

QR Code Specification Document For Retail Payments in Fiji



Merchant-Presented Mode

Version 3.0
Sept 2025

Document History

Date	Version	Amendment/Change Description
11 April 2025	1.0	First Draft
01 Aug 2025	2.0	Updated the first draft (following the submission of written stakeholder feedback)
30 Sept 2025	3.0	Updated the first draft (following in-person industry consultations)

Table of Contents

1. INTRODUCTION	4
1.1 Purpose	4
1.2 Scope	4
1.3 References	7
1.4 Abbreviations	8
2. DATA OBJECTS FOR FJQR	9
2.1 Payload Format Indicator (ID "00")	11
2.2 Point of Initiation Method (ID "01")	11
2.2.1 Merchant Account Information (ID "02" - "51")	11
2.3 Merchant Category Code (ID "52")	12
2.4 Transaction Currency (ID "53")	12
2.5 Transaction Amount (ID "54")	12
2.6 Tip or Convenience Indicator (ID "55")	12
2.7 Value of Convenience Fee Fixed (ID "56")	12
2.8 Value of Convenience Fee Percentage (ID "57")	13
2.9 Country Code (ID "58")	13
2.10 Merchant Name (ID "59")	13
2.11 Merchant City (ID "60")	13
2.12 Postal Code (ID "61")	13
2.13 Additional Data Field Template (ID "62")	13
2.14 Merchant Information - Language Template (ID "64")	16
2.15 RFU for EMVCo (IDs "65" to "79")	16
2.16 Unreserved Templates (IDs "80" to "99")	16
2.17 Cyclic Redundancy Check (IDs "63")	16
3. FJQR MERCHANT ACCOUNT INFORMATION (ID "02" - "51")	17
3.1 Operational Considerations	19
3.1.1 Merchant Registry	19
3.1.2 Public Key Certificates	20
3.1.3 QR Code Generation	21
3.1.4 Customer Application	21
3.1.5 QR Code Scanning & Payment Initiation	22
3.1.6 Merchant Payment Settlement	24
3.1.7 Cross-Cutting Considerations	24
4. ADDITIONAL DATA FIELD TEMPLATE (ID "62")	26

4.1 Scenario 1: Single Receiving Account for All Checkout Counters	26
4.2 Scenario 2: Unique Receiving Accounts Per Checkout Counter	26
4.3 Scenario 3: Merchant Without Multiple Counters	27
5. Digital Signature (ID "80")	28
5.1 UUID Generation and Management	29
5.2 Signature Generation	29
5.3 Verification Workflow	29
APPENDIX	31
Appendix -1: Mapping: FJQR Code Tags with ACH pacs.008.001.07	31
Appendix -2: Example QR Code Breakdown	34
Appendix -3: ACH pacs.008.001.07 Message (fragment) with FJQR Mapping	35

1. INTRODUCTION

The project aims to support the Government of Fiji in its QR code payment standardization process, ensuring a unified and interoperable digital payment ecosystem. This initiative is designed to enhance payment efficiency, accessibility, and security while fostering financial inclusion across the country.

1.1 Purpose

The purpose of this document is to establish a standardized framework for QR code-based payments in Fiji, ensuring interoperability, security, and efficiency across Payment Service Providers (PSPs) participating in the Reserve Bank of Fiji's (RBF) National Payment System (NPS).

This Specification Document outlines the adoption of globally recognized standards, such as the EMV Co. Merchant Presented Model,¹ to facilitate seamless and secure digital transactions. It provides a clear rationale for standardization and details the proposed technical specifications, including data elements related to customers, merchants, transactions, payment schemes, and interoperability support. Additionally, it defines the allocation of data object IDs to ensure consistency and compatibility within Fiji's payment ecosystem.

By implementing this standardized approach, the RBF aims to promote financial inclusion, enhance user experience, and foster a more efficient, secure, and scalable digital payment infrastructure in Fiji.

1.2 Scope

This specification defines the requirements for a standardized QR code payment framework in Fiji, adopting the EMV® Merchant-Presented QR Code (MPM) model. It encompasses both dynamic and static QR code use cases to support a wide range of merchant and customer needs.²

The scope of this specification includes:

EMV® Merchant-Presented QR Code (MPM) Payments: Merchants will generate and display QR codes that customers can scan using mobile banking apps, e-wallets, or other compliant payment applications. The QR codes follow the EMV® standard³ to ensure interoperability across different financial service providers within Fiji.

Static QR Codes: 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 trading-as name, merchant branch identifier, and PSP details. Upon scanning a static QR code, customers first verify the merchant trading-as name

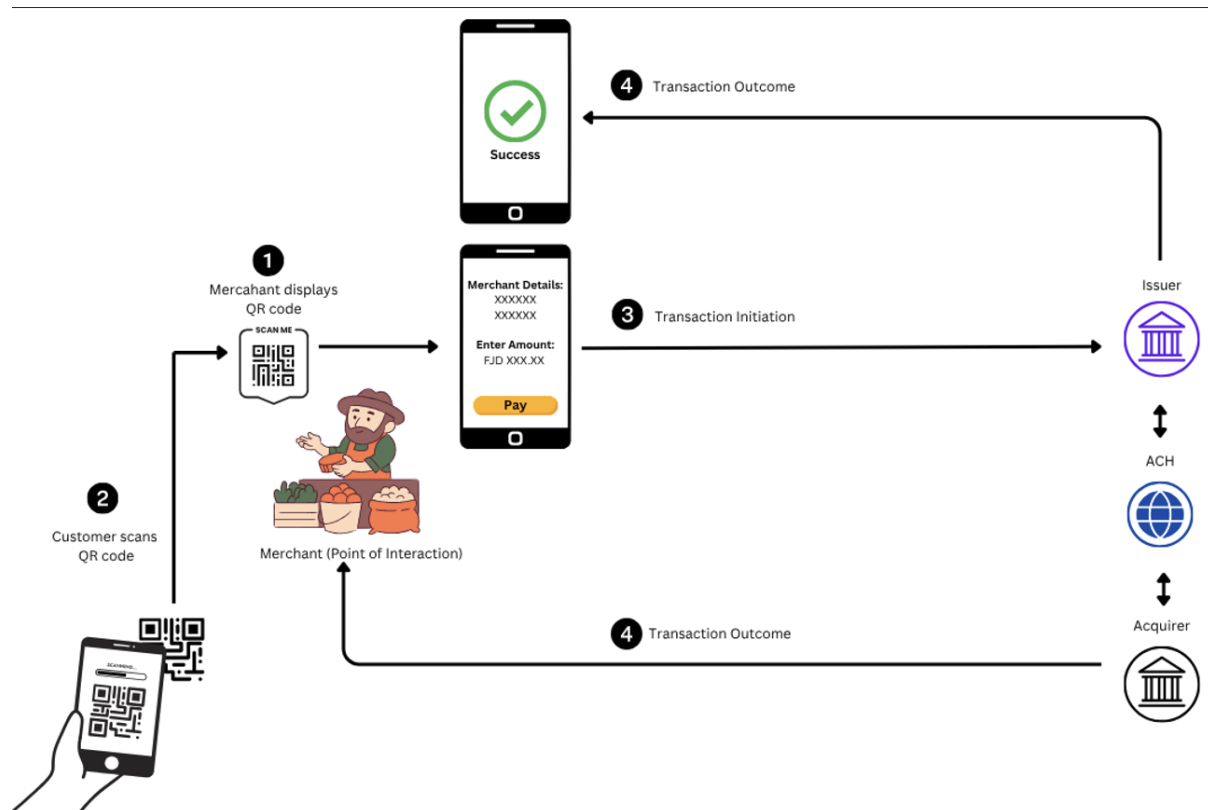
¹ EMV® QR Code Specification for Payment Systems – Merchant-Presented Mode, EMVCo, Version 1.1.

² The FJQR Scheme does not currently include dynamic QR codes, but the design makes provision for this in the future.

³ EMV® QR Code Specification for Payment Systems – Merchant-Presented Mode, EMVCo, Version 1.1.

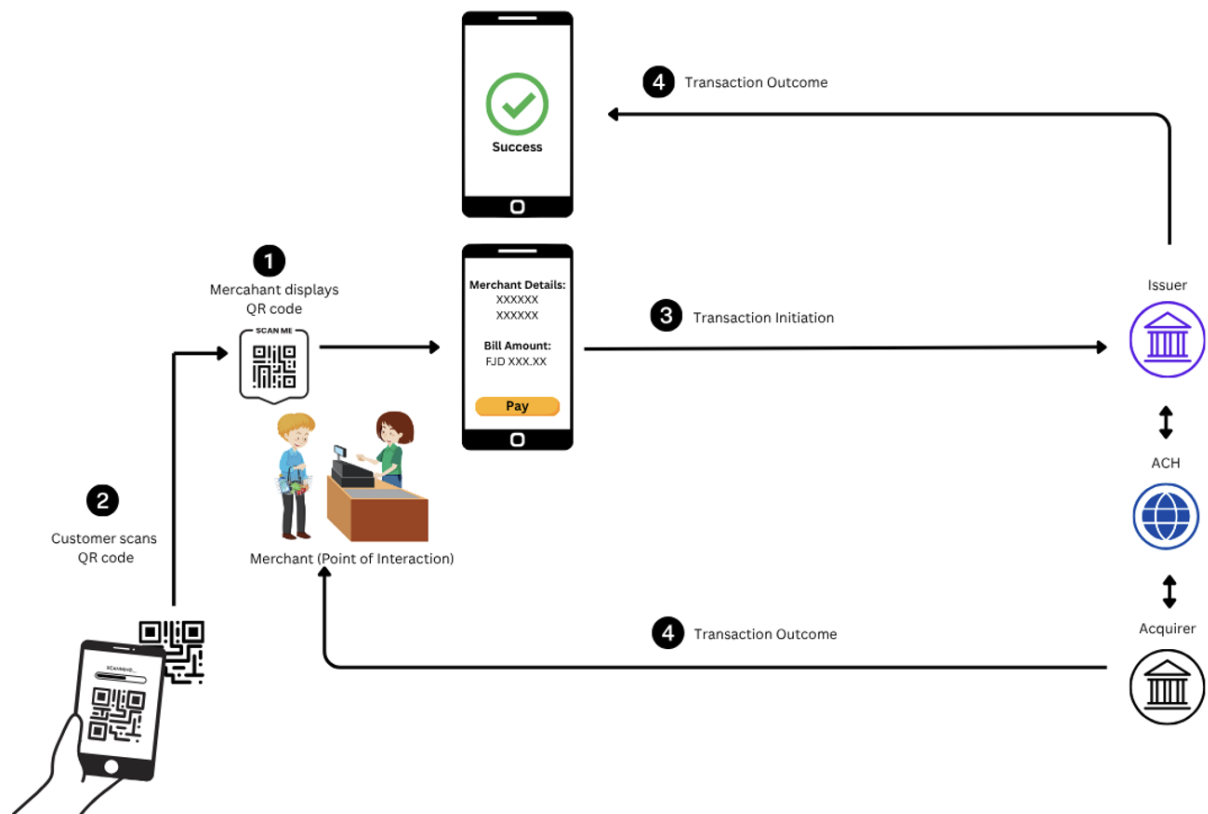
and branch, then manually enter the transaction amount before proceeding with the payment.

Static codes are best suited for smaller businesses, street vendors, or unattended payment scenarios.



- 1) The merchant displays a QR Code which embeds, amongst other information, the merchant's details.
- 2) The consumer scans the QR Code using a mobile application and inputs the amount to initiate the transaction.
- 3) The mobile application sends the transaction initiation request to the issuer.
- 4) The acquirer processes the transaction and informs the merchant. The consumer also receives the transaction outcome notification from the issuer.

Dynamic QR Codes:⁴ Dynamic QR codes are uniquely generated for each transaction and include specific transaction details such as the amount, merchant information, and a unique transaction reference. This allows automatic processing, minimizes manual input errors, and improves transaction traceability and reconciliation.⁵ This process involves having a Point of Sale (PoS) system to generate and manage the QR codes.



- 1) The merchant displays a QR Code that embeds the merchant's details, along with specific transaction details such as the amount and a unique transaction reference.
- 2) The consumer scans the QR Code using a mobile application to initiate the transaction.
- 3) The mobile application sends the transaction initiation request to the issuer.
- 4) The acquirer processes the transaction and informs the merchant. The consumer also receives the transaction outcome notification from the issuer.

⁴ The FJQR Scheme does not currently, but is expected to, accept dynamic QR codes in the future.

⁵ EMV® QR Code Specification for Payment Systems – Dynamic Data Elements, EMVCo, Version 1.1.

1.3 References

This section lists the documents referenced in this specification:

Table 1.1: References

Reference	Publication Name
[ISO/IEC 18004]	Information technology—Automatic identification and data capture techniques - QR Code bar code symbology specification
[ISO 18245]	Retail financial services—Merchant category codes
[ISO/IEC 13239]	Information technology—Telecommunications and information exchange between systems—High-level data link control (HDLC) procedures
[ISO 3166-1 alpha 2]	Codes for the representation of names of countries and their subdivisions— Part 1: Country codes, using two-letter country codes.
[ISO 4217]	Codes for the representation of currencies and funds
[ISO 7816-4]	Identification cards—Integrated circuit cards—Part 4: Organization, security and commands for interchange
[ISO 639]	Codes for the representation of names of languages—Part 1: Alpha - 2 Code
[EMV Book 4]	EMV Integrated Circuit Card Specifications for Payment Systems - Book 4 Cardholder, Attendant, and Acquirer Interface Requirements
[Unicode]	Unicode Standard, specifically the UTF-8 encoding form. For more information, please check: http://www.unicode.org/versions/latest
[UUID]	A universally unique identifier (UUID) as defined in the Internet Engineering Task Force (IETF) RFC 4122: https://tools.ietf.org/html/rfc4122

1.4 Abbreviations

This section lists the abbreviations used in this specification:

Table 1.2: Abbreviations

Abbreviation	Description
ans	Alphanumeric Special
C	Conditional
CDCVM	Consumer Device Cardholder Verification Method
CRC	Cyclic Redundancy Check
ECI	Extended Channel Interpretation
ID	Identifier of the data object
ISO	International Standards Organization
M	Mandatory
N	Numeric
O	Optional
QR Code	Quick Response Code
RFU	Reserved for Future Use
S	String
SDK	Software Development Kit
var.	Variable

2. DATA OBJECTS FOR FJQR

Table 2.1 lists the name of the data object, the ID of the data object, the format of the value field of the data object, the length of the value field of the data object, and whether the presence of the data object at the root level of the QR Code is Mandatory (M), Conditional (C), or Optional (O).

Table 2.1: QR Code Conventions

ID	Name	Format	Length	Presence	Comment
"00"	Payload Format Indicator	N	"02"	M	See Detail in LINK
"01"	Point of Initiation Method	N	"02"	O	See Detail in LINK
	Merchant Account Information				
"02" – "03"	Reserved for Visa	ans	var. up to "99"	M (At least one Merchant Account Information data object in the range "02" to "51" shall be present in a QR code, but more will be present if a merchant has multiple merchant identifiers with multiple payment systems/ schemes.)	See Detail in LINK
"04" - "05"	Reserved for Mastercard	ans			
"06" - "08"	Reserved by EMVCo	ans			
"09" - "10"	Reserved for Discover	ans			
"11" - "12"	Reserved for Amex	ans			
"13" - "14"	Reserved for JCB	ans			
"15" - "16"	Reserved for UnionPay	ans			
"17" - "25"	Reserved by EMVCo	ans			
"26" - "51"	FJQR - Reserved for domestic payment systems	ans			See Detail in LINK
"52"	Merchant Category Code	N	"04"	M	See Detail in LINK

"53"	Transaction Currency	N	"03"	M	See Detail in LINK
"54"	Transaction Amount	ans	Var. up to "13"	C	See Detail in LINK
"55"	Tip or Convenience Indicator	N	"02"	O	See Detail in LINK
"56"	Value of Convenience Fee Fixed	ans	Var. up to "13"	C	See Detail in LINK
"57"	Value of Convenience Fee Percentage	ans	Var. up to "05"	C	See Detail in LINK
"58"	Country Code	ans	"02"	M	See Detail in LINK
"59"	Merchant Name	ans	var. up to "25"	M	See Detail in LINK
"60"	Merchant City	ans	var. up to "15"	M	See Detail in LINK
"61"	Postal Code	ans	var. up to "10"	O	See Detail in LINK
"62"	Additional Field Template	S	var. up to "99"	O	See Detail in LINK
"64"	Merchant Information - Language Template	S	var. up to "99"	O	See Detail in LINK
"65" - "79"	RFU for EMVCo	S	var. up to "99"	O	See Detail in LINK
"80" - "99"	Unreserved Templates	S	var. up to "99"	O	See Detail in LINK
"63"	Cyclic Redundancy Check (CRC)	ans	"04"	M	See Detail in LINK

2.1 Payload Format Indicator (ID "00")

The Payload Format Indicator (ID "00") shall contain a value of "01". All other values are RFU.

2.2 Point of Initiation Method (ID "01")

The Point of Initiation Method (ID "01") shall contain a value of "11" or "12". All other values are RFU.

This has a value of "11" for static QR Codes and a value of "12" for dynamic QR Codes. The value of "11" is used when the same QR Code is shown for more than one transaction while the value of "12" is used when a new QR Code is shown for each transaction.

2.2.1 Merchant Account Information (ID "02" - "51")

The Merchant Account Information (ID "02" to "51") specifies the identity of a merchant. The format and value are unique and specific to a payment system, and several values may be included in the QR Code.

The Merchant Account Information template shall contain a primitive Globally Unique Identifier data object with a data object ID "00" to identify the payment operator and the corresponding merchant account information specific to that payment operator (**Table 2.2**).

The value of the Globally Unique Identifier field shall contain one of the following:

- An Application Identifier (AID) consisting of a RID registered with ISO and, optionally, a PIX, as defined by [ISO 7816-4]. For example, "D840000000".
- A [UUID] without the hyphen (-) separators. For example, "581b314e257f41bfbbdc6384daa31d16".
- A reverse domain name. For example, "com.merchant.name". This is the recommended option for FJQR.

The value of the Globally Unique Identifier field sets the context for the remainder of the template, and the meaning of the other data objects in the template are context-specific and outside of the scope of this specification.

Table 2.2: Data Object ID allocation in ID "26" - "51"

ID	Name	Format	Length	Presence	Comment
"00"	Globally Unique Identifier	ans	var. up to "32"	M	
"01" - "99"	Payment network specific	S	var.	M	

2.3 Merchant Category Code (ID "52")

The Merchant Category Code (ID "52") shall contain an MCC as defined by [ISO 18245]. This MCC should indicate the Merchant Category Code of the merchant.

2.4 Transaction Currency (ID "53")

The Transaction Currency (ID "53") shall conform to [ISO 4217] and shall contain the 3-digit numeric representation of the currency. For example, FJD is represented by the value "242". The value should indicate the transaction currency in which the merchant transacts.

2.5 Transaction Amount (ID "54")

The Transaction Amount (ID "54"), if present, shall be different from zero, shall only include (numeric) digits "0" to "9" and may contain a single "." character as the decimal mark. When the amount includes decimals, the "." character shall be used to separate the decimals from the integer value and the "." character may be present even if there are no decimals. The number of digits after the decimal mark should align with the currency exponent associated with the currency code defined in [ISO 4217].

The Transaction Amount shall not be included if the mobile application prompts the consumer to enter the amount to be paid to the Merchant.

2.6 Tip or Convenience Indicator (ID "55")

The Tip or Convenience Indicator (ID "55"), if present, shall contain a value of "01", "02" or "03". All other values are RFU.

- A value of "01" shall be used if the mobile application should prompt the consumer to enter a tip to be paid to the merchant.
- A value of "02" shall be used to indicate the inclusion of the data object Value of Convenience Fee Fixed (ID "56").
- A value of "03" shall be used to indicate the inclusion of the data object Value of Convenience Fee Percentage (ID "57").

Note that even if the Transaction Amount is not present in the QR Code, this data object may still be present.

2.7 Value of Convenience Fee Fixed (ID "56")

The Value of Convenience Fee Fixed (ID "56") shall be present and different from zero if the data object Tip or Convenience Indicator (ID "55") is present with a value of "02". Otherwise, this data object shall be absent.

The Value of Convenience Fee Fixed, if present, shall only include (numeric) digits "0" to "9" and may contain a single "." character as the decimal mark. When the Value of the Convenience Fee Fixed includes decimals, the "." character shall be used to separate the decimals from the integer value. The "." character may be present even if there are no

decimals. The number of digits after the decimal mark should align with the currency exponent associated with the currency code defined in [ISO 4217].

2.8 Value of Convenience Fee Percentage (ID "57")

The Value of Convenience Fee Percentage (ID "57") shall be present and different from zero if the data object Tip or Convenience Indicator (ID "55") is present with a value of "03" and only values between "00.01" and "99.99" shall be used. Otherwise, this data object shall be absent.

The Value of Convenience Fee Percentage, if present, shall only include (numeric) digits "0" to "9" and may contain a single "." character as the decimal mark. When the Value of the Convenience Fee Percentage includes decimals, the "." character shall be used to separate the decimals from the integer value. The "." character may be present even if there are no decimals.

2.9 Country Code (ID "58")

The Country Code (ID "58") shall contain a value as defined by [ISO 3166-1 alpha 2]. The Country Code should indicate the country in which the merchant transacts. In the context of FJQR, this would be "FJ", encoded as "5802FJ", 02 being the data length.

2.10 Merchant Name (ID "59")

The Merchant Name (ID "59") shall be present. The Merchant Name should indicate the "doing business as" name for the merchant.

2.11 Merchant City (ID "60")

The Merchant City (ID "60") shall be present. The Merchant City should indicate the city of the merchant's physical location.

2.12 Postal Code (ID "61")

If present, the Postal Code (ID "61") should indicate the postal code of the merchant's physical location. Depending on the country, the Postal code is the Zip code or PIN code or Postal code of the merchant.

2.13 Additional Data Field Template (ID "62")

The ID "62" is a template that includes common additional data objects such as Bill Number and Reference Label. It also allows payment operators to define their own additional data objects.

If present, the Additional Data Field Template shall contain at least 1 data object.

- The content of the data object value for IDs "01" to "08", if present, shall be either "****" or a value defined by the merchant. The presence of "****" indicates that the mobile application is responsible for obtaining the necessary information.

- The Additional Consumer Data Request (ID "09"), if present, shall contain one or more of the following characters to indicate that the corresponding data should be provided in the transaction initiation to complete the transaction:
 - "A" = Address of the consumer
 - "M" = Mobile number of the consumer
 - "E" = Email address of the consumer

Note that each unique character should appear only once.

Table 2.3: Data Object ID allocation in ID "62"

ID	Name	Format	Length	Presence
"01"	Bill Number	ans	var. up to "25"	O
"02"	Mobile Number	ans	var. up to "25"	O
"03"	Store Label	ans	var. up to "25"	O
"04"	Loyalty Number	ans	var. up to "25"	O
"05"	Reference Label	ans	var. up to "25"	O
"06"	Customer Label	ans	var. up to "25"	O
"07"	Terminal Label	ans	var. up to "25"	O
"08"	Purpose of Transaction	ans	var. up to "25"	O
"09"	Additional Consumer Data Request	ans	var. up to "03"	O
"10"	Merchant Tax ID	ans	var. up to "20"	O
"11"	Merchant Channel	ans	"03"	O
"12" - "49"	RFU for EMVCo	S	var.	O
"50" - "99"	Payment System-specific templates	S	var.	O

- The Merchant Channel (ID "11"), if present, identifies a characteristic of the channel used for a particular transaction. The values defined and the meaning of the values are listed in **Table 2.4**, **Table 2.5**, **Table 2.6**. All other values not explicitly listed in the tables shall be RFU.

Table 2.4: Merchant Channel: First Character – Media

Value	Meaning
"0"	Print - Merchant sticker
"1"	Print - Bill/Invoice
"2"	Print - Magazine/Poster
"3"	Print - Other
"4"	Screen/Electronic - Merchant POS/POI
"5"	Screen/Electronic - Website
"6"	Screen/Electronic - App
"7"	Screen/Electronic - Other

Table 2.5: Merchant Channel: Second Character – Transaction Location

Value	Meaning
"0"	At Merchant premises/registered address
"1"	Not at Merchant premises/registered address
"2"	Remote Commerce
"3"	Other

Table 2.6: Merchant Channel: Third Character – Merchant Presence

Value	Meaning
"0"	Attended POI
"1"	Unattended
"2"	Semi-attended (self-checkout)
"3"	Other

2.14 Merchant Information - Language Template (ID “64”)

The ID "64" is a template that may be used by a mobile application to present the merchant information in an alternate language.

Table 2.7: Data Object for ID "64"

ID	Name	Format	Length	Presence	Comment
"00"	Language Preference	ans	"02"	M	
"01"	Merchant Name— Alternate Language	S	var. Up to "25"	M	
"02"	Merchant City— Alternate Language	S	var. Up to "15"	O	
"03" - "99"	RFU for EMVCo	S	var.		Data objects reserved for EMVCo

2.15 RFU for EMVCo (IDs "65" to "79")

Data objects in this range are reserved for future use for EMVCo.

2.16 Unreserved Templates (IDs "80" to "99")

For Unreserved Templates with IDs "80" to "99", the primitive data object 'Globally Unique Identifier' with ID "00" shall be included in the template. Its value sets the context for the remainder of the template and the meaning of the other IDs and data objects in the template depends on the specific context.

Zero or more Unreserved Templates may be present. Unreserved Templates can be allocated and used by other parties, such as (domestic) payment systems and value-added service providers, for their own products.

Each payment system provider or value-added service provider puts their data in a separate Unreserved Template ID. For example, the first set of data is placed in ID “80”, the second set of data is placed in ID “81”, and so on.

2.17 Cyclic Redundancy Check (IDs "63")

The CRC (ID “63”) shall be calculated according to [ISO/IEC 13239] using the polynomial '1021' (hex) and initial value 'FFFF' (hex). The data over which the checksum is calculated shall cover all data objects, including their ID, Length and Value, to be included in the QR Code, in their respective order, as well as the ID and Length of the CRC itself (but excluding its Value). Following the calculation of the checksum, the resulting 2-byte hexadecimal value shall be encoded as a 4-character Alphanumeric Special value by converting each nibble to an

Alphanumeric Special character. For example, a CRC with a two-byte hexadecimal value of '007B' is included in the QR Code as "6304007B".

3. FJQR MERCHANT ACCOUNT INFORMATION (ID "02" - "51")

The IDs "02" to "51" are a primitive payment system Merchant Account Information ID which shall be used when the payment system that assigned the Merchant Account Information is implicitly identified by the ID. Allocation of these IDs is described in **Table 2.1**.

There will be at least 1 entry in this section in the FJQR, and there may be several (one for each payment system/scheme the merchant can accept). The data in this entry (up to 99 characters) is interpreted by the payment network to uniquely identify a merchant account via a merchant identifier. The payment system providing merchant identifiers shall further customize the format of the Merchant Account Information ID details.

The Merchant Account Information data objects with IDs "02" - "25" are used by global networks such as UnionPay, Mastercard & Visa. These data fields may be incorporated into an FJQR code, alongside domestic payment systems.

A common QR Code may support multiple merchant identifiers in a single scan; one for each payment system/scheme. This data group is primarily for payment routing purposes. Routing information is based on merchant IDs for a payment system/scheme & does not include any bank account details or mobile money account details.

The Merchant Account Information ID "26" shall be used to identify the merchant's payment account within the context of the Payment Service Provider (PSP) in the FJQR scheme.

"27" – "51" are reserved for additional payment schemes allocated by RBF.

- The Payment System shall use a Global Unique Identifier placed before the merchant account information. The Global Unique Identifier (GUID) is specific to each scheme / Payment System, and will be in the reverse domain name. The GUID for the merchant shall be the merchant alias ID issued and maintained by the PSP identified in "01". This value must be unique within the PSP's domain and may represent a merchant, counter, or terminal depending on the routing model used. Its structure and format are defined by the PSP.
- "01" tag shall contain the SWIFT Code (BIC) of the acquiring Payment Service Provider (PSP), as assigned by the Reserve Bank of Fiji (RBF). The BIC code must conform to [ISO 9362] and be 8 or 11 alphanumeric characters in length. This code uniquely identifies the PSP responsible for managing the alias in Tag "00".
- Optional data objects with IDs 02 to 99 may be included by the PSP to carry additional PSP-specific metadata or routing extensions. These values are interpreted exclusively within the context of the PSP identified in Tag "00" and are outside the scope of this specification. If present, each data object must have a unique ID and a properly encoded length and value according to TLV structure rules.

For Fiji, consider the case where a merchant is acquired by a particular PSP, which has allocated a merchant ID of 234434; and RBF has designated this PSP as SWIFT Code (BIC) - BAAAFJFJAXX. In this case, the Merchant Account Information record example might be “26350016fj.rbf.qr.2344340111BAAAFJFJAXX”, which can be broken down as follows:

Table 2.8: Data Object for ID "26" - "51"

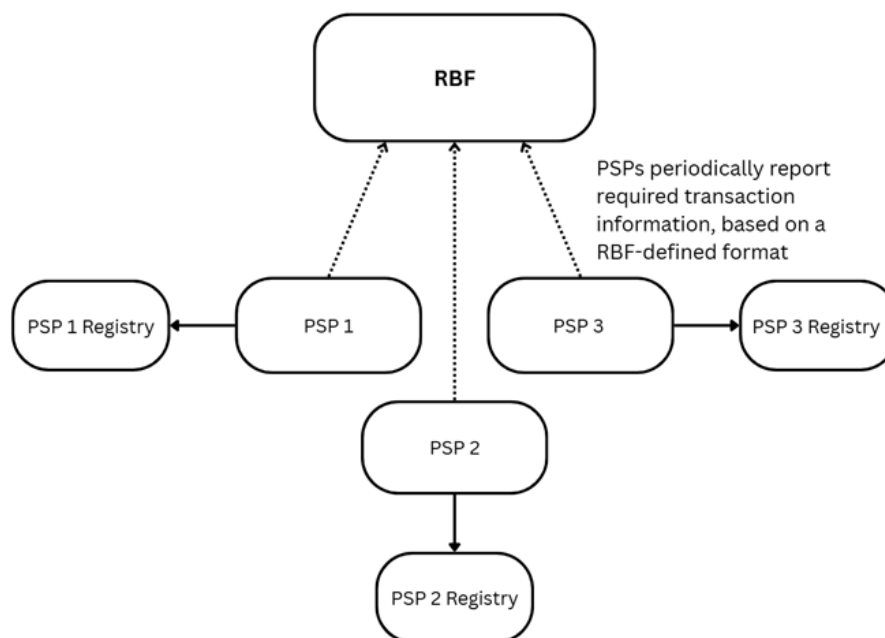
Name	ID	Length	Presence	Example	Explanation
Globally Unique Identifier (GUID) for the merchant	"00"	Variable and defined by the PSP The full length of the template must remain less than 99 characters. PSPs must design their PSP-specific format cognisant of this.	M	fj.rbf.qr.234434	This field is formed from a combination of the merchant ID (alias) and a globally unique domain identifier. The example indicates a 06-character merchant identifier 234434, but the GUID can encompass from 06-character merchant identifier and extend beyond registered under FJQR.
PSP Identifier	"01"	08 to 11 characters	M	BAAAFJFJAXX	SWIFT Code (BIC) of the PSP, as issued by RBF. Used to route the payment.
PSP-Specific Account Extensions	"02" - "99"	PSPs must design their PSP-specific format cognisant of this.	O		Optional fields used by the PSP for additional account-level metadata

3.1 Operational Considerations

The Fiji QR (FJQR) ecosystem relies on federated merchant registries, each managed by Payment Service Providers (PSPs), with oversight provided by the Reserve Bank of Fiji (RBF). Each flow within the system, from merchant onboarding to payment receipt, requires clear operational guidelines to ensure interoperability, security, compliance, and resilience.

The following section outlines the operational considerations for each core flow in the FJQR architecture.

3.1.1 Merchant Registry

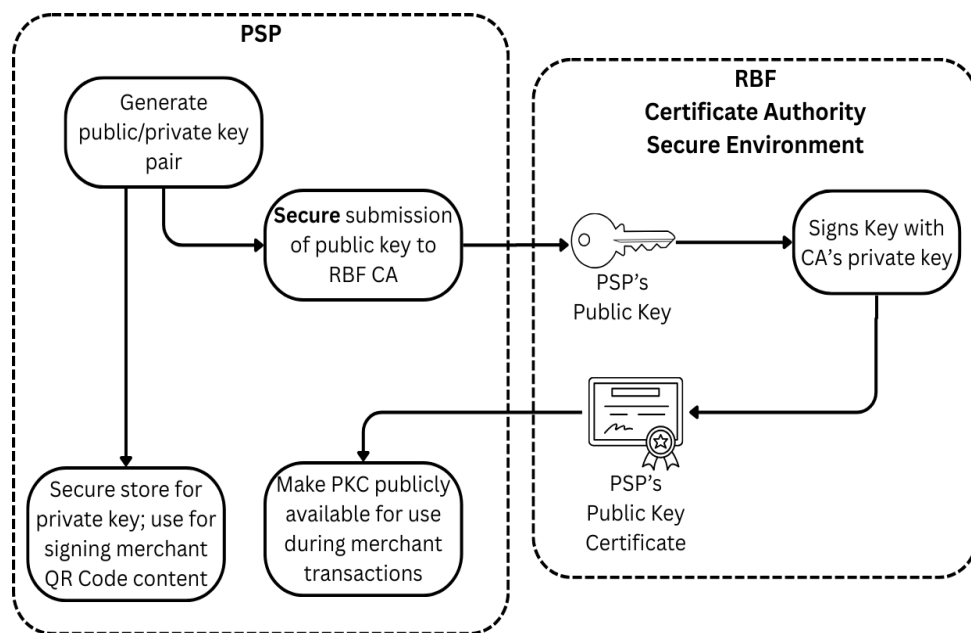


- **Schema Enforcement:** All PSP registries must adhere to a schema reflecting the reporting format defined by RBF, in order to ensure data consistency across the ecosystem.
- **Ownership:** PSPs retain ownership of their merchant registries and may extend the RBF-defined schema to include both additional data needed in the creation and storage of QR codes and any other PSP-specific operational data related to merchants, such as till information.
- **Reporting:** Reporting mechanisms already in place should be extended to ensure RBF has up-to-date oversight of all QR payment transactions, including “on-us” transactions, and relevant merchant information.
- **Governance:** The RBF shall define procedures that all PSPs must follow to ensure that all merchants operate in compliance with existing regulations, in alignment with the Guidelines on Participation in the FJQR Scheme.

- Scalability: Registries must be designed to handle growth in merchant onboarding while maintaining performance.

3.1.2 Public Key Certificates

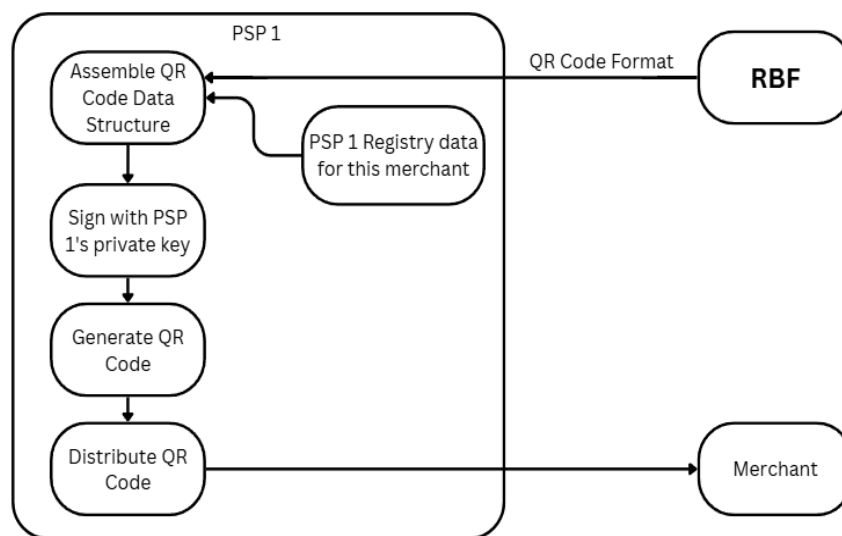
FJQR will integrate with the RBF's existing Certificate Authority (CA) in order to take advantage of the considerable advantages it offers in terms of operational efficiency. For this reason, instead of using public keys for authentication directly, FJQR will make use of public key certificates (PKCs). In this context, PKCs are PSP-specific public keys which are signed by the CA using its private key, in a secure process defined by the CA.



- Key Generation: Each Payment Service Provider (PSP) must generate its own cryptographic key pair (public/private).
- Certification: The Certificate Authority (CA) signs each PSP's public key, producing a Public Key Certificate (PKC), in a secure key-signing ceremony.⁶
- Storage: Each PSP is responsible for the security of its private key, both during storage and in use, and for the storage of its PKC.
- Validation: Any PKC can be validated against the CA's public key. The CA's public key is distributed once (via a hardcoded URL or trusted channel) and must be embedded or retrievable by customer applications.
- RBF Role: RBF is not responsible for hosting PSP (PKCs). Its responsibility is limited to publishing and maintaining the CA's active public key, and for signing PSP's public keys with its private key.

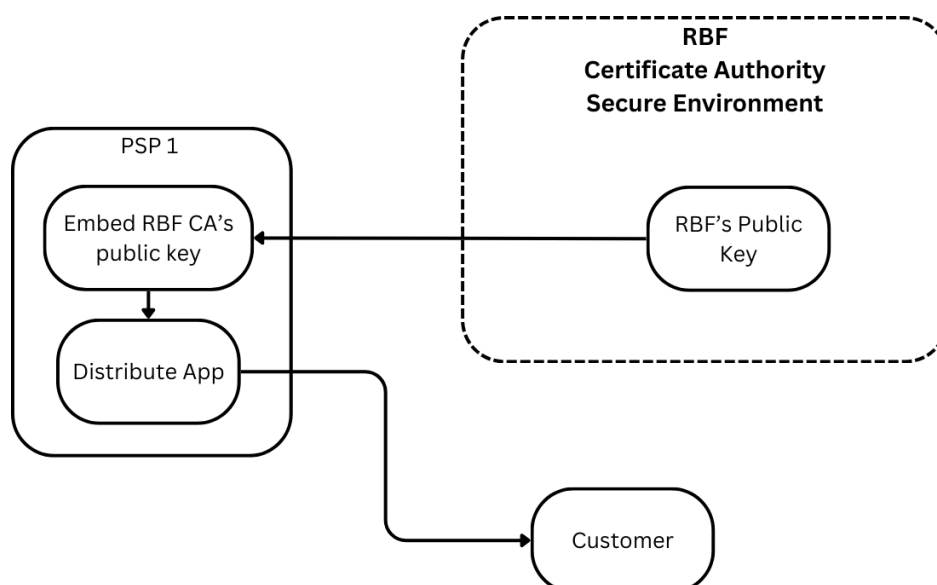
⁶ This key ceremony refers to a formal, controlled process for generating and signing cryptographic keys.

3.1.3 QR Code Generation



- **Standardization:** QR Code format must follow the specifications laid out in this document to ensure cross-PSP interoperability.
- **Data Integrity:** QR codes must be signed with the PSP's private key, corresponding with the previously-generated PKC, ensuring authenticity and preventing tampering.
- **Distribution Controls:** PSPs must ensure only authorized merchants receive valid QR codes, and that the correct QR code(s) are shared with the correct merchants.

3.1.4 Customer Application

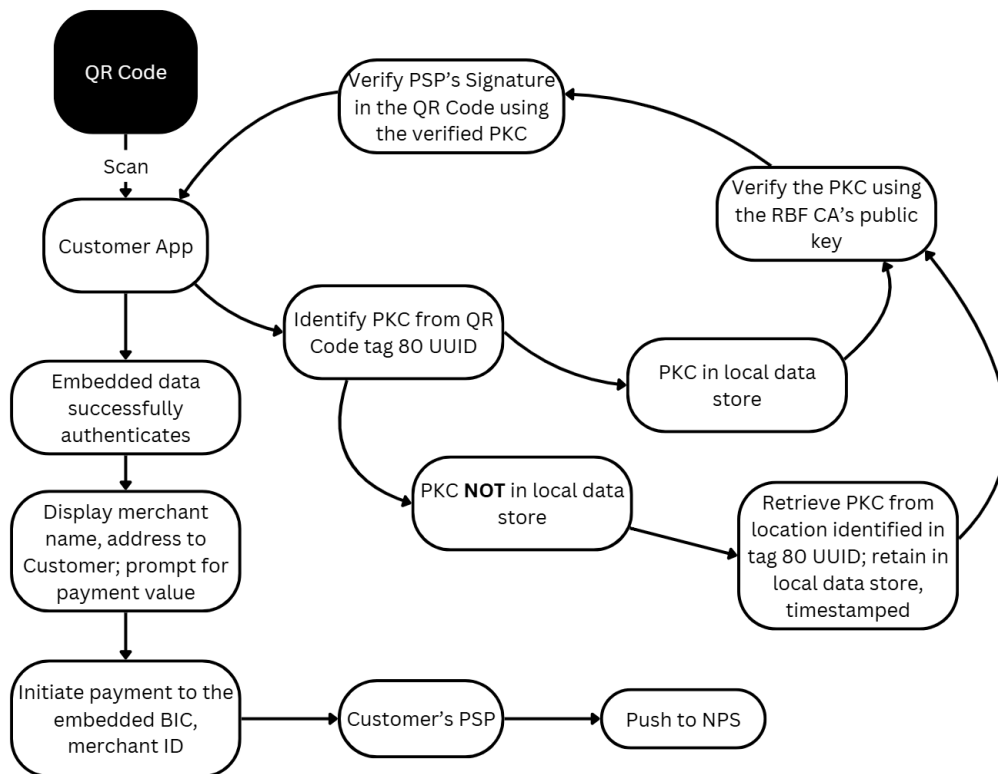


- **Application Generation:** The PSP must retrieve the CA's public key from a trusted source and embed it in the customer app. This is preferred to allowing the customer app to retrieve the public key directly, due to the potential for redirection.
- **Distribution:** The PSP must distribute the app to their customers and personalise it to each customer following their existing processes.
- **PKC Retrieval:** During QR code verification, the app must fetch the PSP's PKC from the PSP (via reverse URL lookup based on UUID in Tag 80).
- **Storage:** For reasons of transactional efficiency, the app must maintain a local store of retrieved PKCs, indexed by PSP/BIC, and accompanied by their timestamps. After a month has elapsed according to the timestamp, these stored PKCs should be deleted and refreshed the next time the acquiring BIC is encountered.

3.1.5 QR Code Scanning & Payment Initiation

Customer applications must implement a PKC-based trust model for the authentication of data during QR code-initiated transactions. The app must first verify the QR code content by checking that the public key/PKC is valid, by checking the signature using the RBF CA's public key embedded in the app. Thereafter, the app checks the validity of the QR code content by using the public key that has been verified in the previous step.

Due to capacity constraints, it is infeasible to embed the PKC in the QR code. Instead, it will be loaded from the PSP at the URL identified in the tag 80 UUID when first encountered. It will then be held in a local datastore (alongside other PSPs' PKCs) managed by the app, and timestamped so that it can be refreshed at regular intervals. This improves the efficiency of transactions and reduces the overall bandwidth requirement.

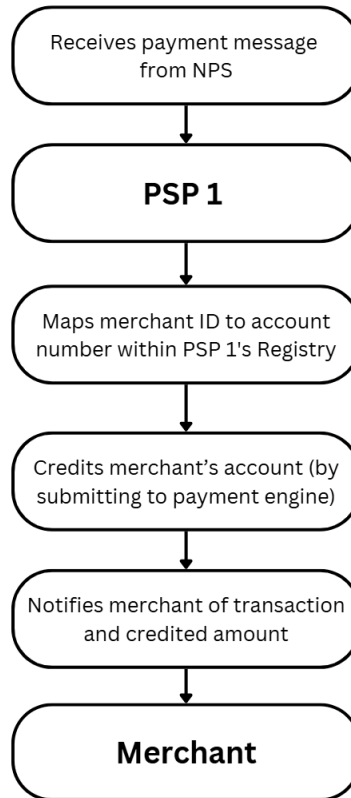


Customer applications must perform two-stage QR code verification:

1. Certificate Validation: The app must validate the PKC using the CA's public key.
2. Signature Verification: Once the PKC is validated, the app must use the PSP's public key (verified from the PKC) to verify the QR code signature.
3. Security Controls: Apps must prevent tampering with the embedded CA public key.
4. Update Mechanism: There is no requirement for monthly synchronization with a central registry; however, consideration should be given to a regular, but infrequent, mechanism to verify that the RBF CA's public key held in the app is up to date (also allowing for overlaps in validity). This should be carried out in alignment with timelines outlined in the Guidelines on Participation in the FJQR Scheme.
5. PKC Validation
 - Extract the UUID from Tag 80 in the QR code.
 - If the identified PKC is not held in the app's local datastore, retrieve the PSP's PKC using the UUID (reverse URL lookup).
 - Validate the PKC using the CA's public key held in the app.
 - Add the key to the app's local datastore and timestamp it.
6. Signature Validation
 - Use the PSP's public key (the validated PKC) to verify the digital signature contained in the QR code.

Only if both validation steps succeed should the app proceed to initiate the payment transaction. If either validation fails, the transaction must be rejected with an appropriate error message to the user.

3.1.6 Merchant Payment Settlement



- Alias Resolution: When the merchant's PSP receives the message from the NPS, the PSP maps/resolves the Merchant ID to the merchant's actual account number using its internal merchant registry.
- Amount Crediting: The PSP credits the merchant's account with the transaction amount.
- Notification: Merchants must be promptly notified of credited amounts with transaction details.

3.1.7 Cross-Cutting Considerations

- Data Encoding Standard: For QR payloads, any sub-tag value particularly in Tag 80.02 (digital signature) exceeding 99 length shall adopt multi-byte length encoding, consistent with BER-TLV standards.
- Security: All communications between PSPs, RBF, and customer apps must use secure protocols (TLS, mutual authentication).
- Reporting & Oversight: RBF must maintain visibility of QR payment information through a monthly report submitted by each participating PSP, that includes the

total number and valuation of all QR payment transactions (both off-us and on-us) processed by the PSP and select merchant information, in alignment with the Guidelines on Participation in the FJQR Scheme.

- Compliance: RBF will ensure compliance of participating PSPs with the FJQR Technical Specifications and Guidelines on Participation in the FJQR Scheme as part of its supervisory/oversight activities.
- Disaster Recovery: PSPs and RBF must maintain backup registries and disaster recovery protocols.
- Interoperability Testing: Regular testing between PSPs to ensure QR code interoperability and seamless cross-PSP payments.

4. ADDITIONAL DATA FIELD TEMPLATE (ID “62”)

ID "62" is used to embed additional information within the QR code to support scenarios where merchants operate multiple checkout counters or store branches. The QR code framework must be flexible enough to handle both per-counter and centralized account payment routing models. This means merchants should be able to choose between assigning unique receiving accounts to each till/counter or using a single unified account for all counters within the same store or branch.

This section outlines three possible configurations that merchants can select when generating QR codes for individual checkout points.

4.1 Scenario 1: Single Receiving Account for All Checkout Counters

Use Case:

The merchant opts to route all payments to a single consolidated receiving account for simplified reconciliation. However, they still require the ability to identify which specific checkout counter processed each transaction.

Design Approach:

- Each checkout counter is issued with a unique QR code, while all codes share the same merchant alias ID (i.e., the same receiving account).
- To distinguish payments by checkout location, Tag “62” is used to embed counter-specific metadata within each QR code.

4.2 Scenario 2: Unique Receiving Accounts Per Checkout Counter

Use Case:

The merchant requires separate receiving accounts for each checkout counter or branch to support financial segregation or ensure operational independence (e.g., for individual reconciliation and reporting)

Design Approach:

- Each counter is assigned a unique merchant alias ID, effectively linking it to a dedicated receiving account.
- Tag “26” (Merchant Account Information) is populated with counter-specific data, ensuring each QR code directs payments to the correct account.

4.3 Scenario 3: Merchant Without Multiple Counters

This scenario applies to single-location merchants or those who operate only one checkout point. Since there is no need to distinguish between multiple counters or branches, there is no requirement for counter-level identification in the QR code.

Design Approach

- The merchant is assigned a single QR code linked to their primary alias account.
- Since the merchant operates only one payment point, Tag “62” is not required for counter-specific data.
- If Tag “62” is included for format consistency, its relevant fields (e.g., Store Label or Terminal Label) may be left blank or omitted.
- This ensures a simple and clean QR payload, with minimal data overhead while remaining fully compliant with the EMVCo standard.

Table 2.9: Data Object for ID "62"

Name	ID	Length	Presence	Example
Mobile Number	"02"	var. up to "25"	O	+679 1234567
Terminal Label	"07"	var. up to "25"	O	Eg. Counter1 and Counter2, or null (for scenario 3)
Promo Code	"50"	Var.	O	Eg. 12345

Table 2.10: Summary Table

Aspect	Scenario 1 <i>Single Receiving Account</i>	Scenario 2 <i>Unique Account per Counter</i>	Scenario 3 <i>Single Merchant, No Counters</i>
Merchant Alias ID	One alias for all counters	Unique per counter	One alias for the merchant
No. of QR Codes Issued	One per counter	One per counter	One QR code only
Payment Receiving Account	single account	One account per counter	single account

5. Digital Signature (ID "80")

From the unreserved templates, ID "80" is used to include a Digital Signature Template in the QR payload. This template ensures the authenticity and integrity of the QR content by linking it to the PSP's certified public key.

- Universally Unique Identifier (UUID) (00) – A required value used as the lookup key to retrieve the PSP's PKC (Public Key Certificate).
- Signature Algorithm ID (01) – An optional code that shows which algorithm was used to create the signature (for example, RSA-2048 with SHA-256).
- Digital Signature (02) – An optional field that holds the Base64-encoded signature of the data, making sure the payload hasn't been changed.

Table 2.11: Data Object for ID "80"

Name	ID	Length	Presence	Example
UUID for PKC Retrieval	"00"	var. up to "32"	M	A Universally Unique Identifier (UUID) [RFC 4122] is assigned to the PSP's PKC.
Signature Algorithm ID	"01"	var.	O	A numeric identifier. E.g. "RSA-2048 with SHA-256".
Digital Signature	"02"	var.	M	The Base64-encoded digital signature of the hashed data payload (all tags before Tag 80). If the Base64-encoded signature exceeds 99 bytes, the length field of Sub-Tag 02 shall use multi-byte length encoding, consistent with BER-TLV standard. For example, a 344-length converts to the 2-byte hexadecimal value (stored as 0x0158) would be encoded as: (0x82 0x01 0x58) where: • 0x82 indicates that the length is specified in the

				next two bytes, and 0x01 0x58 represents the actual length (344 bytes).
--	--	--	--	---

5.1 UUID Generation and Management

- Each PSP must generate a **UUID** for every active Public Key Certificate (PKC).
- The UUID must be unique and conform to [RFC 4122] (Version 4 random UUID recommended).
- Format: 32 lowercase hexadecimal characters without hyphens.
 - Example: [581b314e257f41bfbbdc6384daa31d16](#)
- The UUID is:
 - Submitted with the PSP public key to the RBF CA during PKC issuance.
 - Bound into the PKC as a certificate extension.
 - Inserted into Tag 80–00 in every QR code signed with the corresponding private key.
- The UUID must be used in the PKC retrieval URL:
 - PSP-hosted: <https://keys.<psp-domain>/pkc/<uuid>>
 - RBF mirror (optional): <https://pkc.rbf.fj/fjqr/<uuid>>

5.2 Signature Generation

- The QR payload must be signed by the PSP’s private key.
- Signing scope: all tags *before* Tag 80, encoded in TLV form (ID + Length + Value), excluding Tag 80 and Tag 63 (CRC).
- Hash function: SHA-256 (mandatory); other algorithms may be added by RBF policy.
- Encoding: The resulting signature is Base64-encoded and placed in Tag 80–02.

5.3 Verification Workflow

Customer applications must validate QR codes in two stages:

1. PKC Retrieval & Validation
 - Extract UUID from Tag 80–00.
 - If the identified PKC is not held in the app’s local datastore, then retrieve the PSP’s PKC using the UUID (reverse URL lookup)
 - Validate PKC using RBF CA’s current public key.

2. Signature Verification

- Reconstruct signed payload (all TLVs before Tag 80).
- Use the PSP public key (from PKC) and the algorithm in Tag 80–01 to verify the signature in Tag 80–02.
- If both steps succeed, then proceed with payment. Otherwise, reject QR as invalid.

APPENDIX

Appendix -1: Mapping: FJQR Code Tags with ACH pacs.008.001.07

FJQR Tag	Tag Name	Example	Meaning / Use	Mapped ACH Field (pacs.008.001.07)
00	Payload Format Indicator	01	Always 01 for EMVCo static QR	-
01	Point of Initiation Method	11 = static QR code	For scan type identification	-
26	Merchant Account Info (Fiji-specific)	26350016fj.rb f.qr.23443401 11BAAAFJFJAX X	Includes merchant alias ID and PSP BIC	In QR payments, the payee's Payment Service Provider (PSP) uses the value in <code><CdtTrfTxInf> <PmtTpInf><SvcLvl><Prtry> TTC<Prtry></SvcLvl></PmtTpInf></code> to identify the QR payment. This value includes a merchant alias that must be resolved to the actual beneficiary account number internally. Consequently, in the ACH request message, the field <code>CdtrAcct > Id > Othr > Id</code> corresponds to the merchant ID.
26-00	GUID	fj.rbf.qr.234434	Merchant ID	<code><CdtrAcct><Id><Othr><Id> 234434</Id></Othr></Id>< /CdtrAcct></code>

26-01	PSP identifier	BAAAFJFJAXX	BIC/Swift Code	<CdtrAgt><FinInstnId><BICFI>BAAAFJFJAXX</BICFI></FinInstnId></CdtrAgt>
52	Merchant Category Code	5311	Retail, grocery, etc. (ISO 18245)	Optionally used in <CtgyPurp> or RmtInf
53	Transaction Currency	242 (FJD)	Currency code (numeric ISO 4217)	IntrBkSttlmAmt Ccy="FJD"
54	Transaction Amount	25.00	Customer input amount	IntrBkSttlmAmt
58	Country Code	FJ	Country of transaction	Cdtr > PstlAdr > Ctry
59	Merchant Name	MerchantAA	Display name for consumer	Cdtr > Nm
60	Merchant City	Suva	For local context	Cdtr > PstlAdr > TwNnm (optional)
62	Additional Data	see below	Store/counter ID, terminal label, Promo code etc	RmtInf > Ustrd > CdtrRefInf
62-02	Mobile Number	+6791234567	Optional	RmtInf > Ustrd >

62-07	Terminal Label	Counter2	Which POS terminal or till	<Ustrd>62240211+67912345670708Counter2500512345</Ustrd>
62-50	Promo Code	12345	Optional	
80	Digital Signature	801360032581b314e257f41bfbbdc6384daa31d160110RSA-SHA2560288AbCdEf...123XYZ==	UUID, Signature Algorithm ID, and Digital Signature	-
63	CRC (Cyclic Redundancy Check)	CB2E	Ensures QR integrity	-

Appendix -2: Example QR Code Breakdown

```
00 02 01
01 02 11
26 ...
  00 16 fj.rbf.qr.234434
  01 11 BAAAFJFJAXX
52 04 5311
53 03 242
54 05 25.00
58 02 FJ
59 10 MerchantAA
60 04 Suva
62 ...
  02 11 +6791234567
  07 09 Counter2
  50 05 12345
80 82 018A
  00 32 581b314e257f41bfbbdc6384daa31d16
  01 10 RSA-SHA256
  02 82 0158 AbCdEf...123XYZ==
63 04 CB2E
```

Appendix -3: ACH pacs.008.001.07 Message (fragment) with FJQR Mapping

```
<CdtTrfTxInf>
  <!-- FJQR Tag 54 and 53 -->
  <TtlIntrBkSttlmAmt Ccy="FJD">25.00</TtlIntrBkSttlmAmt>

  <!-- FJQR Tag 59 -->
  <Cdtr>
    <Nm>MerchantAA</Nm>

    <!-- Type of Transaction code -->
    <CdtTrfTxInf>
      <PmtTpInf>
        <SvcLvl>
          <Prtry>TTC<Prtry>
        </SvcLvl>
      </PmtTpInf>
      <Ref>8888</Ref>
    </CdtTrfTxInf>

    <!-- FJQR Tag 26 -->
    <CdtrAcct>
      <Id><Othr><Id>234434</Id></Othr></Id>
    </CdtrAcct>
    <CdtrAgt>
      <FinInstnId><BICFI>BAAAFJFJAXX</BICFI></FinInstnId>
    </CdtrAgt>

    <!-- FJQR Tag 60 -->
    <PstlAdr>
      <TwnNm>Suva</TwnNm>
      <Ctry>FJ</Ctry>
    </PstlAdr>
  </Cdtr>

  <!-- FJQR Tag 62 -->
  <RmtInf>
    <Ustrd>62240211+67912345670708Counter2500512345</Ustrd>
  </RmtInf>
```