All QR Code Labels issued to merchants must include the following (see Figure 4):

- **FJQR Logo:** Clearly displayed according to RBF-issued branding guidelines;
- **Merchant Name:** Displayed prominently above the QR code;
- **Merchant ID:** Displayed prominently below the QR code;

- **PSP Logo:** Logos of the acquiring PSP must be included, ensuring merchants and consumers are informed of the PSP to which payments will be routed;
- **Layout and Colour Schemes:** Standardised background colours, fonts, and layout must be used to ensure a consistent identity;
- **Tampering Prevention:** Use tamper-evident features where feasible and regularly check for unauthorised replacement of QR labels.

PSPs must ensure that no additional branding or marketing content supersedes the official Scheme elements.

QR Code Labels must be kept up to date. If a merchant changes their name or supported payment methods, the QR Code Label must be regenerated and reissued accordingly.

RESERVE BANK OF FIJI