

Annexure 'A' [Statement of work #2309221243]

This Statement of Work is executed between the parties named before in accordance with the Software License Agreement #2309221124 dated 23rd September 2022. between ULIS TECHNOLOGY (P) Limited, henceforth referred as (ULIS) and Mena PayTech Systems Limited (MPTSL) in this document.

Licensee/Licensee affiliates	Mena PayTech Systems Limited DIFC, Dubai - United Arab Emirates
Service/ License Provider	ULIS TECHNOLOGY (P) Limited, UDC#2, Central Warehouse Lane, East Wardhman Nagar Nagpur, MH, INDIA-440008
Effective date and term of the SOW	Effective date: 23rd September 2022 Valid up to: 30 th June 2023
Nature of Services/ License	Deployment of "Artha Pay (Web Browser Based) with AML Based Merchant Onboarding and Customer App for Vault and Auth" from ULIS Product SUITE
Is this Statement of Work for SLA License Based Products and their implementation services?	YES (Software License Agreement with Source code access license)
Scope of Deliverables to be provided to Mena PayTech Systems Limited	The Scope of the product implementation and consultation services and are mentioned in the below section of the document in detail.
Hardware, equipment's to be provided by Mena PayTech Systems Limited.	Yes, all onsite hardware required, and servers will be provided by Mena PayTech Systems Limited to their resources. ULIS will take care of all the offshore hardware requirements.
Use of pre-existing IPR of ULIS/ Customer	Yes, ULIS would be using their current tools and IPR's if any for this delivery.
Use of Open-Source software	All software used for this engagement as per the service/product scope (Annexure-A1) are open source in nature, except for any 3 rd party API's.
Dependencies to be provided by Customer	All required access if any for this engagement to be provided by Mena PayTech Systems Limited to ULIS. Services to be provided by ULIS shall be subject timely provision of all necessary dependencies by Mena PayTech Systems Limited. ULIS should highlight all the requirement before the start of engagement with all the relevant risks and timelines for the same. It is expected that ULIS should highlight Mena PayTech Systems Limited with relevant reminders for any dependencies if any.
Is this Statement of Work for Staff Augmentation Services?	No
For T&M services	Provided as and when required.
Reimbursements	Travel with-in Nagpur, India would be taken care by ULIS. In case of any onsite visits/expenses such as transport, accommodation, per-diem



	etc. shall be reimbursed by the client at actual cost & on submission of the relevant documents.
Points of Contact	Name: Miss. Apurvaa G. Address: UDC #2, Central Warehouse Lane, East Wardhman Nagar, Nagpur, MH, INDIA-440008. Email: apurvaa.g@ulistechnology.com
Invoices to be submitted to	Mena PayTech Systems Limited DIFC, Dubai - United Arab Emirates
Additional operational terms applicable to this SOW	<ul style="list-style-type: none"> a. ULIS shall perform all the technical activities required for consultation, implementation, integration and maintenance of the application. b. No Hiring Clause: No ULIS Resource can directly or indirectly be hired by the client for a period of 24 months from the contract expiry date and/ or in the tenure of the contract without consent. c. Any modifications outside the scope defined in technical description of the application shall be charged over and above. d. Cost for API based integration (not included in Annexure A1) for any third party applications will provided separately on receiving the exact documentation of the functionality and parameters. e. Any delays from Client side in regards to providing Data, Policy, Sign –OFF, any third-party dependency for data or integration, non-availability of Resources, temporary hold of implementation for any reason other than specified above, resulting in deviation of mutually agreed Project Plan will lead to increase of Implementation charges on per man day basis (depending on the team size).

Process Guidelines:

Language of Documentations English

ULIS Product Manager (ULIS SPOC) Name: Pawan Kushwaha
 UDC #2, Central Warehouse Lane, East Wardhman Nagar, Nagpur, INDIA-440008.
 Email: pawankushwaha@ulistechnology.com

Mena PayTech 's Representative (Client SPOC) Name: Mr. Abhishek Shukla
 Mena PayTech Systems Limited
 DIFC, Dubai - United Arab Emirates
 Email: abhi@paydart.co

Completion durations and other Due Dates 12-14 Weeks (23rd September 2022- 30th December 2022)
 6 Month's support duration (initiated within 1 week of UAT signoff) and valid till 30th June 2023.
(The Start Date is subjective to clearance of relevant milestone invoices)

Authorized Signatory (ULIS) _____
 ULIS Technology (P) Limited - Confidential

Authorized Signatory (Mena PayTech Systems Limited) Abhishek Shukla



Milestone based Delivery process:

Milestones	Deliverables
Clearance of [M0]	
	SOW sign-off: Initial payments on Agreement and SOW signoff.
Clearance of [M1]	
	<ul style="list-style-type: none"> • Merchant onboarding and google 2FA • Merchant advance eKYC • Advance eKYC admin console • Merchant console, manage profile, manage sub-merchants, • Admin console, manage merchants, master setups, PSP Setups • Web browser-based Checkout • Card tokenization and fingerprinting <p><i>(Deliverables: Submission of SIT reports and maximum 1 Week of UAT)</i></p>
Clearance of [M2]	
	<ul style="list-style-type: none"> • Merchant console, transaction monitoring, fraud detection dashboard, reporting and MIS, checkout page white labeling. • Admin console, transaction monitoring, fraud detection dashboard, reporting and MIS • Customer's mobile app • Shopping cart plugins • Open APIs <p><i>(Deliverables: Submission of SIT reports and maximum 1 Week of UAT)</i></p>
Clearance of [M3]	
	Staging with submission of SIT reports and integrated UAT Sign off (UAT Time frame 1 week)
Clearance of [M4]	
	Go-Live with deployment support, testing and final delivery.

SOW End Date 30th June 2023

Working Hours 9:30 AM IST to 6:00 PM IST as per respective locations.

Key Personnel Mr. Pawan Kushwaha
 Miss. Apurvaa Gaikwad
 Mr. Ashutosh Singh Lodhi
 Mr. Ajit Rathi

Services The Services overview are described in Attachment 1.

Project Plan Shall be shared post Project KO meetings

ULIS Reporting:

- Detailed project plan will be shared at the start of the assignment and weekly updates to be shared between the SPOC's of both the parties.
- ULIS is to make available all project-related artifacts that are necessary for the Mena PayTech Systems Limited project team to perform its duties to meet the project scope and schedule.
- Mena PayTech Systems Limited is to ensure that the project team is informed about all policies and procedures

Authorized Signatory (ULIS) _____
 ULIS Technology (P) Limited - Confidential

Authorized Signatory (Mena PayTech Systems Limited)

Abhishek Shukla



that it is expected to adhere to.

- For onsite services Mena PayTech Systems Limited is to provide necessary workspaces on its premises (desk, PC/laptop, telephone, rights to enter the building and use IT systems), ideally in the form of a project office. It is also to provide meeting rooms and equipment (video projector, flip chart, etc.) when necessary.
- ULIS is to provide documentation of relevant processes and systems along with requirements. This may include, for example, process descriptions, handbooks, organ grams, system descriptions and product catalogues.
- Formal communications will be through official email id's and by usage of third-party plan forms for virtual meeting on Microsoft Teams Platform, project management on JIRA and tasks management on trello platforms.



ATTACHMENT1







Services and Deliverables Specifications	Services will be invoiced on milestone basis.
Product/Service	"Artha Pay (Web Browser Based) with AML Based Merchant Onboarding and Customer App for Vault and Auth"
Technology for the project	Node.js, CodeIgniter 3.1.13 (HMVC), PHP 7.4, MySQL, HTML, CSS, Bootstrap, JavaScript, jQuery, SHA 256-bit Encryption, Tokenization, Token-based API integrations React Native (for mobile app development), Android Studio and X-Code (for application uploads).
Project Management	ULIS shall remain responsible for end-to-end project management. Project management approach and detailed project plan shall be developed and agreed between parties after project kick-off. Project Plan should highlight and software release plan, project milestones, timelines, tools, resource allocation and dependencies.
Integrations	As per scope in Annexure-1.
Product Deliverables	<p>ULIS shall implement following applications which will constitute Mena PayTech:</p> <ul style="list-style-type: none"> • Artha Pay (Web Browser Based) - Checkout • Master (subjective to the relevant SI and solution) • Merchant Onboarding (web application only) • Fraud Detection Dashboard • CR 1.0.0 • CR 1.0.1 • Integrations as per Annexure -A1
Support & Maintenance	<ul style="list-style-type: none"> • ULIS shall provide 6 months complimentary support initiated within 1 week from date of UAT signoff, in the support period ULIS shall at its cost support and maintain the Mena PayTech Systems Limited and fix any reported issues or bugs. After completion of the warranty period ULIS may be required to provide support and maintain services, which shall be charged on time and material basis. • Support team shall include: (in warranty period) <ul style="list-style-type: none"> ▪ Backend Developer: 1 ▪ Mobile App Developer: 1 ▪ Testing Engineer: 1 ▪ Team Lead available as and when required
Security & Compliance	ULIS shall ensure best in class security implementation for Mena PayTech Systems Limited, including but not limited to ISO 27001 certifications, Auto sign-out, account protection using dual factor authentication or equivalent algorithms. Furthermore, ULIS shall ensure that Mena PayTech Systems Limited does not breach any applicable laws and ensure that its underlying software that is utilized for developing Mena PayTech Systems Limited does not contains or gives direct access to any Harmful Code, circumvent, or modify any security mechanism, transmit any viruses, worms, defects, Trojan horses, or any programming of a destructive nature.
Quality Assurance and Quality Control	ULIS shall cover unit testing, smoke testing, sanity testing, integration testing and regression testing on the product. ULIS shall share corresponding test reports with





	Mena PayTech Systems Limited. ULIS shall also prepare test strategy, test plan and test cases for UAT and provide them to Mena PayTech Systems Limited. ULIS plans to conclude the UAT maximum timeframe of 4weeks.
--	---

Interaction matrix

Name	Designation	Email ID's
Utkarsha Patil	Delivery Manager	utkarsha.p@ulistechnology.com
Pawan Kushwaha	Sr. Product Manager	pawankushwaha@ulistechnology.com
Amol Kothale	Sr. SME (BSFI Vertical)	amol.k@ulistechnology.com
Apurvaa Gaikwad	Head Delivery IBU (BSFI)	apurvaa.g@ulistechnology.com

ULIS Technology (P) Limited	Mena PayTech Systems Limited	Mena PayTech Systems Limited
  Authorized Signatory _____	  Authorized Signatory <u>Abhishek Shukla</u>	  Authorized Signatory _____
Name: Mr. Amol Kothale	Name: Mr. Abhishek Shukla	Name: Mr. Sridhar Gorantla
Title: Sr. Consultant (Finance & Compliances)	Title: Director	Title: Director
Date: 23/09/2022	Date: 23/09/2022	Date: 23/09/2022

Authorized Signatory (ULIS) 
 ULIS Technology (P) Limited - Confidential

Authorized Signatory (Mena PayTech Systems Limited)  Abhishek Shukla
 Page 6 of 18

Implementation Scope | TOR

Terms of Reference Details:

Here is the list of modules and their description that we are going to implement in the as - signed application:

“Artha Pay (Web Browser Based)”

- Advanced Features added to the web app
 - Card Tokenization
- Easy integration
- Built in analytics
- Step-to-step transaction history
- Multi language option

Master (subjective to the relevant SI and solution)

- Login with ID and Password with Google2FA Authenticator
- Analytical Dashboard
 - Transaction analytics and statistics#1
- System User Access Control:
 - Role based system user registration and setup.
 - Allocate the respective access control to the users.
 - This section helps to create admin staff and provide them different access rights.
- Language Setup
 - Easy to add & exclusive, ULIS mechanism for multilingual platform without using any language conversion tools.
 - JSON based dynamic language setup
 - Download the sample file, change the label into desired language and upload, and system is ready with new language option.
- Customer Monitoring#2
 - Store customer’s name, email, mobile no., billing & delivery addresses, city, country.
 - Depending upon email address, store and monitor the transactions.
 - Transaction list with different filters.
 - Customer name
 - Email
 - City
 - Country
 - Transaction amount range
 - Date range
- PSP Setup
 - Option to add PSP and their details
 - Name
 - Email (To, CC)#3
 - Supported MCC (multi-select)
 - Remark
 - Option to update, and active & deactivate
- Merchant Management
 - Option to add merchant users / sub merchant
 - View all the merchant details



- Option to update, activate/deactivate
- Admin can update MCC for any merchant.
- View Merchant registered on the application
 - Uploaded documents for verification
 - KYC Docs uploaded
- Manually update the status on Merchant's KYC at PSP to Approved, Denied or Hold, by default, Pending.
- Update PSP and MID for merchant
- Arthapay will only work on Merchant's platform when merchant's PSP KYC status is Approved, and system status is Active.
- Country Setup
 - Add country with country code
 - Option to flag any country as 'High risk country'.
 - Option to update, activate/deactivate
- IP Tracker:
 - Monitoring across systems to detect particular log events and patterns performed by users.
 - Admin can see which task is performed from which IP Address, Browser, Operating system, Device with time stamp and thus can have a watch on every activity.

Artha Pay (Web Browser Based) – Checkout

- Option for customer to save their card information securely on Artha Pay.
- Consent shall be taken to store the card information.
- Following card details to be saved in an encrypted form using **SHA 256-bit encryption** as per PCI DSS complaint and the data shall be shared with Jumbo Jet #4
 - Card Number
 - Card holder's Name
 - Expiry Date
 - CVV needs to be entered whenever any payment is made. CVV to be entered on Artha Pay screen.
- **First time user:** Capture customer's email id from merchant's request with option to edit it, the card token and fingerprint shall be linked to that email id. Arthapay shall generate a token using **SHA 256-bit encryption** based upon browser, timestamp, & merchant and shall pass the token with card data to Jumbo Jet #4
- **Returning user:** If it is same browser and same merchant, **saved card list**, with limited digits of card's i.e., last 4 digits. **** * 9866 will appear on check out screen. While processing the transaction, Artha Pay will post the Token to Jumbo Jet to process the transaction. Option to add new card details shall also be available for user.
- User can delete already saved cards from the Artha Pay checkout page.
- New token shall be generated for every merchant and browser. That means, if user using the same browser for another merchant, the saved card shall appear but cannot proceed with the transaction. User shall give the consent to save the card data for this new merchant. Artha Pay will generate the new token for that merchant and send the update to the Jumbo Jet.
- Browser & merchant-based card tokenization
- For security reasons, the page will expire automatically in given time
- Capture order, customer, and merchant details #5
- Capture all attempts & response with all the variables along with the tokenisation of information for the unique identification.
- Fingerprint ID profile data with
 - Tokens along with successful & not successful flag
 - Last Time stamp for each token
 - Count of success transactions for each token
 - Payment Methods used with last Time stamp.
 - Count of successful transactions by each payment method.



- Browser name, Device, OS
- Option to see all other alternate payment method of JumboJet, that it will be made available using a single integration with iframe.
- Capture from User browser on every transaction
 - System will create GUID/ Fingerprint ID cookie on the browser
 - All Weblog variables (session/ Device/ IP/ Browser name/ OS/ City/ Country/ etc.)
 - Link the session/ Fingerprint with the card token in the DB

Merchant On-boarding

- Merchant enters email ID and Mobile Number to register. Registration ID will be created.
- Merchants gets an email with URL, link to reset passwords and add Google2FA Authenticator.
- The URL will allow Merchant to login and provide information based on MCC/Business Category.
- Merchant updates Company profile with type, business category, KYC docs, Business expected volumes, and option to choose PSPs to apply for.
- Auto save the application form and option to resume from where it is left.
- MCC dependent fields are predefined in the system and shall appear dynamically when merchant selects their MCC #Z
- Admin sees the application and curates the document. Once the curation is done the status of submission is complete and the documents will be submitted to PSPs. The documents shall be passed to compliance approval console and workflow approvals shall take place.
- Once the eKYC is approved, the email shall be sent to selected PSPs for their approvals, once approved, Admin will manually update the PSP's status from admin console.

Fraud Detection Dashboard

- Analytic Dashboard
- Real-time risk intelligence
- Setting up of High-Risk Countries
 - Transactions from High-Risk Countries will be flagged.
- Automatic Detection of Suspicious IP's
 - Flag and highlight large transaction IP's
 - Flag the IPs where the transaction amount is larger than defined maximum transaction limit. Admin can setup the maximum transaction amount with organization setup.
- Device Identifier
 - Identify the device type (Mobile or PCs), browser, operating system of the device from the transaction is originated.
- Risk Calculation Rating out of 5
 - Flag transactions based on the rules such as
 - IP range, option for admin to make list of anonymous IP Ranges and system matches it with each transaction and flags it.
 - Use of anonymous emails, option for admin to make list of anonymous email ids and system matches it with each transaction and flags it.
 - Billing address

Integrations

- 3rd Party API Integrations to be done by ULIS:
 - Integrations with a Payment Aggregator for Card Data, Token, and Merchant details processing. (T&M basis)
 - Email Server (single integrations, as provided by the MPTSL)



- Google MAPs APIs for address mapping from coordinates (single integrations, as provided by the MPTSL).
- Google2FA Authenticator (single integrations, as provided by the MPTSL)

Reporting & MIS

- Customer's log report
- System user logs report
- Transaction Report and MIS #5
 - Ability to manage all the transaction record and display in the screen
 - Option given to view the transaction by
 - Merchant
 - Status
 - Date
 - Transaction ID
 - Customer Name
 - Customer Mobile Number
 - Customer Email ID
 - Payment Method
 - Order No
 - Merchant ID
 - Card Number
 - Browser
 - Device
 - Select High Risk Country Transaction
 - Select High Risk Transaction Volume
 - Artha Mobile
- Attempt Transaction Report and MIS #5
 - Ability to manage all the attempt transaction record and display in the screen
 - Option given to view the transaction by
 - Merchant
 - Status
 - Date
 - Transaction ID
 - Customer Name
 - Customer Mobile Number
 - Customer Email ID
 - Payment Method
 - Order No
 - Merchant ID
 - Card Number
 - Browser
 - Device
 - Select High Risk Country Transaction
 - Select High Risk Transaction Volume
 - Artha Mobile



End to End Tokenized Communication

- End to End Encryption #8:
 - The application has a SHA-256 based encryption key for secure connections between the server and end user/browser and enable secure and authenticated data transmission.
 - Uniquely coded short session protects from session replication
 - SSL secure communication channels with additional pre-encryption #6
 - Each payment tools credentials are tokenized and encrypted

CR 1.0.0

Transaction Status Updates

- Integration with the PSP aggregator, as Merchants are integrated with MPTSL, MPTSL shall have APIs to integrate with the PSP aggregator. S2S integration (Server to server).
- All payment request & response APIs include below (*subjective to the JumboJet APIs*)
 - Sale
 - Void
 - Refund
 - Refund Reversal
 - PreAuth
 - PreAuth Reversal
 - PostAuth
 - PostAuth Reversal
 - Verify
 - Original Credit
 - Chargeback
 - Chargeback Reversal
 - RFI
 - Fraud Report
 - Disputed
 - Representment
 - MPI
 - Settlement
 - Payment Request
 - Refund Request
 - Refund Void
 - API to load all possible Payment options to load on our checkout page.

Merchant Console

- After registration is completed, Merchant will be notified through the mail and Merchant application ID will be created.
- Merchant will be able to login in the account and view the details of the application submission
 - Application submitted to which PSPs
 - Status of the application (Approved/Pending/Declined)
- Merchant can access to the Test environment as registered and can start integrating.
 - Option to integrate with shopping carts Shopify, Magento, OpenCart
 - Merchant would be able to do a few test transactions to test the integration.
- Checkout Page White Labeling and Color Schemes
 - Option to customize the checkout page color, font, logo, button color from the supported list. By default, the system default design shall be applied.



- Option to choose supported card networks and security icons, limited to 5 each. By default, system generated icon shall be displayed.
- Ability to set default language for checkout page. By default, English language shall be set.
- Checkout page default "Powered by MPTSL" & Logo updation will reflect on bottom of the page
- Once the merchant account is enabled by admin the merchant could access to the live environment.
- Merchant and sub-Merchant Mechanism
 - With registration of a merchant create a sub-merchant account by default in the name of website or business name.
 - The parent merchant won't have any MID but the sub-merchant.
 - The parent merchant can add multiple sub-merchants (businesses), the different MID shall be assigned and the KYC process will be the same i.e., upload required documents, select MCC, select PSPs and post PSP approvals the sub-merchant (business) account gets activated.
 - Parent merchant can see all their sub-merchant (business) account's transactions.
 - No transaction shall be performed direct to the parent merchant, only sub-merchant can have the transactions.
 - Merchant having more than one line of business will have a separate MID by each business line/category.
 - KYC is done on each sub account as the KYC submitted at the time of registration is for the first default sub-account.
 - There shall be an option to add another sub account and As the user proceeds with adding another account the KYC flow would be the same as before.
 - Role based access (RBAC) will allow the admin to create users at sub accounts and for specific modules.
- Referral code for each MID (sub-merchant) on their profile page.
- This referral code can be shared with others, and it can be used while registering.
- New merchant will have a field as optional to enter the Referral code while onboarding.
- Option to enter number of 'Directors in company' during onboarding, and document shall be collected for each director.
- Admin can monitor once referred merchant gets onboarded.
- API documentation for the merchant developers.
- Merchant API side captures on every transaction
 - Merchant
 - Txn ID
 - Amount
 - Date TS
 - Name
 - Email
 - Mobile
 - Address
 - Status
 - Response Code
 - Response Description
 - Payment method
- Transaction Report and MIS #5
 - Ability to manage all the transaction record and display in the screen
 - Option given to view the transaction by
 - Merchant
 - Status
 - Date
 - Transaction ID
 - Customer Name
 - Customer Mobile Number
 - Customer Email ID



- Payment Method
- Order No
- Merchant ID
- Card Number
- Browser
- Device
- Select High Risk Country Transaction
- Select High Risk Transaction Volume
- Artha Mobile

Integrations

- Google2FA Authenticator (single integrations, as provided by the MPTSL)

CR 1.0.1

Customer Mobile Application (Android / iOS)

- While doing transaction from web browser, If the customer's card fingerprint matches with mobile app, then option to 'Pay with Vault' shall appear, customer will enter the registered email id and a push notification shall be sent to associated mobile app for authentication. Once it is authenticating the transaction will move forward.
- Sign Up with email ID
- Sign in with email ID and password
- Home
- My Profile
- Change email ID
 - On changing email ID, all the associated card fingerprint shall be flagged with updated email ID
- The system should inform the customer if the old email address is entered while doing 'Pay with vault' at web browser, stating that the 'You have changed your email ID'.
- My Token List
- Saved Token List
 - Add and Delete option
- Support
- Instant Approval Mechanism
 - Saved Token Transaction notification appears
 - Approve or Deny option
- Transaction reports
 - Duration Filters
 - By Date
 - By Month
 - Clear option
- Vault
 - Securely store cardholder data in card vault
 - Manage cards, add, update, activate, and deactivate
 - PCI DSS & Central Bank compliant card data tokenization
 - Tokenized credit card vaults replace credit card data with placeholder tokens that retain much of the original data's utility
- Auth reversal
 - Request from web browser to mobile app for payment



- Mobile user shall get the push notification, click it take to the transaction details page, select card from the already stored card list or add new card and proceed with the transaction.
- Google 2 factor authentication
 - A security process in which users provide two different authentication factors to verify themselves
 - Email and Mobile One Time Password based verification

Merchant Advance eKYC

- Option is given to do the KYC registration from the
 - Self on-boarding
- Option is given to take every important information from the merchant
- When the registration is completed from the merchant, notification send to the admin department
- Feature given to store all the registration form in the merchant folder, in file manager.
- System can send the document to approval according to the workflow.
- Option to send mail if the document is rejected, notify them to registration again.
- After completing the KYC, system automatically activates the merchant account
- Workflow Process helps to manage and automate their standard processes and easily to boost business and personal productivity.
 - Create merchant approval workflows.
 - Workflow for reviewing, approval, validation
 - Support for serial and parallel workflows
 - Ability to access forms, track progress, review and approve
 - Feature given to collect information, ensure accuracy, trigger workflow
 - Ability to approve the workflow by entering the user password
 - Real-time dashboard to view all the workflow process
 - Instant approval for any document
 - Track and measure your reports with our advance audit trail
 - Ability to sync data to manage all your processes in one place, keeping things simple

Quality Assurance

- Oversight, Monitoring & Evaluation:
 - The application is evaluated by a team of experienced testers using automated and manual processes.
 - Test case reports will be prepared and shared with **Mr. Sridhar**
 - Immediate corrective actions will be undertaken to remedy any deficiency due to human and systems errors, if required and deemed necessary by **Mr. Sridhar**
 - **Global Certification consultation** and assistance in getting PCI DSS and ISO security certification
 - Delivery and implementation of ULIS'es highly secured **256 BIT encrypted proprietary SHA algorithm#8**

Assumptions and Considerations

- Payment's functionalities are subjective to acquirer, central bank compliance, card network compliance and local government regulations. Any modification in them shall cause deviation in respective TOR.
- Final requirement closure with signed SOW.
- Deliverable doesn't include mobile app, merchant panel/ consoles or any kind of dashboard or panel except for super admin panel.
- All integrations required with the payment gateway, payment acquirer, merchants, and or to any other third-party system shall be charged on T&M basis and final duration for that shall be quotes after receiving the related API documentation.
- All deliverables and CR's (if any) will be with UI designed and developed by ULIS team which is compliant to MPTSL Brand guidelines for font family and color coding.

- SPOC will be provided by MPTSL, and project management/team lead/team coordinator shall be provided by ULIS.
- Deployment activities on production/go live server are excluded from this proposal, such services shall be decided on the later stage if needed by the client. As free 7 days assistance shall be provided by ULIS team to the client's deployment team in any condition.
- Generic form with dependencies for Merchant onboarding shall be shared by client.
- 3 Shopping carts plugins Shopify, Magento, OpenCart are considered in TOR. If required more that shall be calculated on T&M basis.
- Checkout page background colour, font family and button colour shall be selected from the supported options list.

Documentation

- Project Management:
 - Project charter
 - KO Deck
 - Project Plan
 - RACI Matrix
- Technical documents:
 - Code execution structure
 - Installation guide
 - In-house environment deployment guide
 - System architecture diagram
- Testing documentation:
 - Test scenarios
 - UAT report
- Data architecture diagram:
 - ER diagram
 - System flow and activity diagram
- API documentation:
 - Payment gateway integration
 - Payment status check
 - Internal API for transaction list to share with integrated application like CRM, Financial module.
- User documentation:
 - User manuals for super admin console

References

#	Description
1	Subjective to accessibility of transaction amount and currency.
2	Subjective to compliances to save customer information and transaction details.
3	Limited to 1 To , up to 5 CC
4	APIs are required to transfer the data to Jumbo Jet platform
5	The Jumbo Jet payment checkout form and Artha Pay checkout form shall be deployed on same domain name only.
6	SSL are installed on server side where the system is deployed.
7	Generic form with dependencies for Merchant onboarding shall be shared by client.
8	Applicable on card data, token, system ids, and other sensitive data.
9	It is server dependent; the auto backup shall be scheduled on server side.



Authorized Signatory (ULIS) _____
ULIS Technology (P) Limited - Confidential



Authorized Signatory (Mena PayTech Systems Limited) Abhishek Shukla