REQUEST FOR OFFER

Instant Payments for the Maldivians

JUNE 9, 2019

Maldives Monetary Authority

Maldives Monetary Authority

1. Contents

Table of Figures

2. Glossary of Terms and Abbreviations

Terms and Abbreviations	Details
AIPs	Account Information Providers
Addressee	The addressee of the message to be forwarded
API	Application Programming Interface
B2B	Business to Business
B2G	Business to Government
BCP	Business Continuity Plan
Beneficiary bank	The beneficiary party within the Instant payment system (receiving bank or receiving PSP) Can receive both financial (payment instruction) or non-financial (request to pay) transactions.
BIC	Business Identifier Code (SWIFT code)
Bulk function	Functionality within the instant payment system that is capable of receiving large numbers of transactions in one bulk, that are in turn unbundled and processed as single transactions, then at the end of processing it is capable of sending back the response messages in bulk – together with a summary report – to the sender bank.
C2B	Consumer to Business – interactions between companies and their clients.
Central Proxy Database	Database to centrally store the secondary identifications.
CSM	Clearing and Settlement Mechanism
DB	Database
DRP	Disaster Recovery Plan
EACHA	European Automated Clearing House Association
FTE	Full Time Equivalent Is a unit of measure of an employee's or group's productivity.
FTP	File Transfer Protocol
G2P	Government to Person
G2B	Government to Business
GUI	Graphical User Interface
Interoperability	The ability to cooperate. The common interpretation and enforcing or functions determined by the accurately defined, clear, understandable, unambiguous payment scheme (SCT Inst). It enables participants (originator and beneficiary institutions as well as clearing houses / CSM) to execute their payment instructions irrespective of their geographical location, IT architecture and the availability of banks through various clearinghouses.
ISTQB	International Software Testing Board
KYC	Know Your Client
MMA	Maldives Monetary Authority
MNO	Mobile Network Operators
MPSD	Maldives Payment System Development (MPSD)
MRTGS	Maldives RTGS
OTP	One Time Pin
Originator	The originating party within the Instant payment system (sender bank or sender PSP) Can initiate both financial (payment instruction) or non-financial (request to pay) transactions.
Overlay service	Auxiliary service building on the Instant payment system raising basic service to a higher level thereby increasing user satisfaction and transaction

	numbers.
P2B	Person to Business
P2P	Peer to Peer or Person to Person – transactions between private individuals.
P2G	Person to Government
Payer	The addressee of the transaction in case of Request to Pay transactions, the party required to pay, i.e. the one to be debited.
Proxy	Secondary account identifier. A different type of unique identifier capable of identifying the bank account e.g. mobile phone number, email address, personal tax id, VAT number, etc.
PSP	Payment Service Provider
QA	Quality Assurance
QR	Quick Response
Requester	In case of Request to Pay transactions the initiating party. The beneficiary of the financial transaction.
RFI	Request for Information – general / orientation request for information. Before issuing the tender the customer requests general information from the potential suppliers in order to map the abilities of companies and their products, and eventually selecting based on this information which companies are to be invited to the tender. For better comparison a pre-determined format is used to collect the information.
RFO	Request for Offer – The customer signals their need to source a particular product or service and requests the suppliers to provide a proposal regarding this need containing their conditions and prices. Within the RFO document the customer details their needs and requirements regarding the product or service as well as listing their expectations towards the suppliers.
RTGS	Real Time Gross Settlement
Sender	Sender of the message to be forwarded.
STP	Straight-Through Processing
TCO	Total Cost of Ownership
TOGAF	The Open Group Architecture Framework
UAT	User Acceptance Test
UPG	Unified Payment Gateway

3. Overview

3.1. Introduction and Background

As part of the evolution of the Maldives Payment System Development (MPSD), the Maldives Monetary Authority (MMA) embarked on a multi-phase initiative to modernize the current payment clearing and settlement ecosystem and infrastructure in order to better support the long-term effectiveness and efficiency of the Maldivian economy (see Section 4 for a description of current payment arrangements in the Maldives).

The requirements described in this Request for Offer (RFO) emphasize the need for increasing the end-to-end speed of payments while ensuring the efficiency and safety of the payments system. With the future of payments in mind, the system will be open and flexible to accommodate and foster innovation and competition in the Maldivian payments domain.

The primary objective of the project is to ensure that users are able to make and receive payments instantly irrespective of the island they live on or where and with whom they bank.

3.2. Purpose

The objective of this document is to provide information and articulate the requirements of the MMA. This document was created for use by potential solution providers (hereinafter referred to as vendors) of the Instant Payment System and Central Infrastructure of the MMA.

The document was prepared by the MMA and distributed to the vendors that registered to the RFI with reference number IL-PRC/2019/09 within the prescribed deadline.

This section of the RFO provides an overview of the overall intended outcome of the MPSD initiative. Section four (4) provides an overview of current payment arrangements in the Maldives. Section five (5) details the procurement process. Section six (6) defines the scope of the RFO. Vendors are expected to study Section seven (7) in detail in order to familiarize themselves with the scope of the MPSD initiative. Section seven (7) details the exact requirements from a functional and non-functional point of view. Vendors are expected to answer this section providing as much detail as deemed necessary to prove that the proposed solution meets the requirements.

The implementation of the MMA Instant Payment System will facilitate easier entry for new financial institutions and third-party payment service providers, providing a uniform, modern core system for participating service providers, thus creating an appealing environment for innovative payment solutions. The open and flexible infrastructure will benefit private individuals and business clients, who, in a wide range of payment scenarios, would be able to enjoy the advantages of immediate and efficient electronic payment solutions in addition to traditional cash settlements.

3.3. Expected timelines for the Instant Payment implementation

The vendor is expected to propose a viable Project Plan taking into consideration the expectation of MMA to launch the first services 9 months after the procurement contract is signed between MMA and the vendor.

3.4. Business Objectives and Scope

Following the review undertaken by the MMA and after careful consideration of various use-cases, the primary needs as well as the future vision of the Maldivian economy were identified. The main focus of the project is set on addressing the following:

3.4.1. Fast payments:

a) The system will enable all Maldivians to send and receive money instantly regardless of the island on which they live or the payment solution they use.

b) Transactions will be transparent with rich and informative messages for both payer and payee, and will be received instantly.

c) End users will have access to funds in real time and will be able to use it immediately.

3.4.2. Easy payments:

a) The process of making payments will be more flexible and modular.

b) Users will be able to use easy-to-remember identifiers such as email addresses, phone numbers, biometrics and social media handles to execute payments.

c) The simple account-to-account instant payment system will enable innovation and enhance the customer experience for Maldivians.

d) Easy-to-use and cost-effective digital and integrated payment solutions will be introduced to eliminate cheques and reduce the level of cash in circulation.

3.4.3. Open payments:

a) Payment service providers will have access to the account-to-account domestic payment scheme, providing them with digital and integrated payment services.

b) Open application programming interfaces (APIs) and rich transaction information will promote data-driven innovation and new value propositions.

c) The system will be flexible and potential payment service providers will have activity based access to the system.

3.4.4. Safe payments:

a) Secure payment will be ensured through the use of multiple-factor authentication.

b) Payment processes will be standardized and automated to minimize costs and risks

c) System errors will be minimized and fraud will be resolved quickly.

d) Payment regulations will be developed as the payment system continues to evolve to ensure that users and payment service providers have a high level of confidence in the payment system.

4. The National Payment System of the Maldives

4.1. Country Background

The Maldives is an archipelago consisting of around 1200 islands strewn across the Indian Ocean. Less than 200 of these islands are inhabited by a population of around 400,000. The economy is heavily reliant on cash due to geographical distribution of the population and limited access to financial services in the outer islands.

Fishing was traditionally the key sector and, although, it still provides a livelihood for a significant share of the people in outer islands, tourism is by far the dominant sector in the Maldivian economy today, accounting for about a quarter of the GDP. The country's GDP stood at US$5.35 billion with a per capita of US$10,449 in 2018.

4.2. Financial Sector

The financial sector of the Maldives is dominated by the commercial banking sector. Currently, there are eight banks in the Maldives, of which four are locally incorporated. A single bank dominates the retail banking segment with approximately 75 percent of bank account holdings and over 80 percent of the retail payment transactions. The rest of the financial sector is comprised of five insurance companies, three other financial institutions specialized in leasing and housing finance and the stock exchange.

4.3. Current Payments Ecosystem

Maldives Monetary Authority (MMA) began developing the National Payments System in the Maldives with the implementation of the Maldives Real Time Gross Settlement System (MRTGS) in 2011, the Automated Clearing House (ACH) in 2012 and facilitating the implementation of an MNO-led Mobile Payment System in 2016. It is important to realize that despite the introduction of electronic payment methods, "Cash is King" for businesses and individuals for making payments in the Maldives.

The penetration of the formal banking sector is relatively high with a total 509,795 deposit accounts which represents 422,765 individual accounts and 87,030 corporate/business accounts. The total number of deposit accounts of the individuals represents 85% of the adult population (18 years and above) of the Maldives.

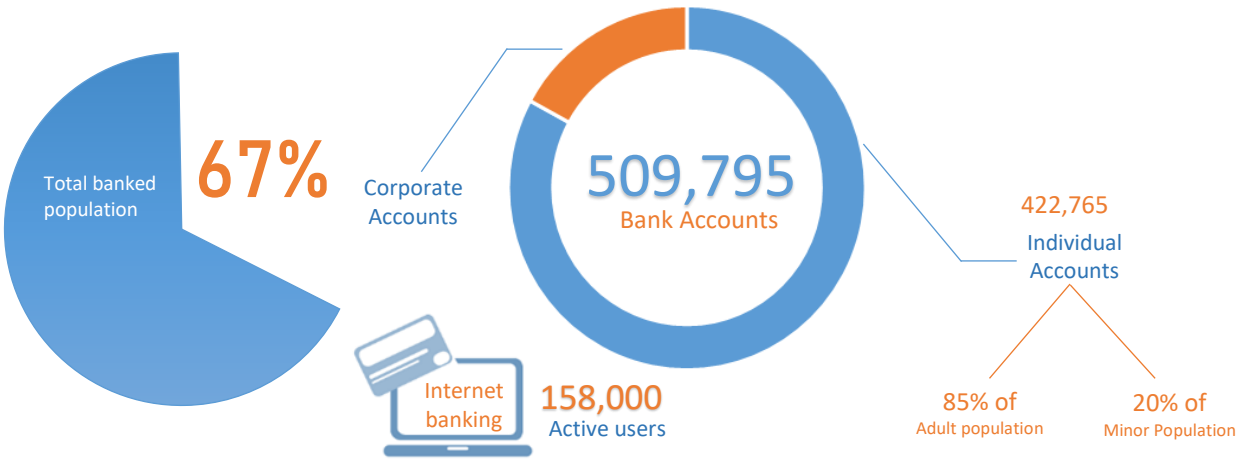

Figure 1. Details of the account holding

A single local bank dominates the industry with approximately 75% of these deposit account holdings. The lack of an ideal level of competition and the shallowness of financial markets are challenges to the development of both the financial sector and the payments ecosystem.

Although the majority of the country's population have bank accounts, access to financial and payment services is still challenged by the geographical nature of the country and the size of the population. Whilst there are a total 54 bank branches, 127 ATMs and 7,590 POS terminals in the country; more than 35% of these bank branches and over 50% of the ATM and POS infrastructure is based in the greater Male' region. The rest of the infrastructure is distributed across the 184 inhabited islands throughout the country.

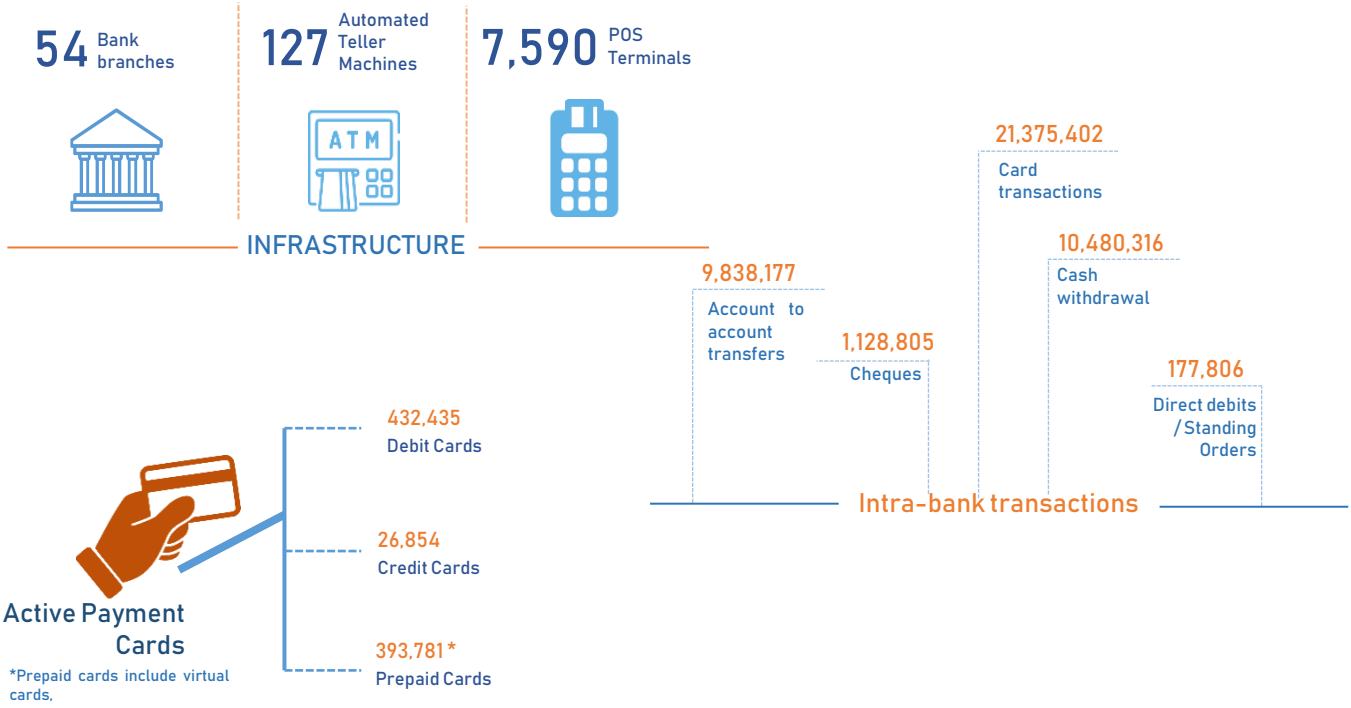

Figure 2. Details of the existing infrastructure

4.3.1. Inter-bank Clearing and Settlement System

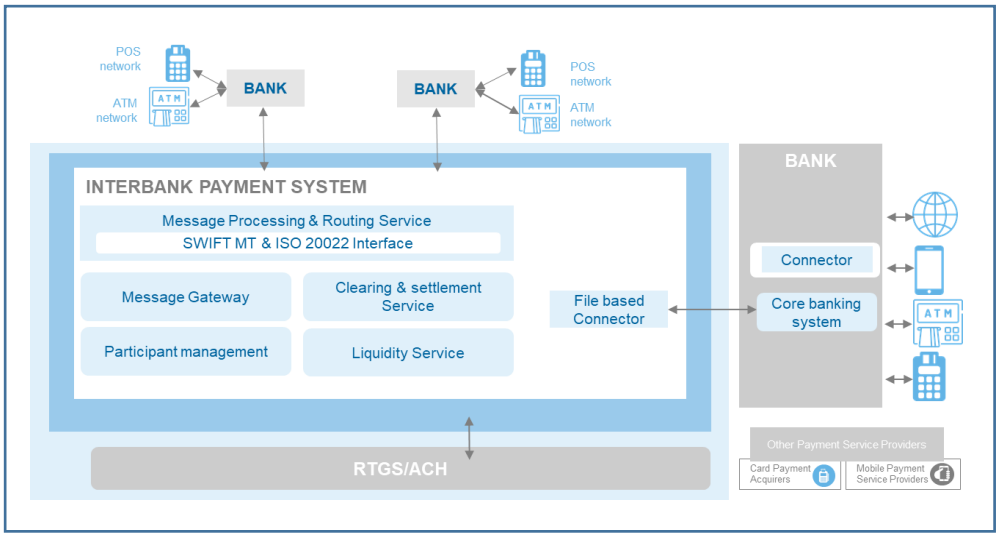

Figure 3. Inter-bank Clearing and Settlement System

Currently, all inter-bank transactions are executed via the MRTGS system and the ACH system, which are both operated by the MMA. The MRTGS system processes and settles urgent, high value inter-bank transactions, and is based on the SWIFT messaging standard. Meanwhile, the ACH system is a session-based clearing system for low value batch transactions consisting of three components, namely, direct credits, direct debits and cheque imaging and truncation. The ACH is based on the ISO20022 messaging standard However, only the direct credit and cheque imaging and truncation components of the ACH system are currently in operation.

The participants of the MRTGS and ACH systems are currently the banks operating in the Maldives, and the services are only available through them during banking hours, and mostly by visiting the banks in person. However, as these systems are not fully integrated with some of the participating banks' internal core banking systems, straight-through processing has still not been achieved, which leads to inefficiencies and delays even with the MRTGS system.

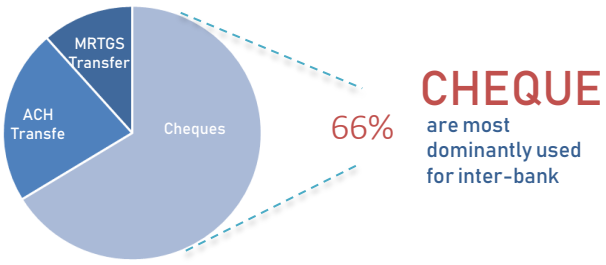

Figure 4. Payment made through RTGS/ACH

Since the payment systems are not integrated to the General Ledger of MMA, there are delays and significant inefficiencies associated in payment processing as well as extending the services to the banks as a regulator.

4.3.2. Payment services

Card Payments

Card payments have become increasingly popular over the years, and are the dominant electronic means of payment in the Maldives. Presently only banks are engaged in issuing cards while card payment acquiring business is carried out by some banks and acquiring agents in Maldives. In the absence of local payment schemes, international schemes are used for domestic transactions as well. The foreign bank branches and non-bank players acquire these transactions through foreign banks.

Maldivian economy is highly dependent on the tourism sector as it has been the highest income generator for the economy. Hence, there is a great demand from tourism sector to accept payment via cards, as it offers a secure and efficient means of paying for goods and services by tourists. As a result, international card acquiring services for the payment of goods and services at tourist establishments have been a significant segment of the payments services in the economy. These entities are well established and strengthened their position in the payment industry throughout the past 28 years, by holding a significant share of the credit card transactions which amounts to more than 50% of total volume and value of credit card transactions.

Mobile Payments

A recent initiative to mitigate difficulties arising from the spatial orientation of the islands in the Maldives is the introduction of mobile payment services. With full mobile service coverage across the country and a high penetration of mobile phones within the population, payment solutions that utilize the mobile telecommunications network have the potential to reduce the prevalence of cash in the economy and achieve financial inclusion. However, mobile operators are faced with challenges in linking their services with the banks due to absence of a common platform that connects the banks and mobile payment service providers. Also, as the efficiency of such solutions is dependent on the underlying payments system infrastructure, the delays in settlement and other inefficiencies remain unresolved.

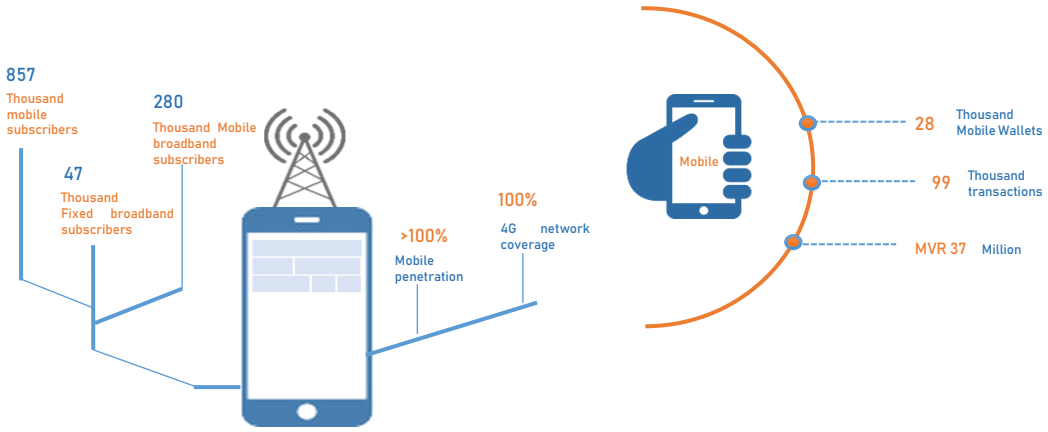

Figure 5. Mobile Payments

4.3.3. Users of Payment System

Government

MMA acts as a banker to the government. Hence, all the government payments are processed by MMA. The government has opened number of accounts (transaction accounts) in commercial banks, mainly for managing income and expenditure of atoll councils, island councils as well as government operated health centres and schools at the respective islands.

Government payments are mostly processed via electronic means; MRTGS/ACH for domestic payments and SWIFT for international payments. MMA in collaboration with Ministry of Finance and Treasury, have established a mechanism to receive payment instruction to MMA in an electronic format. However, presently only local account transfer requests are received via electronic mechanism, rest are all received in paper form, which includes foreign transfers, cash withdrawals etc.

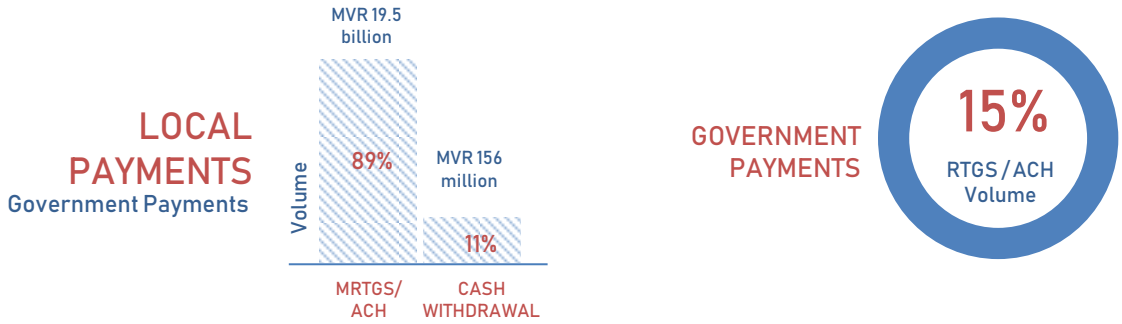

Figure 6. Government Payments

A significant part of the government payments includes distribution of pension and social benefits. These payments are deposited to bank accounts. However, beneficiaries living in the outer islands have limited access to their bank accounts. Hence, the bank visits these islands by Dhoni (speed boat) on a monthly basis to facilitate cash withdrawals. In 2018, banks had appointed 312 cash agents at 166 islands and made 2000 Dhoni trips to different islands in order to facilitate cash withdrawals, which is highly costly and risky.

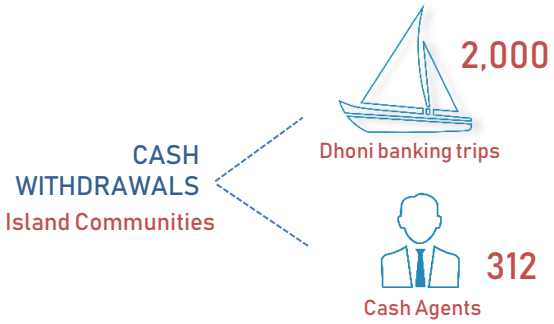

Figure 7. Cash withdrawals via Dhoni trips and Cash Agents

Receipts such as taxes, customs duty and other fees collected by government authorities are highly cash/cheque based. MMA in collaboration with the Maldives Inland Revenue Authority (MIRA), established a mechanism to collect tax payments via MRTGS system in 2015. This allows MIRA to obtain details of tax payments processed through MRTGS on a daily basis, via an electronic connection established between MMA and MIRA. The volume of tax payments processed through MRTGS system has significantly increased from 2015 to 2018, as a result of public trust and confidence over this mechanism. However, cash and cheques are still the most dominantly used.

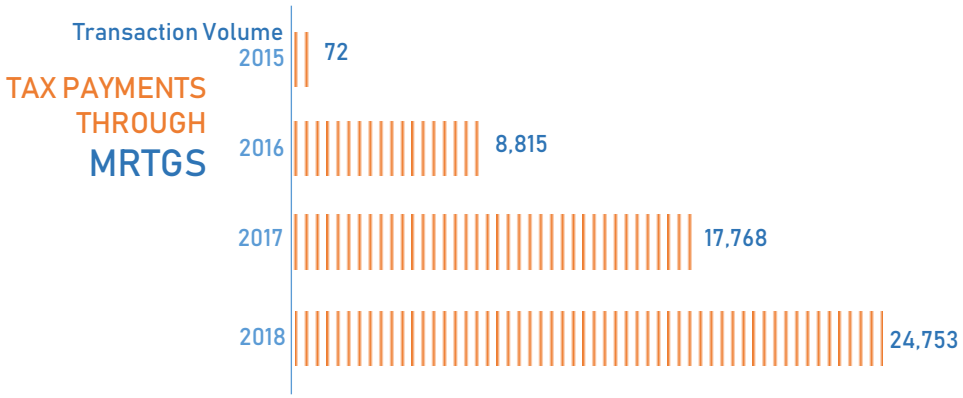

Figure 8. Tax payments through MRTGS

Moreover, in the absence of an easily accessible single payment window, like a common payment gateway, each respective authority responsible for collecting payments or fees makes separate arrangements with the respective commercial bank by installing POS terminals and payment gateways, resulting in inefficiencies and increase in associated costs in payment collection. Each year government pays a significant amount to the banks as fees and charges for obtaining these services.

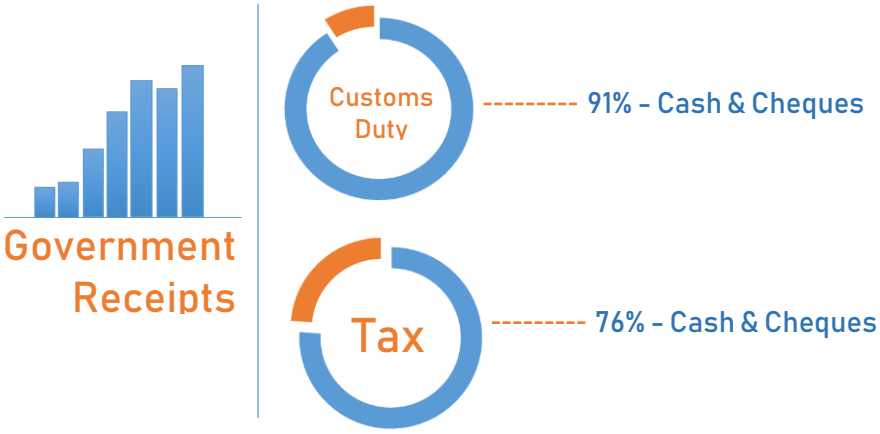

Figure 9. Government receipts via Customs Duty and Tax

Bill Payments

The basic utility services such as water, electricity, telephone services are provided by the State-Owned Enterprises (SOEs) of the government and the private sectors service providers. While State Electric Company (STELCO) and Male' Water and Sewerage Company (MWSC) provide service to the Male' region, Fenaka Corporation Limited (Fenaka) is mandated with providing water, electricity and sewerage services to the island communities. Other services such as telephone, internet and TV cable are provided by both SOEs and the private sector.

Most of these service providers have facilitated electronic payments through cards, internet banking and Mobile Apps. Although there is an increase in usage of electronic payments, cash and cheques are still widely used in bill payments, especially in Island communities. And the usage of cash in island communities is alarmingly high as only 9% of bill payments were made electronically. This is mainly due to limited availability of electronic payment services in the island communities.

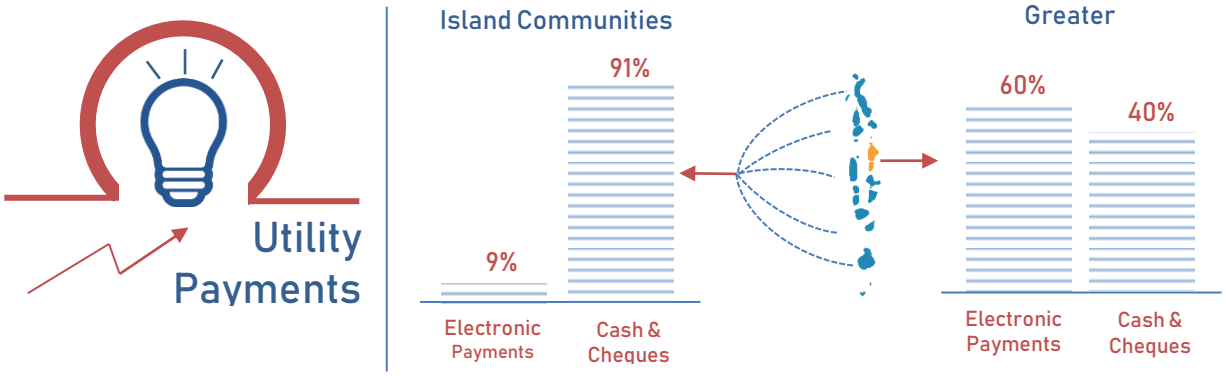

Figure 10. Utility Payments

Despite 85 percent of the adult population being bank account holders, there are significant hurdles to access financial and payment services. While the provision of payment services is dominated by the banking industry, in addition to low level of awareness; the limited access to banking facilities for segments of the population living in smaller more isolated islands have led to a high reliance on cash for transactions. The dominance of cash remains even in regions with relatively high access to banking services as a result of inefficiencies induced by limited choice leading to high transaction costs.

4.3.4. Key Challenges in the existing payments ecosystem

The following are the key challenges in the Maldivian ecosystem:

a) Lack of interoperability and interconnectivity between service providers.

b) Lack of STP / automation within the banks / MMA.

c) Lack of availability of funds in real time.

d) Limited access to systems and services.

e) Lack of innovative payment solutions.

f) Lack of competition in the banking sector.

g) High transaction costs.

h) Lack of awareness of the available services.

5. Procurement Approach

This section of the RFO document includes information about both the procurement process and how vendors are required to respond to the requirements detailed.

5.1. Procurement Timelines

Below you will find the procurement timetable and related deadlines, with the list of required tasks:

Details	**Timeline**
Issue of RFO	June 09, 2019
Vendor inquiries submission deadline	June 19, 2019
Answer vendor inquiries	June 24, 2019
Final vendor proposal submission deadline	July 18, 2019 at 1500hrs (GMT+5).
Contract negotiation kick off with selected vendor	August 29, 2019
Contract awarding with selected vendor	September 30, 2019

Note: all dates and/or times specifies above are in accordance with Maldivian Time Zone (GMT+5).

5.2. Vendor Inquiries

All contact with the MMA in connection with this RFO should be made only through the MMA's Designated Contact listed below. Responses to vendor inquiries will be provided at the MMA's earliest convenience, however, before the aforementioned deadline via email.

The MMA Designated Contact will provide to every vendor's main contact, notice of each inquiry received and the reply thereto, without revealing the source of the inquiry.

5.3. Designated Contact

All contact with the MMA in connection with this RFO should be made through the MMA Designated Submission is required in electronic format and way, to the address:

Mr. Abdul Jaleel Hussain
Email address: procurement@mma.gov.mv

For all submitted proposals, a receipt will be issued by the point of contact, in the form of a response e-mail, until 17:00 GMT+5 on July 21, 2019.

5.4. Preparation of Proposal

This section of the RFO document details the structure and format vendors must adhere to.

5.4.1. Language

Vendors are required to submit a proposal and all the relevant documents in English.

5.4.2. Responses to Requirements

Requirements are structured in sections and subsections. Each section or subsection requires an answer from the vendor. Vendors must prepare proposals so that they include a detailed response for each requirement described in the respective section/subsection.

With regards to the Functional and Non-Functional requirements included in Section 7.2 and Section 7.3 each section's heading is immediately followed by a response compliance box, as follows:

Requirement Number	**Solution Compliance**
MMA-FR-XXX	Standard/Customization/Future/Not Compliant
Description of Solution Vendors to add description of their proposed solution	

The response compliance box includes the following information about the requirements:

a) The box marked "Requirement Number" is the unique identifier of the requirements described in the section.

b) The box marked "Solution Compliance" may include one of the following options:

Standard	Covered by standard functionality (configuration only and no customisation). The vendor will be able to demonstrate the functionality out of the box. Confirm if customisation can be done by MMA or has to be done by the vendor.
Customisation	The software needs customisation. The vendor needs to specify the expected size of customisation (small/medium/large).
Future	The functionality will be included at no cost in a future release. The vendor needs to specify the expected date of such a future release.
Not Compliant	Vendor cannot offer the requirement and has no intention of offering it now or in the future.

The vendor is expected to indicate which of the above best describes the solution being offered.

c) The box marked "Description of Solution" is where the vendor is required to add a detailed description of how the proposed solution meets the stated requirement.

The vendor is expected to provide the answers in a single document. References to Appendixes are permitted for more detailed supporting documentation (i.e., financials, CV's, detailed reference list, etc.).

5.4.3. Formal Requirements

The Proposals should comply with the following formal requirements:

a) Vendors are expected to declare that their proposal is valid for, and commitments included in their proposals are upheld for, not less than **180 days**.

b) Vendor shall seal the Technical and Financial proposals in separate envelopes, duly marking the envelopes as "TECHNICAL" and "FINANCIAL". The envelopes shall then be sealed in an outer envelope and be addressed as per "Appendix C: Format of Addressing the Bid Envelope" of this RFO.

c) The soft copy of the proposals must be submitted in a searchable PDF format.

d) The PDF documents should be signed with firm signature and all the pages must be initialized.

e) The attachment containing the Proposal and enclosed other documents should not be larger than 10 MB. If the archive is larger than this threshold amount, please send the proposal in multiple parts.

5.5. Final Vendor Proposal Submission

All responses must be sent by courier to the address as per Appendix C: Format of Addressing the Bid Envelope before the deadline. Responses should be organized according to the response structure provided in Subsection 5.4.3.

The same response must also be sent via email to procurement@mma.gov.mv before the deadline. Responses should be organized according to the response structure provided in Subsection 5.4.3.

Responses to the RFO are due on **July 18, 2019 at 1500hrs (GMT+5)**. The MMA will reject proposals submitted later than this time and date.

5.6. Evaluation and Award Process

Due to the strict deadline requirements for the MMA implementation project, the ability of the vendor to deliver the solution in accordance with the requirements of the Instant Payment System in a timely manner, underpinned by a proven technology in a "live" environment (cite the relevant references), or tested in a validated test environment (cite the relevant references), is considered a major factor for evaluation of the Proposals.

Based on the above, a weighted evaluation system based on the following principles will be used:

a) Proposals will be evaluated in segments, each against the corresponding requirement code of the structure.

b) Solutions corresponding to the relevant requirements are quantified on a weighted scale, where the top part will include solutions with references and validated tests, while the bottom section will indicate solutions under or before development.

c) When evaluating the proposals, the MMA will consider whether the supplier undertakes quantifiable activities with specified deadlines, and included relevant, straightforward and realistic solutions for the corresponding requirements.

d) When evaluating costs, the MMA will consider the total cost of ownership (TCO) projected for 5 years, wherein the MMA will devote special attention to license related and other legal risks incurring expense risks (e.g. risk of cancellation, penalties, warranty, adherence to law, and maintenance and support expenses).

During the evaluation we will apply the following weighting model to measure business and technical content, pricing, and organisational and professional preparedness:

Consideration	Weight	Description
Price	20 %	TCO for 10 years (USD)
Compliance with specific requirements	50 %	Meeting functional and non-functional requirements (quantity, quality, feasibility, technology considerations) for each module.
References	10 %	Whether the supplier is able to provide references that can be verified to support compliance with the functional and non-functional requirements.
Project management	10 %	Detailed project plan (resource plan, scheduling, feasibility, etc.)
Company background and compliance with legal requirements	10 %	Compliance with the formal requirements (Subsection 5.4.3).

The evaluation framework includes criteria that may lead to immediate disqualification, for example in case of breach of confidentiality requirements in connection with the proposal process.

5.7. Terms and Conditions

5.7.1. RFO Terms and Conditions

The terms and conditions set out below apply to this RFO process, use of RFO responses in supporting MMA planning, and any subsequent discussions and presentations related to the RFO responses.

a) The vendor is responsible for all costs and expenses incurred in connection with the preparation and delivery of a response to this RFO, and the MMA bears no liability for any costs incurred by the vendor in connection with this RFO or any subsequent discussions or presentations.

b) The vendor will make reasonable efforts to ensure that all aspects of its response reflect the actual capabilities of its product and service offerings, and any capabilities that are planned but not currently available are clearly indicated.

c) The vendor agrees to keep this RFO and the supporting documents included with the RFO confidential.

d) The material provided in connection with this RFO is being provided to assist vendors in understanding the MMA's intentions and to provide guidance in structuring responses, and does not purport to constitute all information that may be relevant to a responding party. The MMA does not make any representation or warranty as to the accuracy or completeness of the information provided.

e) It is the vendor's responsibility to obtain any clarifications of any details relating to the RFO. The MMA will endeavour to respond to all written requests for clarification within the given timeframes. Information provided in response to requests for clarification will be provided to all vendors regardless of who made the request. The MMA will not reveal the source of any such request.

f) The MMA is under no obligation to discuss or explain how it has viewed or used the contents of any RFO response.

g) The MMA is under no obligation to include RFO respondents in any future tender process.

h) The MMA reserves the right to use any and all information contained in a Proposal.

i) This RFO does not constitute and is not intended to be an offer by the MMA. By providing a response, the vendor agrees that this provision supersedes any custom, usage, agreement or term implied by law to the contrary.

j) No vendor will have, as a result of participating in the RFO, any claim against the MMA or its members for compensation of any kind whatsoever, any claim based on ambiguity in the RFO documents. By submitting a response each vendor will be deemed to have agreed that it has no claim, and to have agreed that any rule of construction to the effect that any ambiguity is to be resolved against the drafting party will not be applicable in the interpretation of this RFO.

k) The MMA will not be liable to any vendor for any direct, indirect, special, incidental, or consequential damages in connection with this RFO.

l) The MMA is committed to exercising integrity and responsibility in its business activities, including the avoidance of real or perceived conflicts of interest.

5.7.2. Deliverables

The vendor must provide the deliverables described in the list below:

a) Implemented and functioning system modules
b) Source code deposited (source code escrow)
c) Documentation:
    i. Detailed system requirements and system design
    ii. Test plan
    iii. User manual
    iv. Operations manual / System handbook
    v. Integration specifications
    vi. Interface specifications
d) Testing:
    i. QA final report for UAT start
    ii. Performance testing report
    iii. Penetration test report
e) Training:
    i. Training
    ii. Training material

Please note that this list is not exhaustive and contains the minimum deliverable related content to be included in the Proposal. The MMA reserves the right to expand the list and include a more detailed list of deliverables in the Contract.

6. Scope

6.1. Infrastructure

The core of the infrastructure; Unified Payment Gateway (UPG) will be an open API based modular system that comprise of an account-based, real-time payments system augmented with the functionality of Smart Addressing. All banks in the Maldives will be directly linked to the system and it will facilitate Account Information Providers (AIPs) to provide account information through the UPG to Payment Service Providers (PSPs) to offer innovative payment services to the customers. It will support seamless integrated solutions combining the payment process and provide convenient, and value-added solutions.

Smart Addressing will allow customers to make payments using easy to remember addresses and identifiers such as national identification numbers, mobile numbers, email addresses and social media handles. The sharing of bank account numbers and other sensitive information should no longer be required.

6.2. Unified Payment Gateway (UPG)

UPG facilitates AIPs to provide account information through the gateway to PSPs based on set of system rules that are in line with the legal framework. The UPG enables customers to view and manage multiple bank accounts through a single interface, consolidating various banking features including seamless funds routing & merchant payments. The UPG will include the following functionalities.

a) Should be able to manage ISO20022, ISO8583 and SWIFT FIN messaging standards.
b) Allow account-based funds transfer.
c) Enable users to send and receive payments instantly as well as use the funds immediately.
d) Ability to operate the platform in Differed Net Settlement (DNS) mode.
e) Allow users to make payments via different channels including but not limited to mobile app, web, kiosks, smart devices, and schemes.
f) Allow users to make payments using different addresses and identifiers.
g) Allow different use cases such as P2P, P2B, P2G, G2P, G2B, B2G, B2P (for example for reimbursements and rebates) and B2B payments.
h) Allow the payment initiator and beneficiary to receive instant confirmation.
i) Should support 'Request to Pay' as an overlay, and allow users to add additional information or reason codes such as 'Can't Pay', 'Can only Pay x', 'Will pay on a specific date', so that the requestor is informed why the payment has not been made.
j) Should be scalable and flexible to cater for increasing volumes.
k) Allow PSPs to access to accounts in AIPs network (e.g., Banks, MNOs) to make payments on behalf of customers.
l) AIPs will connect to UPG through stateless APIs.
m) UPG will allow KYC verification for new customers during the registration process and update proxy DB in the shared service layer.
n) Allow PSPs to access account information of AIPs.
o) Allow PSPs and AIPs to do KYC verification by accessing the respective National Registration databases (for individuals and businesses).
p) Allow multi-factor customer authentication (i.e. password, PIN, tokens, biometrics, OTP).

6.3. Smart Addressing

a) Allow customers to use simple, easy to remember addresses (e.g., identifiers such as ID card, email, phone numbers) to make payments.

b) Allow AIPs and PSPs to connect to National Registration databases (for example: information on individuals through Department of National Registration, legal entities through Ministry of Economic Development and tourists and expatriates through Maldives Immigration) to complete customer enrolment and "Know Your Customer" verification processes.

c) Allow AIPs and PSPs to access identification information to provide various services (i.e. customer registration, verification, and authentication) using any supported address.

d) Smart addresses should be issued and managed by PSPs to ensure that the customer is uniquely identified by the PSPs.

e) Smart Addressing eliminates the need for sharing of bank account numbers and other sensitive information required to make payments.

6.4. Clearing

a) Allow real-time multilateral clearing between the participants, to facilitate the processing of payments to beneficiaries in real-time.

b) Should use ISO20022 messaging standard and be flexible to incorporate rich data to capture additional transaction information.

c) Allow processing and clearing of payments on a 24x7x365 basis.

d) Allow secure and reliable real-time payments with finality.

e) Customers should be able to access and use the funds immediately.

f) Allow the payment initiator and beneficiary to receive instant confirmation.

g) Provide date and time stamp for each step in the end-to-end payment process.

h) Allow direct participation by AIPs by having a settlement account at MRTGS or indirect participation by having an agreement with a settlement participant in MRTGS.

i) Allow the allocation of clearing and settlement limits for UPG participants, where the payment instructions are validated against these limits.

j) Allow the undertaking of clearing and settlement within the system, without depending on the existing MRTGS system.

k) Allow the system to perform clearing and settlement at configurable pre-defined intervals.

l) Allow the system to check against the threshold limits in the accounts and top-up the accounts where necessary by transferring funds from participant's settlement account into UPG allocation account or transfer from participants UPG allocation account to their settlement account.

m) Allow online liquidity management for direct participants.

n) Allow calculation and application of several types of fees to be charged from participants.

6.5. Digital Bank

a) The Digital or virtual bank provides a pre-created account for each entity in the Maldives (i.e. individuals and businesses).

b) Provide a white-labelled solution to enable customers to move funds from one entity to another.

c) Provide a white-labelled solution (online payment gateway) which allows to make online payments through local scheme.

d) Customers will have the choice of activating the accounts by performing KYC procedures in order to use it for making payments.

e) Allow account management (KYC, opening account, managing transactions).

f) If a Bank is fully integrated to UPG, it should allow the banks to opt to use the white labelled solution or the bank's own mobile application to provide the services.

g) Banks not fully integrated to UPG

   i. If a bank is not integrated at API level, it should allow customers to top-up their accounts at the Digital Bank using their bank accounts;

   ii. The top-up can be done automatically or manually by providing a separate user interface.

h) Allow banked customers as well as unbanked customers to use their Digital Bank account, however unbanked customers will have access to limited services.

i) Allow the creation of transaction limits.

6.6. Fraud, Security and Monitoring

a) Ensure application security and risk mitigation by incorporating but not limited to security controls, clear segregation and proper error handling and logging.

b) Allow user authentication to access interface functionalities and transaction types.

c) Allow segregation of duties by applying four-eye principles based on transaction limits and other system functions such as changing roles and security access.

d) Ensure data integrity and security.

e) Support encryption of data at rest and in transmission.

f) Support encrypted network sessions.

g) Allow message encryption.

h) Protect network and application traffic by using cryptographic security.

i) Must have detailed audit trails and logs.

j) Allow fraud detection and prevention by:

   i. Providing a rules engine and analytics to facilitate applying customized policies and take automated decisions;

   ii. Providing a platform to aggregate detection of potential fraud from various channels;

   iii. Enabling to map and analyse the financial relationships between customer accounts, transactions and other channels;

   iv. Monitoring for trends in order to raise alerts for suspected risks;

   v. Facilitating the creation of different scenarios for AML in addition to the rules;

   vi. Enabling to block attempts by fraudsters;

   vii. Enabling to protect against specific risks by applying necessary limits.

6.7. Support / Maintenance

a) Provide high quality and reliable onsite and off-site support.

b) Provide required training for the functional and technical team.

c) Provide onsite support for 6 months.

6.8. Timeline

MMA Instant Payment implementation project milestones that must be included in the vendors project plan and schedule, are the following:

Milestone	Deadline
Planning and Clarification deadline	dd-mm-yyyy
Delivery deadline	dd-mm-yyyy
UAT acceptance	dd-mm-yyyy
Trainings	dd-mm-yyyy
Pilot of the national system	dd-mm-yyyy
Go-live	dd-mm-yyyy
Special Support phase (6 months)	dd-mm-yyyy
Support and maintenance phase	dd-mm-yyyy

7. Requirements for Proposal Content

Vendors should provide information, evidence, and other relevant information as responses to the requirements stated below. Vendors should prepare their proposals providing a detailed description of their ability to satisfy each of the requirements detailed in this RFO. During the preparation of the proposal, emphasis should be on completeness and clarity of content.

Please also refer to the RFO reply checklist included in the Offer submission form (Appendix A)

7.1. Vendor Qualifications

7.1.1. Overview and Consortium Information

Vendors must submit the proposal as a sole vendor, a vendor with one or more subcontractors, as member of a consortium or a joint venture. The vendor is fully responsible for all aspects of the Proposal and, if applicable, the resulting Contract. In the case of the vendor being a Consortium, a Joint Venture, or any other single- or multi-member organisation, all members of such organisation must responsibly perform according to the Contract and one organisation of the group must be the responsible single point of contact.

If the vendor is a subsidiary, the vendor must disclose the information required above for its parent and/or holding company.

Each vendor/Consortium must provide a concise profile to include the following:

a) The name and address of the vendor submitting the Proposal.
b) Type of business entity (e.g., partnership, corporation etc.).
c) Date and Place of incorporation (or other form of organization), if applicable.
d) The vendors contact information: name, address, telephone number and email address.
e) Name and location of the vendor's major offices.
f) The name, address, telephone number, and email address (if available) of the vendors accounting or auditing firm.
g) Overview of the structure of vendor / Consortium Members' organization including details of ownership.
h) A description of the business units of the Potential Consortium members, highlighting those to be involved in the project.
i) Proof of financial viability, including audited financial statements for the past three years for all the Consortium members.
j) Proof of a professional liability insurance that shows a coverage of risk that is proportional to both:
    i. The expected amount of the software implementation contract and penalties built in the contract;
    ii. The expected amount of the support contract estimated for 5 years.
k) The vendor must be a business in good standing with its customers and the business community. The Vendor must state whether any of the following have occurred:
    i. If, during the last five (5) years, the vendor has had a contract terminated for default or cause, the vendor must submit full details including the other party's name, address, and telephone number;
    ii. If, during the last five (5) years, the vendor, a subsidiary, parent company, or holding company was the subject of any order, judgment, or decree of any jurisdictional authority barring, suspending, or otherwise limiting the right or license of the vendor to engage in any business,

practice, or activity or, if trading in the stock of the company, has ever been suspended, the vendor must submit full details along with date(s) and explanation(s);

iii. The vendor must list all contract delivery or performance issues for the last three (3) years, where such issues ultimately led to payment of liquidated damages, any sort of penalties, contractual payment deductions, or any other material compensation, goodwill, or consideration in any form. Each listed incident must be described in brief including incident jurisdiction, nature date(s) or period, and value. Equal incidents can be accumulated and summarized per jurisdiction provided the total occurrence count of such incident is given. It should be noted that items listed under this section are for due diligence purposes only and will not be the reason for rejection of a Proposal;

iv. If any of the references and experience descriptions in subsection 7.1.2. is based on prior projects conducted by a subcontractor of the vendor, a good standing statement with the same content elements as described in this subsection must also be established for the respective subcontractor.

7.1.2. References

The vendor is required to demonstrate corporate experience, technical capability, and financial means to support the Contract.

The vendor must describe, in detail, its current and historical experience with projects with similar solution components to the MMA instant payment systems and related services; that is, descriptions and references of payment system implementation projects of comparable complexity and sensitivity that have been conducted by the vendor within the past 5 years.

Each reference description must include the following details:

a) Name, country and type of financial institution (bank/clearing house/other).
b) Estimated contract value, reflecting the estimated total revenue during the full contract period.
c) Term of the contract including effective dates.
d) Reason for contract termination, if the contract is no longer in effect.
e) Types of services directly provided by the vendor under the contract and whether the vendor was a prime contractor or subcontractor.
f) Types and number of systems or components provided by the vendor.
g) Names of experts and their duties working on the reference project, in case they are still employed by the vendor and are proposed experts for the Contract.
h) Names, titles, addresses and telephone numbers that may be contacted to verify the reference.
i) The vendor must – if available – include statistics or test reports of relevant experiences, e.g. performance statistics, in order to provide evidence of their ability to meet the requirements described in the Requirements specification Section 7.2 and Section 7.3.

The MMA may check the references to ensure that the proposed products and/or services are in place and operational. If the vendor has a subcontractor that will provide a significant part of the deliverables, then experience information for that entity must be included.

7.1.3. Experts and Qualifications

The vendor is required to demonstrate its expert resources to support the Contract. The vendor must describe a pool of experts (including employees and subcontractors) who must be involved in this project. The vendor must express commitment that the offered experts will be involved in the project. During the implementation, the MMA's Project Manager will have the right to check whether offered experts are involved in the project.

For each of the experts, the following details must be included:

a) Full professional résumé.
b) Proof of listed professional qualifications.
c) Term and type of employment with the vendor.
d) Planned role in the project.
e) Citing your references, list the roles of the expert in previous projects.

Minimum qualification requirements for some of the roles are as follows:

a) Business Analysis Team Lead: minimum experience of 5 years as a Payment System Business Analyst.
b) Chief Architect: Relevant industry certification, e.g. TOGAF 9 Certification.
c) Chief Developer: minimum experience of 5 years as a chief developer in a relevant field.
d) Software developers: minimum 5 developers with a minimum experience of 5 years as a software developer in a relevant field.
e) Project manager: minimum experience of 5 years as a project manager of payment system projects and relevant industry certification, e.g. PRINCE2 Practitioner/Agile, PMP, PMI-ACP, etc.
f) Test manager: relevant industry certification e.g. advanced level ISTQB, etc.
g) Cyber security manager: relevant industry certification, e.g. CISSP, ECSA, etc.

7.1.4. Certifications

If the vendor has Certificates of the following standards, it must be enclosed to the Proposal:

a) ISO 27001
b) ISO 22301
c) ISO 9001
d) PCI DSS

7.2. Solution Functional Requirements

The vendor must present its proposed solution, product capabilities and functions, in accordance with the requirements described in the following sections.

7.2.1. Functional Solution Overview

Vendors must offer a complete solution complying with all the functionalities described by MMA explaining how the proposal is covering all the requested functional components as shown in the Figure 11:

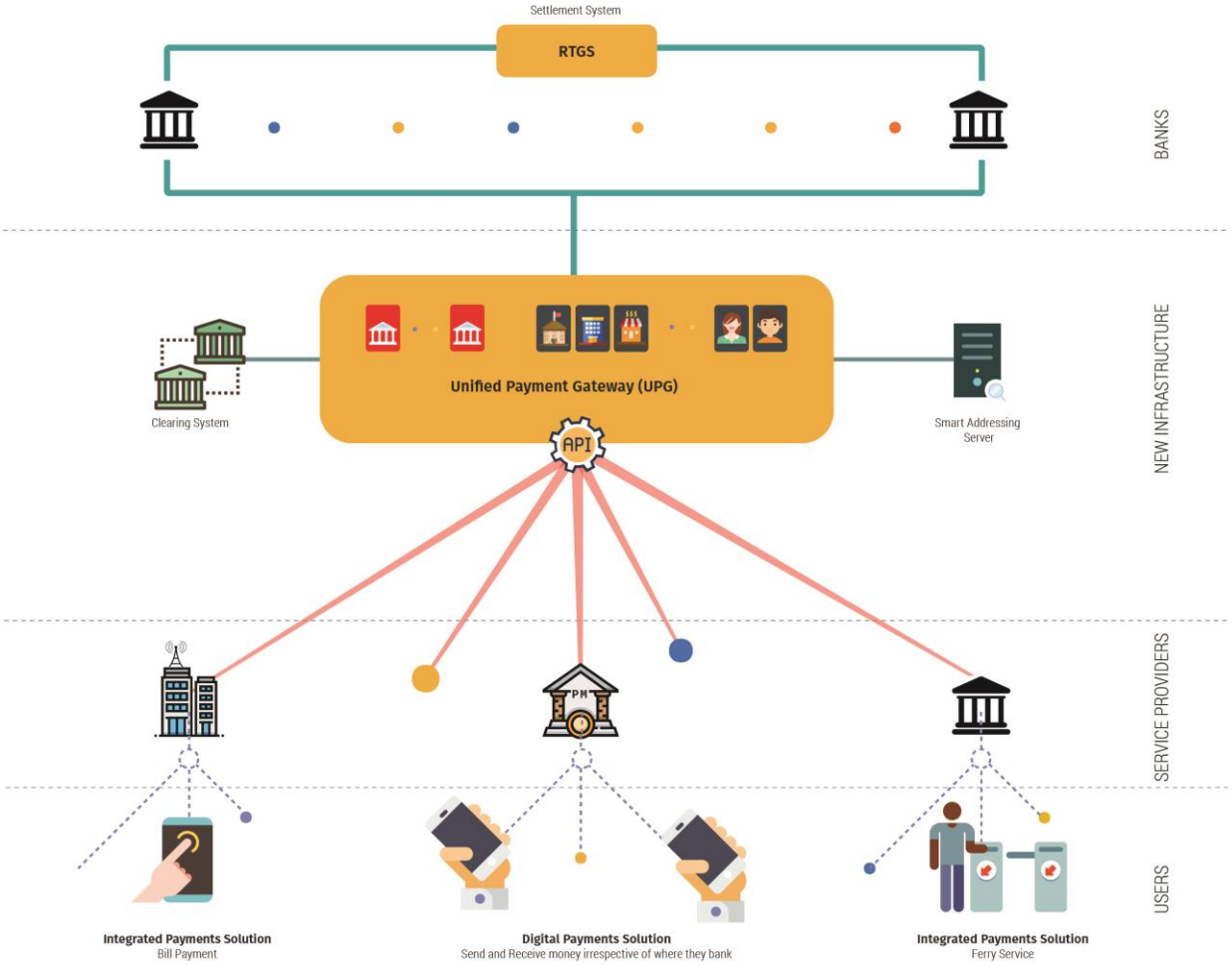

Figure 11. Functional Solution Overview

The minimum requirements of the above described solution are:

a) Overview of the proposed system and modules.
b) System parameterization: Vendors are expected to provide a detailed description of all business and technology level features that can be configured in their solution by the MMA without involvement of the vendor.
c) High-level logical architecture diagrams.
d) Interfaces with external systems.
e) All use cases, payment flows and overlay services supported by the solution.
f) How new overlay services can be implemented.
g) Describe sample use cases, payment flows or overlay services and how MMA can customise them.

7.2.2. Unified Payment Gateway

UPG facilitates AIPs to provide account information through the gateway to PSPs based on set of system rules that are in line with the legal framework. The UPG enables customers to view and manage multiple bank accounts through a single interface, consolidating various banking features including seamless fund routing & merchant payments.

Requirement Number	**Solution Compliance**
MMA-FR-UPG-001	

The UPG system should have an interface layer able to manage various message standards with at minimum ISO20022, ISO8583 and SWIFT FIN.

Requirement Number	**Solution Compliance**
MMA-FR-UPG-002	

The UPG interface layer must be easy to adapt in order to simplify integration with an AIP's back office applications.

Requirement Number	**Solution Compliance**
MMA-FR-UPG-003	

The UPG system should have an interface layer able to manage both synchronous (Stateless API) and asynchronous (queue and FTP) interface protocols in order to easy the integration with AIPs and PSPs.

Requirement Number	**Solution Compliance**
MMA-FR-UPG-004	

The UPG must allow PSP's to perform account to account fund transfers. Please specify how the UPG will manage the process.

Requirement Number	Solution Compliance
MMA-FR-UPG-005	

The UPG must allow PSPs to make payments on behalf of customers, accessing the accounts of the connected AIPs, including accounts held in the Digital Bank module. Please specify how the UPG will manage the process.

Requirement Number	Solution Compliance
MMA-FR-UPG-006	

The UPG must allow PSPs to make payments initiated by both the sender (initiator) and the receiver (beneficiary).

Requirement Number	Solution Compliance
MMA-FR-UPG-007	

The UPG must allow the management of Corporate Payments. Please specify how the UPG will manage these.

Requirement Number	Solution Compliance
MMA-FR-UPG-008	

Please describe how the solution UPG complies with the different use cases, i.e., P2P, P2B, P2G, G2P, G2B, B2G, B2P and B2B payments.

Requirement Number	Solution Compliance
MMA-FR-UPG-009	

The UPG must enable users to send and receive payments instantly, see Requirement Number MMA-NFR-023.

Requirement Number	Solution Compliance
MMA-FR-UPG-010	

The UPG must allow the payment initiator and beneficiary to receive instant confirmation.

Requirement Number	Solution Compliance
MMA-FR-UPG-011	

The UPG must allow payments to be made via different channels including but not limited to mobile app, web, kiosks, smart devices and card schemes. Please specify how the UPG will manage the process.

Requirement Number	Solution Compliance
MMA-FR-UPG-012	

The UPG must allow users to make payments using different addresses / identifiers including but not limited to virtual account ID, ID card, email, phone numbers. Please specify how the UPG will manage the process.

Requirement Number	Solution Compliance
MMA-FR-UPG-013	

The UPG must allow PSPs to access account information of the AIPs connected to the system including accounts held in the Digital Bank module in order to enable PSPs to view and manage multiple bank accounts through a single interface. Please specify how the UPG will manage the process.

Requirement Number	Solution Compliance
MMA-FR-UPG-014	

The UPG must allow KYC verification for new customers during the registration process through the integration with the National Registration databases (including but not limited to: Department of National Registration, Legal entities through Ministry of Economic Development and tourists and expatriates through Maldives Immigration). Please specify how the UPG will manage the process.

Requirement Number	Solution Compliance
MMA-FR-UPG-015	

The UPG must allow participant's to populate and update the Smart Addressing Module through various interfaces. Please specify how the UPG will manage this process.

Requirement Number	Solution Compliance
MMA-FR-UPG-016	

The UPG must allow multi-factor customer authentication (i.e. password, PIN, tokens, biometrics, OTP). Please specify how the UPG will manage the process.

Requirement Number	Solution Compliance
MMA-FR-UPG-017	

The UPG must interface with the Clearing Module in real time for validation against clearing and settlement limits. Please specify how the UPG will manage the process.

Requirement Number	Solution Compliance
MMA-FR-UPG-018	

The UPG must keep track of every transaction processed by the system with its status for a period of minimum 7 years with a unique time stamp. Please specify how transaction information are stored and how queries and reporting on this data does not affect system performance as specified in Requirement Number MMA-NFR-023.

Requirement Number	Solution Compliance
MMA-FR-UPG-019	

The UPG must provide a check transaction status API to enable AIPs and PSPs to enquire in real time on a specific transaction. Please explain what keys are used for searches and how these enquiries will not affect system performance as specified in Requirement Number MMA-NFR-023.

Requirement Number	Solution Compliance
MMA-FR-UPG-020	

The UPG must provide MMA with web-based tools to proactively track all transactions and activities within the system.

Requirement Number	Solution Compliance
MMA-FR-UPG-021	

The UPG must provide MMA with a wide set of enquiries to monitor the status of every transaction processed by the system. Please explain what keys are used for enquires, how the MMA can customized the enquires and how these enquiries will not affect system performance as specified in Requirement Number MMA-NFR-023.

Requirement Number	Solution Compliance
MMA-FR-UPG-022	

The UPG must provide MMA with a wide set of customisable reports for monitoring, reconciliation, profitability tracking, statistical analysis purposes. Please explain how reports are managed, generated and customized by the MMA. What standard reports are provided? How running report affect system performance as does specified in Requirement Number MMA-NFR-023.

Requirement Number	Solution Compliance
MMA-FR-UPG-023	

The UPG must manage AIPs and PSPs registration details into the system to allow transaction only from authorised participants.

The registration details should contain at minimum:

a) Legal name of the entity.
b) Institution identifier (i.e. BIC code).
c) Address.
d) Swift Code (If relevant).
e) Contacts.
f) Participation type (AIP, PSP) and details (e.g. joining date, validity, currencies traded).
g) Participation status (active, suspended, revoked).

Requirement Number	Solution Compliance
MMA-FR-UPG-024	

The UPG must conduct specified input tests on the transaction messages prior to processing any transaction related content of the messages. The controls should include but not be limited to the following:

a) Prevent duplicate transactions.
b) Prevent inappropriate message formats.
c) AIPs and PSPs authentication and authorization status.

7.2.3. Smart Addressing

Requirement Number	Solution Compliance
MMA-FR-SA-001	

The Smart Addressing module must allow customers to use simple, easy to remember addresses (e.g.: identifiers such as ID card, email, phone numbers) to make payments.

Requirement Number	Solution Compliance
MMA-FR-SA-002	

The Smart Addressing module must manage registration, update and deregistration of customers. It must support normal Create, Read, Update, and Delete (CRUD) processes.

Requirement Number	Solution Compliance
MMA-FR-SA-003	

The Smart Addressing module must manage lookup of customer records using any of the addresses.

Requirement Number	Solution Compliance
MMA-FR-SA-004	

The Smart Addressing module must allow AIPs and PSPs to access address information to provide various services (i.e., customer registration, verification, and authentication) using any address eliminating the need for sharing of bank account numbers and other sensitive information required to make payments.

Smart addresses should be issued and managed by PSPs to ensure that customers are uniquely identified by the PSPs. Please explain how access is provided.

Requirement Number	Solution Compliance
MMA-FR- SA-005	

The Smart Addressing must keep track of every address processed by the system with its status for a period of minimum 7 years with a unique time stamp.

Requirement Number	Solution Compliance
MMA-FR- SA-006	

The Smart Addressing must provide a check address status API to enable AIPs and PSPs to enquiry in real time on a specific transaction.

Requirement Number	Solution Compliance
MMA-FR- SA-007	

The Smart Addressing module must provide MMA with web-based tools to proactively track all addresses and activities within the system.

Requirement Number	Solution Compliance
MMA-FR- SA-008	

The Smart Addressing module must provide MMA with a wide set of configurable (by MMA) enquiries to be able to check any customer details registered in the system. Please explain how these enquiries will not affect system performance as specified in Requirement Number MMA-NFR-023.

Requirement Number	Solution Compliance
MMA-FR- SA-009	

The Smart Addressing module must provide MMA with a wide set of customisable reports for monitoring, and statistical analysis purposes. Please explain how these reports will not affect system performance as specified in Requirement Number MMA-NFR-023.

Requirement Number	Solution Compliance
MMA-FR- SA-010	

The Smart Addressing Module must conduct specified input tests on the transaction messages prior to processing any transaction related content of the messages. The controls should include but not limited to the following:

a) Prevent duplicate transactions.
b) Prevent inappropriate message formats.
c) Prevent duplicate customer.
d) Prevent duplicate addresses: one customer can have multiple identification addresses but a specific address can only belong to one customer.

7.2.4. Clearing

Requirement Number	Solution Compliance
MMA-FR-CL-001	

The Clearing Module must allow real-time multilateral net clearing between the participants.

Requirement Number	Solution Compliance
MMA-FR-CL-002	

The Clearing Module must allow MMA to configure the system to perform several settlement cycles per day through a web-based GUI.

Requirement Number	Solution Compliance
MMA-FR-CL-003	

The Clearing Module must be able to generate settlement instructions in SWIFT FIN standard formats to facilitate automated integration with the MRTGS system. Please explain how this integration would be done.

Requirement Number	Solution Compliance
MMA-FR-CL-004	

The Clearing Module must be able to generate and export settlement instructions in multiple file formats to be further processed manually into the MRTGS system.

Requirement Number	Solution Compliance
MMA-FR-CL-005	

The Clearing Module must allow clearing of payments on a 24x7x365 basis.

Requirement Number	Solution Compliance
MMA-FR-CL-006	

The Clearing Module must allow secure and reliable real-time payments with finality and confirmation so customers can access and use the funds immediately.

Requirement Number	Solution Compliance
MMA-FR-CL-007	

Allow direct participation by having a settlement account at MRTGS or indirect participation by having an agreement with a settlement participant in MRTGS.

Requirement Number	Solution Compliance
MMA-FR-CL-008	

The Clearing Module must allow UPG participants to allocate clearing and settlement limits/caps, where the payment instructions are validated against these limits. Limits will be configured by direct participants through a web-based GUI.

Requirement Number	Solution Compliance
MMA-FR-CL-009	

The Clearing Module must allow UPG direct participants to allocate clearing and settlement limits/caps for UPG indirect participants, where the payment instructions from indirect participants are validated against these limits. Limits for indirect participants will be configured by the related direct participants through a web-based GUI and can be set as a fix value or a percentage of the overall limit/cap.

Requirement Number	Solution Compliance
MMA-FR-CL-010	

The Clearing Module must be able to block the processing of new transactions when the above limits are exceeded.

Requirement Number	Solution Compliance
MMA-FR-CL-011	

The Clearing Module must notify the direct and indirect participants when their limit is reached or is close to being reached in a configurable manner.

Requirement Number	Solution Compliance
MMA-FR-CL-012	

The Clearing Module must support clearing and settlement within the system, without depending on the existing MRTGS system.

Requirement Number	Solution Compliance
MMA-FR-CL-013	

The Clearing Module must provide an automated and manual mechanism to top-up or decrease the limits/caps where necessary by reserving/releasing liquidity from the settlement account.

Requirement Number	Solution Compliance
MMA-FR-CL-014	

The Clearing Module must allow online liquidity monitoring and management for direct participants through a web-based GUI.

Requirement Number	Solution Compliance
MMA-FR-CL-015	

The Clearing Module must keep track of every transaction processed by the system with its status for a period of minimum 7 years with a unique time stamp.

Requirement Number	Solution Compliance
MMA-FR-CL-016	

The Clearing Module must provide the MMA and the direct participants with web-based tools to proactively monitor and manage their liquidity position and track all transactions and activities within the system.

Requirement Number	Solution Compliance
MMA-FR-CL-017	

The Clearing Module must provide MMA and direct participants with a wide set of configurable (by the MMA) enquiries to monitor the status of every payment transaction processed by the system. Please explain how these enquiries will not affect system performance as specified in Requirement Number MMA-NFR-023.

Requirement Number	Solution Compliance
MMA-FR-CL-018	

The Clearing Module must provide MMA with a wide set of customisable reports for monitoring, reconciliation, statistical analysis purposes. Please explain how these reports will not affect system performance as specified in Requirement Number MMA-NFR-023.

Requirement Number	Solution Compliance
MMA-FR-CL-019	

The Clearing Module must provide transactions statement details to direct participants in electronic format to enable them to fulfil their reconciliation and regulatory reporting requirements.

Requirement Number	Solution Compliance
MMA-FR-CL-020	

The Clearing Module must manage AIPs and PSPs registration details into the system to allow transaction only from authorised participants.

The registration details should contain at minimum:

a) Legal name of the entity.
b) Institution identifier (BIC code).
c) Address.
d) Swift Code (If relevant).
e) Contacts.
f) Participation type (direct/indirect) and details (e.g. joining date, validity, currencies traded).
g) Participation status (active, suspended, revoked).

Requirement Number	Solution Compliance
MMA-FR-CL-021	

The system should conduct specified input tests on the transaction messages prior to processing the payment related content of the messages. The controls should include but not limited to the following:

a) Prevent duplicate transactions;
b) Prevent inappropriate message formats; and
c) Participant authentication and authorization status.

Requirement Number	Solution Compliance
MMA-FR-CL-022	

The Clearing Module must provide the ability to calculate several types of fees that can be charged to participating members in accordance with MMA pricing policy. Fees can be calculated based on several criteria including but not limited to those listed below:

a) Enrolment fee (yearly, monthly).
b) Number of transactions processed.
c) Value of the transaction processed.
d) Number of payments processed (clearing and settlement fees).
e) Number of authorizations.
f) On request activities.

There must be the possibility to automatically send the fees for clearing and settlement through the Clearing Module.

7.2.5. Digital Bank

Requirement Number	Solution Compliance
MMA-FR-DG-001	

The Digital Bank Module must be able to create a wallet (or virtual account) which can be provided to any customer (Maldivian individual, business, expatriate or tourist). The wallet can be linked to a bank account or card giving an AIP that is not connected to the UPG the ability to provide the digital services to its customers. The wallet can also be issued to any unbanked customer.

Requirement Number	Solution Compliance
MMA-FR-DG-002	

The Digital Bank Module must be able to manage the wallet with at minimum the following functions:

a) Opening the account for individuals and businesses.
b) Activate the account.
c) Top-up of the account and transfer of funds back to bank account or card. Top-up should be manual or automated if account below a configurable limit.
d) Managing transactions.
e) Setting the allowed transactions (system wide, per AIPs/PSPs, per wallet type (bank/unbanked), per wallet).
f) Setting up of transaction limits per wallet (system wide, per AIPs/PSPs, per wallet type (bank/unbanked), per wallet).

Requirement Number	Solution Compliance
MMA-FR-DG-003	

The Digital Bank Module must be able to pre-create wallets. The user will have the choice to activate the digital wallet or link it to bank account or operate both. The customers can activate the wallet for making transactions performing the KYC procedures.

Requirement Number	Solution Compliance
MMA-FR-DG-004	

All Digital Bank Module functionalities can be accessed through GUI, API or messaging interfaces.

Requirement Number	Solution Compliance
MMA-FR-DG-005	

The Digital Bank module must provide a white labelled mobile banking application that can be proposed by MMA to the AIPs and PSPs. The application can be used by the banked, unbanked and corporate customers.

The application must offer the following functionalities:

a) Registration (including KYC checks).
b) Transfer money Account-to-Account.
c) Transfer money Account-to-Wallet.
d) Transfer money Wallet-to-Wallet.
e) Transfer money Wallet-to-Account.
f) Transfer money Wallet-to-card.
g) Transfer money Card-to-Wallet.
h) Collect Money.
i) Scan and Pay.
j) Check balance and transaction history.
k) Manage linked account/card (Add/Remove).
l) Configurable alerts when a linked card is about to go out of date.
m) PIN Management (Create/Change PIN).
n) Generate QR.
o) Utility Bill Payments.
p) Insurance Payments.
q) Merchant Registration.
r) Notification management.
s) Select Language.
t) Complaint Management (Raise Complaint).
u) Send Feedback.
v) Privacy (Disable Specific Unique Identifier/UPG ID).
w) Block User.
x) Manage Profile.
y) Logout.

Please specify how the application will perform the above functionalities.

Requirement Number	Solution Compliance
MMA-FR-DG-006	

The Digital Bank mobile application module must offer the possibility to top up the wallet in multiple ways including but not limited to:

a) Linked account.
b) International card.
c) Domestic card.

Please specify how the mobile application will manage the process.

Requirement Number	Solution Compliance
MMA-FR-DG-007	

The Digital Bank mobile application module must offer a payment solution for tourists or temporary visitors of Maldives. Please specify the various options available and clearly specify their pricing in Appendix B.

Requirement Number	Solution Compliance
MMA-FR-DG-008	

The Digital Bank mobile application module must be compatible with Android & iOS Mobile phones.

Requirement Number	Solution Compliance
MMA-FR-DG-009	

The Digital Bank mobile application module must allow multi-factor customer authentication (i.e. password, PIN, tokens, biometrics, OTP).

Requirement Number	Solution Compliance
MMA-FR-DG-010	

The Digital Bank mobile application module must support customizable branding, enabling PSPs to implement their logos, brand colours, and images.

Requirement Number	Solution Compliance
MMA-FR-DG-011	

The Digital Bank mobile application module must be easily integrated through API's with external systems such as core banking systems, in order to send and receive transactions details, process login requests, get lists of accounts and cards, etc…

Requirement Number	Solution Compliance
MMA-FR-DG-012	

The Digital Bank mobile application module must be a multi-tenant application with strict segregation of data (customer data, audit logs, master data, security elements, etc.) between the various AIPs/PSPs using the white labelled application.

Requirement Number	Solution Compliance
MMA-FR-DG-013	

The Digital Bank mobile application module must provide a multi-layered security role and authorisation management system to guarantee strict security boundaries between MMA, operators and AIPs/PSPs business operators. Changes will require 'four eyes' authorisation processes.

Requirement Number	Solution Compliance
MMA-FR-DG-014	

The Digital Bank module must provide a white labelled online payment gateway which allows making online payments through local payment scheme.

7.2.6. Fraud Detection and Prevention

Requirement Number	Solution Compliance
MMA-FR-FDP-001	

The Fraud Detection and Prevention module must provide a Case Management tool to manage the life cycle of a suspicious or fraudulent transaction (open for investigation, take appropriate actions, add remarks, and classify alerts).

Requirement Number	Solution Compliance
MMA-FR-FDP-002	

The Fraud Detection and Prevention module must provide a flexible rules engine in order to apply various different fraud prevention models. The solution must be easily adaptable to new fraud patterns.

Requirement Number	Solution Compliance
MMA-FR-FDP-003	

The Fraud Detection and Prevention module must monitor in real-time the spending patterns and statistical data of users, wallets, cards and merchants from various channels, applying customisable business rules with the objective rapidly detect and stop fraudulent or suspicious transactions.

Requirement Number	Solution Compliance
MMA-FR-FDP-004	

The Fraud Detection and Prevention module must be able to manage black, white, and fraud lists.

Requirement Number	Solution Compliance
MMA-FR-FDP-005	

The Fraud Detection and Prevention module must be able to pre-test new rules on historical data in order to avoid new rules to impact transaction processing.

Requirement Number	Solution Compliance
MMA-FR-FDP-006	

The Fraud Detection and Prevention module must provide a rules engine and analytics to facilitate applying customized policies and take automated decisions.

Requirement Number	Solution Compliance
MMA-FR-FDP-007	

The Fraud Detection and Prevention module must be able to map and analyse the financial relationships between customer accounts, transactions and other channels.

Requirement Number	Solution Compliance
MMA-FR-FDP-008	

The Fraud Detection and Prevention module must be able to create alerts when suspicious transactions have triggered specific rules. The system must also be configured to send alerts through SMS and email notifications.

Requirement Number	Solution Compliance
MMA-FR-FDP-009	

The Fraud Detection and Prevention module must be a multi-tenant application with strict segregation of data (customer data, audit logs, master data, security elements etc) between the various AIPs/PSPs using the tool.

Requirement Number	Solution Compliance
MMA-FR-FDP-010	

The Fraud Detection and Prevention module must provide a multi-layered security role and authorisation management system to guarantee strict security boundaries between MMA operators and AIPs/PSPs business operators. Changes will require 'four eyes' authorisation processes.

7.3. Solution Non-Functional Requirements

7.3.1. Non-Functional Solution Overview

Vendors must describe the architecture and technical details of the proposed system.

The minimum requirements of the description of the proposed solution are:

a) Availability, Scalability and reliability of the system.
b) Detailed technical, logical and physical architecture diagrams.
c) Technical Interfaces with external systems.
d) A complete and detailed Bill of Material for the Hardware and 3rd party software needs for the requested performance, with the following minimum details:
    i. Number and type of servers (CPU, memory, disk type and size, etc.);
    ii. Type and Number of licenses for 3rd party Software (license provider, version, licensing model, etc.).

7.3.2. Non-Functional Requirements

All the modules proposed by the vendor must comply with the Non-Functional requirements listed in this section.

Requirement Number	**Solution Compliance**
MMA-NFR-001	

All functionalities available with the Modules should be available through usable, graphical interfaces where internal and external users can effectively, efficiently and securely manage the functions of the system.

Vendors should describe in detail how the GUIs of their solutions support the functionalities listed above. Beside the description, the following documentation is expected:

a) User manuals to live systems or systems in the testing stage.
b) Screenshots on how the GUI of the vendors solutions fulfil the requirements above.

Requirement Number	**Solution Compliance**
MMA-NFR-002	

The system must support the use of industry leading browsers. At a minimum it must support Internet Explorer, Microsoft Edge, Firefox and Google Chrome. Each release of the system must be tested and compatible with current versions of the supported browsers and maintain backwards compatibility for up to a year.

Requirement Number	**Solution Compliance**
MMA-NFR-003	

The system must be able to send alerts to business/operational users via the GUI or via email/SMS/instant messaging for any critical event registered in any of the modules.

Requirement Number	Solution Compliance
MMA-NFR-004	

A client-side API is necessary for participants to have access to the modules. The API must handle all security and integrity requirements.

Requirement Number	Solution Compliance
MMA-NFR-005	

The system must support modern API authentication schemes.

Requirement Number	Solution Compliance
MMA-NFR-006	

The system must support a secure two-way authentication scheme with external systems.

Requirement Number	Solution Compliance
MMA-NFR-007	

The system should provide configurable authentication for APIs in non-production environments, allowing access for testing purposes.

Requirement Number	Solution Compliance
MMA-NFR-008	

The system must provide a configurable API rate limit to mitigate purposeful or accidental denials of service and avoid congesting the application.

Requirement Number	Solution Compliance
MMA-NFR-009	

For the sake of business continuity, transaction time and performance goals, the system should be able to provide continuous information about its operation.

Requirement Number	Solution Compliance
MMA-NFR-010	

To reach the pre-set performance indicators, the solution must be able to function in a redundant, load balanced, failover capable and distributed operational model.

The system must be fault tolerant during processing in case of:

a) One node failure (or restore).
b) One location failure (or restore).

c) One process failure (or restore).
d) One database failure (or restore).
e) Network failure (or restore).
f) Power failure (or restore).

Requirement Number	Solution Compliance
MMA-NFR-011	

The system must be able to implement patches on all hardware and software components without any service interruptions. There are no pre-set maintenance windows defined. All end of day functions must run in a way that operation is not interrupted.

Requirement Number	Solution Compliance
MMA-NFR-012	

The system must have a complete DRP and BCP process, with the goal of uninterrupted, 24/7 operation. All incidents must be handled by MMA.

Requirement Number	Solution Compliance
MMA-NFR-013	

The system must support a redundant, load balanced, failover capable, distributed operational model. In case of any incident, all database connections must be re-established consistently without any manual input and mirrored databases 're-synced'.

Vendors should describe in detail how their solutions support the implementation of the requirements listed below:

a) The implemented system must consist of multiple parallel operating processing servers. Each of these servers are capable of operating in failover, load balancing mode. The failure of one component must not result in service outage, and the failure is transparent towards the users.
b) In case of unscheduled system restarts the system must automatically ensure business data consistency. There must not be uncertain transaction statuses and unfinished operations must be rolled back and repeated. Databases must be kept in 'sync' automatically.
c) The system must use independently operating processing components ensuring that the failure of a physical or logical unit does not influence the performance or availability and the service level is not diminished.
d) The system tolerates the outages resulting from network interruptions; it consistently and automatically tries to rebuild the connection. The occurred failure must be displayed on screen and in the event log using an informative message.

Requirement Number	Solution Compliance
MMA-NFR-014	

The system must provide a front-end to monitor the availability and performance of the application. The monitor component must be used to monitor the health of the system resources. The monitor must also be used to start and stop a resource and monitor the performance of a resource. The component must also be used to set parameters for a resource, e.g., the size of the thread pool. The monitoring component must provide system level reports and graphs for analysis purpose.

Requirement Number	Solution Compliance
MMA-NFR-015	

All System components must be able to handle an increased load due to an increase in messages and transactions, especially on peak days

The system must be able to utilise additional hardware resources (memory, processor core numbers, and additional processing server) to increase the performance.

The System should take future growth into consideration with no or minimal impact to existing interfaces and implemented solutions.

Requirement Number	Solution Compliance
MMA-NFR-016	

Operating the system should be mostly automated, with minimal manual task to avoid any possible mistakes.

Requirement Number	Solution Compliance
MMA-NFR-017	

The system must support all input and output validation and provide appropriate error handling at the presentation, business logic and data layers.

Requirement Number	Solution Compliance
MMA-NFR-018	

There are no special preferences for hardware and 3rd party Software.

a) In case there is no technological barrier to it, the use of Oracle DB (12C or later) is preferred. Deviation from this is possible after thorough reasoning and discussion.
b) In case there is no technological barrier or any other consideration, the use of an application server is preferred, more precisely the WebLogic and JBoss EAP current versions. Deviation from this is possible after thorough reasoning and discussion.
c) In case there is no technological barrier or any other consideration, the use of OEL/RHEL Linux as the operating system is preferred.

Requirement Number	Solution Compliance
MMA-NFR-019	

The business and technical performance of the system should support internal monitoring. To support this function, the proposed solutions should provide detailed statistics regarding attributes defined by MMA.

Vendors are invited to present how their solution provides this functionality.

Requirement Number	Solution Compliance
MMA-NFR-020	

The system must be capable of scaling both horizontally and vertically, granting the ability to add more capacity to the system as needed.

Requirement Number	Solution Compliance
MMA-NFR-021	

The system should be flexible and have the ability to rapidly integrate and deploy new capabilities, improvements and fixes with little to no effect on other components.

Requirement Number	Solution Compliance
MMA-NFR-022	

The system must provide toolsets (e.g., stubs, mocked components, APIs) to allow isolated testing of each interfacing component, service or application.

Requirement Number	Solution Compliance
MMA-NFR-023	

One of the main expectations towards the system is that it should ensure high-performance operation. The proposed solution should provide the vendor with a solution that:

a) Enables high-speed processing of transactions;
b) Has a robust capacity to handle peak loads;
c) Can operate 24/7 without interruptions.

The vendor should describe in detail how their solution ensures compliance with the performance targets listed below:

a) The system must process an end to end transaction within 5 seconds.
b) The system must be able to handle operation at a minimum of at least 400 transactions / second
c) The system must support at least 20 concurrent users and must be scalable to add more users in a short period.
d) The system must be able to process payments, including payments over the alternate network, through necessary Risk Controls in <1 second.

e) The system must have a general GUI response time within 2 seconds while moving between functions/screens.
f) The system must not take longer than 3 seconds to complete any one enquiry
g) The system must not take longer than 5 seconds for any one User to login.
h) The system must not take longer than 3 seconds to generate common reports.
i) Any enquiries or reporting must not affect overall system performance.
j) The system must operate 24/7 with no interruptions.

Requirement Number	Solution Compliance
MMA-NFR-024	

The system must handle message timeouts. The given transaction must be terminated in case more than a certain number of seconds have passed compared to the timestamp value, the transactions has to be moved into a failed end state, and both the originator and the beneficiary must be notified in case this is relevant. The timeout value should be a parameter that can be configured by MMA.

7.3.3. Security

The information stored at, and transmitted through the system must remain confidential. All exchanges of information between the modules and the participants of the service need to be encrypted using strong algorithms and key sizes. For reasons of confidentiality, integrity and availability, the solution has to be developed using a secure development life cycle methodology. This will decrease the likelihood of vulnerabilities and the attack surface.

MMA prefers a solution compliant with EU General Data Protection Regulation (GDPR) and other standards used in the payment industry.

The following chapters provide detailed information about the specifications of IT Security.

Requirement Number	Solution Compliance
MMA-NFR-025	

The system must have password policy capabilities for different user groups and roles. For all local authentications the policy must be enforced. All user access parameters must be customisable by MMA.

Requirement Number	Solution Compliance
MMA-NFR-026	

The system must support the choice of single or dual factor authorization for every user functionality within the system.

Requirement Number	Solution Compliance
MMA-NFR-027	

All access must be role based. Separate roles must be established for security, business, operations, support, and audit functions. All roles must be customisable for different access rights by MMA. Changes to security setting must have 'four eyes' authorisation.

Requirement Number	Solution Compliance
MMA-NFR-028	

Allow segregation of duties by applying four-eye principle based on transaction limited or process, i.e., changing permissions on roles.

Requirement Number	Solution Compliance
MMA-NFR-029	

The system must automatically lock user accounts that exceed a maximum login attempts threshold as configured by MMA.

Requirement Number	Solution Compliance
MMA-NFR-030	

The system must not allow any Participant to view or perform any function for any other Participant if the relevant permission has not been granted.

Requirement Number	Solution Compliance
MMA-NFR-031	

The system must be able to log off the user automatically and completely after a period of inactivity (this must be controlled by parameters).

Requirement Number	Solution Compliance
MMA-NFR-032	

All users and endpoints must be uniquely identified, connections are only allowed with the standard settings and requirements of MMA.

Requirement Number	Solution Compliance
MMA-NFR-033	

The system must be able to integrate with external Identity Management Services (or User Privilege Management Tools).

Requirement Number	Solution Compliance
MMA-NFR-034	

The system must provide full audit trails for all activities within the system including, but not limited to; parameter changes, allocation of user permissions, user activity, unsuccessful access attempts and transaction activity, changes and details over a period of 7 years.

Requirement Number	Solution Compliance
MMA-NFR-035	

All audit trails must contain time stamps and be protected against tampering.

Requirement Number	Solution Compliance
MMA-NFR-036	

Data segmentation must be established between production, staging, QA, test and development environments. The database and all application related storage must be able to support encryption and this must be configurable via parameters. The integrity of all data and program code must be protected.

Requirement Number	Solution Compliance
MMA-NFR-037	

Network security is based on the same principles as any other IT security area. The solution must be able to use encryption to provide confidentiality for authentication and integrity protection; digital signatures to provide authentication, integrity protection, and non-repudiation; checksums/hash algorithms to provide integrity protection and authentication.

Network level segmentation must be established between production, staging, QA, test and development environments.

Requirement Number	Solution Compliance
MMA-NFR-038	

All interfaces must be secured and data confidentiality, security integrity and availability must be guaranteed. All data communication between users, components of the solution and external Users must support strong encryption techniques to support the critical nature of the system.

The system must support encryption of data at rest and in transmission and allow message encryption.

Requirement Number	Solution Compliance
MMA-NFR-039	

The system must protect the integrity of all critical and sensitive configuration files and check the integrity before starting the system (HASH).

Requirement Number	Solution Compliance
MMA-NFR-040	

It must not be possible to disable the security features other than where documented and agreed.

Requirement Number	Solution Compliance
MMA-NFR-041	

The system must meet the appropriate cyber security standards.

7.4. Delivery and Methodology

7.4.1. Training

The vendor must present its proposed training plans that include the following topics as a minimum requirement:

a) Architecture, technology, interfaces.
b) System operation and administration.
c) Error handling and support relations, processes.
d) Training for operators.
e) Business parameterization, processes, tasks, GUIs.
f) Training for security professionals, including cyber risk management.
g) Introductory training of the system for testers.
h) Participant training.

The training on security and cyber risk management should be delivered early in the project (within 6 months from the start). The vendor must provide a full description of the training sessions including the length and the maximum attendees number. After training sessions, further consultation and on-site support might be needed, please include these options in the Pricing. After the trainings, vendors are also expected to provide all training material to the MMA for further use (such as integrating the training material into the MMAs internal training suite) in electronic format.

7.4.2. Support Capabilities

The vendor must present its proposed solution for support services after go-live, with respect to the following requirements:

a) The MMA expects the vendor to offer 24/7/365 post go-live support for the delivered system under terms of a contract for an indefinite period.
b) Technical support must be dedicated support, with a 24/7/365 availability.
c) Incident management should be part of the support service. The incident management support should be designed to effectively and efficiently help the MMA prevent system outages. Vendors are expected to provide a support service model in their proposals with sufficient assurance for this requirement. The MMA intends to establish a framework for the incident management support in a service level agreement (SLA). In the expected incident management scheme system failures should be categorized according to a 5-step grading scale.
d) The MMA must use the ticketing system of the Vendor, as well as a dedicated hotline for high-priority issues.

e) Support service should also cover the following services:
   i. 6 months Special post go-live support including 4 weeks post go-live on-site presence and off-site priority support.
   ii. General post go-live support and maintenance services including, but not limited to providing an online, secure ticketing system, remote troubleshooting, installation and updating assistance, usability assistance etc. for a period of five (5) years.
   iii. A hotline service for incident management purposes.
   iv. All new versions.
   v. A support package covering developments related to minor changes in the system related to functionality, performance, usability or security issues, as well as changes in the regulatory environment. The vendor should define a quarterly FTE-cap for support services under this service element.
   vi. An Account or Support Manager with agreed SLA and escalation procedures to vendor executives.

7.4.3. Change Management

The MMA must use the ticketing system for the vendor for change management administration purposes as well. Please note, that the change management process is applicable during both the software implementation phase and the live system support.

In order to assess the vendor's compliance with the internal change management regulations of the MMA, the vendor must present how its ticketing system is able to support the realization and documentation of the following change management process steps:

a) Business requirements definition.
b) Analysis and requirement collection.
c) Planning, system design.
d) Acceptance of requirement specification and system design.
e) Development, system documentation.
f) Acceptance and installation permission.
g) Installation to test environment.
h) Testing phase: error tickets, test reports.
i) Acceptance and installation permission.
j) Go-live and launch of live operation, installation report.

7.4.4. Software Quality

The vendor must present its solution / documentation / internal processes regarding the following topics:

a) Detailed introduction of quality controls that ensure the quality of the proposed solution in accordance to the Requirements specification.
b) Presentation of Quality Assurance Plan in accordance with the quality controls in use or planned during development and implementation.
c) Demonstration of IT security technology and product assurance.
d) Testing methodology (including handling of test data) and supporting tools.
e) Detailed description of the error management procedure.

7.4.5. Project Management

Vendors must present their Project Plan for the implementation. The plan should include the following elements as a minimum:

a) Project management methodology.
b) Project schedule and milestones with dependencies.
c) Deliverables related to each milestone.
d) Payment milestones and amounts of invoices at milestones considered as partial delivery.
e) Resource plan, including resource needs from the MMA.
f) Planned on-site/off-site number of days.
g) Test plan.
h) Risk management plans.
i) Role specification of experts (incl. project managers and subcontractors), and RACI matrix.
j) Regular executive oversight reviews.

During preparation of the Project Plan described above, the vendor must consider the following:

Due to the high-risk environment and the core requirements related to the secure and uninterruptable operation of the system, it is essential that the product complies with performance and information security requirements.

Therefore, the vendor is requested to provide two performance and penetration tests during the implementation project:

a) The first must be conducted on the product final release.
b) The second must be conducted at the UAT phase at MMA premises.

The penetration tests need to be performed by an independent entity.

Vendors are expected to include in their project plan a detailed description on how they will conduct the performance and penetration test assessments.

The results of the performance and penetration tests will be part of the acceptance criteria

7.4.6. Software Development Plans

Vendors must enclose its detailed Development Methodology in its Proposal.

The vendor must give a detailed presentation of its software roadmap for the next five years. Please include any future planned functionalities and support for new technologies, OS, DB, hardware and software updates, with regards to the MMA's future plans (see below):

Vendors must specify their solutions 'Version support plans', i.e., current version -1 is supported by the vendor, how often are new version released, when will the MMA have to upgrade the solution. All of this should be built into the TCO, licensing and support costs.

Vendors must include description of any other optional functions that are not mentioned in the Requirements Specification, but that it believes can improve the overall solution. Please, include pricing information of these, where applicable in the Pricing table (Appendix B).

7.5. Pricing

The vendor must provide pricing information by filling out the Pricing Table (Appendix B) taking the below instructions into consideration:

a) Prices should be indicated in USD.

b) The costs will include reimbursable expenses.

c) The MMA will not be held responsible for any government taxes and/or levies. Vendors are expected to take this into consideration.

d) Implementation, software license and support service costs should be presented in different worksheets of Appendix B (Pricing Table).

e) The vendors are expected to propose a turnkey price including all costs (including but not limited to licenses, implementation services, travel and accommodation). The MMA will not accept any hidden and/or additional costs; the financial proposal should be comprehensive and all inclusive.

f) The vendor is required to clearly identify and explain all assumptions upon which charges are predicted. Vendors should also state if any change us subject to special conditions, and clearly specify those conditions and quantify the impact upon the charges.

g) The expected content of the worksheets in the Pricing Form is described in the subsections below.

7.5.1. Implementation Costs

Implementation Costs must be indicated according to the Project Milestones proposed under subsection 5.5. Milestones included in the Pricing Table (Appendix B) should be identical to the Payment Milestones included in the project management section of the vendor's proposal. Please provide separate prices for every project phase.

7.5.2. Software License Fee

Software license fees should be presented for each year during the period after go-live, under terms of the vendors license policy. The MMA prefers a model where the license fee is invoiced in a single payment.

The vendor is expected to present the cost estimation of the delivered solution's software license fee (including customisations) considering that the software source codes, along with consequent versions and patches, as well as all relevant documentation, are placed in custody at a solicitor approved by both the MMA and the vendor. Source code is only released to the MMA under special contractual terms to be later agreed upon.

7.5.3. Post Go Live Support

Support service fees should be described ensuring that the requirements stated in RFO subsection 7.4.2. (Support capabilities) are met. If the vendor proposes multiple alternative options as a response to RFO, fees for all options must be included in the Pricing form.

The vendor is also expected to indicate a man/days fee per professional profile for future additional software development and implementation services.

APPENDIX A: OFFER SUBMISSION FORM

Date:

RFO Reference Number:

Contract: Request for Offer Instant Payments for the Maldivians

To:
Procurement Section
General Services Division
Maldives Monetary Authority
Boduthakurufaanu Magu, Male'
Republic of Maldives

Dear Sir/Madam,

Having examined the Request for Offer Documents, the receipt of which is hereby acknowledged, we, the undersigned, offer to undertake the above-named Contract in full conformity with the said RFO Documents for the sum of **XXXX USD (value in letters)** in accordance with the terms and conditions of the Contract.

We undertake, if our Offer is accepted, to commence the services for the Maldives Payment System Development Project within the respective times stated in the RFO Documents.

We agree to abide by this RFO, which consists of this letter (Offer Submission Form) and the enclosures listed in the Checklist below, for a period of 6 (six) months from the submission deadline of Offers as stipulated in the RFO Documents, and it shall remain binding upon us and may be accepted by you at any time before the expiration of that period.

Until the formal final Contract is prepared and executed between us, this Offer, together with your written acceptance of the Offer and your notification of award, shall constitute a binding contract between us. We understand that you are not bound to accept the lowest or any Offer you may receive.

Dated this [insert: ordinal] day of [insert: month], [insert: year].

Signed:
Date:

In the capacity of [insert: title or position]

Duly authorized to sign this bid for and on behalf of [insert: name of Bidder]

RFO Checklist *Please provide the relevant section and page number in the 'Yes' box and indicate the corresponding page numbers in the response document*	*Please tick the appropriate box*		*Reference in response documents*
	Yes	**No**	
Vendor Qualification			
Overview and consortium information			
References			
Experts and qualifications			
Certifications			
Solution Functional Requirements			
Functional Solution Overview			
Unified Payment Gateway			
Smart Addressing			
Clearing			
Digital Bank			
Fraud detection and prevention			
Solution Non Functional Requirements			
Non-functional Solution Overview			
Non-functional Requirements			
Delivery and Methodology			
Training			
Support capabilities			
Change Management			
Software Quality			
Project Management			
Software Development Plans			
Pricing Table			

APPENDIX B: PRICING TABLE

Cost Summary	Implementation Costs (USD)	Software License Fee (USD)	Total (USD)
a) Unified Payment Gateway			
b) Smart Addressing			
c) Clearing			
d) Digital Bank			
e) Fraud, Security and Monitoring			
Grand Totals			

*Please provide the cost breakdowns where applicable.

Post Go Live Support	USD
a) Annual maintenance fee	
b) Onsite support fee for 6 months	

*Please provide the cost breakdowns where applicable.

Name of Bidder:	
Authorized Signature of Bidder:	

APPENDIX C: FORMAT OF ADDRESSING THE BID ENVELOPE

[Please do not stick courier/postage or any other stickers over the writings/markings]

DO NOT OPEN BEFORE:

July 18, 2019, 1500hrs (GMT+5).

Name of the Bid:

INSTANT PAYMENTS FOR THE MALDIVES

Invitation for bids reference number: IL-PRC/2019/50

Procurement Section, General Services Division,
Maldives Monetary Authority
Boduthakurufaanu Magu
Malé 20182
Republic of Maldives

[Name and Address of the Bidder]