# Annex (A)

| TRC’s Technical Requirements for the E-KYC | |
|---|---|
| | |
| **I.** | **Introduction** |
| | E-KYC refers to the process of Knowing Your Customer procedure in an electronic paperless environment and involves capturing all of needed information from different types of Jordanian government issued Identification cards, Jordanian passports and foreign passports.<br>E-KYC shall also include the use of certified digital identities and facial recognition functionalities for online identity verification.<br>The intended scope of work of this E- KYC document is to establish a common base for all licensed telecom operators in the kingdom who are interested in developing, installing and implementing E-KYC solution to identify and verify the identity of their client(s) relationship and to allow their client (s) to perform remote verification, authentication and registration of new and existing telecom services subscriptions to fixed and mobile public telecommunication services through using their own smart phone mobile terminals and web portals.<br>Interested licensed operators in implementing E-KYC solution shall provide the TRC in advance with all needed supporting documentation and compliance sheets showing the full compliance and adherence of his/her potential E- KYC solution to all the requirements, functions, specifications, and capabilities set out in this reference document before commercially contracting with any potential solution vender for the supply the E-KYC platform solution. Furthermore, the licensed operators shall conduct a proof of concept for his/her proposed E-KYC solution to TRC’s evaluation committee and shall seek its formal acceptance on the proposed solution before being officially implemented and launched.<br>Failure to comply with one or more of the requirements, functions, specifications and capabilities set out in this reference document including its introduction part shall result in disqualifying the proposed E-KYC solution and the TRC will not issue an approval letter to the concerned operator to proceed with implementing the proposed E-KYC solution(s). |
| **II.** | **General Requirements** |
| **A.** | Built and implemented as a digital end-to-end platform solution complying with all governmental existing regulatory, technical and procedural guidelines and requirments. furthermore, it shall comply with those which come into force in the future from time to time. A detailed flow chart for the whole process of E-KYC shall be provided and obtain TRC approval on. |
| **B.** | Operating over different operating systems platforms that are commonly used in mobile and tablets terminals such as Android and iOS operating systems. |
| **C.** | Being Tested, operated and used by many other telecom operators. Vendors of E-KYC solutions adopted by other sectors including banking and government are considered as an advantage. |
| **D.** | E-KYC solution shall be fully operating only on-premises. |

# Annex (A)

| | |
|---|---|
| **E.** | Having proven successful use cases records  and implementations. Such records shall be provided to TRC in the form of original recommendation letters from at least two mobile network operators and/ or financial institution and/or government entities showing their E-KYC detailed scope of work or use, date of brining into use and submitting any other supporting information. |
| **F.** | Offering full administration and management through using a graphical user interface (GUI). |
| **G.** | Having web based application interface for management purposes. |
| **H.** | Operates with very a high availability on all E-KYC system components 24/7. |
| **I.** | Fully operating on licensed operator premises without any third party interaction or intrusion to the E-KYC platform. |
| **J.** | Operator to guarantee his customer accessibility to the KYC platform on 24/7 access with no down-time for on boarding clients (availability 99.99%). However, the E-KYC system availability shall comply with other systems availability of MoDEE as stated in the agreed SLA's whenever a connection is needed to it. |
| **K.** | Operate for customers as a mobile application. Additional operation on a standalone web-portal is considered as an advantage.  It shall also be available as an API and as an SDK for licensed operator. |
| **L.** | Provides seamless experience and complete process from authentication to archiving. |
| **M.** | An echo friendly solution with online electronic archiving for all consumers captured information. |
| **N.** | Online dashboard providing local and remote monitoring and generation of customizable reports needed. Search and filter functions of data reports shall be available. Data provided on-line shall be available for two years time. Other data shall be provided offline by other listed approaches. |
| **O.** | Ability to generate reports at standard file formats including but not limited to CSV,XLS, XML and at:<br>1. Real time / on line basis ( For two year duration)<br>2. In background (when evaluation is time-consuming)<br>3. Via batch processing  ( Sent upon request)<br>4. Specific date (Sent upon request)<br>5. Regular time interval  (Sent upon request) |
| **P.** | Shall  implement Authentication Application Programming Interface (API) development to allow integration with the operators or entities to offer seamless online experience and interconnection with civil status and passport department (CSPD) ,Public Security Directorate (PSD) and with any other approved entitity by TRC . Offline capability shall also be available and only used during API data servers downtime. |
| **Q.** | Short time (Less than five minutes) for onboardi ng  customers prcoess  with  high success rate. Support high registration volumes / users increases without compromising on the response time. |

# Annex (A)

| | |
|---|---|
| **R.** | Customer acceptance policy. Access to E-KYC data is subject to the consent of the customer being provided. |
| **S.** | Accessing registration services remotely and securely through purely digital channels. This wont apply for retail channels. |
| **T.** | All requests and responses shall be registered /logged for audit purposes. The logs shall capture details of customer registration process. |
| **U.** | Allow customers to:<br>1. Perform On-Line selection of one of the available packages and line number, whenever is applicable, offered by licensed network operator.<br>2. Use their own terminal camera, whenever is applicable, to capture the related service information which might inculde SIM card number, MSISDN,...etc.<br>3. Automatically generate and provide the customer an electronic copy of the subscription contract once the line is registered. |
| **V.** | Providing the customer (s) the capability to view all exsisiting registered line numbers (subscriptions) under his/her name whether it is active or inactive. This functionality shall also be implemented either on the proposed E-KYC solution or at licensed operator's mobile applications and/or electronic web sites with all needed verficiation method(s). this capability shall be made avialable at the time of launching the E-KYC. |
| **III.** | **Bidder Related Requirements ( E-KYC Platform Solution vendor)** |
| **A.** | Shall be an officially registered local company having a long term presence in the Jordanian market with local team of engineers and IT personnel capable of providing support and maintenance 24/7. |
| **B.** | Shall have proven records of experience in developing and commissioning similar software platform solutions where references shall also be provided TRC. Operator should be accounted on implementation, sharing proven records for successful use cases and implementations for any third party system/service needed. |
| **C.** | licensed Operator Shall be committed to contract for having 24/7 support with solution vendor to have a dedicated hotline number and a team with a less than one hour response time and less than 8 hours resolution for critical tasks. |
| **D.** | Operator must be committed to perform any needed customization and addition of any new requested features within (90) working days. |
| **E.** | If the solution vendor represents an international company or technology, it must provide an official letter confirming their official relationship and providing support for the project for not less than 3 years. This requirement will be applied in case of no breach of contract between the operator and solution vendor. |
| **IV.** | **Information Required** |
| **IV.1** | The proposed E-KYC solution shall support all data acquisition as stated on locally governmental issued ID's and passports for different types of clients including civilians, military and foreigners. Moreover, the system shall also support all foreign passports. |
| **IV.2** | The E- KYC software platform solution shall provide the capability to acquire and display the data listed below for establishing and maintaining a relationship between the licensed operator and customer(s): |

# Annex (A)

| | |
|---|---|
| **A.** | Full name in English and Arabic as stated on the official ID/Passport for Jordanians |
| **B.** | National number for Jordanians |
| **C.** | Customer ID/passport photo |
| **D.** | Full name and data as acquired by the PSD for non- Jordanians. |
| **E.** | Subscriber Line number MSISDN, line offer type and registration location. |
| **F.** | Activation date for Subscriber Line number MSISDN |
| **G.** | Archiving subscriber selfie photo |
| **H.** | Official registration ID issued For non-civilian subscribers including military and security personnel. For this purpose the licensed operators shall be provided the adopted templates for the list of approved ID's and have an access to validate relevant information with the concerend governmental authority. |
| **I.** | Residential address as stored on ID's |
| **J.** | Maximum allowable subscriber line (MSISDN) count number is three (3) for foreign non-Jordanians customers and thirty (30) for Jordanians from each licensed operator. |
| **V.** | **Verification and Authentication Requirements** |
| **V.1** | Integration with the Civil Status and Passports Department (CSPD), Public Security Directorate (PSD) and/ or any other TRC's approved source as an additional step of authentication and data matching. |
| **V.2** | For Identity Authentication, the solution shall support and perform the following: |
| **V.2.A.** | Security marks / genuineness validation for national IDs: implementation of Jordan ID’s “star” mark on the back of ID. Validation points: Size, Position and color. Clients photocopy of ID's/passport shall not be supported. |
| **V.2.B.** | Machine Readable Zone (MRZ) validation and data extraction from the MRZ zone of all ID documents including international passports. Validation points are:<br>1. Cross comparison of MRZ information with visual zones for Jordanian documents.<br>2. MRZ check digits<br>3. Dates and their correctness<br>4. Document format number<br>5. ISO country codes |
| **V.2.C.** | Optical Character Recognition (OCR) for ID’s and passports. |
| **V.2.D.** | Showing the result of successfully detecting and validating all the visible security marks as a percentage score of the level of assurance. |
| **V.2.E.** | Support different and configurable enrolment and security levels. |
| **V.2.F.** | Liveness and presence of the customer and the use of active anti-spoofing / protection from attacks to ensure face isn’t captured from a photo or video. |
| **V.2.G.** | Configurable functionality to check the face image against the stored one at the Civil Status and Passport Department (CSPD) database. Furthermore, it also shall be done to the images stored at the Public Security Department (PSD) database whenever it is available. |

# Annex (A)

| | |
|---|---|
| **V.2.H** | Confirmed accuracy score by an international accreditation bodies shall be above 95 % for all extracted ID's information written in English language. Furthermore, the above score value will be subject to its availability for Arabic language by such an accreditation bodies. |
| **V.2.I.** | All visual checks and MRZ analysis results will provide back general decision on document status along with the percentage score of the level of assurance. |
| **V.2.J** | Store the immutable customer consent for gathering, validating authenticating and data visibility and access with the licensed operator. |
| **V.2.K** | Have multiple user groups with configurable access privileges and E-KYC access controls on the licensed operator level. |
| **VI.** | **Security of E-KYC Software Platform Solution** |
| **A.** | The offered solution shall implement state-of-the-art international best security standards to protect operator's and costumers' data from any unauthorized access or illegal use. This shall also be applied on the standalone, mobile application/SDKs/APIs. |
| **B.** | Implemented security standards shall be highlighted and described in bidders offer. |
| **C.** | The solution shall run on native browser with additional plug-ins that should be free to use, downloadable and should support at the minimum Edge, Chrome, Firefox, etc. |
| **D.** | Should not require opening of any special protocols or ports for connecting the user client to the licensed operators's web/ application server. All communications should be performed using highly secured protocols and ports. |
| **E.** | Implement data encryption on data communication channels between the licensed operator and the customer side. Data encryption between licensed operators, CSPD and PSD shall be based on its availability from CSPD and PSD side. |
| **F.** | 1:1 Facial recognition algorithm should be listed in NIST (accuracy, Mask Matching, effect of age difference and ethnicity) |
| **G.** | Liveliness capturing should be fully comply with (Presentation Attack detection standard) such as FIDO, Google , ISO/IEC 30107-3 test cases |
| **H.** | The solution provider should study samples of Facial Images in CSPD (for Jordanian) and PSD (for foreigners) and confirms its validity for use in 1:1 facial recognition and provide the TRC with any observation, if any, to process it and to obtain highest score in comparing faces. |
| **I.** | E-KYC system shall pass intensive penetration and security tests concudted by a Third Party. Testing shall be performed in accordance with the best adopted international standards. A successfull testing completion certificate shall be provided to TRC for evaluation. |
| **VII.** | **E-KYC Mobile Application Secure Architecture** |
| **A.** | SSL Pinning should be implemented at client side so as the attackers will never be able to intercept and inspect mobile traffic to understand API's syntax. |
| **B.** | Root detection control should be implemented to prevent the users to install the mobile application into rooted devices. |
| **C.** | The source code of client application should be obfuscated so as the attacker will never be able to understand the source code in case of a successful reverse engineering. |

# Annex (A)

| | |
|---|---|
| **D.** | All the encryption keys should never be stored in the code; otherwise, they should be stored in a secure location so as the attacker will never be able to obtain them in case of successful reverse engineering. |
| **E.** | All the API tokens should never be stored in the code; otherwise, they should be stored in a secure location so as the attacker will never be able to obtain them in case of successful reverse engineering. |
| **F.** | Client file tampering detection should be implemented to detect if the attacker has successfully repackaged the client file with any malicious functionality. |
| **G.** | The mobile application should utilize secure communication channel (HTTPS) to communicate with the backend API's server. |
| **H.** | The backend server should only allow strong cryptography ciphers to ensure that the secure channel is not vulnerable to cryptography algorithms vulnerabilities. |
| **I.** | A robust session management functionality should be implemented to ensure that only authenticated and authorized users can disclose sensitive data. |
| **J.** | The application should ensure that only authenticated users can disclose their data and in case they are trying to do any kind of manipulation to disclose other users' data; the application should prevent them. |
| **K.** | The API endpoints should implement rate limit features to prevent the attacker from conducting guessing and brute forcing attacks against users' passwords, OTPs. |
| **L.** | The API endpoints should implement rate limit features to prevent the attacker from developing automated scripts that will be utilized to gather ID's information. |
| **M.** | The API gateway that is responsible to receive all the API calls from the client should be hosted in the DMZ behind a web application firewall. |
| **N.** | The communication between the API gateway and the internal services should be controlled by the internal deployed firewalls. |
| **O.** | All the sensitive data of the clients should be encrypted in the database to ensure that unauthorized users can't disclose clients' information. |
| **VIII.** | **Proof Of Concept Requirments** |
| **A.** | Demonstration of Right face and secuirty marks to ID/Passport |
| **B.** | Demonstratation of wrong face to ID/Passport |
| **C.** | Demonstatation of selfie to ID/Passport (Anti- spoofing) |
| **D.** | Demonstate Expired ID/Passport |
| **E.** | Edited Digit on ID/Passport |
| **F.** | Show Valid ID/Passports Results |
| **G.** | Demonstate international Passports |
| **H.** | Demonstratration of ID/Passport Copy wrong verification |
| **I** | Demonstartion of all on-boarding and verification processes |