



**MINISTRY OF DIGITAL ECONOMY AND ENTREPRENEURSHIP  
REQUEST FOR PROPOSAL (RFP)**

**Mobile Application for Ministry of Justice**

**PROPOSAL DEADLINE: 10/9/2025.**

**RFP NO: 42/eGovt/2025.**

**Contents**

Section 1: INTRODUCTION .....	6
1.1 RFP Purpose .....	6
Section 2. PROJECT DEFINITION AND OVERALL SOLUTION DESCRIPTION .....	8
2.1 Project Definition.....	8
Section 3. SCOPE OF THE PROJECT.....	10
3.1 Component 1 – Mobile Application Delivery .....	11
3.1.1 Design and Development .....	11
3.1.2 Service Integration .....	12
3.1.3 Testing and Quality Assurance .....	13
3.1.4 Deployment and Release Support .....	14
3.1.5 Training and Knowledge Transfer .....	15
3.1.6 General Project Deliverables Summary .....	15
3.2 Component 2 – Required Infrastructure .....	16
3.3 Component 3 – Information Security .....	17
3.4 Component 4 – Support and Maintenance.....	19
Section 4. ADMINISTRATIVE PROCEDURES & REQUIREMENTS .....	23
4.1 Response Procedures .....	23
4.2 Response Format .....	23
4.3 Response Submission .....	25
4.4 Response Evaluation .....	26
4.5 Financial Terms .....	28
4.6 Legal Terms .....	29
4.7 Conflict of Interest .....	37
4.8 Secrecy & Security .....	38
4.9 Document Property.....	38
4.10 Removal and/or Replacement of Personnel.....	38
4.11 Other Project-Related Terms .....	38
Section 5. ANNEXES .....	39
5.1 List of Acronyms .....	39
5.2 E-Government Implementation Framework .....	39
5.3 National e-Government Contact Centre Required Information .....	67
5.4 Technical Proposal Response Format .....	70
5.5 Financial Proposal Response Format.....	75
5.6 Joint Venture Agreement Template .....	81
5.7 Confidentiality Undertaken .....	83

5.8	Key RFPs Dates & Deadlines .....	86
5.9	Support Procedures & Policies .....	86
5.9.1	<i>Escalation Procedures &amp; Penalties</i> .....	87
5.10	Sample Arabic Contract Agreement (Attached).....	89
5.11	customer journey Experience standard and quality standard.....	90
5.12	SAML configuration .....	96
5.13	Questions and Answers Template .....	96
5.14	E-Service Performance KPI's .....	97
5.15	SDLC Security Minimum Requirements .....	99
5.16	سياسة استخدام موارد تكنولوجيا المعلومات (attached) .....	102
5.17	Performance Test Checklist (Attached) .....	102

## DISCLAIMER

THIS DOCUMENT IS A REQUEST FOR PROPOSAL (RFP), AND SHALL NOT BE CONSTRUED IN WHOLE OR PART AS A DIRECT OR INDIRECT ORDER. IT SHALL NOT BE CONSTRUED AS A REQUEST OR AUTHORIZATION TO PERFORM WORK AT THE EXPENSE OF MOJ. THE INFORMATION IN THIS RFP IS INTENDED TO ENABLE BIDDERS TO FORMULATE A PROPOSAL IN RESPONSE TO THE PROJECT REQUIREMENTS SET FORTH. ALTHOUGH THIS RFP CONTAINS SUCH ENABLING INFORMATION, BIDDERS MUST MAKE THEIR OWN INDEPENDENT ASSESSMENTS AND INVESTIGATIONS REGARDING THE SUBJECT MATTER OF THIS RFP. MOJ DOES NOT GUARANTEE THE ACCURACY, RELIABILITY, CORRECTNESS OR COMPLETENESS OF THE INFORMATION IN THIS RFP. THE BIDDER REMAINS RESPONSIBLE IN RELATION TO IDENTIFYING ANY FURTHER INFORMATION THAT IS REQUIRED TO PREPARE THE PROPOSAL. THIS RFP SHALL CONSTITUTE PART OF THE CONTRACT THAT WILL BE SIGNED BETWEEN MOJ AND THE WINNING BIDDER.

## ***RFP Organization***

This RFP provides the information to enable bidders to submit written proposals for the sought solution. The organization of the RFP is as follows:

### ***Section 1: Introduction***

This section outlines the RFP's purpose and its organization.

### ***Section 2: Project Definition and Overall Solution Description***

This section provides general definition of the project scope and a high-level description of the solution to be implemented.

### ***Section 3: Scope of the Project***

This section defines scope of work, proposal requirements and deliverables for the Project.

### ***Section 4: Administrative Procedures and Requirements***

This section describes the administrative rules and procedures that guide the proposal and its processes.

### ***Section 5: Annexes***

This section includes all annexes to the RFP.

## Section 1: INTRODUCTION

### 1.1 RFP Purpose

The purpose of this Request for Proposal (RFP) is to elicit responses from qualified local IT bidders (either alone or having joint venture with local/international IT firms) for the design, development, and implementation of a **mobile application solution** for the Ministry of Justice (MOJ), – hereafter referred to as the Project.

This project aligns with the MOJ's strategic efforts to enhance the delivery of judicial and legal services by leveraging modern digital technologies and expanding service accessibility through smart devices.

From the perspective of the Ministry of Justice, the main objectives of the project are to:

- Enhance user experience by providing a convenient, secure, and user-friendly mobile platform to access a wide range of judicial e-services.
- Improve service efficiency by reducing the need for in-person visits and enabling end-to-end digital processing of transactions.
- Increase transparency and accuracy through real-time status tracking, automated notifications, and integration with MOJ's internal systems.
- Empower citizens, lawyers, and relevant stakeholders to interact with the Ministry's services remotely with ease and reliability.
- Ensure seamless integration with the Ministry's existing digital infrastructure and allow for future scalability to accommodate additional services.

This project is focused on transforming how users access and interact with the Ministry of Justice's digital services through a modern and user-centric mobile application.

We aim to develop a smart, secure, and intuitive solution that enhances public access to judicial and legal services by leveraging the latest in mobile technology. Our objective is to simplify and streamline the user experience—enabling individuals to submit requests, track progress, receive notifications, and complete transactions digitally, with minimal effort and maximum transparency.

We envision a comprehensive platform that serves a wide range of users, including citizens, legal professionals, and institutional stakeholders. The mobile app will feature a sleek and accessible interface designed to meet diverse user needs while maintaining high standards of usability and accessibility.

The Ministry of Digital Economy and Entrepreneurship Technology (MoDEE) is actively seeking a highly qualified bidder who possesses the necessary expertise to deliver functional requirements and present a meticulously planned and all-encompassing implementation framework.

The winning bidder must demonstrate exceptional project management and leadership skills to ensure the successful completion of the project within the stipulated timeframe. It is imperative that the chosen bidder strictly adheres to agreed-upon tasks and achieves the desired goals and objectives, thereby ensuring optimal efficiency and effectiveness in project management.

Additionally, the winning bidder will bear the responsibility of financing the lump sum cost of the project, as outlined in section 5.5.

## Section 2. PROJECT DEFINITION AND OVERALL SOLUTION DESCRIPTION

### 2.1 Project Definition

The Ministry of Justice Mobile Application Redevelopment Project is a full-scale initiative to rebuild the mobile application from the ground up, with no reliance on the current version. The objective is to develop a completely new mobile application that shall serve as a unified and comprehensive platform for delivering the Ministry's digital services.

The new application shall integrate a total of **57 electronic services**, covering a wide range of judicial, legal, and administrative functions provided by the Ministry of Justice. It shall be built using modern technologies and best practices to ensure high performance, scalability, accessibility, and security across all major mobile platforms.

The application shall feature an intuitive and user-friendly interface designed to meet the needs of various user segments, including individuals, legal professionals, and institutions. Key functionalities shall include service request submission, real-time case and request tracking, electronic payments, document uploads, appointment scheduling, and in-app notifications.

The application shall interoperate with the Ministry's existing electronic services systems, particularly the backend systems, through standardized APIs provided by the Ministry of Justice, ensuring seamless data exchange and service continuity.

The application will be developed based on existed APIs and the winning bidder shall build the needed UI/UX.

The application's login mechanism shall Integrate with the Ministry of Justice's electronic portal login, using the same username and password, and allow Single Sign-On (SSO) through the "Sanad" account.

This initiative reflects the Ministry's commitment to digital transformation by replacing the legacy mobile application with a next-generation solution that shall provide a reliable, secure, and efficient experience for all users.

الخدمات الخاصة بالقضاة على التطبيق	
1	خدمة الاخبارات الواردة من مديرية الامن بكافة انواعها ( حماية الاسرة , المراكز الامنية ... ) ومعالجتها
2	خدمات الاستعلام عن الدعاوى و الطلبات و التبليغ والجلسات الخاصة بالقاضي / المدعي العام
3	خدمة التوقيع الرقمي ومعالجة الطلبات الاجرائية و طلبات اخلاء السبيل و الاستبدالات و الاستدعاءات و طلبات العقوبات السالبة للحرية و التبليغ و المحاضر و القرارات و قرارات و الطلبات المتفرقة التي ترد على حسابات القضاة .
4	خدمة ارسال المهام على الدعاوى مع ربطها على شكل اشعار على تطبيق الموظف
5	التوسع في الربط مع انظمة المجلس القضائي لغايات تفعيل خدمات الخاصة بالقضاة مثل الاجازات و التقييم السنوي والاعتراض على التقييم واستعراض السيرة الذاتية
6	خدمة استعراض الدورات الخاصة بالقاضي
7	خدمة استعراض التقارير كمدور القاضي و امد القضايا الخاصة بالقاضي
8	تفعيل الخدمات بما يشمل المدعين العامين ورؤساء المحاكم
الخدمات الخاصة بالمحامين	
1.	خدمات الاستعلام وتشمل :
9	استعلام الدعاوى و الطلبات و التبليغ والجلسات



10	استعلام عن المبالغ المحولة الى البنوك في القضايا التنفيذية
11	استعلام عن مستندات الصرف في الدعاوى
12	استعلام عن التبليغ الصادرة والالكترونية
13	استعلام عن معاملات الكاتب العدل
14	خدمة الإستعلام عن الرسائل النصية ورابط التبليغ
15	خدمة الاستعلام عن قضايا الوكيل
16	خدمة تقرير المفصل بأرقام القضايا التنفيذية للمحامي
2.	خدمات الكاتب العدل
17	تسجيل طلب كاتب العدل واجراء عملية التوقيع بشكل الالكتروني على الوثيقة مع الرابط الخاص بجلسة كاتب العدل ( من خلال استخدام API الخاص بالبوابة الالكترونية ) . مع ادخال بعض تقنيات الذكاء الاصطناعي التي تساعد في تسهيل عملية التسجيل .
3.	خدمات الدفع الالكتروني :
18	خدمة الدفع الإلكتروني لامانات الدعاوى التنفيذية والجزائية وصدار كف الطلب , وملفات الايجار
19	خدمات دفع الرسوم المتوفرة على البوابة الالكترونية ( من خلال استخدام API الخاص بالبوابة الالكترونية )
4.	خدمات الدعاوى
20	خدمة يداع الاوراق القضائية ( من خلال استخدام API الخاص بالبوابة الالكترونية ) مع توقيع الرقمي على اللوائح واي اوراق قضائية تحتاج الى توقيع.
21	خدمة تقديم الاستدعاءات ( من خلال استخدام API الخاص بالبوابة الالكترونية )
22	خدمة طلبات الاجرائية مع توقيع الرقمي على اللوائح واي اوراق قضائية تحتاج الى توقيع
23	خدمة التوقيع الرقمي على الوثائق والمستندات المقدمة من قبل المحامي
24	خدمة اضافة وكيل على الدعاوى ( من خلال استخدام API الخاص بالبوابة الالكترونية )
5.	خدمات المحاكم:
25	خدمة تنبئ قرار المحامي لطلب المساعدة القانونية
الخدمات الخاصة بالافراد	
1-خدمات الاستعلام وتشمل:	
26	استعلام الدعاوى و الطلبات و التبليغ والجلسات
27	استعلام المخالفات الجزائية
28	استعلام عن المبالغ المحولة الى البنوك في القضايا التنفيذية
29	استعلام معاملات الكاتب العدل
30	تتبع مستندات الصرف في الدعاوى
31	الاستعلام عن التبليغ الصادرة والالكترونية
32	خدمة الإستعلام عن الرسائل النصية ورابط التبليغ
33	خدمة تقرير المفصل بأرقام القضايا التنفيذية
34	الاستعلام عن الخبراء
خدمات الكاتب العدل	
35	تسجيل طلب كاتب العدل واجراء عملية التوقيع بشكل الالكتروني على الوثيقة مع الرابط الخاص بجلسة كاتب العدل ( من خلال استخدام API الخاص بالبوابة الالكترونية ) . مع ادخال بعض تقنيات الذكاء الاصطناعي التي تساعد في تسهيل عملية التسجيل .
خدمات الدفع الالكتروني	
36	خدمة الدفع الإلكتروني لامانات الدعاوى التنفيذية والجزائية وصدار كف الطلب , وملفات الايجار واتعاب الخبرة .
37	خدمات دفع الرسوم المتوفرة على البوابة الالكترونية ( من خلال استخدام API الخاص بالبوابة الالكترونية )
3-خدمات المحاكم :	

38	خدمة طلبات العقوبات المجتمعية
39	خدمة تقديم طلب المساعدة القانونية
40	خدمة الاعتراض على طلب المساعدة
41	تقديم شكوى على طلب المساعدة القانونية
42	خدمة انتقال كاتب العدل ( الإنتداب )
43	خدمة تقديم شكوى على خبير
	خدمات الموظفين
44	خدمة اصدار كشف الراتب
45	خدمة اصدار على كشف حوافز
46	خدمة اصدار لمن يهمل الامر
47	خدمة اصدار سيرة الذاتية
48	خدمة اصدار استمرارية راتب
49	خدمة تقديم طلب اجازة بدون راتب
50	خدمة تقديم المقترحات
51	خدمة التعميم
52	الاستعلام عن الاجازات والمغادرات
53	خدمة تقديم الطلبات للموارد البشرية
54	بيانات الموظف على نظام الدوام
55	خدمة الاستعلام عن شريحة الراتب
56	خدمة تقديم طلبات مالية لمديرية الشؤون المالية
57	تعديل البيانات الشخصية

### Section 3.SCOPE OF THE PROJECT

#### ➤ Important notes:

- There are certain activities to be performed and deliverables to be provided by the winning bidder during the execution of the Project. More detailed information on each of them is given in the next paragraphs. The bidder shall provide Mobile Application, and deliverables. In addition, to support, maintenance, and warranty, including any requirements or activities needed for the proper functioning of the system besides those outlined in the following listing, and the cost of these requirements or activities should be included in the fixed lump sum price submitted by the bidder.

Note that bidders should detail in their proposals all recommended mechanisms and methodologies through which their services and deliverables will be accomplished. All the final documentation deliverables of the project are required to be prepared in Arabic. Nevertheless, very technical documents such as DB design, architecture design, etc. can be accepted in the English language.

- Regarding questions and answers (Q&As), the bidder is required to use the template for the questions and answers annex (5.13) and to send it by email as a Word file.

- Final deliverables submitted by the winning bidder should be attached to original official letters properly bounded, stamped, and signed by the winning bidder as shall be defined and approved by Modee in cooperation with MOJ.
- The winning bidder should ensure that the Mobile Application architecture, design, and implementation include the use of GSB in system integration and information exchange.
- The winning bidder shall develop the required solution using any programming technology and provide all the required licenses.
- The required solution will be deployed centrally at e-Government private Cloud GPC.
- The duration time for implementing this project is (180 calendar days)
- The winning bidder is required to perform the operations and support activities for 24 months after obtaining the preliminary acceptance for the application under the scope of this RFP.

➤ **Important Definitions:**

- Preliminary Acceptance: the official acceptance by MODEE after the winning bidder finishes and delivers all work defined in the scope of work and before the start of maintenance.
- Final Acceptance: the official acceptance by MODEE after the winning bidder finishes and delivers all work in the contract and after the maintenance period.

### 3.1 Component 1 – Mobile Application Delivery

#### Required Activities and Deliverables

In order to complete the project successfully and in alignment with the Ministry of Justice's digital transformation strategy, the awarded bidder **shall perform** all activities listed below. It is the bidder's responsibility to include **any additional activities necessary** to achieve full functionality, integration, and deployment of the solution, even if not explicitly stated in this document. All such activities and related costs **must be covered** within the bidder's **fixed lump sum price**.

#### 3.1.1 Design and Development

The bidder shall design and develop a completely new mobile application (Android and iOS) from scratch using modern technologies and best practices. This phase shall include the following:

#### 3.1.1.1 UI/UX Design

- Create a responsive, user-friendly, and accessible interface, supporting Arabic (RTL) and English.
- Design wireframes, interactive prototypes, and UI components that reflect the 59 e-services to be offered.
- Ensure the design supports accessibility standards (WCAG) and is optimized for various devices and screen sizes.
- Conduct design review sessions with Ministry stakeholders to validate concepts and collect feedback.

#### Deliverables:

- Wireframes and mockups for all screens
- UI/UX design prototypes
- Arabic and English language interface versions
- Approved visual design assets (icons, fonts, colors, etc.)
- Design review reports and feedback logs

#### 3.1.1.2 Application Development

- Implement the features and service flows defined during the design phase.
- Use scalable, secure, and maintainable coding practices.
- Ensure compatibility with the latest versions of **Android** and **iOS**.
- Implement **push notifications**, secure session management, and **offline handling** where applicable.

#### Deliverables:

- Fully functional Android and iOS apps (compiled and testable)
- Source code (clean, commented, and structured)
- API integration code modules
- Build and deployment scripts
- Developer documentation

#### 3.1.2 Service Integration

The mobile application shall integrate a total of **57 electronic services** provided by the Ministry. Integration shall be based on APIs provided by the Ministry of Justice.

##### 3.1.2.1 Activities:

- Establish secure, reliable, and real-time connections to backend systems.

- Use **RESTful APIs or other integration protocols** as provided by MoJ.
- Implement proper **authentication, authorization, and data validation** mechanisms.
- Ensure proper error handling and fallbacks for unavailable services.

**Deliverables:**

- Integrated service flows for all 57 e-services
- Verified API connections and test results
- Documentation for integration logic and configurations
- Security test reports for API calls

### 3.1.3 Testing and Quality Assurance

The bidder shall implement a full testing lifecycle to ensure functionality, performance, and security of the application.

#### 3.1.3.1 *Activities:*

- Conduct **unit, integration, and system testing** across all modules.
- Perform **usability testing** to validate user experience and accessibility.
- Conduct **security and performance testing**, including addressing vulnerabilities identified by MoJ or MoDEE.
- Iterate based on feedback and perform bug fixes.
- Comply with customer journey Experience and quality standards that mentioned in Annex 5.11.
- Prepare the app on testing/staging environment to be identical to production environment in the following points:
  - Testing environment is fully Integrated to all web services and web forms
  - Testing environment is fully integrated to staging e-payment gateways and shared government services
- Perform all needed activities in the User Acceptance Testing that should be done in cooperation with MODEE and MoJ , all bugs and defects should be solved in order to get the approval of publishing the app.

**Deliverables:**

- Detailed test plan and test cases aligned with test data
- Unit test and integration test results
- Usability testing reports
- Performance and security test reports
- Final UAT sign-off
- Customer journey experience and quality standards compliance sheet

**NOTE: MODEE reserves the right to perform their own functional and non-functional test including security, performance, load, stress, quality and customer journey test on the**

**solution (2 rounds test) and provide the reports to the winning bidder to apply bug fixing and recommendations to ensure system functionalities.**

**In case an additional round of testing is needed after the official 2 rounds, the cost will be covered by the winning bidder, Following are the estimated cost in JD for each testing type for each service.**

#	Item Description	Additional round (JD)
1.	Quality Test (per service)	620
2.	Customer Journey Test	440
3.	Performance test	100
4.	Load test	100
5. s	Stress test	100
6.	Security	150

### 3.1.4 Deployment and Release Support

The bidder shall support the Ministry in deploying the application and ensuring a successful launch on diffreent stores.

#### 3.1.4.1 *Activities:*

- Prepare all deliverables for production release.
- Coordinate with the Ministry's team to **upload the applications to Google Play and Apple App Store** under MoJ accounts.
- Resolve any issues that arise during the review and approval process.
- Ensure store listing compliance (icons, descriptions, metadata).

#### **Deliverables:**

- Production-ready application packages (APK/IPA)
- Store listing content (in Arabic and English)
- Deployment documentation and release notes

- Support logs during deployment

### 3.1.5 Training and Knowledge Transfer

The bidder shall deliver training and transfer full technical knowledge to Ministry staff.

#### 3.1.5.1 *Activities:*

- Conduct training sessions for administrators, technical team, and support staff.
- Provide documentation for future maintenance and support.
- Transfer full ownership of source code and related artifacts.

#### **Deliverables:**

- Training materials and session agendas
- Source code and configuration files
- System architecture and integration diagrams
- User and admin manuals
- Knowledge transfer completion report

---

### 3.1.6 General Project Deliverables Summary

Deliverable	Description
UI/UX Design Package	Wireframes, mockups, and visual assets
Mobile Applications	Fully functional Android and iOS apps
Source Code	Full commented code and repositories
API Integrations	57 services integrated via MoJ APIs
Testing Artifacts	Plans, reports, and test results
Deployment Package	Ready-to-publish apps and documentation
Training & Docs	Training sessions, manuals, and transfer reports
Maintenance Logs	Logs and reports during support phase
Project plan	
Weekly progress meeting report	

### 3.2 Component 2 – Required Infrastructure

#### **Required Activities**

The winning bidder is required to perform the activities mentioned below regarding solution Infrastructure:

1. Must provide the solution hosted on MOJ datacenter and fully integrated with Hyper-V.
2. Must provide the solution design architecture that includes the required virtual machines (VMs), databases (DBs), or any other related services .
3. Must describe each component's functionality and role in the architecture, knowing that MOJ provides 3-tiers architecture for management and security purposes (Web, App, Data).
4. Must provide the required sizing (computing specifications) that will be utilized for VMs and DBs.

\* MOJ provides the bidders with different services as in the below table.

MOJ Services		
1	Virtual Machines	
	Option 1	Windows Server 2022\2019 Enterprise Edition (Licensed)
	Option 2	Any other OS is the bidder responsibility to provide, install, configure, and license it. Any required licenses must be included in the financial proposal as optional item.
2	Databases	
	Option 1	Oracle Database
3	Other services	
	1.	Load Balancer (LB), the bidder must propose the needed throughput
	2.	web application Firewall (WAF)
	3.	Publishing & DNS
	4.	Micro segmentation
	5.	Object storage
	6.	Backup as a Service; the bidder must provide the required backup policy
	7.	Warm DR on infrastructure level; the bidder must provide business continuity plan for all proposed solution components
	8.	antivirus
	9.	SSL certificate
	10.	Government Email services
	11.	SMS Gateway integration

#### **Technical proposal requirements**

The bidder is required to provide the following information in the technical proposal in relation to the required infrastructure:

- State the commitment to perform all the activities mentioned in the winning bidder activity section above
- Proposed Logical Infrastructure Architecture showing all needed components, and integrations with the current existing solution.
- VMs & DBs functionality needed for the solution

**Note: If during implementation found that the infrastructure component described in the technical proposal submitted by the winning bidder does not fulfill the requirement of the scope of this project, then the winning bidder must provide all additional needed infrastructure components and the cost of all of these additional components will borne by the winning bidder**



### **Financial proposal requirements**

The bidder is required to provide list of all costs associated with the required infrastructure components, services, and licenses in the financial proposal.

### **Deliverables**

The winning bidder is required to provide the below deliverables:

1. Comprehensive logical infrastructure architecture
2. Computing resources required to host the solution (sizing)
3. Description and functionality for each infrastructure component
4. All required licenses

## **3.3 Component 3 – Information Security**

### **Required Activities**

- API Security : the winning bidder should follow the OWASP API Security Top 10 guide when implement and develop the APIs in addition to Modee API requirement
- Web application security: the winning bidder should make sure that any new Portlets developed are protected against web application threats. At latest OWASP Top 10 vulnerabilities(OWASP Top 10:2021)
- For secure development the bidder should follow the OWASP Application Security Verification Standard (ASVS) and Mobile Application Security Verification Standard (MASVS) and Web Security Testing Guide project and apply the applicable control from them
- Input validation must be done on the client side and server side
- Two factor authentication/OTP must be implement on the user login and the password policy must have the minimum standard requirement
- Ensure registration, credential recovery, and API pathways are hardened against account enumeration attacks by using the same messages for all outcomes
- Establish and use a secure development lifecycle and Establish and use a library of secure design patterns or paved road ready to use components
- Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session identifier should not be in the URL, be securely stored, and invalidated after logout, idle, and absolute timeouts
- Design and build secure connections and communication channels using TLSv2 or above and only Strong Cipher is used
- Ensure all login, access control, transaction and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts and held for enough time

- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.
- Work with MODEE to add the service on the web application firewall(WAF)
- MODEE reserves the right to perform their own vulnerability assessment and/or penetration test on any task that has been done by the bidder and provide the vulnerability reports to the winning bidder to apply appropriate recommendations to ensure system security. Another security test should be conducted to ensure recommendations are reflected
- The winning bidder should follow the baseline security requirements in annex 5.15
- Agree on both “Information Security Policy/ [bit.ly/3tcxct1](https://bit.ly/3tcxct1)” and “سياسة استخدام موارد تكنولوجيا المعلومات” Annex (5.16).

### **Technical proposal requirements**

The bidder is required to provide the following information in the technical proposal in relation to the Information Security:

- State the commitment to perform all the activities mentioned in the winning bidder activity section above
- Risk Assessment plan or methodology.
- List of policies to be developed.
- Proposed security design of controls to be applied within the design in all layers: network security, host security, application security, data security, and access management, if any.
- Proposed approach(s) to ensure confidentiality, integrity, availability, authenticity, auditing, non-repudiation and accountability of data and services usage for the solution.
- Proposed Approach to insure the security of the database
- Proposed approach(s) to ensure security for the following requirements:
  - Separation of duties depending on Need-to-Know and Need-to-Do.
  - Input validation, data processing and output integrity and confidentiality.
  - Secure data at rest, in use and in transit, including encryption and hashing algorithms and encryption keys management.
  - Secure messaging according to the WS-Security Standard.
  - Secure transactions and messaging among all stakeholders and solution components.
  - Ensure secure identification, authentication and user profile management.
  - Ensure user privacy, including but not limited to, cookies management, users log file and behavior.

- Ensure secure exception and error management that is both user-friendly and not revealing sensitive and structure data.
- Proposed design for secure connections between clients and the System.
- Proposed design for secure connections between the System and back-end systems.
- Proposed solution for encrypting internet communication channels.
- Proposed secure user identification and authentication approach.
- Proposed design to protect Portlets against web application threats. The solution should ensure that it is not vulnerable to OWASP Top 10 latest vulnerabilities. I.e. design to secure session management; security control such as session time out and secure channel and access to session store should be used.

### **Financial proposal requirements**

The bidder is required to provide list of all costs associated with the information security of the System in the financial proposal.

### **Deliverables**

The winning bidder is required to provide the deliverables mentioned below:

- Risk assessment and mitigation report (is applicable)
- Security testing reports
- State the Compliance to the customer Journey/experience requirements mentioned in Annex (5.11)

### **3.4 Component 4 Project Management**

The winning bidder shall provide a simplified Project Management Plan to ensure timely delivery (within 180 calendar days) and required quality, covering at minimum:

- **Work plan and detailed timeline** outlining major phases and milestones.
- **Periodic progress reports** (weekly/monthly) summarizing progress, challenges, and mitigation actions.
- **Simplified Risk Management Plan** focusing on schedule and technical risks related to mobile interfaces and service integration.
- **Project closure plan** including final delivery procedures and knowledge transfer.

### **3.5 Component 5 – Support and Maintenance**

To execute “Operation Support and Maintenance” component of this project, the winning bidder is required to perform the activities mentioned below for 24 months after obtaining the preliminary acceptance for the system under the scope of work. Noting that any additional

related activities needed for the proper functioning of the system should be provided by the winning bidder and its cost should be included in the fixed lump sum price submitted by the winning bidder:

- Assign a contact person / account manager to be responsible during the support and maintenance period of this contract.
- Provide support and maintenance services on 24x7 for severities 1&2 and 7x5 for severities 3&4 basis for the implemented solution by a team which possesses the proper knowledge and proven experience of the proposed solution.
- Ensure the availability of qualified resources at the local partner's premises to provide on-site support when needed.
- Provide detailed implementation plan for any pre-planned maintenance operation that may affect entity services availability, functionality or stability, with necessity to provide roll-back plan before commencing with maintenance operation
- Issue a service report after each and every site visit registering the reported incident, its root cause and the followed procedures that resulted in the successful resolution including the taken and/or suggested recommendations and measures that shall prevent such incidents / issues from reoccurring in the future.
- Comply with the service level requirements defined and as shown in Annex (5.9) of this document.
- Provide a renewal of the software license (if any and requested) to cover the maintenance and support period.
- Provide communication channels to enable the entity to report incidents that should be tracked and monitored until final resolution by the winning bidder, and keeping entity informed about the status for these incidents until the final resolution.
- Use a ticketing system that records all reported incidents and service request and ensuring MoJ have access to both the system and report incident the generated incident-reports, and it shall be able to integrate with the ticketing system in Modee if requested.
- Applying the latest fixes, patches and required updates to the installed software during the support and maintenance period (if required) while ensuring system's integrity, reliability, conformity, and normal operation for all system features including the content

### **Technical proposal requirements**

The bidder is required to provide the following information in the technical proposal in relation to this component:

- State the commitment to perform all the activities mentioned in the winning bidder activity section above
- Provide bidder's methodology of providing the support and maintenance services required in this RFP

- Demonstrate the technical capability for the team who will be in charge for maintaining and supporting the proposed solution, by providing the team qualifications and number of people who will be dedicated for supporting and maintaining the installed solution.
- Provide the appropriate escalation matrix and procedures (with contact details for concerned parties) that guarantees performing corrective measures in case needed and in actions within a guaranteed manner.

### **Financial proposal requirements**

The bidder is required to provide the following information in the financial proposal in relation to the “Operations Management” component:

- List all costs associated with the support and maintenance and licenses ( if any)

### **Deliverables**

- Service reports for all reported and resolved incidents approved by a representative from the owner.
- Proof of licenses renewal ( if any available in the scope)



## Section 4.ADMINSTRATIVE PROCEDURES & REQUIREMENTS

### 4.1 Response Procedures

All inquiries with respect to this RFP are to be addressed to the Modee in writing by e-mail with the subject "DIGITAL TRANSFORMATION PROJECT FOR MINISTRY OF FOREIGN AFFAIRS and EXPATRIATES (MOJ )". Inquiries can only be addressed to [ ] by []. Responses will be sent in writing no later than [ ]. Questions and answers will be shared with all Bidders' primary contacts.

### 4.2 Response Format

Bidders responding to this RFP shall demonstrate up-to-date capabilities and experience in providing similar services and similar engagements of the same scope and size (Mobile Application). These services and engagements must be performed by the bidder during the last 7 years **(2 similar successfully accomplished projects is required).**

#### **Important Note:**

- 1) Bidders must detail the description about Scope, size and year for each project according to the below template

Project Name	
Start date	
End date	
Project size and number of services	
Detailed Project components	
Client contact number and email	

Bidders shall demonstrate the following specific capabilities:

- Experience in designing, developing and implementing mobile application and portal.
- IT experience in software and other IT related areas specified in this RFP.
- Experience in Information Security
- Experience in project planning and management.
- Experience in providing post implementation support and maintenance
- Experience in quality assurance and quality control
- Experience in change management Practice.

**Note:** Where some skills are not available, the bidder should joint venture or sub-contract with a reputable **local/international firm** to cover for this specific skill, services or equipment provided that all partners to a joint venture will be jointly and severally responsible towards Modee In case of subcontracting, the subcontractor has to be approved by Modee and the contractor will be liable for all works performed by the sub-contractor.

Bidders' written response to the RFP must include:

*Part I: Technical Proposal*

- A. Corporate capability statement : Corporate capability statement must include all the following:
- Corporate technical capabilities and experience in implementing similar solutions together with detailed description and reference to each component underlined in Section 3: Scope of the project.
  - Detailed proposed Team Resumes (with names) (each resume will be subjected to the approval of Modee, in case of replacements the winning bidder has to abide by Modee requirements for replacements and approvals. In the implementation phase Modee reserves the right to request replacement of any resource that cannot fulfill the job)
  - Description and references to similar projects performed in the last 7 years.
  - Reference to appropriate work samples
  - If a bidder is a joint venture, partners need to be specified with the rationale behind the partnership. Corporate capability statement should be provided for all partners
  - Current client list, highlighting potential conflict of interest
  - Submit work plan allocation resources with their percentage of involvement
  - Project Organizational Structure
- B. Technical proposal: The technical proposal should include the approach to achieving the scope of work defined in this RFP and delivering each of the major components as specified in the Deliverables section. In order for the evaluation to progress



quickly and effectively, bidders are requested to provide Part I of their proposal as per the format described in Annex 5.4.

## *Part II: Financial Proposal*

The financial proposal should include a cost summary and a detailed cost analysis section. The cost summary must provide a fixed lump sum price in Jordan Dinars for the overall scope of work and deliverables including all fees, taxes including sales tax. The supporting detailed cost analysis should provide a breakdown and details of the pricing should be provided. The day rates and expenses for any consultants should be included separately along with the time for which they will be required. The bidder will provide separately all professional fees and expenses (travel, project equipment, accommodation and subsistence, etc) for the duration of the project. The pricing should show the proposed linkage between deliverables and payments. Financial proposal should include the Form of Bid (عرض المناقصة) and **summary of remuneration** (خلاصة بدلات الأتعاب) attached in the Arabic Sample Agreement under ملحق (الاتفاقية رقم 2 و رقم 3) duly filled; signed and stamped by the bidder. The Financial proposal should be submitted in separation of the technical proposal. In order for the evaluation to progress quickly and effectively, bidders are requested to provide their proposal as per the format described in Annex 5.5.

- على الفريق الثانى ان يشمل سعره الضريبة العامة على المبيعات بنسبة (16 %) الا اذا كانت الشركة خاضعة للضريبة العامة على المبيعات بنسبة (0) % (بموجب كتاب رسمي من هيئة الاستثمار يرفق مع العرض المالى) يتم عكس هذه النسبة على السعر المقدم من قبلها.
- فى حال عدم توضيح الضريبة العامة على المبيعات على السعر المقدم من قبل الشركة يعتبر سعر الشركة شامل للضريبة العامة على المبيعات بنسبة 16 %.

## *Part III: Bid Security*

*This part includes the original Bid Guarantee.*

### **4.3 Response Submission**

Bidders must submit proposals to this RFP **on joneps** no later than 03:00 PM on [10/9/2025] (Jordan Local Time).

Ministry of Digital Economy and Entrepreneurship

Tender No: [42/eGovt2025]

Tendering Department – 3rd floor

Ministry of Digital Economy and Entrepreneurship

8th circle

P.O. Box 9903

Amman 11191 Jordan

Tel: 00 962 6 5805642

Fax: 00 962 6 5861059

Proposals should be submitted as 2 separate parts each part in **ON JONEPS** , respectively, as follows:

- **Part I “ MOJ mobile APPLICATION PROJECT - Technical and Corporate Capabilities Proposal”**. Inclusion of any cost or price information in the technical proposal will result in the bidder’s proposal being disqualified as irresponsible.( ON JONEPS)
- **Part II “ MOJ mobile APPLICATION PROJECT – Financial Proposal”**. (ON JONEPS)
- **Part III “ MOJ mobile APPLICATION PROJECT – Bid Bond”** This part (envelope) should contain 1 hard copy. This part should not contain any reference to cost or price. Inclusion of any cost or price information in the technical proposal will result in the bidder’s proposal being disqualified as irresponsible.( سيتم إيداع الكفالة الاصلية او الشيك المصدق بوحدة العطاءات والمشتريات / وزارة الاقتصاد الرقمي والريادة ط3)

**Note:**

Regardless of method of delivery, the proposals must be received by JONEPS no later than 03:00PM [10/9/2025] (Amman Local Time). Modee will not be responsible for premature opening of proposals not clearly labeled.

#### 4.4 Response Evaluation

All responses to the RFP will be evaluated technically and financially and the winning proposal will be selected on the basis of “best value” in terms of technical superiority as well as cost effectiveness. Technical and financial proposals shall be reviewed by the Purchase Committee at the Ministry and evaluated in accordance with the following procedure:

The overall proposal will be evaluated according to the following criteria:

1. Overall Technical Proposal 70%
2. Overall Financial Proposal 30%

1. The overall bidders mark will be calculated as follows:

$$(30 \times \text{least value of financial proposals}) / \text{bidder financial proposal value} + (\%70 \times \text{bidder technical mark})$$

Technical proposal shall be first evaluated according to the following criteria:

2. References in similar projects – Mobile Application (30.00%) (2 projects in the last 7 years).
3. Staff Qualifications and Experience (30.00%):

Minimum CVs required **(minimum Bachelor Degree for all CVs):**

1. One Solution Architect, minimum 5 years of relevant experience.
2. Two senior mobile Developers: minimum 5 years of relevant experience.
3. Two junior mobile Developers: minimum 2 years of relevant experience.
4. One Backend/Integration Developer minimum 5 years of relevant experience.
5. One System engineer , minimum 5 years of relevant experience (systems, network)
6. Information security specialist, minimum 5 years of relevant experience.
7. One Project manager (PMP certified or equivalent), minimum 5 years of relevant experience.
8. One CTFL Certified Senior Quality engineer / specialist with minimum 5 years of relevant experience.
9. Two Quality testers with minimum 2 years of relevant experience
10. One UI/UX Designer: minimum 5 years of relevant experience.

**Note: include a copy/ image for the requested professional certificate for each resource within the technical proposal**

4. Proposed Approach and Methodology in correspondence to the RFP requirements including to the following components (40%):
  1. Mobile Application Delivery
  2. Required Infrastructure
  3. Information Security
  4. Operation Support
  5. Quality Management

Only those bidders that qualify in the technical proposal (qualification mark 70% or above), will have their financial offers reviewed. The Financial proposal will be evaluated only for companies who qualify. The financial offer of those who do not qualify will not be opened and will be returned. MODEE reserves the right not to select any offer. MODEE also assumes no responsibility for costs of bidders in preparing their submissions.

#### 4.5 Financial Terms

Bidders should take into consideration the following general financial terms when preparing and submitting their proposals:

5. All prices should be quoted in Jordanian Dinars inclusive of all expenses, governmental fees and taxes, including sales tax
6. The type of contract will be a fixed lump sum price contract including costs of all software or/and hardware, licensees, documentation, maintenance, support, knowledge transfer, training, warranty, and professional fees, profits and over heads and all other expenses incurred
7. A clear breakdown (table format) of the price should be provided including price for consulting time, other expenses, etc.
8. The bidder shall bear all costs associated with the preparation and submission of its proposal and Modee will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the proposal process.
9. The bidders shall furnish detailed information listing all commissions and gratuities, if any, paid or to be paid to agents relating to this proposal and to contract execution if the bidder is awarded the contract. The information to be provided shall list the name and address of any agents, the amount and currency paid and the purpose of the commission or gratuity.
10. The Bidder shall submit a (Tender Bond) proposal security on a form similar to the attached format in Jordanian Dinars for a flat sum of (3000J.D) (in a separate sealed envelope. The bond will be in the form of certified cheque or bank guarantee from a reputable registered bank, located in Jordan, selected by the bidder
11. r. The bidder shall ensure that the (tender bond) proposal security shall remain valid for a period of 90 days after the bid closing date or 30 days beyond any extension subsequently requested by the Purchase Committee, and agreed to by the bidder.
12. Any proposal not accompanied by an acceptable proposal security (tender bond) shall be rejected by the Purchase Committee as being non-responsive pursuant to RFP.
13. The proposal security of a joint venture can be in the name of all members participating in the joint venture submitting the proposal or in the name of one or more members in the joint venture.
14. The proposal security of the unsuccessful bidders will be returned not later than 30 days after the expiration of the proposal validity period.
15. The winning bidder is required to submit a performance bond of 10% of the total value of the contract within 14 days as of the date of award notification letter.

16. The proposal security of the winning bidder will be returned when the bidder has signed the contract and has furnished the required performance security.
17. The proposal security may, in the sole discretion of the Purchase Committee, be forfeited:
  - If the bidder withdraws its proposal during the period of proposal validity as set out in the RFP; or
  - In the case of winning bidder, if the bidder fails within the specified time limit to sign the contract; or sign the joint venture agreement in front of a notary public in Amman, Jordan; or furnish the required performance security as set out in the contract.
18. The winning bidder has to pay the fees of the RFP advertisement issued in the newspapers.
19. Modee is not bound to accept the lowest bid and will reserve the right to reject any bids without the obligation to give any explanation.
20. Bidders must take into consideration that payments will be as specified in the tender documents and will be distributed upon the winning submission and acceptance of the scope of work and of the deliverables and milestones of the scope of work defined for the project by the first party.
21. Modee takes no responsibility for the costs of preparing any bids and will not reimburse any Bidder for the cost of preparing its bid whether winning or otherwise.

#### 4.6 Legal Terms

Bidders should take into consideration the following general legal terms when preparing and submitting their proposals:

- If the Bidder decides to form a joint venture, Each partner in the joint venture shall be a business organization duly organized, existing and registered and in good standing under the laws of its country of domicile. The Bidder must furnish evidence of its structure as a joint venture including, without limitation, information with respect to:
  - the legal relationship among the joint venture members that shall include joint and several liability to execute the contract; and
  - the role and responsibility of each joint venture member
- The Bidder must nominate a managing member (leader) for any joint venture which managing member will be authorized to act and receive instructions on behalf of all the joint venture members

- All bidders should duly sign the joint venture agreement attached to this RFP under Annex 5.6 by authorized representatives of the joint venture partners without being certified by a notary public and to be enclosed in the technical proposal in addition to authorization for signature on behalf of each member. Only the winning bidder partners in a joint venture should duly sign the joint venture agreement attached to this RFP under Annex 5.6 by authorized signatories and this agreement is to be certified by a Notary Public in Jordan
- 22. The bidders shall not submit alternative proposal. Alternative proposals will be returned unopened or unread. If the bidder submits more than one proposal and it is not obvious, on the sealed envelope(s), which is the alternative proposal, in lieu of returning the alternative proposal, the entire submission will be returned to the bidder and the bidder will be disqualified.
- 23. The proposal shall be signed by the bidder or a person or persons duly authorized to bind the bidder to the contract. The latter authorization shall be indicated by duly-legalized power of attorney. All of the pages of the proposal, except un-amended printed literature, shall be initialed by the person or persons signing the proposal.
- 24. Any interlineations, erasures or overwriting shall only be valid if they are initialed by the signatory (ies) to the proposal.
- 25. The bid shall contain an acknowledgement of receipt of all Addenda to the RFP, the numbers of which must be filled in on the Form of Bid attached to the Arabic Sample Agreement
- 26. Modee requires that all parties to the contracting process observe the highest standard of ethics during the procurement and execution process. The Special Tenders Committee will reject a proposal for award if it determines that the Bidder has engaged in corrupt or fraudulent practices in competing for the contract in question.

**Corrupt Practice** means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution>

**Fraudulent Practice** means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of Modee, and includes collusive practice among Bidders (prior to or after proposal submission) designed to establish proposal prices at artificial non-competitive levels and to deprive MOJ of the benefits of free and open competition.

- 27. No bidder shall contact Modee, its employees or the Special Tenders Committee or the technical committee members on any matter relating to its proposal to the time the contract is awarded. Any effort by a bidder to influence Modee, its employees, the Special Tenders Committee or the technical committee members in the Purchase Committee's proposal

evaluation, proposal comparison, or contract award decision will result in rejection of the bidder's proposal and forfeiture of the proposal security

28. The remuneration of the Winning Bidder stated in the Decision of Award of the bid shall constitute the Winning Bidder sole remuneration in connection with this Project and/or the Services, and the Winning Bidder shall not accept for their own benefit any trade commission, discount, or similar payment in connection with activities pursuant to this Contract or to the Services or in the discharge of their obligations under the Contract, and the Winning Bidder shall use their best efforts to ensure that the Personnel, any Sub-contractors, and agents of either of them similarly shall not receive any such additional remuneration.
29. A business registration certificate should be provided with the proposal
30. If the bidder is a joint venture, then the partners need to be identified with the rationale behind the partnership. Corporate capability statement should also be provided for all partners.
31. The laws and regulations of The Hashemite Kingdom of Jordan shall apply to awarded contracts.
32. The Bidder accepts to comply with all provisions, whether explicitly stated in this RFP or otherwise, stipulated in the government Procurement ByLaw 8 of 2022 and its Instructions, , and any other provisions stated in the Standard Contracting sample Arabic Contract Agreement Annexed to this RFP including general and special conditions, issued pursuant to said Unified Procurement ByLaw 8 of 2022 and its Instructions
33. Modee takes no responsibility for the costs of preparing any bids and will not reimburse any bidder for the cost of preparing its bid whether winning or otherwise.
34. Bidders must review the Sample Arabic Contract Agreement provided with this RFP and that will be the Contract to be signed with the winning bidder. Provisions in this Sample Arabic Contract Agreement are not subject to any changes; except as may be amended by MODEE before tender submission; such amendments are to be issued as an addenda.
35. Proposals shall remain valid for period of (90) days from the closing date for the receipt of proposals as established by the Special Tenders Committee.
36. The Special Tenders Committee may solicit the bidders' consent to an extension of the proposal validity period. The request and responses thereto shall be made in writing or by fax. If a bidder agrees to prolong the period of validity, the proposal security shall also be suitably extended. A bidder may

refuse the request without forfeiting its proposal security; however, in its discretion, the Special Tenders Committee may cease further review and consideration of such bidder's proposal. A bidder granting the request will not be required nor permitted to modify its proposal, except as provided in this RFP.

37. Modee reserves the right to accept, annul or cancel the bidding process and reject all proposals at any time without any liability to the bidders or any other party and/withdraw this tender without providing reasons for such action and with no legal or financial implications to Modee.
38. Modee reserves the right to disregard any bid which is not submitted in writing by the closing date of the tender. An electronic version of the technical proposal will only be accepted if a written version has also been submitted by the closing date.
39. Modee reserves the right to disregard any bid which does not contain the required number of proposal copies as specified in this RFP. In case of discrepancies between the original hardcopy, the other copies and/or the softcopy of the proposals, the original hardcopy will prevail and will be considered the official copy.
40. MOJ reserves the right to enforce penalties on the winning bidder in case of any delay in delivery defined in accordance with the terms set in the sample Arabic contract. The value of such penalties will be determined in the Sample Arabic contract for each day of unjustifiable delay.
41. Bidders may not object to the technical or financial evaluation criteria set forth for this tender.
42. The winning bidder will be expected to provide a single point of contact to which all issues can be escalated. MOJ will provide a similar point of contact.
43. MOJ is entitled to meet (in person or via telephone) each member of the consulting team prior to any work, taking place. Where project staff is not felt to be suitable, either before starting or during the execution of the contract, MOJ reserves the right to request an alternative staff at no extra cost to MOJ.
44. Each bidder will be responsible for providing his own equipment, office space, secretarial and other resources, insurance, medical provisions, visas and travel arrangements. MOJ will take no responsibility for any non-Government of Jordan resources either within Jordan or during travel to/from Jordan.



45. Any source code, licenses, documentation, hardware, and software procured or developed under '**MOJ mobile APPLICATION PROJECT**' is the property of MOJ upon conclusion of 'The Project'. Written consent of MOJ must be obtained before sharing any part of this information as reference or otherwise.
46. Bidders are responsible for the accuracy of information submitted in their proposals. Modee reserves the right to request original copies of any documents submitted for review and authentication prior to awarding the tender.
47. The bidder may modify or withdraw its proposal after submission, provided that written notice of the modification or withdrawal is received by the Purchase Committee prior to the deadline prescribed for proposal submission. Withdrawal of a proposal after the deadline prescribed for proposal submission or during proposal validity as set in the tender documents will result in the bidder's forfeiture of all of its proposal security (bid bond).
48. A bidder wishing to withdraw its proposal shall notify the Special Tenders Committee in writing prior to the deadline prescribed for proposal submission. A withdrawal notice may also be sent by fax, but it must be followed by a signed confirmation copy, postmarked no later than the deadline for submission of proposals.
49. The notice of withdrawal shall be addressed to the Special Tenders Committee at the address in RFP, and bear the contract name "**MOJ mobile APPLICATION PROJECT**" and the words "Withdrawal Notice".
50. Proposal withdrawal notices received after the proposal submission deadline will be ignored, and the submitted proposal will be deemed to be a validly submitted proposal.
51. No proposal may be withdrawn in the interval between the proposal submission deadline and the expiration of the proposal validity period. Withdrawal of a proposal during this interval may result in forfeiture of the bidder's proposal security.
52. The Bidder accepts to comply with all provisions, that are explicitly stated in this RFP and any other provisions stated in the Standard Sample Arabic Contract Agreement attached hereto and Tendering Instruction and attached hereto.
53. The winning bidder shall perform the Services and carry out their obligations with all due diligence, efficiency, and economy, in accordance with the

highest generally accepted professional techniques and practices, and shall observe sound management practices, and employ appropriate advanced technology and safe methods. The Winning Bidder shall always act, in respect of any matter relating to this Contract or to the Services, as faithful advisers to MOJ, and shall at all times support and safeguard MOJ's legitimate interests in any dealings with Sub-contractors or third parties.

54. If there is any inconsistency between the provisions set forth in the Sample Arabic Contract Agreement attached hereto or this RFP and the proposal of Bidder; the Sample Arabic Contract Agreement and /or the RFP shall prevail
55. MOJ reserves the right to furnish all materials presented by the winning bidder at any stage of the project, such as reports, analyses or any other materials, in whole or part, to any person. This shall include publishing such materials in the press, for the purposes of informing, promotion, advertisement and/or influencing any third party. MOJ shall have a perpetual, irrevocable, non-transferable, paid-up right and license to use and copy such materials mentioned above and prepare derivative works based on them.
56. Bidders (whether in joint venture or alone) are not allowed to submit more than one proposal for this RFP. If a partner in a joint venture participate in more than one proposal; such proposals shall not be considered and will be rejected for being none-responsive to this RFP.
57. **Amendments or reservations on any of the Tender Documents:** Bidders are not allowed to amend or make any reservations on any of the Tender Documents or the Arabic Sample contract agreement attached hereto. In case any bidder does not abide by this statement, his proposal will be rejected for being none-responsive to this RFP. If during the implementation of this project; it is found that the winning bidder has included in his proposal any amendments, reservations on any of the tender documents or the Contract; then such amendments or reservations shall not be considered and the items in the tender documents and the Contract shall prevail and shall be executed without additional cost to MOJ and the winning bidder shall not be entitled to claim for any additional expenses or take any other legal procedures.
58. Nothing contained herein shall be construed as establishing a relation of principal and agent as between MOJ and the Winning Bidder. The Winning Bidder has complete charge of Personnel and Sub-contractors, if any, performing the Services and shall be fully responsible for the Services performed by them or on their behalf hereunder.
59. The Winning Bidder, their Sub-contractors, and the Personnel of either of them shall not, either during the term or after the expiration of the Contract, disclose any proprietary or confidential information relating to the Project,

the Services, the Contract, or MOJ 's business or operations without the prior written consent of MOJ . The Winning Bidder shall sign a Non-Disclosure Agreement with MOJ as per the standard form adopted by MOJ . A confidentiality undertaking is included in annex 5.7.

60. Sample Arabic Contract Agreement Approval:

**Bidders must review the Sample Arabic Contract Agreement version provided with the RFP, which shall be binding and shall be signed with winning bidder.**

**Bidders must fill out, stamp and duly sign the Form of Bid (نموذج عرض المناقصة) attached to the Arabic Sample Agreement under (2) ملحق رقم (2) and enclose it in their financial proposals.**

**Bidders must fill out the summary payment schedule form sub annex 3 (الملحق رقم 3) which is part of the Arabic Sample Contract version provided with the RFP, sign and stamp it, and enclose it with the Financial Proposal.**

**Bidders must also fill out and duly sign the Financial Proposal Response Formats under Annex 5.5 of this RFP and enclose it in the financial proposals.**

**Proposals that do not include these signed forms are subject to rejection as being none responsive.**

- **PROHIBITION OF CONFLICTING ACTIVITIES**

Neither the Winning Bidder nor their Sub-contractors nor their personnel shall engage, either directly or indirectly, in any of the following activities:

- During the term of the Contract, any business or professional activities in Jordan or abroad which would conflict with the activities assigned to them under this bid; or
- After the termination of this Project, such other activities as may be specified in the Contract.

- **INTELLECTUAL PROPERTY RIGHTS PROVISIONS**

- Intellectual Property for the purpose of this provision shall mean all copyright and neighboring rights, all rights in relation to inventions (including patent rights), plant varieties, registered and unregistered trademarks (including service marks), registered designs, Confidential Information (including trade secrets and know how) and circuit layouts, and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.

- Contract Material for the purpose of this provision shall mean all material (includes documents, equipment, software, goods, information and data stored by any means):
    - a) Brought into existence for the purpose of performing the Services;
    - b) incorporated in, supplied or required to be supplied along with the Material referred to in paragraph (a); or
    - c) Copied or derived from Material referred to in paragraphs (a) or (b);
  - Intellectual Property in all Contract Material vests or will vest in MOJ . This shall not affect the ownership of Intellectual Property in any material owned by the Winning Bidder, or a Sub-contractor, existing at the effective date of the Contract. However, the Winning Bidder grants to MOJ , or shall procure from a Sub-contractor, on behalf of MOJ , a permanent, irrevocable, royalty-free, worldwide, non-exclusive license (including a right of sub-license) to use, reproduce, adapt and exploit such material as specified in the Contract and all relevant documents.
  - If requested by MOJ to do so, the Winning Bidder shall bring into existence, sign, execute or otherwise deal with any document that may be necessary or desirable to give effect to these provisions.
  - The Winning Bidder shall at all times indemnify and hold harmless MOJ , its officers, employees and agents from and against any loss (including legal costs and expenses on a solicitor/own client basis) or liability incurred from any claim, suit, demand, action or proceeding by any person in respect of any infringement of Intellectual Property by the Winning Bidder, its officers, employees, agents or Sub-contractors in connection with the performance of the Services or the use by MOJ of the Contract Material. This indemnity shall survive the expiration or termination of the Contract.
  - The Winning Bidder not to benefit from commissions discounts, etc. The remuneration of the Winning Bidder stated in the Decision of Award of the bid shall constitute the Winning Bidder sole remuneration in connection with this Project and/or the Services, and the Winning Bidder shall not accept for their own benefit any trade commission, discount, or similar payment in connection with activities pursuant to this Contract or to the Services or in the discharge of their obligations under the Contract, and the Winning Bidder shall use their best efforts to ensure that the Personnel, any Sub-contractors, and agents of either of them similarly shall not receive any such additional remuneration.
- THIRD PARTY INDEMNITY

Unless specified to the contrary in the Contract, the Winning Bidder will indemnify MOJ , including its officers, employees and agents against a loss or liability that has been reasonably incurred by MOJ as the result of a claim made by a third party:

- Where that loss or liability was caused or contributed to by an unlawful, negligent or willfully wrong act or omission by the Winning Bidder, its Personnel, or sub-contractors; or
- Where and to the extent that loss or liability relates to personal injury, death or property damage.

- LIABILITY

- The liability of either party for breach of the Contract or for any other statutory cause of action arising out of the operation of the Contract will be determined under the relevant law in Hashemite Kingdom of Jordan as at present in force. This liability will survive the termination or expiry of the Contract. Winning bidder's total liability relating to contract shall in no event exceed the fees Winning bidder receives hereunder, such limitation shall not apply in the following cases (in addition to the case of willful breach of the contract):
  - gross negligence or willful misconduct on the part of the Consultants or on the part of any person or firm acting on behalf of the Consultants in carrying out the Services,
  - an indemnity in respect of third party claims for damage to third parties caused by the Consultants or any person or firm acting on behalf of the Consultants in carrying out the Services,
  - infringement of Intellectual Property Rights

#### 4.7 Conflict of Interest

61. The Winning bidder warrants that to the best of its knowledge after making diligent inquiry, at the date of signing the Contract no conflict of interest exists or is likely to arise in the performance of its obligations under the Contract by itself or by its employees and that based upon reasonable inquiry it has no reason to believe that any sub-contractor has such a conflict.
62. If during the course of the Contract a conflict or risk of conflict of interest arises, the Winning bidder undertakes to notify in writing MOJ immediately that conflict or risk of conflict becomes known.
63. The Winning bidder shall not, and shall use their best endeavors to ensure that any employee, agent or sub-contractor shall not, during the course of the Contract, engage in any activity or obtain any interest likely to conflict with, or restrict the fair and independent performance of obligations under the Contract and shall immediately disclose to MOJ such activity or interest.

64. If the Winning bidder fails to notify MOJ or is unable or unwilling to resolve or deal with the conflict as required, MOJ may terminate this Contract in accordance with the provisions of termination set forth in the Contract.

#### 4.8 Secrecy & Security

The Winning bidder shall comply and shall ensure that any sub-contractor complies, so far as compliance is required, with the secrecy and security requirements of MOJ , or notified by MOJ to the Winning bidder from time to time.

#### 4.9 Document Property

All plans, drawings, specifications, designs, reports, and other documents and software submitted by the Winning bidder in accordance with the Contract shall become and remain the property of MOJ , and the Winning bidder shall, not later than upon termination or expiration of the Contract, deliver all such documents and software to MOJ , together with a detailed inventory thereof. Restrictions about the future use of these documents, if any, shall be specified in the Special Conditions of the Contract.

#### 4.10 Removal and/or Replacement of Personnel

65. Except as MOJ may otherwise agree, no changes shall be made in the key Personnel. If, for any reason beyond the reasonable control of the Winning bidder, it becomes necessary to replace any of the key Personnel, the Winning bidder shall provide as a replacement a person of equivalent or better qualifications and upon MOJ approval.
66. If MOJ finds that any of the Personnel have (i) committed serious misconduct or have been charged with having committed a criminal action, or (ii) have reasonable cause to be dissatisfied with the performance of any of the Personnel, then the Winning bidder shall, at MOJ 's written request specifying the grounds thereof, provide as a replacement a person with qualifications and experience acceptable to MOJ .

#### 4.11 Other Project-Related Terms

MOJ reserves the right to conduct a technical audit on the project either by MOJ resources or by third party.

## Section 5. ANNEXES

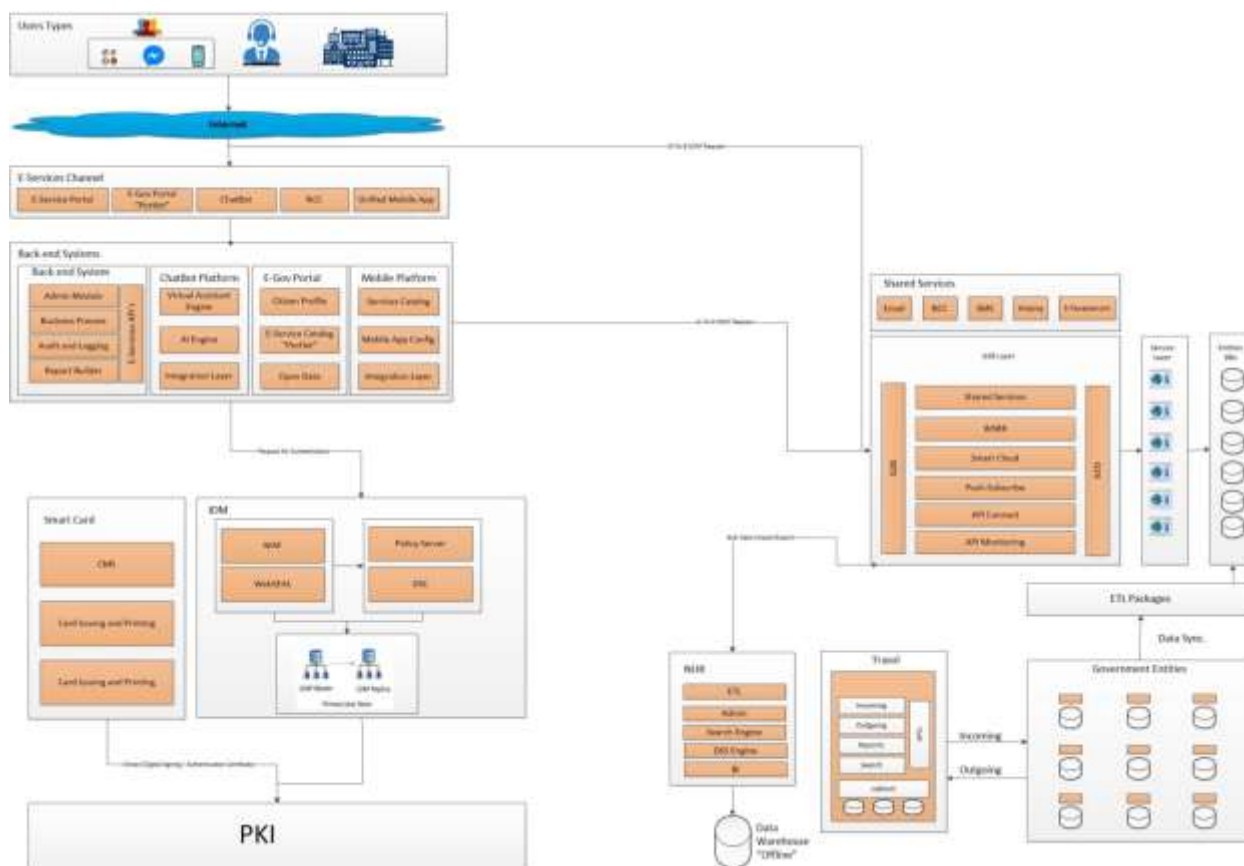
### 5.1 List of Acronyms

TERM	DESCRIPTION
ADC	Access and Delivery Channel
CC	Contact Center
CMS	Content Management System
eGAF	e-Government Architecture Framework
GID	General Intelligence Department
GoJ	Government of Jordan
IT	Information Technology
KPI	Key Performance Indicator
Modee	Ministry of Digital Economy and Entrepreneurship
MOJ	Ministry of Justice
PM(O)	Program Management (Office)
PSD	Public Security Directorate
RFP	Request For Proposal
SENS	Secure Enterprise Nervous System
SGN	Secure Government Network
SMS	Short Message Service
SOA	Service Oriented Architecture

### 5.2 E-Government Implementation Framework

#### Implementation Framework

This section provides a definition of a general framework for e-government infrastructure components that is based on the concept of the e-Government Architecture Framework (eGAF) and Service Oriented Architecture (SOA) as well as two other major initiatives – e-Government Portal and Secure Government Network – that are major supporting infrastructure components for e-Services. In addition to other important initiatives like the e-Government Contact Center, National Payment gateway(EFAWATEERcom), Government Service Bus (GSB), and National E-gov Portal.



## e-Government Architecture

As the facilitator of the implementation and delivery of governmental e-Services, the e-Government Program has been working diligently to define its target e-Government federated enterprise architecture, which is meant to enable seamless integration and secure interoperability of services between distributed entities cohesively and cost effectively using SOA. The responsibility of the implementation and delivery of government e-Services lies upon the government and its various entities:

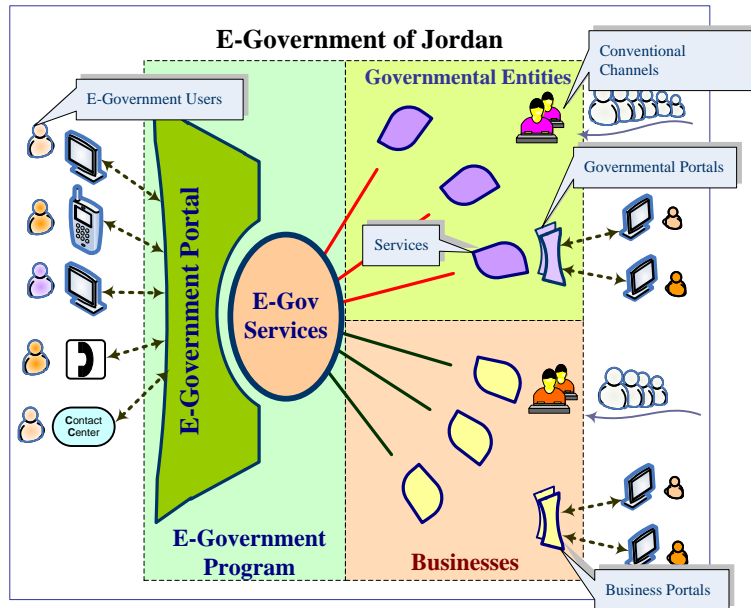
The e-Government Program plays the role of the “e-Services enabler” by providing the components that constitute the Central e-Government Service Delivery Platform;

The other governmental entities (mainly ministries) play the role of the “e-Services providers” by composing and operating their e-Services, having the choice to either outsource these services, or operate them in-house.

The following diagram presents a high-level view of the various e-Government stakeholders, and depicts the federated, customer-centric nature of the e-Government architecture<sup>1</sup>:

<sup>1</sup> The diagram is meant to present a high-level view of the e-Government from a business perspective; hence many businesses and technical details do not appear for the sake of the overall understanding.

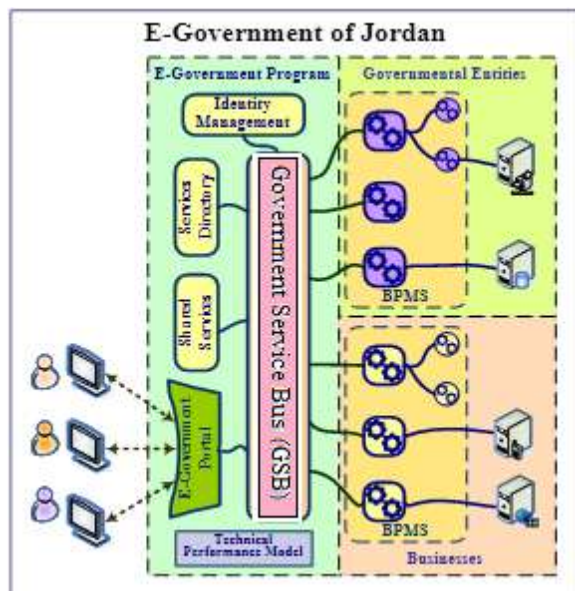




**Figure 5.4.1: e-Government of Jordan High-level View**

The e-Government portal of Jordan is customer-centric, i.e. all e-Services are centered on customers' needs. Currently, the e-Government Web Portal, which constitutes the central web informational portal of the e-Government, co-exists with a number of other governmental portals. Ultimately, the e-government's portal will turn into a multi-channel, one-stop-shop for all government e-Services, and will support various access and delivery channels (e.g. Web, SMS, Kiosks, etc.).

The following diagram depicts the main building blocks for the e-Government target architecture:



**Figure 5.4.2: e-Government Architecture High-level View**

As shown in the above diagram, the e-Government Program will provide a central Government Service Bus (GSB) that will serve as a unique point of traffic. It will take care of routing service invocations towards service providers and of returning responses back to the service clients (which could be the portal or some other service as in the case of cross-organizational e-Services). The e-Government Program will also provide a set of shared services (for instance National Payment Gateway ,EFAWATEERcom, notification gateway, etc.) that can be invoked from within the context of any e-Service, promoting reuse of components across the government and thus reducing the costs by eliminating the needs for dedicated implementations of components that perform the same functionalities offered by any of the central shared functionalities at the entities side. The services directory will maintain an active list of all available services as well as their interface specifications. A central identity management solution will be used to federate identities, provide (when applicable) single-sign-on, facilitate propagation of user identities and attributes across the e-Government trust domain, and enable account provisioning. Finally, a central technical performance model will be put in place to enable concerned technical stakeholder at the e-Government Program to monitor the health and performance of the overall e-Government and identify issues and bottlenecks as well as potential areas for improvement. In order to prevent vendor lock-in, all of the above components will be built solely upon open standards, such as Web Services, SOAP. Where necessary, all service providers shall conform to the above standards in order to interoperate with other components within the e-Government framework.

The e-Government of Jordan Program will also provide Government Entities with an Enterprise Architecture Framework and methodology to help them in building their Enterprise Architecture in respect of the above principles. The e-Government Program will also provide help and support on how to apply this framework to aid the entities during the course of the framework implementation.

The e-Government Program will provide all necessary documentation and support in order to enable project implementers to produce deliverables that are in line with the e-Government architecture vision in the form of a Reference Model Winning PSPs shall have to access the necessary documentation.

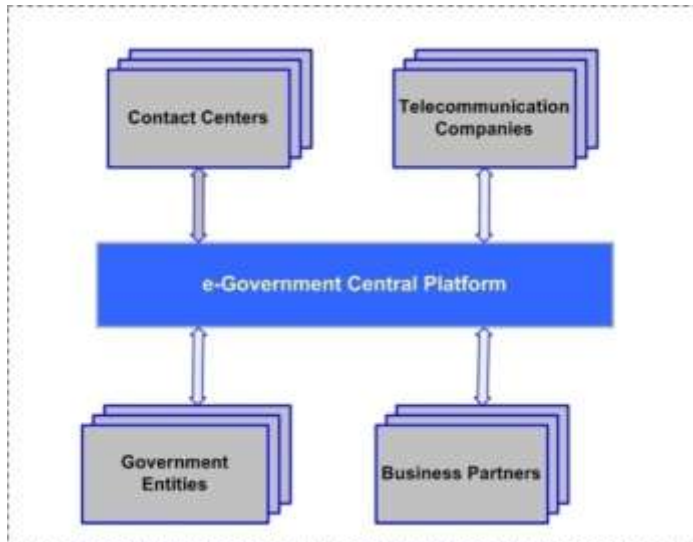
## **E-GAF & SOA**

The primary delivery models for e-government are:

- Government-to-Citizen (G2C)
- Government-to-Business (G2B)
- Government-to-Government (G2G)

Jordan e-government program is capitalizing over the G2G, G2B, and G2C service models in order to provide information integration between the different government entities to improve government processes efficiency, easy end users accessibility, increase transparency and reduce total cost of ownership.

The following figure depicts the different parties involved in the integration.



**Figure 5.4.3: Government of Jordan Integrating Participating Parties**

As seen in the figure above the following parties are involved in integration:

- **Government entities:** Government entities form the major customer and beneficiary for the business integration service provided by the e-government central platform. G2G integration model shall introduce efficient mechanism for integrating the government entities in order to deliver G2C, G2E and G2B services.
- **Telecommunication companies:** Telecommunication companies are considered business partners. The program will be responsible for providing the G2B integration services between those companies and the government entities. One example of such services can be the SMS notification.
- **Business partners:** The program will be responsible for providing the G2B integration service between business partners and government entities. Example for such business partners: payment service providers (PSP) and private banks.
- **Contact center:** Contact center's business is to serve the government entities end users. The program will be responsible for providing the G2B integration services between those contact centers and the government entities.

The IT infrastructure in the government entities and other business partners in Jordan is heterogeneous across operating systems, applications and software packages. Existing applications are used to run current business processes; so starting from scratch to build new infrastructure is a very expensive and non-practical option. Hence; government entities should quickly respond to business changes with agility; leverage existing investments in applications and application

Infrastructure in order to address newer business requirements; support new channels of interactions with clients and partners (other government entities); and feature an architecture that supports business oriented model.

SOA is efficient for large and distributed systems where other types of integration are more complex and costly.

### **Jordan e-Government Business Integration Patterns**

The business integration patterns that will be enabled by the central platform infrastructure are:

- Vertical e-Services integration pattern: defines the pattern in which services are provided end-to-end by one government entity. It's true that such services are provided by one government entity but their integration pattern may use some of the e-government central platform shared services such as authentication, online payment, notification, contact center ... etc.
- Cross organizational e-Services integration pattern: defines the pattern in which a government service requires the involvement of several government entities in order to be delivered.
- Composite e-Services integration pattern: defines the pattern in which a service flows across multiple government entities and contribute to e-Government overall objectives (e.g. GRP).
- Shared e-Services integration pattern: shared services are defined as the 'enablers', providing technology-based functionality that are central to the provision of vertical and cross-organizational services. Their ultimate ownership belongs to the e-government central platform as part of the federated architecture framework.

### **Jordan Information Interoperability Framework (IIF)**

The Jordan e-government program has initiated an information interoperability framework that will manage and standardize the exchange of common and shared information between the different parties involved in the e-government of Jordan such as the government entities, central platform and business partners.

The IIF mandates that all the parties should speak the same language and this includes:

- Protocol: SOAP/HTTP(s)
- Content type: XML
- Standards: Jordan e-government standards
- Format: IIF format

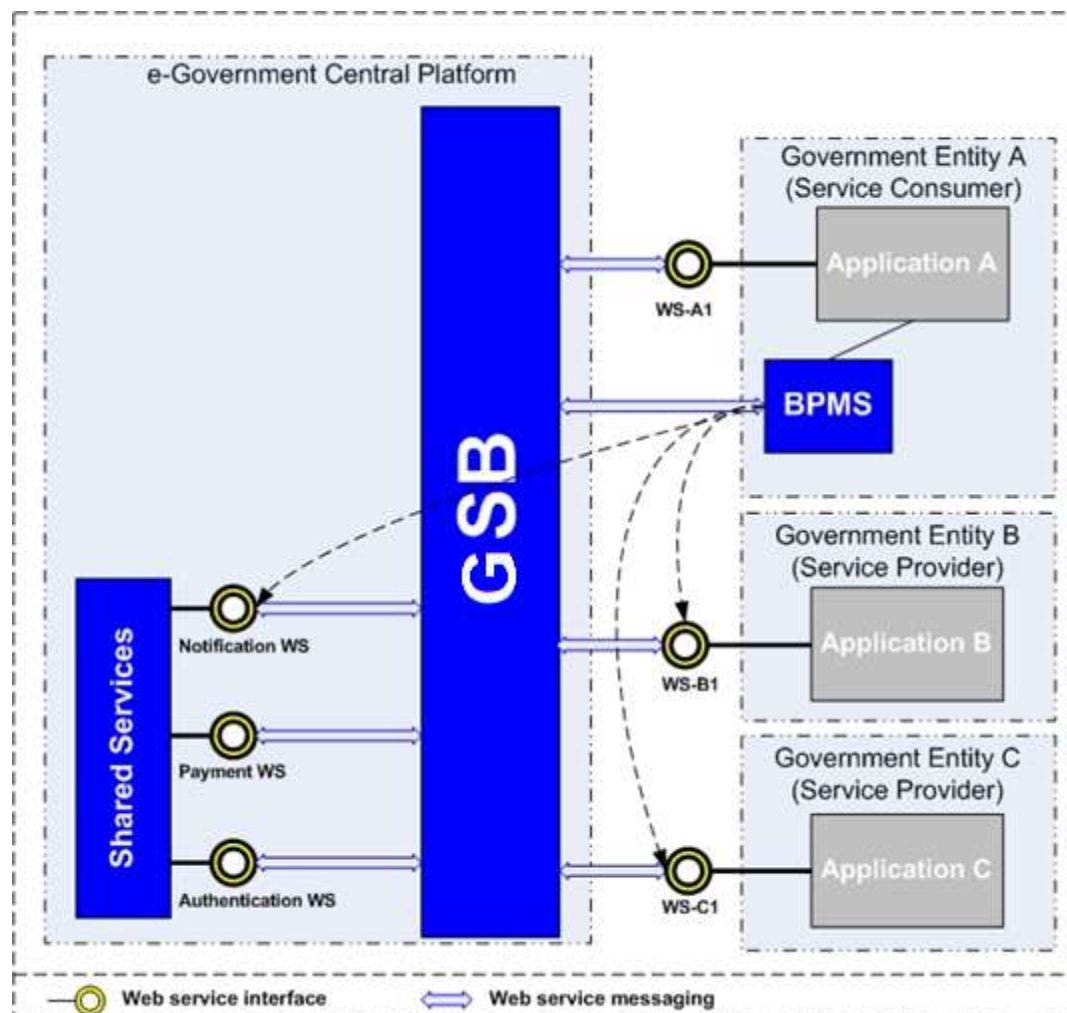
Note : For any new service that will be integrate with GSP it's recommended to be implemented using the WCF standard.

### **E-GAF and Business Process Management (BPM)**

The government entities in Jordan will provide cross organizational services whose logic is distributed across other government entities and business partners including the central platform. The main provider of a service [Principle Service Provider] will host the workflow of the Cross Organizational Service. Hence, the national GSB of Jordan will not host the workflow of any

Government Entity Service, nevertheless, it should enable integration between different entities' services to constitute a Cross Organizational Service.

A government entity will utilize the central platform integration services published web services, and other government entities published e-Services to compose the business processes for their cross organizational e-service. The following figure depicts the relation between the integration infrastructure provided by the e-government central platform and the BPM components at the government entities premises.



**Figure5.4.4: E-GAF and BPM**

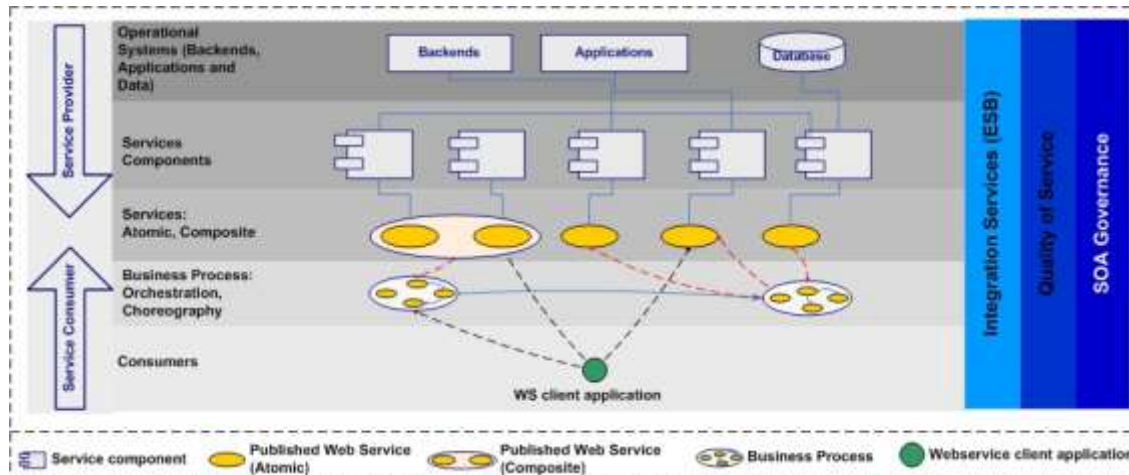
As depicted in the figure above, the application in government entity “A” starts a business process that includes executing tasks at government entity “B”, “C” in addition to the notification services provided by the e-government central platform. The application at “A” will communicate with the Business Process Management System (BPMS) component<sup>2</sup> at its

<sup>2</sup> WFMS: A software application that stores process definitions and runs jobs based on those process definitions via its workflow engine component. The workflow engine is the runtime execution module.

premises to execute the complete process. The BPMS component invokes the entity “B” Web service (WS-B1), entity “C” Web service (WB-C1) and the Notification WS web services according to the rules that had been set earlier in its rule engine.

### E-GAF Integration Reference Model

The following figure depicts the E-GAF integration reference mode.



**Figure 5.4.5: E-GAF Integration Reference Model**

As depicted in the figure above; the reference model crosses the different parties involved in the SOA architecture: service consumer; integration services (GSB), and the service provider.

The consumer will implement the Web service client application that contains either direct calls to published Web services or calls to the orchestrated or choreographed or business processes.

The provider publishes his services (atomic and composite) through the GSB. The services are enabled by a set of components (JavaBean, EJB, COM, DCOM, PLSQL ... etc.). Such components form the bridge between the backend applications, business applications and databases on one side and the web services on the other side.

The integration services at the central platform represented by the GSB form the mediator between the service consumer and service provider. The GSB provides several services and functionalities such as integration hub, services registry, security, intelligent routing ...etc.

Security, audit, high availability, manageability are quality of service attributes for the integration model.

### Secure Government Network

The Secure Government Network (SGN) is a large initiative linking all government entities to a secure Government Network as a part of a recently developed Connectivity Strategy.

The main role of the SGN is to provide connectivity to government entities. Currently, the following services are provided through the SGN:

- File sharing/exchange between government's entities connected through the SGN.
- E-mail services (electronic services that include email messaging solution, calendar, personal communications tools, etc.).
- Inter-application communication

Upon request, Modee will provide the winning bidder with related document(s) describing in detail Connectivity Strategy and detailed requirements related to SGN.

### **Government Service Bus (GSB)**

#### **GSB Integration Requirements**

The Government Service Bus (GSB) is the central enabling set of components of the e-Government infrastructure that is based on Service Oriented Architecture (SOA). The GSB provides an infrastructure that removes any direct connection between service consumers and providers. Consumers connect to the bus and not the provider that actually implements the service. This provides location independence to all services.

The GSB also implements further value add Infrastructure or “Fabric” services. For example, security, transaction, scalability, directory, registry and delivery assurance are implemented centrally within the bus instead of having these buried within the applications or at the government agency back-ends.

The GSB architecture enables governmental entities to connect and use ready-made components of the e-Government. The diagram below shows the conceptual architecture of the GSB.

IBM WebSphere Data Power SOA Appliances are purpose-built, easy-to-deploy network devices that simplify, secure, and accelerate your XML and Web services deployments while extending your SOA infrastructure. Data Power provides configuration-based approach to meet Modee’s edge ESB requirements. The DataPower Appliance provides many core functions to applications, such as service-level management, routing, data and policy transformations, policy enforcement, access control, and hardened security—all in a single “drop-in” device.

For Modee, Data Power provides the following key benefits.

- Platform for Vertical e-Services integration: Web services from different government entities (service providers) can be securely exposed using Data Power.
- Cross Organizational e-Services Platform: Data Power provides role-based access control to ensure the right level of secure access for cross-organizational e-Services.



- Composite e-Services integration platform: Data Power is the service composition layer that exposes composite services to service consumers.
- Shared e-Services integration platform: Data Power supports modular service integration architecture.

When deploying this IBM appliance in your network, you secure your enterprise at the Application Layer vs. at the Network Layer. DataPower is a next-generation appliance that operates on MESSAGES instead of PACKETS. This enables offloading security checks and structural checks from the service providers, thereby simplifying integration while minimizing performance degradation.

### **Solution Benefits**

Using IBM Data Power as the ESB appliance, this provides the following benefits:

- Ease of implementing security and web services in a purpose-built appliance resulting in reduced Development Lifecycle and implementation costs.
- Configuration, rather than coding: This approach offers faster time to market compared to traditional coding approaches for service integration.
- Offloading tedious security tasks from Service Providers (Government entities), preventing potential performance degradation
- Appliance approach provides greater security compared to software based solutions (removes periodic operating system patches, OS vulnerabilities, virtualization layer vulnerabilities, regular software patches, etc.)
- Purpose built firmware, offering wire-speed processing.
- Prepare your environment for the future: DataPower is ready for mobile and web 2.0
- Extensible architecture: add-on modules can be turned on as required.
- Highly fault tolerant device (multiple power supplies, multiple network ports) with in-built load balancing & clustering options.

The Data Power Appliance is purpose-built, easy to consume and easy to use. Data Power delivers security, common message transformation, integration, and routing functions in a network device. IBM approach helps you to leverage and scale your existing infrastructure investments.

### **Solution components and features**

The below sections list the used components and the utilized features within the Data Power appliance during the implementation of the Edge ESG to help meet Modee requirements:

- **Logging**

IBM Data Power appliance offers a bunch of different options when it comes to logging. Modee's main concerns when it came to logging were:



- The ability to troubleshoot a problem when one arises: As for this point in the solution IBM Data Power offers a feature called ‘debug probe’, this feature can be enabled to log the messages temporarily and then view them at each stage within the policy execution, this also offers information like the requested and source URL/IP which should be sufficient when a problem arises at the message level.
- Being able to view and track events as they occur (mostly errors): As for this DataPower’s out of the box logging behavior should suffice, it offers the ability to filter the logs based on the component from which they originated and the ability to increase and decrease the level of logging details based on the current need.
- DataPower auditing: Out of the box, DataPower offers the ability to log any administrative actions, by which user where they performed and when (this also included some lower level relevant action logging).

- **Security using SSL certificates**

When it comes to SSL, the solution includes two different implementations:

- Standard SSL over HTTP (for G2G services)

In this scenario DataPower is issued a certificate which the service consumers should trust and accordingly be able to authenticate DataPower boxes and perform transport layer encryption. As for between DataPower and the service providers, DataPower should receive a copy of the public certificate of the entities it will connect to in order to trust them.

- SSL with mutual authentication (for G2B services)

As for this scenario the communication with the backend services is still done in the same manner but the communication with the consumers is done differently. In this case the first part still stands true where DataPower is still issued a certificate which the service consumers should trust but the difference is that the service consumers themselves should also be issued certificates which the DataPower should receive (public certificates) in order to perform a mutually authenticated connection.

**Mutual authentication** or **two-way authentication** (sometimes written as 2WAY authentication) refers to two parties authenticating each other at the same time. In technology terms, it refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity. As for the certificates issuing three different options were discussed:

- Purchasing internationally trusted certificates

- Using the new Jordan PKI to issue new certificates (in the future)
- Using self-signed certificates (this option will not be used)

DataPower supports four different formats when it comes to certificates and key:

- DER
- PEM
- PKCS #8
- PKCS #12

Note: DataPower offers notifications for the box administrators/developers when an SSL certificate is going to expire within a month to insure minimized service downtime and a minimal impact of this event.

- **Web services proxy**

A 'Web Service Proxy' provides security and abstraction for remote web services. It is the object where most of the implementation will be performed and where the majority of the other features are contained. A Web Service Proxy makes it easier to implement certain features for web services based on a WSDL file.

The first step of implementing a web service in DataPower is always obtaining the WSDL (by uploading to the device or fetching from WSRR), after doing so the Web Service Proxy starts offering options starting with specifying the end point to be exposed and the protocol to be used. After that one can start applying the required policy. In the current scenario we have two policies to be applied per service the first (client to server) at the service level and another policy to apply on the way back but on a lower level and that is the operation level.

On the client to server policy:

- Within the AAA action the service credentials will be extracted from the message (Password-carrying UsernameToken element from WS-Security header), this identity will be validated against LDAP to decide whether the consumer is eligible to consume the service based on whether the identity is a member of the service group or not.
- At this stage the SLA is enforced.
- An attribute containing the identity's access level to the services is queried and stored in context variables.

- The identity within the message is replaced with another identity which is meant to authenticate DataPower boxes at the service provider's side.
- The destination URL is replaced with the actual service provider's URL instead the one that came with the message here.

On the way back (server to client) each response to a consumer is filtered based on the consumer's access level to a service using a transformation action (an XSLT style sheet) and finally the response is returned to the consumer here. Guidelines for web service integration

#### 5.2.1.1 *IBM API Connect*

“IBM API Connect is an end-to-end solution that allows users to create, secure, manage, socialize, monetize and analyze APIs. It provides a powerful set of capabilities from turning backend RESTFUL or SOAP services into managed services. This is done by publishing APIs to API Gateways, while enforcing lifecycle and governance controls on those APIs. API Connect enables users to expose APIs, through a developer portal, targeting application developers both inside and outside their organization. Additionally, the solution's analytics tooling helps API providers and API consumers better understand the health and consumption of deployed APIs.”

[1]

The following table explains the key steps of the API lifecycle in more detail. [2]

Table 1. Key phases of the API lifecycle	
Lifecycle Phase	Description
Create	<p>Develop and write API definitions from an API development environment, eventually bundling these APIs into consumable products, and deploying them to production environments.</p> <p>For tutorials, walk-throughs, and in-depth guides for building, testing, and deploying APIs and Products in API Connect, see <a href="#">Tutorials</a>, and <a href="#">Developing your APIs and applications</a>.</p>

Table 1. Key phases of the API lifecycle

Lifecycle Phase	Description
Secure	<p>Leverage the best-in-class API Gateway, gateway policies, and more, to manage access to your APIs and back-end systems.</p> <p>To learn more about adding security to your API, see <a href="#">Configuring API security</a>.</p> <p>To learn more about how to add API Gateway policies to your API, see <a href="#">API policies and logic constructs</a>.</p>
Manage	<p>Governance structures are built in to the entire API lifecycle, from managing the view/edit permissions of APIs and Products being deployed, to managing what application developers can view and subscribe to when APIs are deployed.</p> <p>To understand and leverage API Connect management and governance controls along the API lifecycle, see <a href="#">Managing your APIs</a>.</p>
Socialize	<p>API Connect comes with an advanced Developer Portal that streamlines the onboarding process of application developers, and can be completely customized to an organization's marketing standards.</p> <p>To understand more about using the Developer Portal, see <a href="#">Developer Portal: Socialize your APIs</a>.</p>
Analyze	<p>Developers and Product Managers alike are given the tooling in API Connect to understand their API traffic patterns, latency, consumption, and more to make data driven insights into their API initiatives.</p>

### 5.2.1.2 *IBM MQFT*

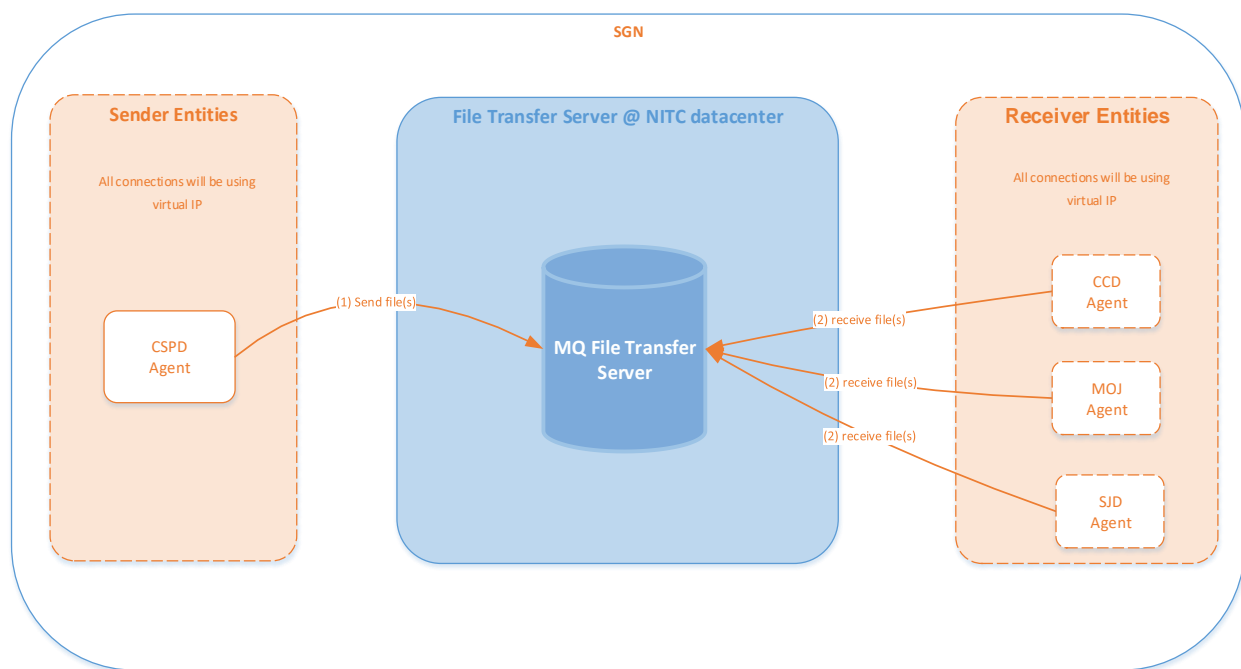
IBM MQ Files Transfer solution is based on MQFT agents, which plays the role of either sender or receiver in case of sending files or receiving files. The same agent can be acting as both sender and receiver at the same time.

Files will be transferred across the centralized MQ infrastructure hosted in the NITC data center.

File transfers will be triggered using the following methods:

- Scheduled file transfers
- Manual file transfers
- Automatic file transfers based on monitoring a system directory

A governmental entity will be able to either send or receive files when they have the MQFT agent installed and connected from their side to the centralized MQFT environment in the NITC data centre.



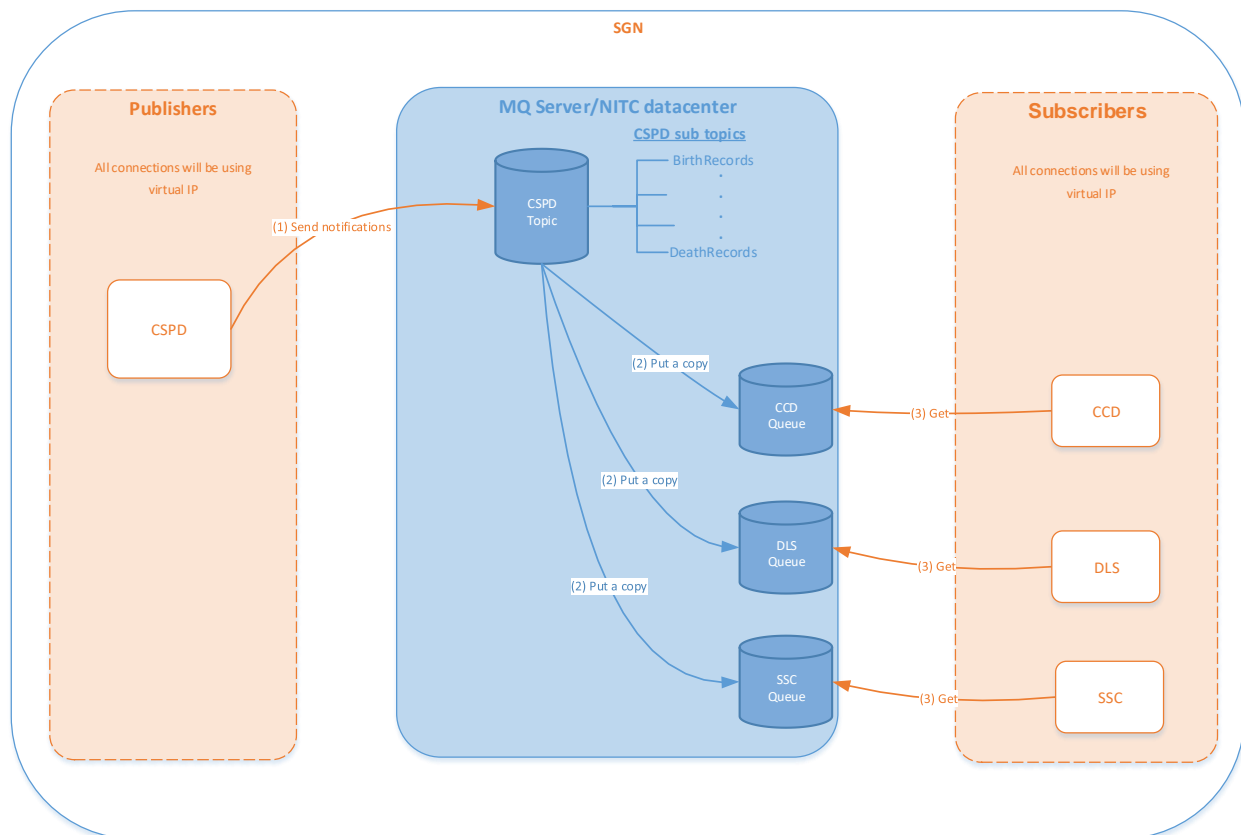
**Figure (File Transfer)**

### 5.2.1.3 *IBM Publish – Subscribe*

IBM MQ Publish - Subscribe solution will provide the following functionalities:

- The solution will provide one topic for each publisher

- The solution will provide a web service facility to be used for the publications
- The publisher will either use MQ APIs or the available web service to connect to the MQ server and send publication messages. We recommend that each publisher should use MQ APIs to connect to MQ server and send the publication messages
- Publication message structure and format is considered to be the responsibility of the publisher
- It is recommended to limit the size of the publication message by using paging techniques or by sending the needed information only without extra data
- The solution will enable the system administrator to control manual subscriptions
- The administrator will create a subscription for each subscriber per topic of interest
- The solution will provide a dedicated queue for each subscriber per topic subscription
- The subscriber is responsible to connect to the MQ server hosted in the NITC using MQ APIs, and retrieve the publication messages from own queue
- Each subscriber will have access to own queue(s) only



**Figure (publish-subscribe Business Case)**

## Government to Government - SGN

The below is a list containing all the guidelines for a service provider willing to expose a service or a service consumer willing to integrate with the GSB:

- 1- Messages should comply with the **XML + SOAP** standards.
- 2- All the currently implemented services follow the **SOAP** standard **version 1.1**.
- 3- The SOAP header must contain a **Password-carrying Username Token** element from WS-Security header.
- 4- The currently followed approach mandates that the **Username Token should not be signed**.
- 5- The SOAP message should not be encrypted nor signed.
- 6- The current followed approach mandates **not using Timestamp** token so that consumers with a different time or time zone settings could consume the service.
- 7- Both the service provider and consumer must implement and **use transport layer security**
  - a. SSL version 2 should not be used
  - b. SSL version 3 should not be used
  - c. Weak ciphers and hashes should not be used
  - d. The usage of strong ciphers only is strongly recommended
  - e. It is mandatory to use TLS v1.0 , v1.1 or v1.2
  - f. The usage of message compression is not recommended
  - g. The usage of insecure legacy SSL should not be permitted
- 8- The recommended certificate format to be used is **DER encoded binary X.509 certificates (.cer)**
- 9- The recommended **RSA key length** for the issued and used certificates and keys is **2048**.
- 10- Services that can provide large chunks of data at once (ex. Search based services) are recommended to **use** some sort of **pagination** and not to return all the data at once if the result is considered large enough.
- 11- All the **data fields within the message body** should be marked as **optional** from the provider's side and the service consumer should be able to handle any missing or empty fields appropriately (regardless of data type).
- 12- The message providers are free to build the message body structure as they see fit to the service requirements as long as they comply with the relevant points mentioned above.
- 13- **Using any additional feature** from WS-Security or WS-Standards in general is **not recommended** unless verified and approved to be supported by the GSB.

## Government to Business - Edge

In addition to all the above mentioned guidelines in the G2G section above, any entity outside the government (outside the SGN network) who would like to integrate with the GSB must comply with the below:

- 1- The entity must comply with the **mutual authentication** or **two-way authentication** (sometimes referred to as 2WAY authentication) specifications.

Establishing the encrypted channel using certificate-based mutual authentication involves:

- A client requests access to a protected resource.
- The server presents its certificate to the client.
- The client verifies the server's certificate.
- If successful, the client sends its certificate to the server.
- The server verifies the client's credentials.
- If successful, the server grants access to the protected resource requested by the client.

Note: To establish this approach the entity should provide its public certificate to the GSB team (regardless of being a service provider or a service consumer) to ensure its trust as well as to receive the public certificate from GSB and insure that it is trusted from the entity's side as well.

Sample request message



```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">

<s:Header>

  <ActivityId CorrelationId="bcf08350-0ad0-4e6a-b596-9994e137b45c"

  xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">9dc40624-
  0ae7-4984-8806-4e251982b213</ActivityId>

  <o:Security s:mustUnderstand="1"

  xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
  secext-1.0.xsd" >

    <o:UsernameToken u:Id="uuid-1349a92e-13f7-41d1-bdde-0021a9c1d276-79">

      <o:Username>UserName</o:Username>

      <o:Password>*****</o:Password>

    </o:UsernameToken>

  </o:Security>
</s:Header>

<s:Body>

  <operation xmlns="http://tempuri.org/" >

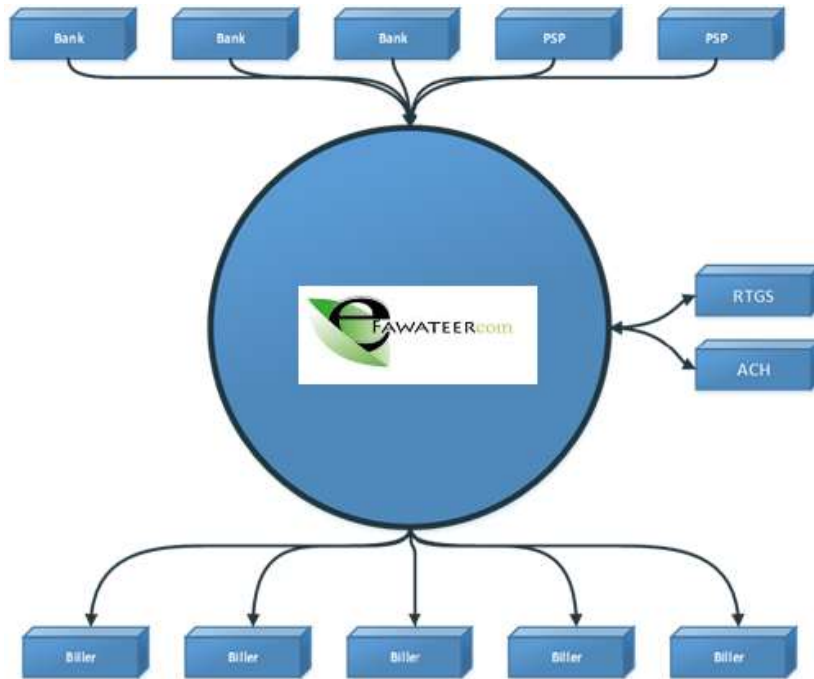
    <NationalNo>123456789</FirmNationalNo>

  </operation>
</s:Body>

</s:Envelope>
```

### ***eFAWATEERcom:***

eFAWATEERcom solution has the ability to connect different banks and PSPs with different billers and/or financial houses or services providers, and at the same time, the solution integrates with the RTGS and the ACH for settlement.



**Figure 5.4.6 eFAWATEERcom Switch**

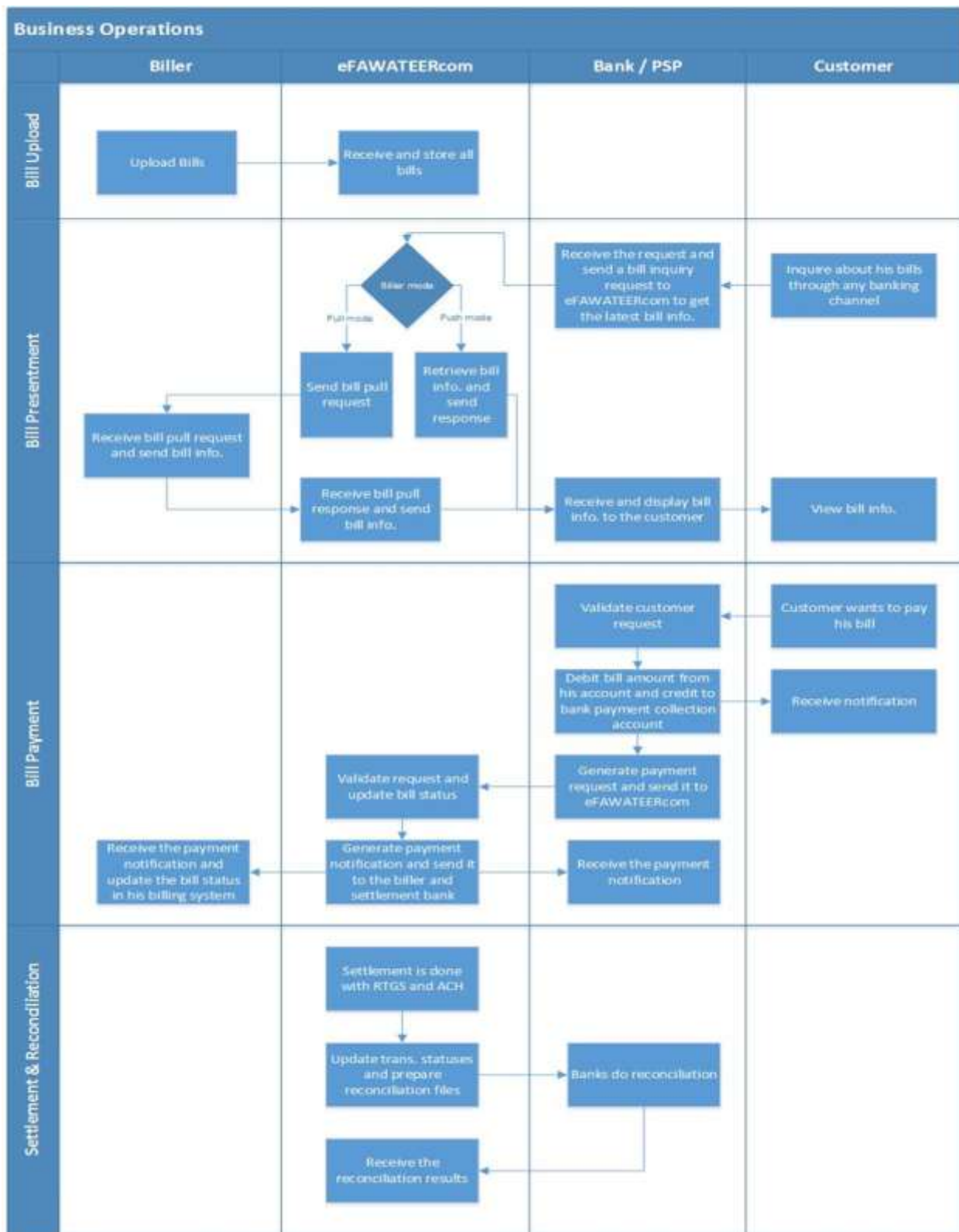
### ***Business Process Operations (BPOs) of eFAWATEERcom***

The following workflow shows the main stages that eFAWATEERcom consists of:

- Bill Upload
- Bill Presentment
- Bill Payment
- Settlement and Reconciliation

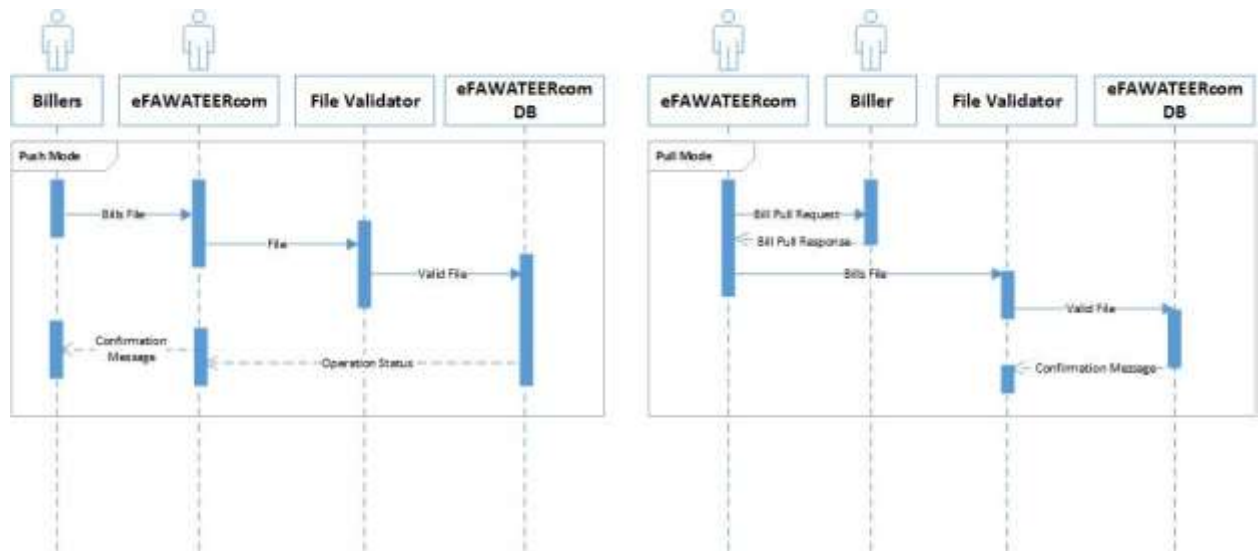
#### **Note:**

The solution is capable of supporting different types of payments (periodic, one-off, non-existing bill, non-banked customer payments) in addition to handling all payment status cycle (New, Updated, Sent, Completed).



**Figure 5.4.7 Business Process Operation**

## Bill Upload

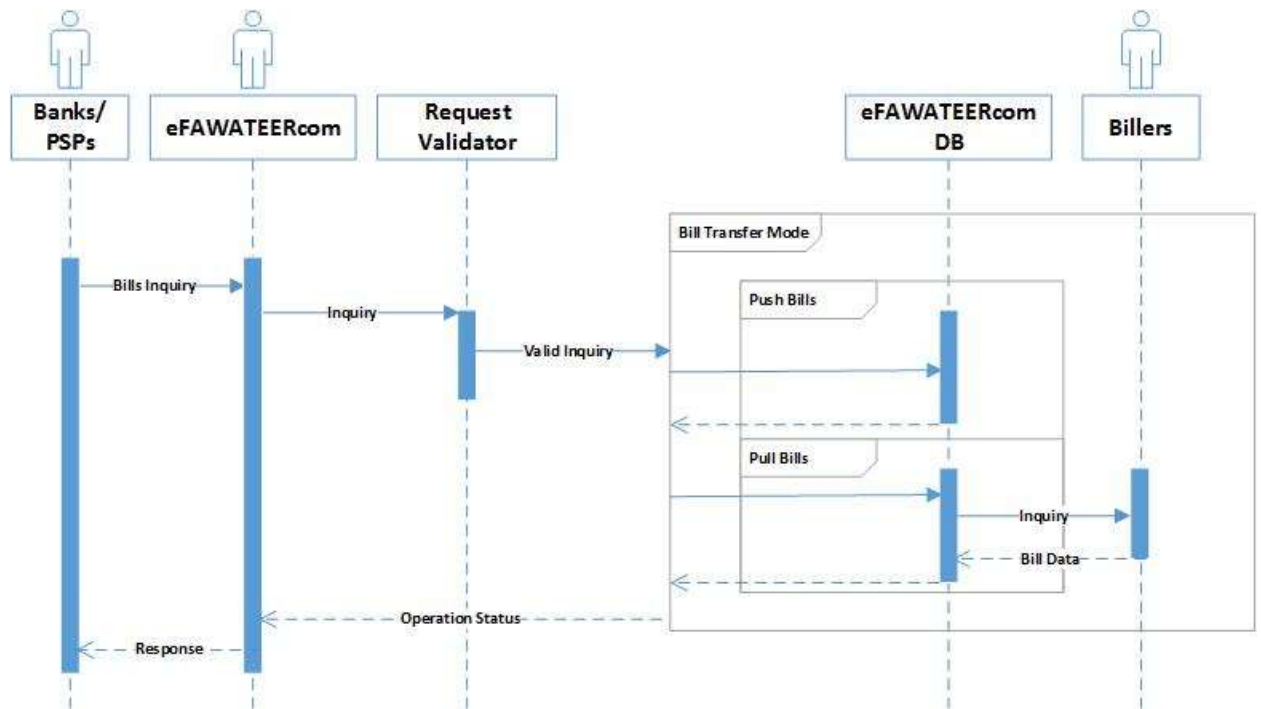


**Figure 5.4.8 Bill Upload Process**

The previous workflow describes in general the bill upload process:

- Billers are required to upload bill summary data to eFAWATEERcom on a regular basis using the Bill Upload Process; this process can be:
  - Biller initiated (Push) via web service using XML file structure or file transfer using different formats such as XML, CSV, or any other flat file structure that can be defined as part of the gap analysis.
  - eFAWATEERcom initiated (Pull) via web service using XML file structure, and can be performed through eFAWATEERcom.
    - On receiving the uploaded bills, eFAWATEERcom performs certain validations on the bills to maintain bills data accuracy. These are:
      - Data Validations.
      - Business Validations.
        - If the file/batch has errors/inconsistencies, the systems reject the entire file/batch of records and return it to the biller for reprocessing, and it will mention the rejection reason.
        - Each bill on eFAWATEERcom database carries a code that shows the status of the bill such as BillNew, BillUpdated, or BillExpired.
        - The solution will response to billers after a successful bill upload operation is performed successfully.

### *Bill Presentment (Bill Inquiry)*

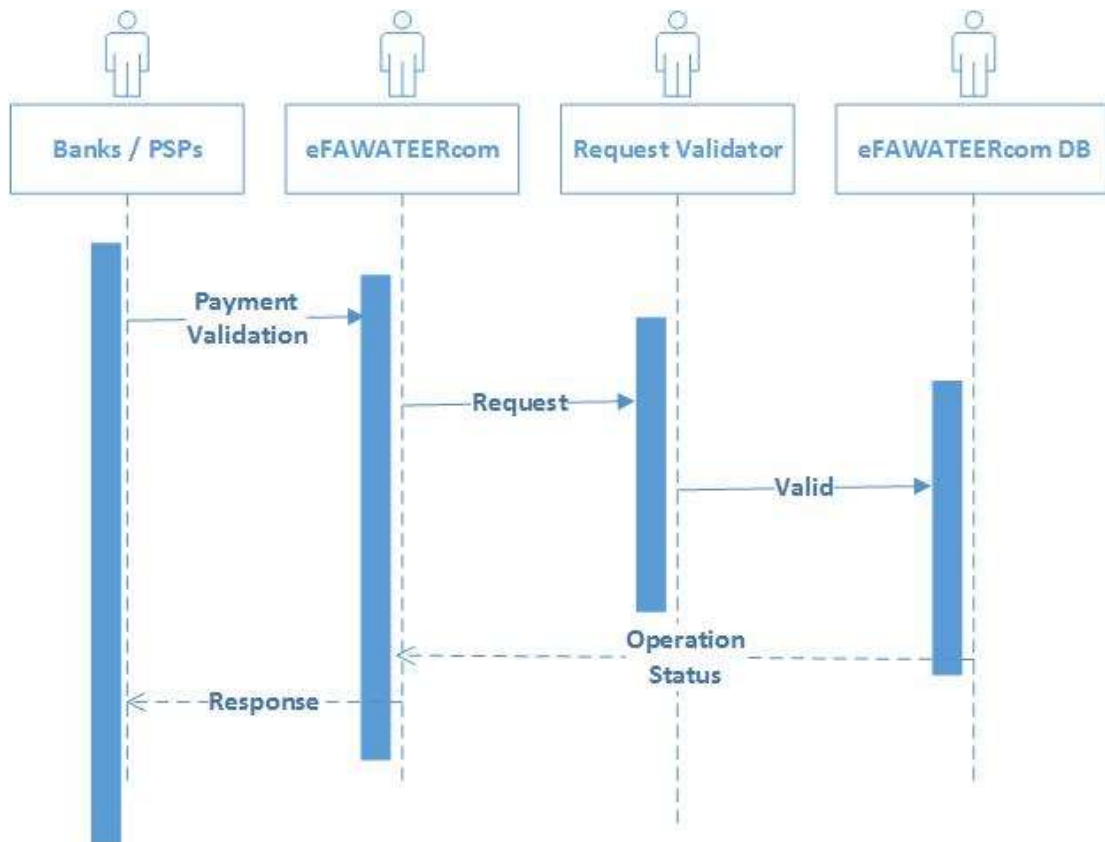


**Figure 5.4.9 Bill Presentment**

The previous workflow describes in general the bill presentment process:

- Bank applications may query eFAWATEERcom for bill and associated payment data using a bill inquiry message. The query can take the form of a Bill-Specific (single) Query in which the Bank wishes to view bill data for a specific account or bill number. Conversely, a Customer Profile query permits the Bank to query on any Customer associated bills (multiple) within the eFAWATEERcom system using a variety of parameters.
- The bill inquiry request contains a set of information that entered by the customer such as 'Bill No.' plus a set of information that are provided from the bank application such as [Biller Code, Billing No.].
- eFAWATEERcom verifies all the business rules (active, inactive, etc...) to be validated for each request, and based on the verification result, it either accepts or rejects the request.
- The response of bill inquiry may contain one or more records based on the criteria used in the query and might return zero results as well.
- All transactions occur across a wide range of channels such as Bank ATM, Internet Banking, Bank Teller, Call Center and Point of Sale.

## Bill Payment

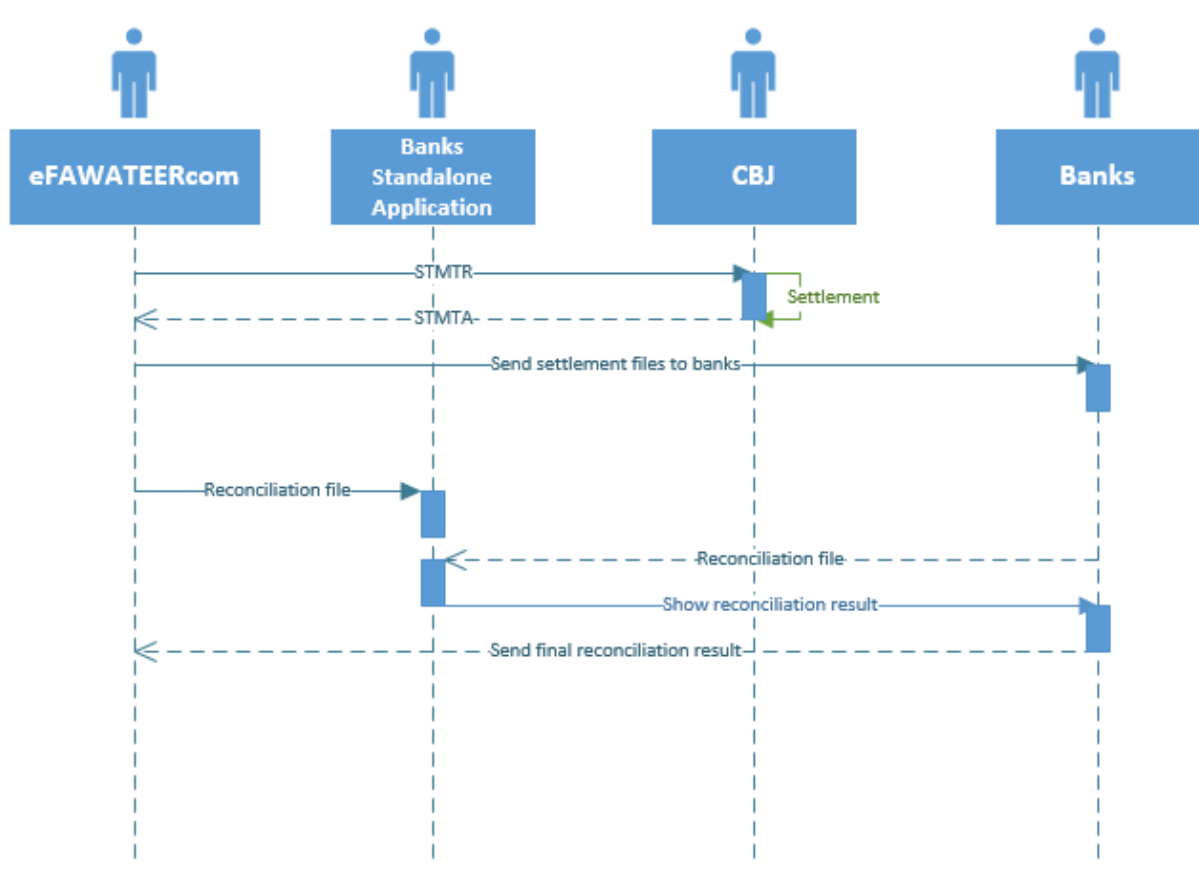


**Figure 5.4.10 Bill Payment Sequence**

The previous workflow describes in general the bill payment process:

- The Payment process permits Banks to create new payment records in eFAWATEERcom. The process is intended to ensure the customer pays according to Biller intent, and it involves a validation of Biller's payment rules.
- If the funds are not sufficient, the bank shouldn't send a bill payment request for eFAWATEERcom.
- A payment collection account will be set-up in each Settlement Bank.
- Banks must record data about all payments in storage termed as eFAWATEERcom Payment Log.
- All transactions occur across a wide range of channels such as Bank ATM, Internet Banking, Bank Teller, Call Center, and Point of Sale.

### Settlement & Reconciliation



**Figure 5.4.11 Settlement & Reconciliation Process**

The previous workflow describes in general the settlement and reconciliation process:

- eFAWATEERcom sends a settlement file to RTGS (STMTR) that includes all payments details in totals.
- CBJ “RTGS” will process the STMTR file and sends the response (STMTA) to eFAWATEERcom system.
- Same operation is repeated for the purpose of the fees totals, meaning that settlement with RTGS will happen for the payments and the fees separately.
- eFAWATEERcom sends two settlement files to the Banks/PSPs including the net total payments and total fees in CSV format, where each file will contain one row for the total payments and in the other file one row for the total fees.

- eFAWATEERcom will allow paying banks to reconcile their payment transactions using the standalone application (Which is a website that is used for reconciliation purposes) where each bank is supposed to upload its data and match with eFAWATEERcom data.
- As for settlement banks, and for any unmatched payment transaction (After receiving settlement payment and fees notifications from RTGS end of that particular day), they can use the standalone application for investigating their transactions statuses.
- Paying banks can send their reconciliation results to eFAWATEERcom, where the result file will be placed automatically on the bank inward FTP directory where eFAWATEERcom support team will investigate unmatched payments.

**More details will be given upon award.**

## **E-Government PUSH SMS API Connectivity**

### **1. Send SMS API:**

***`http://bulksms.arabiacell.net/vas/http/send_sms_http?login_name=login&login_password=password&msg=messageText&mobile_number=9627XXXXXXXX&from=senderID&tag=X&delivery_date=XXXX-XX-XXXX:XX&charset=XXXXXX&unicode=X&dlr=X&dlr-url=http://xyz.com/get_status.php?msg_id=XXXXXX&status=%d`***

#### **- Parameters:**

<b>Parameter Name</b>	<b>Description</b>
mobile_number (Mandatory)	Mobile number of the user. Mobile number should be in the international format, example 962790000000
msg (Mandatory)	SMS text.
delivery_date (Optional)	Message sending date, the date should be with format (yyyy-mm-dd hh:mm).
login_name (Mandatory)	Login name used to access your account over the SMS PUSH Interface.
login_password (Mandatory)	Password used to access your account over the SMS PUSH Interface.
from (Mandatory)	Sender ID or name already reserved and defined over the SMS PUSH Interface.
tag (optional)	Message Type : 1. معاملة حالة عن اعلام 2. وارشادية توعوية 3. ترويجية



	4. داخلي اتصال
Charset (Optional)	Message characters-set, (windows-1256 or UTF-8).
Unicode (Optional)	1 for Arabic Message. 0 for English Message.
dlr (Optional)	Request delivery report on the sent messages, 1. Delivered messages. 2. Undelivered messages. 3. All messages delivery statuses (Delivered and Undelivered).
dlr-url (Optional)	URL to be fetched if the dlr parameter is present. eGov PUSH SMS Sender will replace parameter '%d' in the provided URL with 1 for delivery success or 2 for delivery failure, URL must be encoded and length should not exceed 100 chars.

**- API Responses:**

**In case of success message submitting to the eGov PUSH SMS Sender, the below are the possible return messages:**

- I01-Job (Job ID) queued for processing. (For messages with message date equal to the current date and time)
- I02-Job (Job ID) has been scheduled. (For messages with message date greater than the current date and time)

**And below are listing of possible errors could be returned by the system.**

**- Errors:**

- E01-Invalid USERNAME or PASSWORD.
- E02-Account Expired.
- E03-Account Inactive.
- E04-Empty SMS message.
- E05-Invalid mobile number.
- E06-SMS balance already expired.
- E07-SMS balance already consumed.
- E08-Database error.
- E09-One of the following parameters missing, USERNAME, PASSWORD, MESSAGE TEXT OR MOBILE NUMBER.
- E010-Invalid delivery date.
- E011-Date and time for scheduled messages should be greater than the current date and time.
- E012-You cannot schedule SMS job(s) after SMS expiry date.
- E013-You cannot schedule SMS job(s) after account expiry date
- E014-Not allowed to send SMS through HTTP interface.
- E015-SMS message exceeded the max size for the selected language.
- E016-Invalid sender ID, sender ID must be in English chars and less than or equal 11 in length, space and special characters not allowed.
- E-022- dlr values should be 1, 2 or 3 only.
- E-021- dlr-url length exceeded 100 chars.

## 2. View Account details and Scheduled Messages API:

*[http://bulksms.arabiacell.net/vas/http/sch\\_tasks\\_http?login\\_name=login&login\\_password=password&action=n](http://bulksms.arabiacell.net/vas/http/sch_tasks_http?login_name=login&login_password=password&action=n)*

### - Parameters:

Parameter Name	Description
login_name (Mandatory)	login name used to access your account over the SMS PUSH Interface.
login_password (Mandatory)	Password used to access your account over the SMS PUSH Interface.
Action (Mandatory)	0 : to list all the scheduled messages. 1 : return user credit details (SMS balance), SMS expiry date, Sub-account expiry date and allowed Sender IDs (Comma separated)

### - API Responses:

**In case of success request, the returned values will be one of the responses mentioned in the description column for parameter (Action). And below are listing of possible errors could be returned by the system.**

### - Errors:

- E01-One of the following parameters missing, USERNAME, PASSWORD or ACTION.
- E02-Invalid USERNAME or PASSWORD.
- E03-no schedule tasks.
- E04-Sorry, Account Inactive.
- E05-Sorry, Account Expired.
- E06-Error, Invalid action number.

### 5.3 National e-Government Contact Centre Required Information

The offered e-service solution should provide contact center agents users with enough privileges and access to Information for them to perform their required role.

In addition to the above the winning bidder is required to deliver the following for contact center use:

#### **Documentation and training on the following:**

- Objectives and benefits of the E-Service (before /after description)
- Benefits of the E-Service
- Target population
- Provide support for the E-Service application – How to use it
- Provide information about the status – When will the end user see the result
- Provide technical support in case of problems
- Or execute the whole transaction on behalf of the customer?

#### **E-Service frequently asked questions**

- Technical
- Business (informational)

Furthermore, a number of categories of queries / contact reasons and contact drivers are anticipated:

- Difference between e-Service and physical, traditional service
- How to use
- Payment
- Fulfillment (the paper work)
- Status information
- Technical support
- Complaints

The winning bidder is required to review the above contact reasons and add to them if necessary. In addition to contact reasons types definition, the winning bidder to provide all related information to the anticipated questions. (Answer to the questions illustrated in the matrix below)

#### **Question & Answer Matrix - Illustrative**

Moment: Category:	Pre-use	During use	Post use
----------------------	---------	------------	----------

<b>Difference between E-Service and traditional service</b>	“What are the benefits, compared to going to the relevant government entities?”	“I have completed this process now, should I not go somewhere to pick up the paperwork?”	“I used to receive notification via letter, is the e-mail I just received replacing the letter?”
<b>How to use</b>	“How long will it take to complete the process? I use dial-up Internet access and do not want to spend a fortune of phone costs” “What kind of information do I need to have in order to complete the process?”	“I have filled in this information on that screen, what do I do next?”	
<b>Status information</b>		“I have completed the E-Service process, when will I receive confirmation that it went OK?”	“I received confirmation last week that the process was completed. Can you see where my request is?”
<b>Payment</b>	“I do not trust your online payment; can I make the payment separately?”		“Can you please confirm that you received my payment?”
<b>Fulfillment</b>	“If I submit the request tomorrow, when will I receive the output?”		“It has been 2 weeks since I was supposed to receive my paperwork. Why haven’t I received it already?”
<b>Technical support</b>	“What are the minimum systems requirements?” “I cannot access the application, is the website down?”	“I think my browser’s pop-up blocker is interfering with the application, is that correct?” “The application crashed while I was entering my information, is everything lost?”	
<b>Complaints</b>	“I do not have Internet access and cannot use the E-Service, this is discrimination”	“I am having problems completing the transaction and the	“I have completed the transaction but did not receive the paperwork

		person trying to help me was very rude”	and was charged for it, this is scandalous”
--	--	--	--

**The winning bidder should make the following information ready to the contact center team to learn about:**

- The Service
- The issues related to the current processes
- The changes and improvements made with the E-Service
- The processes surrounding the E-Service
- The remaining issues that people have to deal with around the E-Service
- The impact on the Civil Servants population
- identify the as-is situation in the relevant government entities, as well as the expected changes due to the introduction of E-Service
- Activities that the contact center could / need to “piggyback” in order to complete the whole process.

## 5.4 Technical Proposal Response Format

### **Introduction**

#### **Executive Summary**

*This includes the bidder's understanding of the terms of reference, scope of work and necessary skills, and company profile. This involves including an overview of the main points contained in the proposal with references to sections where more detailed discussion of each point can be found (maximum 4 pages).*

#### **Approach**

*A detailed description of how the bidder will undertake each major area in the SCOPE OF THE PROJECT and DELIVERABLES section, required resources (bidder, ministry and third party) and any special skills required, the deliverables (format and structure), use of any methodology and how it will cover the scope, use of any standard tools, and duration of any work streams.*

#### **[Activity 1]**

#### **Implementation Approach**

Actions	Approach
<i>Provides a listing of the actions needed for the Activity</i>	<i>Describes the bidder's approach for implementing the action; including</i> <ul style="list-style-type: none"><li><i>Process (i.e. steps)</i></li><li><i>Standard methodologies adopted</i></li><li><i>Scope of involvement for each stakeholders</i></li></ul>
...	...

#### **Deliverables**

Deliverables	Format and Structure
<i>Provides a listing of the deliverables of the Activity</i>	<i>Describes the format (e.g. MS Word document) and Structure (e.g. Outline, indicating the scope and content) of each deliverable.</i>
...	...

#### **[Activity 2]**

#### **Implementation Approach**

Actions	Approach
<i>Provides a listing of the actions needed for the Activity</i>	<i>Describes the bidder's approach for implementing the action; including</i> <ul style="list-style-type: none"> <li>▪ <i>Process (i.e. steps)</i></li> <li>▪ <i>Standard methodologies adopted</i></li> <li>▪ <i>Scope of involvement for each stakeholders</i></li> </ul>
...	...

#### ***Deliverables***

Deliverables	Format and Structure
<i>Provides a listing of the deliverables of the Activity</i>	<i>Describes the format (e.g. MS Word document) and Structure (e.g. Outline, indicating the scope and content) of each deliverable.</i>
...	...

#### ***[Activity...]***

#### ***Implementation Approach***

Actions	Approach
<i>Provides a listing of the actions needed for the Activity</i>	<i>Describes the bidder's approach for implementing the action; including</i> <ul style="list-style-type: none"> <li>▪ <i>Process (i.e. steps)</i></li> <li>▪ <i>Standard methodologies adopted</i></li> <li>▪ <i>Scope of involvement for each stakeholders</i></li> </ul>
...	...

#### ***Deliverables***

Deliverables	Format and Structure
<i>Provides a listing of the deliverables of the Activity</i>	<i>Describes the format (e.g. MS Word document) and Structure (e.g. Outline, indicating the scope and content) of each deliverable.</i>
...	...

#### ***Work Plan and Duration***

*The work plan and duration for the overall consulting work, including any dependencies between the separate items in the scope. The bidder should provide*

[illegible]



---

---

---

---

---

---

**Expected Role in MOJ Project**

---

---

---

---

---

---

---

---

---

---

---

---

**Education**

---

---

---

**Employment Record:**

(a)	Employment Record	From date — present
	Employer	_____
	Position held	_____ _____
(b)	Employment record	_____ — _____
	Employer	_____
	Position held	_____ _____

(c) Employment record \_\_\_\_\_ — \_\_\_\_\_

Employer \_\_\_\_\_

Position held \_\_\_\_\_  
\_\_\_\_\_

**Languages:**

Reading  
Writing

Speaking

Language 1

Language n

-----  
-----

Signature

Date

*Other Information*

*Appendices*

## 5.5 Financial Proposal Response Format

Please indicate the overall estimated cost of your proposed solution.

Cost should be broken down as per the schedules below as well as the detailed scope of work presented in section 3 of this document.

The price quotation should be all-inclusive fixed lump sum price and provided in Jordanian Dinars (JD). All prices are inclusive of all fees, finance rate and taxes. All prices are for site delivery.

**Project Total Cost (Lump Sum Contract Amount) for the total compensation for the whole WORK contemplated under this proposal: [ JD]**

**The bidder is required to finance lump sum cost of the project according to Annex 5.5**

Services	Amount
Mobile Application and Portal Delivery	
Required Licensees (if any)	
Infrastructure component	
Information Security	
Customer journey Experience standard and quality standard	
Operations Support, Maintenance and Warranty	
Project Management	
Quality Management	
Total	

**Total Amount in Words: (Only -----  
-----Jordanian Dinars)**

***Project Detailed Cost:***

***1. Mobile Application and Portal Delivery:***

Mobile Application and Portal Delivery	Re-source	Unit cost (man day cost) <u>per re-source</u>	Number of Units (man days) per re-source	Total Cost	Comments
	<i>Skill 1</i>				
	<i>Skill 2</i>				
	<i>Skill N</i>				
	<i>Skill 1</i>				
	<i>Skill 2</i>				
	<i>Skill N</i>				
	<i>Skill 1</i>				
	<i>Skill 2</i>				
	<i>Skill N</i>				
<b>TOTAL</b>					

Total Amount in Words: (Only -----  
-----Jordanian Dinars)

## 2. Integration points with stakeholders mentioned in section 2.1.2

Integration points with stakeholders	Re-source	Unit cost (man day cost)	Number of Units (man days)	Total Cost	Comments
<i>[ List all activities associated with Integration points with stakeholders ]</i>	<i>Skill 1</i>				
	<i>Skill 2</i>				
	<i>Skill N</i>				

<b>TOTAL</b>	
--------------	--

**Total Amount in Words: (Only -----  
-----Jordanian Dinars)**

**1. ITEMS requested to be costed separately (If any )**

	<b>Re- source</b>	<b>Unit cost (man day cost)</b>	<b>Number of Units (man days)</b>	<b>Total Cost</b>	<b>Comments</b>

**2. Software Licenses (if any)**

<b>Software Supplier</b>	<b>Name of Software</b>	<b>License Metrics (i.e. by number of clients, pro- cessor power or other</b>	<b>No Li- censes</b>	<b>Unit price</b>	<b>Total</b>	<b>two years maintenance (24/7) and up- grade</b>	<b>Total (Includ- ing mainte- nance)</b>
			<b>TOTAL</b>				

(i) Use several lines in the table if the license complexity warrants

**Total Amount in Words: (Only -----  
-----Jordanian Dinars)**

### 3. Information Security:

Information Security	Resource	Unit cost (man day cost)	Number of Units (man days)	Total Cost	Comments
<i>[List all activities associated with Information Security]</i>	<i>Skill 1</i>				
	<i>Skill 2</i>				
	<i>Skill 3</i>				
	<i>Skill N</i>				
<b>TOTAL</b>					

Total Amount in Words: (Only -----  
-----Jordanian Dinars)

### 4. Knowledge Transfer Training and Customer Journey/Experience

Knowledge Transfer, and Training	Resource	Unit cost (man day cost)	Number of Units (man days)	Total Cost	Comments
<i>[ List all activities associated with Knowledge Transfer, Training and Customer Journey/Experience]</i>	<i>Skill 1</i>				
	<i>Skill 2</i>				
	<i>Skill 3</i>				
	<i>Skill N</i>				
<b>TOTAL</b>					

Total Amount in Words: (Only -----  
-----Jordanian Dinars)

5. **Operation Support, Maintenance and Warranty:**

- List all costs associated with the Operations, support and maintenance component for **36 months after obtaining the preliminary acceptance for MOJ system under the scope of this RFP**

Operations Support	Re-source	Unit cost (man day cost)	Number of Units (man days)	Total Cost	Comments
	<i>Skill 1</i>				
	<i>Skill 2</i>				
<b>TOTAL</b>					

6. **Project Management**

Project Management	Re-source	Unit cost (man day cost)	Number of Units (man days)	Total Cost	Comments
<i>[ List all activities associated with <b>Project Management</b>]</i>	<i>Skill 1</i>				
	<i>Skill 2</i>				
<b>TOTAL</b>					

Total Amount in Words: (Only -----  
-----Jordanian Dinars)

7. **Quality Management**

Quality Management	Re-source	Unit cost (man	Number of Units (man days)	Total Cost	Comments
--------------------	-----------	----------------	----------------------------	------------	----------

		day cost)			
<i>[ List all activities associated with Quality Manage- ment]</i>	<i>Skill 1</i>				
	<i>Skill 2</i>				
	<i>Skill n</i>				
<b>TOTAL</b>					

Total Amount in Words: (Only -----  
-----Jordanian Dinars)

#### 8. Other Costs (if any)

**Note (1):** The Itemized Financial Proposal will be examined prior Contract Award in order to ascertain that the items are correctly calculated. The itemized prices are for reference only and the lump sum price shall constitute all costs ...etc. incurred by the bidder for the execution of the project. Should any arithmetical error be found, it will be corrected and the Proposal Value will be amended accordingly. Modee encourages all bidders to study carefully their prices and to submit their final and lowest prices.

**Note (2):** The bidder shall also take into account that all the rates quoted in his Price Proposal shall be fixed throughout the Contract duration and that no adjustment to such rates shall be accepted by Modee, except when otherwise provided for in the Contract.



## 5.6 Joint Venture Agreement Template

### Standard Form of Joint-venture Agreement

#### JOINT-VENTURE AGREEMENT

#### اتفاقية ائتلاف

It is agreed on this  
day.....of.....2008 between:-  
..... Represented by Mr.

تم الاتفاق في هذا اليوم / / الموافق

.....

..... ويمثلها السيد

..... Represented by Mr.

..... ويمثلها السيد

.....

..... Represented by Mr.

..... ويمثلها السيد

.....

1- To form a Joint Venture to execute the works specified in the Contract of the Central Tender No. ( / )  
..... which  
was signed or to be signed with the Employer.

1- على تشكيل ائتلاف فيما بينهم لتنفيذ أشغال عقد العطاء رقم ( / ) المتعلق ب..... المبرم أو الذي سوف يبرم مع صاحب العمل.

2- All parties of the Joint Venture shall be obliged to perform all works agreed upon with the employer which are specified in the tender contract, and they are jointly and severally responsible for all works related to tender no. ( / ) and the contract pertaining thereto. Should one party fails or delays to perform its obligations either partially or totally, it shall be the responsibility of all other parties jointly and severally without reservation to execute all obligations set under the contract with the Employer to the same standards specified by the contract .

2- يلتزم جميع أطراف الائتلاف بإنجاز جميع الأشغال المتفق عليها مع صاحب العمل والمنصوص عليها في عقد العطاء ويكونون متضامنين ومتكافلين في مسؤولياتهم نحو صاحب العمل فيما يخص كافة الأشغال المتعلقة بالعطاء رقم ( / ) والعقد الخاص به. وفي حالة تخلف أو تأخر أحد أطراف الائتلاف عن إنجاز المسؤوليات المناطة به تنفيذها جزئياً أو كلياً يلتزم بقية الأطراف مجتمعين و / أو منفردين دون تحفظ بإنجاز جميع الالتزامات المحددة بالعقد الموقع مع صاحب العمل بالشكل المتفق عليه في العقد.

3- The parties to the Joint Venture nominate ..... as leader of the Joint Venture. Any correspondence between the Employer and the parties to the Joint Venture shall be addressed to such leader.

3- يعين أطراف الائتلاف رئيساً للائتلاف،..... لإدارة العطاء رقم ( / ) ، وأي مراسلات تتم بين صاحب العمل والائتلاف، التجمع أو المشاركة توجه إليه

4- يسمى أطراف الائتلاف السيد ..... ممثلاً لرئيس الائتلاف ومفوضاً بالتوقيع نيابة عن الائتلاف على كافة الأوراق والعقود الخاصة بالعطاء رقم ( / ) وبتمثيل الائتلاف أمام المحاكم المختصة والدوائر الرسمية وغير الرسمية في كافة الأمور العقدية والإدارية والمالية والقضائية المتعلقة بالعطاء رقم ( / ) والعقد الخاص به .

4- The parties to the Joint Venture nominate Mr..... as a representative of the leader and he is authorized to sign on behalf of the Joint Venture all documents and contracts related to tender no. (     /     ), and to represent the Joint Venture before all competent courts and non official bodies in all contractual, administrative , financial and legal issues related to tender No. (     /     ) and the contract pertaining thereto .

5- The parties to the Joint Venture have no right to terminate this agreement or substitute the leader's representative until the works awarded to them by the contract to this tender are completed and shall remain responsible before the employer until the works are finally taken over as per the conditions of taking over specified in the Tender / Contract documents .

6- This agreement is written in both Languages Arabic and English should any discrepancy in interpretation arise the Arabic text shall be considered the authentic.

5- لا يحق لأطراف الائتلاف أو أي طرف فيه فسخ الائتلاف فيما بينهم أو تبديل ممثل رئيس الائتلاف إلا بعد انتهاء الأشغال المحالة عليهم بموجب العقد الخاص بهذا العطاء وتكون مسئولياتهم تجاه صاحب العمل قائمه إلى حين تسليم الأشغال استلاماً نهائياً حسب شروط الاستلام المحددة في وثائق العقد / العطاء

6- حررت هذه الاتفاقية باللغتين العربية والإنجليزية في حالة نشوء أي اختلاف في تفسير أي من بنودها تعتبر لغة العقد المعتمدة هي اللغة العربية وملزمة للطرفين

الطرف الثالث

الطرف الثاني

الطرف الأول

Third Party

Second Party

First Party

.....

.....

.....

توقيع الشخص المخول  
بالتوقيع قانونياً  
**Signature of the  
Authorized Personnel**

.....

.....

.....

الخاتم  
المعتمد  
**Seal**

## 5.7 Confidentiality Undertaken

### **Confidentiality Undertaking**

This Undertaking is made on [DATE] by [NAME] “[Consultant]” to the benefit of MOJ , “[Principal]” [Entity Address].

**WHEREAS**, MOJ possesses certain financial, technical, administrative and other valuable Information (referred to hereinafter as Confidential Information)

**WHEREAS**, [Consultant], while performing certain tasks required by the Principal in connection with the ..... (The Project), did access such Confidential Information,

**WHEREAS**, the Principal considers the Confidential Information to be confidential and proprietary.

#### **Confidential Information:**

As used in this Agreement, the term “Confidential Information” means all information, transmitted by Principal or any of its subsidiaries, affiliates, agents, representatives, offices and their respective personnel, consultants and winning bidders, that is disclosed to the Winning bidder or coming to his knowledge in the course of evaluating and/or implementing the Project and shall include all information in any form whether oral, electronic, written, type written or printed form. Confidential Information shall mean information not generally known outside the Principal, it does not include information that is now in or hereafter enters the public domain without a breach of this Agreement or information or information known to Winning bidder by Third Party who did not acquire this information from Principal”.

The Consultant hereby acknowledges and agrees that;

- (1) The Confidential Information will be retained in the Principal’s premises and will not be moved without the express written consent of the Principal. All Confidential Information shall be and remain the property of the Principal, and such Confidential Information and any

- copies thereof, as well as any summaries thereof, shall be promptly returned to the Principal upon written request and/or destroyed at the Principal's option without retaining any copies. The Winning bidder shall not use the Confidential Information for any purpose after the Project.
- (2) It will use all reasonable means and effort, not less than that used to protect its own proprietary information, to safeguard the Confidential Information.
  - (3) The Winning bidder shall protect Confidential Information from unauthorized use, publication or disclosure.
  - (4) It will not, directly or indirectly, show or otherwise disclose, publish, communicate, discuss, announce, make available the contents of the Confidential Information or any part thereof to any other person or entity except as authorized in writing by the Principal.
  - (5) It will make no copies or reproduce the Confidential Information, except after the Principal's written consent.

**Remedy and damages:**

The Winning bidder acknowledges that monetary damages for unauthorized disclosure may not be less than 20% of the Project and that Principal shall be entitled, in addition to monetary damages and without waiving any other rights or remedies, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

**Employee Access and Control of Information**

It is understood that the Winning bidder might need from time to time to discuss the details of confidential Information with other individuals employed within its own or associated companies in order to support, evaluate, and/or advance the interests of the subject business transaction. Any such discussion will be kept to a minimum, and the details disclosed only on a need to know basis. Prior to any such discussion, the Winning bidder shall inform each such individual of the proprietary and confidential nature of the Confidential Information and of the Winning bidder's obligations under this Agreement. Each such individual shall also be informed that by accepting such access, he thereby agrees to be bound by the provisions of this Agreement. Furthermore, by allowing any such access, the Winning bidder agrees to be and remain jointly and

severally liable for any disclosure by any such individual that is not in accordance with this Agreement.

### **Miscellaneous**

The obligations and rights of the Parties shall be binding on and inure to the benefit of their respective heirs, successors, assigns, and affiliates. This Agreement may be amended or modified only by a subsequent agreement in writing signed by both parties. Winning bidder may not transfer or assign the Agreement or part thereof. No provision of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of the Principal, its agents or employees, nor shall any waiver of any provision of this Agreement constitute a waiver of any other provision(s) or of the same provision on another occasion. This Agreement shall be construed and enforced according to Jordanian Law. The Winning bidder hereby agrees to the jurisdiction of the Courts of Amman, Jordan and to the jurisdiction of any courts where the Principal deems it appropriate or necessary to enforce its rights under this Agreement.

### **Term of Agreement**

The obligations of the parties under this Agreement shall continue and survive the completion of the Project and shall remain binding even if any or all of the parties abandon their efforts to undertake or continue the Project.

IN WITNESS WHEREOF, the Winning bidder hereto has executed this Agreement on the date first written above.

**Consultant:**

**By:** \_\_\_\_\_

**Authorized Officer**

## 5.8 Key RFPs Dates & Deadlines

ITEM	DATE (DD/MM/YY)
Date of RFP distribution	ON JONEPS
Deadline for submission of bidders' questions to RFP	ON JONEPS
Expected date for answers to bidders' questions	ON JONEPS
Proposal deadline	10/9/2025

## 5.9 Support Procedures & Policies

### **Severity Levels:**

#### ➤ **Severity One (Urgent)**

A severity one (1) issue is a catastrophic production problem which may severely impact the Required Service\Solution Availability, In such case, part or all Required Service\Solution production components are down or not functioning; loss of production data and no procedural work around exists.

#### ➤ **Severity Two (High)**

A severity two (2) issue is a problem where the Required Service\Solution is functioning but in a severely reduced capacity. The situation is causing significant impact to portions of business operations and productivity of Required Service\Solution. The system is exposed to potential loss or interruption of service.

#### ➤ **Severity Three (Medium)**

A severity three (3) issue is a medium-to-low impact problem which involves partial non-critical functionality loss one which impairs some operations but allows the Required Service\Solution users/administrators to continue to function. This may be a minor issue with limited loss or no loss of functionality or impact to the client's operation and issues in which there is an easy circumvention or avoidance by the end user.

#### ➤ **Severity Four (Low)**

Important problem but it can wait no loss of functionality or impact to the client's operation and issues in which there is an easy circumvention or avoidance by the end user.

**Table 1: Response, Resolution, times for different severity levels**

Severity	Response Time	Resolution Time
1	1 hour	8 hours.
2	2 hours	24 hours
3	4 hours	3 working days
4	8 hours	5 working days

\* Support is required to be 24x7 basis for severities 1&2 while 7X5 basis for severities 3&4

**Response Time:** Time taken to acknowledge receiving of reported incident calculated from the time sending an email explaining the incident, opening a ticket on bidder ticketing system, or conducting a phone call with the assigned support engineer by the bidder or bidder's first line of support.

**Resolution Time:** Time taken to solve the reported incident completely. Resolution Time is calculated from the end of the defined response time for each severity level as shown in the above table.

\* Releasing new version of the application on mobile phone stores will not considered from the resolution time as long as the winning bidder submitted the approved version to the mobile phone store and waiting the approve from the store.

#### **5.9.1 Escalation Procedures & Penalties**

For incidents classified as Severity Level 1, 2, 3 & 4, if bidder:

1. Passed the Response Time: first level of escalation will be applied by notifying bidder's Technical Support Manager or the assigned contact person.
2. Passed the Resolution Time: if no accepted reason form MOJ then, MOJ is entitled to fix the problem and to apply penalty on the winning bidder in accordance with the following criteria in the below table and all costs incurred by MOJ for fixing the problem will be charged to the winning bidder and deducted from his dues or the performance/maintenance bond

**Table 2: Penalties**

Severity	Definition	Penalty
----------	------------	---------

1	Must be done, essential to business survival. Business can't continue	A penalty of 24 J.D. shall be applied for each day or part of day pass the resolution time. This penalty will be applied until resolving the incident. After 2 days, if the incident not resolved then MOJ have the right to called 3rd party to resolve the incident and all cost incurred by MOJ for fixing the problem will be charged to winning bidder in addition to above penalites.
2	Should be done, near essential to business survival.	A penalty of 20 J.D. shall be applied for each day pass the resolution time. This penalty will be applied until resolving the incident. After 3 days, if the incident not resolved then MOJ have the right to called 3rd party to resolve the incident and all cost incurred by MOJ for fixing the problem will be charged to winning bidder in addition to above penalites.
3	Could be done, high benefit to business if time and resources are available.	A penalty of 16J.D. shall be applied for each day pass the resolution time. This penalty will be applied until resolving the incident. After 4 days, if the incident not resolved then MOJ have the right to called 3rd party to resolve the incident and all cost incurred by MOJ for fixing the problem will be charged to winning bidder in addition to above penalites.
4	Important problem but can wait	A penalty of 10 J.D. shall be applied for each day pass the resolution time. This penalty will be applied until resolving the incident. After 5 days, if the incident not resolved then MOJ have the right to called 3rd party to resolve the incident and all cost incurred by MOJ for fixing the problem will be charged to winning



		bidder in addition to above penalites.
--	--	---

#### 5.10 [Sample Arabic Contract Agreement \(Attached\)](#)

<Sample contract in Arabic attached>

## 5.11 customer journey Experience standard and quality standard

الرقم	المعيار	تطبيق المعيار
1.1 شمولية برامج تصفح الانترنت ( Browser Compatibility ) مثل:		
1.1.1	الخدمة الإلكترونية تعمل بكفاءة على برنامج تصفح الانترنت المدعوم "Google Chrome"	
1.1.2	الخدمة الإلكترونية تعمل بكفاءة على برنامج تصفح الانترنت المدعوم "Mozilla Firefox"	
1.1.3	الخدمة الإلكترونية تعمل بكفاءة على برنامج تصفح الانترنت المدعوم " Microsoft Edge "	
1.1.4	الخدمة الإلكترونية تعمل بكفاءة على برنامج تصفح الانترنت المدعوم "SAFARI"	
1.2 خاصية الاستجابة و الاستخدامات المتعددة ( Responsiveness and Capability Cross-Platform ) : إمكانية استخدام واستعراض الخدمات الإلكترونية عن طريق كافة الوسائط الالكترونية		
1.2.1	الاستجابة على الكمبيوتر/اللاب توب: ● توافق وظهور الأقسام والحقول والأزرار بشكل كامل ومرتب واستخدامها بسهولة، للاتجاهين العمودي والأفقي. ظهورها على جميع أنواع و أحجام الأجهزة المدعومة.	
1.2.2	الاستجابة على الأجهزة اللوحية ● توافق وظهور الأقسام والحقول والأزرار بشكل كامل ومرتب واستخدامها بسهولة، للاتجاهين العمودي والأفقي. ● ظهورها على أنواع و أحجام الأجهزة المدعومة المختلفة.	
1.2.3	الاستجابة على أجهزة الموبايل ● توافق وظهور الأقسام والحقول والأزرار بشكل كامل ومرتب واستخدامها بسهولة، للاتجاهين العمودي والأفقي. ● ظهورها على أنواع و أحجام الأجهزة المدعومة المختلفة.	
1.3 ربط و تكامل الأنظمة ( System Integration )		
1.3.1	الخدمة الإلكترونية مبربطة مع جميع الأنظمة ذات العلاقة الضرورية لعمل الخدمة أو لتسهيل استخدام الخدمة مثل (CRM, Billing, payments Gateway, CSPD) ويتعين على مزود الخدمة الاحتفاظ بسجل حول كافة الإجراءات التي تتم عبر هذه الأنظمة (يتم تحديد بند خاص لكل تكامل مع جهة معينة حسب نطاق عمل كل خدمة. مثال البنود أدناه):	
1.3.2	التكامل مع الأحوال المدنية (CSPD)	
1.3.3	التكامل مع بوابة الدفع الالكتروني اي فواتيركم (payments Gateway)	
1.3.4	التكامل مع (CRM)	
1.4 تطبيقات الهاتف النقال ( Mobile App ) :تأكيد تكامل وربط الخدمة على تطبيق سند		
1.4.1	قابلية الاستخدام بسهولة ووضوح على نظام التشغيل: Android	
1.4.2	قابلية الاستخدام بسهولة ووضوح على نظام التشغيل : IOS	
1.4.3	قابلية الاستخدام بسهولة ووضوح على نظام التشغيل : Huawei	

1.5 الوقت اللازم للتحميل ( Load Time )	
1.5.1	وقت التحميل الخاص بالصفحات ووقت التنقل بين الصفحة الرئيسية مع الصفحات المرتبطة بها يجب ان يكون خلال 7 ثواني كحد أقصى من خلال الويب و من 4-5 ثواني من الموبايل والجهزة اللوحية، مع التأكد من استخدام تطبيقات وبرامج متخصصة باختبار سرعة التحميل.
1.6 تحليلات غوغل (Google Analytics):	
ربط الخدمة الالكترونية مع تحليلات غوغل Google Analytics	

## 2- الخصائص و المميزات (Features):

الرقم	المعيار	تطبيق المعيار
2.1 متعددة اللغة ( Bi-Lingual )		
2.1.1	الخدمة الإلكترونية متوفرة باللغة العربية بشكل صحيح من حيث الصياغة و الوظائف و ضمان توحيد نوع الخط.	
2.1.2	الخدمة الإلكترونية متوفرة باللغة الإنجليزية بشكل صحيح من حيث الصياغة و الوظائف و ضمان توحيد نوع الخط ( اذا لم يكن خيار اللغة الانجليزية موجوداً بنطاق عمل المشروع، يجب أن لا يكون الخيار متوفراً على أي من الشاشات الخاصة بالخدمة).	
2.1.3	محرك البحث (Search Engine) الخدمات الالكترونية تحتوي على محرك بحث يمكنه البحث والتحقق من الكلمات الرئيسية و الخيارات المتعددة عند الحاجة إلى ذلك، توفر الخدمة على محركات البحث العالمية مثل: Google	
2.3 التقييم ورصد آراء المستخدمين (Rating and feedback forms)		
2.3.1	الخدمة الالكترونية توفر خيار التقييم للمستخدم لقياس مدى رضى مستخدم الخدمة (بخدمتكم لأنه واجبنا) حتى يتمكن مستخدم الخدمة من إضافة ملاحظات و أسئلة.	
2.3.2	وضع رقم مركز الاتصال الوطني في حال ورود أي استفسارات أو شكاوي 06-5008080 بالربط مع هذه الوظيفة على موقع الحكومة الإلكترونية.	
2.4 الربط مع حسابات مواقع التواصل الاجتماعي		
يتم تزويد روابط فعالة لكافة قنوات التواصل الاجتماعي لل (المؤسسة الحكومية أو الحكومة الالكترونية) بالربط مع هذه الوظيفة على موقع الحكومة الإلكترونية		
2.5 رسالة التأكيد اللحظي على الشاشة ( On-Screen Message Confirmation )		
يتم عرض رسالة توضح إما إتمام العملية أو عدمه على الشاشة لكل إجراء يقوم به مستخدم الخدمة لتبليغ المستخدم نتيجة الإجراء الذي قام به و الخطوات القادمة المطلوبة من المستخدم		
2.6 الصفحة الرئيسية (Home Page)		
سهولة التنقل بين الصفحات من خلال زر "رجوع" و زر "التالي" وتوفر أيقونة الصفحة الرئيسية على كافة الصفحات حتى تساعد مستخدم الخدمة على التنقل بسهولة		

### 3- المصادقة والتحقق (Validation, Verification):

الرقم	المعيار	تطبيق المعايير
3.1	<b>فحص الوظائف (Functionalities)</b> كافة وظائف الخدمة تم فحصها بشكل كامل وتعمل بنجاح (بناء على نتائج فحص الجودة).	
3.2	<b>فحص الروابط (Links- URLs)</b> كافة الروابط تعمل و يتم تحميلها بنجاح.	
3.3	<b>مجموعة تجربة المستخدم:</b> (من ضمن مدخلات وزارة الريادة والاقتصاد الرقمي للتأكد من صحته وإرسال دليل) تم عقد جلسة لتجربة المستخدم (10-20 شخص من مختلف الفئات) لتقييم تقبل مستخدم الخدمة للخدمة.	

### 4- دليل المستخدم (User Manual):

الرقم	المعيار	تطبيق المعيار
4.1	<ul style="list-style-type: none"> <li>توفير دليل مستخدم واضح وبدون اخطاء املائية يتضمن خطوات استخدام الخدمة، ويجب أن يتضمن الدليل الكتابي على صور عملية تشرح كيفية استخدام الخدمة الإلكترونية لمساعدة المستخدم أثناء استخدامه للخدمة</li> <li>توفير فيديو تعليمي يوضح خطوات الاستخدام (توفير فيديوهات تعليمية مع شرح صوتي أو كتابة توضيحية توضح بشكل كامل خطوات الاستخدام للخدمات)</li> </ul>	

### 5- معلومات مستخدم الخدمة (Customer Information):

الرقم	المعيار	تطبيق المعيار
5.1	<b>فحص إمكانية الدخول اسم المستخدم/ كلمة المرور</b> الخدمة الإلكترونية تطبق الدخول الموحد من بوابة الحكومة الإلكترونية باستخدام الرقم الوطني/ كلمة المرور (IDM sign in)	

### 6 - هندسة/ هيكلية المعلومات (Information Architecture):

الرقم	المعيار	تطبيق المعيار
6.1	<b>الخط والألوان (Fonts &amp; color Schemes)</b> محتوى الخدمة الإلكترونية موحد من ناحية الخط (النوع) والألوان مع محتوى الموقع الإلكتروني للمؤسسة أو موقع بوابة الحكومة الإلكترونية ضمن معايير المواقع الإلكترونية للمؤسسات الحكومية للتمكن من اعطاء تناسق الشكل و المظهر لكافة خدمات الإلكترونية.	
6.2	<b>الملكية (Ownership)</b> الخدمة الإلكترونية تظهر بوضوح ملكية المؤسسة الخاصة بها ، و أنها جزء من خدمات الحكومة الإلكترونية من خلال إضافة الشعارات المشتركة و ذلك على مستوى كافة الخدمات.	

6.3	<b>هيكلية الصفحات (Information Structure)</b> ترتيب المعلومات (روابط، القوائم المنسدلة، القوائم) بطريقة تمكن مستخدم الخدمة الوصول للمعلومات المطلوبة من خلال 5 نقرات كحد أقصى.
6.4	<b>التلميحات و رسائل الخطأ (Tooltips and Error messages)</b> ظهور التلميحات و رسائل الخطأ بالوقت الصحيح و بصيغة تمكن مستخدم الخدمة من معرفة ما هو مطلوب فوراً .
6.5	<b>الصور و البانرز (Images and Banners)</b> استخدام صور وشعارات و بانرز ذات درجة وضوح عالية في أي خدمة إلكترونية.

#### 7- سهولة الاستخدام (Usability-UX/UI) :

الرقم	المعيار	تطبيق المعيار
7.1	<b>كفاءة الاستخدام:</b> سهولة استخدام الخدمة بدون وجود معيقات لإتمام الخدمة.	
7.2	التصميم العام للخدمة واضح و مفهوم للمستخدم و يسهل تعلم استخدامها و التجول فيها و مناسب للمستخدم المستهدف.	
7.3	تواجد الوظائف الأساسية في أماكن متوقعة و سهل الوصول إليها، مع توضيحات كافية بخصوص الخدمة أو الوظيفة.	
7.4	وضوح تسمية المصطلحات المستخدمة في الخدمة بما يتناسب مع وظائفها.	

#### 8- مميزات ذوي الاحتياجات الخاصة:

الرقم	المعيار	تطبيق المعيار
8.1	خاصية تكبير وتصغير الخط	
8.2	خاصية قارئ الشاشة	
8.3	خاصية التحكم بتفاوت الوان و لمعان الشاشة و صفاء اللون	
8.4	خاصية تباعد المسافات بين الكلمات	

#### 9- التواصل مع متلقي الخدمة (SMS & Emails) :

الرقم	المعيار	تطبيق المعيار

	الرسائل النصية (SMS)	9.1	<ul style="list-style-type: none"> <li>● صياغة النص صحيحة لغوية باللغة المناسبة ومعبرة واحترافية.</li> <li>● مرسل الرسالة تبعيته واضحة للجهة الرسمية الحكومية المعنية</li> <li>● النص يحتوي على المعلومات الهامة لمتابعة الطلب (مثلاً رقم الطلب، او حالته، او روابط محددة للدخول لها...الخ حسب طبيعة الخدمة).</li> <li>● في حال كانت تحتوي على رمز تفعيل يجب توضيح مدة صلاحيته والاحتفاظ بها حسب الحاجة</li> </ul>
	البريد الإلكتروني ((Emails	9.2	<ul style="list-style-type: none"> <li>● صياغة النص صحيحة لغوية باللغة المناسبة ومعبرة واحترافية.</li> <li>● مرسل الرسالة تبعيته واضحة للجهة الرسمية الحكومية المعنية</li> <li>● النص يحتوي على المعلومات الهامة لمتابعة الطلب (مثلاً رقم الطلب، او حالته، او روابط محددة للدخول لها...الخ حسب طبيعة الخدمة).</li> <li>● في حال كانت تحتوي على رمز تفعيل يجب توضيح مدة صلاحيته و الاحتفاظ بها حسب الحاجة</li> <li>● وجود شعار الجهة الرسمية الحكومية و أن البريد الالكتروني تابع للخدمات الإلكترونية.</li> <li>● جملة ترحيبية بمتلقي الخدمة، مع مراعاة جنسه (مثلاً: السيد/ة).</li> <li>● إتجاه النص سليم وفقاً للغة المناسبة.</li> <li>● عدم استخدام ألوان تحذيرية كالأحمر</li> <li>● عدم استخدام أنواع خطوط غير متداولة أو غير واضحة،</li> <li>● عدم استخدام التأثيرات إلا عند الحاجة فقط (مثلاً الخط Bold).</li> <li>● وجود معلومات التواصل ليستخدمها متلقي الخدمة في حال كان لديه استفسار او واجه مشكلة.</li> </ul>

## 10- قنوات الدفع

الرقم	المعيار	تطبيق المعيار
10	الربط مع الدفع الإلكتروني	

## 11- التكامل والربط

الرقم	المعيار	تطبيق المعيار
11.1	الربط مع الدخول الموحد (سند) (للأردنيين المقيمين)	
11.2	في حال وجود تسجيل للشركات والمؤسسات الى النظام يجب ادخال المعلومات التالية لاسترجاع بيانات المنشأة: 1- الرقم الوطني للمنشأة 2- تاريخ انشاء المنشأة	
11.3	ربط دخول موظفين لل-backend system بال Active directory	

11.4	يجب استرجاع جميع الوثائق المطلوبة من خلال الربط و في حال وجود وثائق بحاجة لارفاق يجب تزويدنا بها لأخذ الموافقة عليها
11.5	الربط مع التوقيع الرقمي في حال وجد وثائق او مخرجات تحتاج الى توقيع
11.6	مخرجات الخدمة يجي ان تحتوي على QR CODE MODEE

## 12- متطلبات بدء فحص القبول

الرقم	المعيار	تطبيق المعيار
12.1	يجب اضافة بطاقة خدمة وأن تظهر بعد اختيار الخدمة وقبل تقديم الطلب، يجب ان تحتوي بطاقة الخدمة على ما يلي: 1.- شروط تقديم الخدمة 2. الوثائق المطلوبة 3. الرسوم ان وجدت 4. الزمن المعياري لتقديم الخدمة	
12.2	اضافة إقرار بصحة البيانات وبالصيغة التالية: <input type="checkbox"/> أتعهد بصحة البيانات المدخلة ووافق على استرجاع بياناتي الشخصية والاطلاع عليها ومعالجتها من قبل الجهات والأطراف المعنية ذات العلاقة، وذلك لغايات التقديم والحصول على الخدمة. " I confirm that the data entered is accurate, and I agree to have my personal data retrieved, viewed, and processed by the relevant authorities and parties concerned for the purposes of applying for and obtaining the service. ملاحظة: تم اضافة الإقرار في الشاشة التي توضح تعليمات استخدام الخدمة بحيث يتم إضافة checkbox تتضمن هذه الصيغة وبعد الموافقة من قبل المستخدم يتمكن من الدخول للخدمات ويكون متطلب إجباري.	
12.3	الموافقة على تصميم ومحتوى والصيغة القانونية للمخرج (الشهادة، الرخصة..) من المؤسسة باللغتين العربية والانجليزية	
12.4	الفحص مع المؤسسة وأخذ الموافقة على شاشات الخدمة	
12.5	ان يتم السماح بإرفاق ملفات بالصيغ التالية فقط: - امتداد PDF - امتدادات images	
12.6	توفير وثيقة متطلبات النظام (SRS,BRD) نهائية وموافق عليها	
12.7	توفير حالات فحص مطابقة مع وثيقة متطلبات النظام مع البيانات الخاصة بها	

	توفير رابط الفحص على البيئة التجريبية وعدم إجراء أي تعديل أثناء عملية الفحص	12.8
	توفير قائمة web\ x form والتأكد أنها تعمل بالطريقة الصحيحة (ملاحظة : ال Web\X Form هي الشاشات المبنية لإدخال موافقات أو طلب معلومات من الجهات التي لا يتوفر ربط مباشر معها أو لا تتوفر المعلومة المطلوبة في الرابط الموجود)	12.9

### 5.12 SAML configuration

The configuration of a SAML federation takes place through the exchange of metadata between Identity Provider (IdP) and Service Provider (SP).

The metadata is a file that contains the information of the environment and must contain at least the following information:

- Entity ID - a globally unique identifier used in software configurations
- Cryptographic Keys - the key that is used to sign or encrypt SAML tokens
- Protocol Endpoints (bindings and locations) - the URLs where authentication (SingleSignOnService) and logout (SingleLogoutService) is performed with the related supported protocols (REDIRECT - POST - ARTIFACT)

The steps to configure a federation are:

1. The SP generates the metadata file and sends it to the IdP (IDM Team): the metadata will contain the information of the SP environment such as EntityID, Cryptographic Key, Protocol Endpoints
2. the IdP generates the metadata file and sends it to the SP: the metadata will contain the information of the IdP environment such as EntityID, Cryptographic Key, Protocol Endpoints
3. The SP imports the metadata of the IdP in its environment and configures the federation: the association of the 2 entities (SP - IdP) takes place and the subsequent authentication calls will follow the SAML standards.  
Example: in the authentication request (AuthnRequest), the Issuer tag must be set with the EntityID stored in the metadata of the SP
4. The IdP imports the metadata of the IdP in its environment and configures the federation: the association of the 2 entities (IdP - SP) takes place and the subsequent authentication calls will follow the SAML standards.

### 5.13 Questions and Answers Template

DIGITAL TRANSFORMATION PROJECT FOR THE MINISTRY OF FOREIGN AFFAIRS and EXPATRIATES (MOJ )

**Tender No. ()**

Taking into consideration the requirements outlined in the RFP and this Q&A document, bidders need to respond based on their experience in projects of similar size and scope

<b>Q1</b>	
<b>A1</b>	--



<b>Q2</b>	
<b>A2</b>	--
<b>Q3</b>	

#### 5.14 E-Service Performance KPI's

The below stated MODEE KPIs values to be achieved over internet for non-cached pages, cached numbers should be much less, also many on the numbers depends on gateway bandwidth at MODEE. The below sections act as the accepted thresholds for all MODEE developed websites and vendor should assure they are in comply with these guidelines before requesting Performance and stress test from MODEE.

<b>Performance Metrics for E-services Criteria / Element</b>	<b>Description</b>	<b>Value / Measurement</b>
Time to First Byte	Time elapsed for the first byte of a website to make it to the visitor's browser	Less than 3 sec
Time to Last Byte	Time elapsed when every byte of a website has made it to the visitor's browser	Less than 6-9 sec
Time to Connect	Time elapsed from initial request to when the connection between the visitor's browser and an origin server is established	Less than 2 sec
Page Load Time ( for both E-services and Informational Wesbites)	Page load time is the average amount of time it takes for a page to appear on your client's screen. To measure page load time, you should be testing website speed using available tools.	Largest Concertful Paint (LCP): should occur within 3 seconds of when the page first starts loading. First Input Delay (FID): pages should have a FID of 200 milliseconds or less. Cumulative Layout Shift (CLS): pages should maintain a CLS of 0.1. or less.
Time to Start Render	Time elapsed when the first visible element appears on the blank page	Less than 6 sec
Throughput:	The quantity of useful work	[15 request/second]

### Content Complexity Metrics for E-services

Criteria / Element	Description	Value / Measurement
Capacity	The capability of the newer system to handle a number of simultaneous requests from the network for the application and the volume of data that it can handle from each of the users (Internal users through the LAN as well as external users through the internet/ dedicated WAN). In addition to the H/W capacity such as processing capability of all servers including DB, Apps. [CPU Utilization: 80%, Memory Utilization: 80%.	
Weight Basis		
<b>Page Weight</b>	Total weight of assets including requests, domains, HTML, JavaScript, CSS, images, media and others	Not exceeding 2 – 4.5 MB
<b>JS Weight</b>	Weight of Java Scripts	Not exceeding 1600 KB
<b>CSS Weight</b>	Weight of Cascading Style Sheets	Not exceeding 1800 KB
<b>Image Weight</b>	Weight of site images	Not exceeding 1.75- 2.5 MB
Count Basis		
<b>Asset Count</b>	Total number of assets including requests, domains, HTML, JavaScript, CSS, images, media and others	Not more than 100
<b>Image Count</b>	Images count in a site	Less than 50

- For Informative websites that need to have higher asset resources CDN network should be used.
- For any web services that used Video asset CDN network should be used.

### Site Availability and Access Metrics:

Criteria / Element	Description	Value / Measurement
<b>Uptime (Availability) in stress test</b>	System availability uptime vs. system downtime within Stress test	99 %
<b>Active Users</b>	The number of concurrent users that the website should be handled during the load test, with lowest error rate ratio.	The number of concurrent users will be determined during the project initiation phase. If not mentioned, the default value will be 200 users. Error rate less than 0.9%

### 5.15 SDLC Security Minimum Requirements

The following are baseline security requirements that are set to help developer teams and architects deliver a secure system to MoDEE.

These requirements should be fulfilled in addition to:

- 1- the requirements of previous contracts; i.e. the RFP and Information Security component, and
- 2- all the remediation recommendations resulting from the penetration tests.

#	Item
<b>OWASP Top 10, do all the required to protect the e-services against:</b>	
<b>1.</b>	<p>The delivered system should be protected and secured against OWASP Top 10</p> <ol style="list-style-type: none"> <li>1. <u>1. Broken Access Control</u></li> <li>2. <u>2. Cryptographic Failure</u></li> <li>3. <u>3. Injection</u></li> <li>4. <u>4. Insecure Design</u></li> <li>5. <u>5. Security Misconfiguration</u></li> <li>6. <u>6. Vulnerable and Outdated Components</u></li> <li>7. <u>7. Identification and Authentication Failure</u></li> <li>8. <u>8. Software and Data Integrity Failure++++</u></li> <li>9. <u>9. Security Logging and Monitoring Features</u></li> <li>10. <u>10 Server-Side Request Forgery</u></li> </ol>
<b>2.</b>	The system should pass the penetration test by MoDEE

<b>HTTPS protocol</b>	
<b>3.</b>	Use HTTPS protocol on login and sensitive data transfer pages
<b>Software Updates</b>	
<b>4.</b>	Make sure that all SW components used in development are updated and supported by security patches.
<b>5.</b>	Make sure that all used platforms on servers and back-end officers are up to date and supported by security patches.
<b>6.</b>	Use the latest version of communication protocols; secure versions
<b>Restrict File Uploads</b>	
<b>7.</b>	Validate uploaded file types on the server side
<b>8.</b>	Store files uploaded by clients in separate folders and databases
<b>9.</b>	Restrict types of uploaded files
<b>10.</b>	Ban double extension files
<b>11.</b>	Use antimalware detection like Sandboxing technology on the app and web servers.
<b>Using Captcha</b>	
<b>12.</b>	Use secure CAPTCHA that can protect against bots.
<b>13.</b>	Passing CAPTCHA is mandatory before submission
<b>14.</b>	Can the CAPTCHA use can collect as minimum user data as possible?
<b>15.</b>	Collect the user's consent before any data collection
<b>Users Passwords</b>	
<b>16.</b>	Use a strong password policy and provide strong password setting guides, For example, 8 4 Rule.
<b>17.</b>	Store passwords as encrypted hashed values?
<b>18.</b>	Lock the account locked after three failed logins
<b>Viruses and Malware</b>	
<b>19.</b>	Use antimalware on the production, Staging, and Development environment; the developer should report to the PM or system team if the antimalware does not exist or is not updated.
<b>Adjust Default Settings</b>	
<b>20.</b>	Are account configuration default settings changed for both the hosting environment and content management system
<b>Error Messages</b>	
<b>21.</b>	The error message displays information that the visitor needs, without revealing the structure of any component of the website.
<b>22.</b>	Detailed errors kept in the server log?
<b>Secure APIs</b>	
<b>23.</b>	Do APIs use HTTPS?
<b>24.</b>	Use token-based API authentication like OAuth 2.0
<b>25.</b>	Tokens should have an expiration time
<b>26.</b>	Configure limit rate on API. i.e. have a limitation on how many times the client is allowed to call it?

27.	Validate API parameters
28.	IDs should be opaque and globally unique. For example, rather than using the ID “1002 “and “1003 “use “r5t844fsg6fssf2vfrb9bd8”.
29.	Add a timestamp to the Request, so it only accepts requests within a reasonable timeframe.
30.	Filter the API-returned data on the backend side.
31.	Prevent request manipulation
32.	Publishing Swagger files is not allowed
<b>User Authentication and Authorization</b>	
33.	Use MFA authentication
34.	Use SANAD authentication services whenever possible Use LDAP protocol to validate admins on the admin portal
<b>OTP requirements</b>	
35.3	An expiry time should be added to the OTP value so that the value will expire after a certain time and the value of the expiry time should not exceed 5 minutes.
36.	A lockout feature should be implemented in case the user has inserted too many wrong OTP values in the reset password functionality.
37.	The OTP value should not be used more than once.
38.	OTP request should only hold user ID, phone number or email address should be fetched from the DB.
<b>5.11. Security Logging and Auditing</b>	
39.	Are the website security transactions audited for adequate time?
40.	Are logs securely transmitted to a preferably remote system for analysis, detection, alerting, and escalation?
41.	All system components should be time-synchronized.
<b>General</b>	
42.	Design 3-Tier Architecture
43.	Use SANAD registration and log in wherever possible
44.	Deliver a list of servers for both production and staging environments. The document should describe the functionality of these servers and should define all the ports needed on each machine in the 3 layers and the IP addresses it communicates with (to configure host-based FW)
45.	Web servers’ configuration files should not hold any application data.
46.	The system should be protected by the WAF.
47.	Hard-coded credentials are not allowed
48.	Do not publish Admin pages; these should only be used inside SGN
49.	All back-office employees should have OTP
50.	<ul style="list-style-type: none"> <li>Assure micro-segmentation is in place for all VM’s</li> <li>Antivirus in place on all VMs</li> </ul>
51.	<ul style="list-style-type: none"> <li>The system should be protected by the WAF</li> <li>X-Forwarded IP Address should be configured</li> </ul>

52.	Define all data used with its security level as defined in the Data Classification policy (embedded in (سياسة استخدام موارد تكنولوجيا المعلومات) and apply security controls as per the policy
53.C	<p>Comply to the policies:</p> <ul style="list-style-type: none"> <li>- <u>سياسة استخدام موارد تكنولوجيا المعلومات</u></li> <li>- <u>سياسة أمن الموردين</u></li> <li>- <u>سياسة أمن المعلومات العامة</u></li> <li>- <u>MODEE minimum security baseline</u></li> </ul>

- VPN connection is prohibited and if there is a need, the access should be provided from the entities only with multi-factor protected and the VPN connection must be from Jordan.

5.16 (attached) سياسة استخدام موارد تكنولوجيا المعلومات

5.17 Performance Test Checklist (Attached)