الهيئة العامة للمعلومات المدنية

The Public Authority For Civil Information

Kuwait National Mobile ID

Service Provider Onboarding Requirements

Version 1.3 February 2021

CONFIDENTIALITY STATEMENT

Revision History

Document Revision	Description of Change	Effective Date	Remarks
1.0	First Version	18/05/2020	
1.1	Redesign	15/07/2020	
1.2	Amendments to the agreement	30/11/2020	
1.3	Amendments to the agreement	01/02/2021	Responsibility of messages

1 Introduction

This document describes the prerequisites of PACI Mobile ID Service Provider onboarding process.

1.1 Overview

The Kuwait Mobile ID is a secure mobile-based Digital ID derived from the Civil ID. It can be used for identity verification, authentication to online e-services and applying trusted digital signature to documents and transaction.
Various Service Providers (SPs) including government agencies, oil sector companies, banks, private companies, and others can integrate their applications and public e-services with the Mobile ID service to incorporate the aforementioned authentication and signing capabilities.
The purpose of this document is to describe and detail the onboarding process and requirements for service providers who wish to subscribe in the Mobile ID platform to integrate the Mobile ID App into their applications and e-services.

1.2 Definitions, Acronyms, and Abbreviations

CID: Civil ID

KNMID: Kuwait National Mobile ID

MID: Kuwait Mobile ID

OS: Operating System

OTP: One-Time Password

OWASP: Open Web Application Security Project

PACI: The Public Authority for Civil Information

PIN: Personal Identification Number

PN: Push Notification

QR: Quick Response Code

RAM: Random Access Memory

SDK: Software Development Kit

SP: Service Provider

T&C: Terms and conditions.

1.3 References

- KNMID SP Integration Guide

2 Service Provider Onboarding Process

2.1 Process Overview

The process for the Service Provider (SP) to subscribe with PACI for Mobile ID integration is described below:

1. ***Fill Subscription Request*** –The applying SP should fill the *Mobile ID Subscription Request* form, sign it, and submit it to PACI for approval and processing. Please refer to Appendix I for the form.

2. ***Sign SP Subscriber Agreement*** –Once the MID subscription request is approved, the SP needs to sign the *Mobile ID SP Subscriber Agreement* with PACI. Please refer to Appendix III for the agreement.

3. ***Obtain the SDK*** –PACI will provide the SP an SDK which is required for integrating the Mobile ID features into SP' applications or e-services. The SDK includes all needed libraries, resources and technical documentation. Furthermore, PACI will provide the SP access to the Mobile ID Development System and a corresponding development *SP Client Certificate*.

4. ***Develop and Integrate*** – The SP performs needed development work to integrate with the Mobile ID. The SP needs to do full integration testing against PACI' Mobile ID Development system to verify all related functionality. The SP' e-service must meet a set of technical requirements and guidelines which are detailed in .

5. ***Get Certified*** –The SP informs PACI about their readiness for certification testing. Within the certification testing, PACI will verify that the SP's application/e-service meets all PACI Mobile ID integration, security, and usability requirements. For that purpose, PACI will ask the SP to provide access to SP' Test application/e-service to assess the user experience, conduct a few transactions, and verify the compliance. Please refer to for the *Mobile ID Integration Guidelines and Technical Requirements*.

6. ***Rollout*** – When the SP passes PACI' certification testing, the SP is issued the required production *SP Client Certificate* and becomes ready to roll out their application/e-service to production.

Appendix I

Service Provider Subscription Request Form

SP Subscription Request Form

1- Organization & Contact Details – *Fill the service provider's main details*

Organization

Name

Type

Address

Website

Logo

Attach organization logo in PNG Format, 512 x 512 px, Transparent background if applicable

Contact

	Name	Title	Email	Mobile No.
Primary				
Technical				

Third Party Vendor (If applicable)

2- E-Service Details – *List and describe below the service provider's e-services / applications to be integrated with Mobile ID*

1

Name & Description

Target Audience & Their Size

Service Channels

Required MID Capability

- ☐ Mobile ID QR Verification
- ☐ Authentication with QR
- ☐ Authentication with PN
- ☐ Digital Signature
- ☐ Notifications

Integration Purpose

2

Name & Description

Target Audience & Their Size

Service Channels

Required MID Capability

- ☐ Mobile ID QR Verification
- ☐ Authentication with QR
- ☐ Authentication with PN
- ☐ Digital Signature
- ☐ Notifications

Integration Purpose

3

Name & Description

Target Audience & Their Size

Service Channels

Required MID Capability

- ☐ Mobile ID QR Verification
- ☐ Authentication with QR
- ☐ Authentication with PN
- ☐ Digital Signature
- ☐ Notifications

Integration Purpose

4

Name & Description

Target Audience & Their Size

Service Channels

Required MID Capability

- ☐ Mobile ID QR Verification
- ☐ Authentication with QR
- ☐ Authentication with PN
- ☐ Digital Signature
- ☐ Notifications

Integration Purpose

3-Technical Details — *Provide below technical details on service provider's application environment*

E-Service or Application Environments

- ☒ Production *(mandatory)*
- ☐ Additional Production Node ( )
- ☒ Test / Staging *(mandatory)*
- ☐ Disaster Recovery
- ☐ Development

Public IP Range / Public IPs

Callback Base URL — *The callback URL will be invoked to post the response of an asynchronous API request. It must be HTTPS secure with a globally trusted SSL certificate*

Production	
Test	
DR	
Development	

Required End-user Data Fields — *For each selected field, please specify the reason why it is required by your services*

☒ Civil No	
☐ Civil ID Serial No	
☐ Civil ID Expiry Date	
☐ Name - Arabic	
☐ Name - English	
☐ Date of Birth	
☐ Nationality	
☐ Gender	
☐ Other <*Please specify*>	

Required Assurance Level for Authentication – *If you're providing sensitive or critical service, you need to consider High.*

☐ Low	☐ Medium	☐ High
Self-Registration (smart phone)		Registers at a PACI office/ special kiosk machine
Facial Recognition	Facial Recognition Liveness Detection	Facial Recognition Liveness Detection Physical Civil ID **Digital Signing**

Digital Signature will only be available through the High Assurance Level

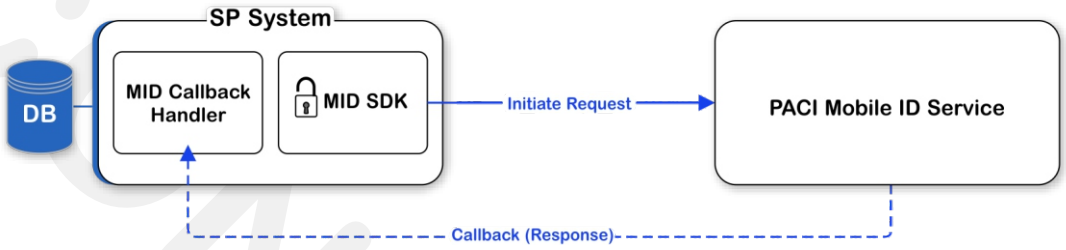
Appendix II

Mobile ID Integration Guidelines and Technical Requirements

Mobile ID Integration Guidelines and Technical Requirements

The following technical requirements must be met by service providers who intend to integrate PACI's Kuwait Mobile ID App into their e-services and applications to incorporate trust services (strong authentication, digital signature, identity verification, sending notifications …) using the Mobile ID SP SDK.
It should be noted that PACI mandates passing the **SP Certification Test** for the target e-services before rolling them out to production to verify that the below requirements are met in the SP's e-service or application.

1- Infrastructure Requirements



- ***Basic Requirements***
  - The SP shall establish a Production Environment and a Test Environment.
  - Test Environment shall be for integration purposes, pre-production testing, and certification testing.
  - The Test Environment must be separate from Production Environment
  - Each Environment shall include the following components related to MID integration:
    - *MID SP Client* – A server acting as the client interfacing with the PACI MID services. This server shall run the SDK and have network outbound access to PACI MID services.
    - *MID Callback Handler* – A server/service acting as the handler for callback sent back from PACI MID services. It shall allow inbound access from PACI MID services.
    - *MID Audit Database* – A database for storing full details on all transaction done against PACI MID.

- ***Security Requirements***
  - The SP shall take full responsibility to secure their network and entire infrastructure before integrating with Mobile ID. This includes but not limited to implementation and utilization of firewalls, endpoint security, antivirus, antimalware, etc.
  - The SP shall make sure to limit access to SP MID Environment only to authorized and accountable users, and implement a proper security policy and procedures such as segregation of duties, two factor authentication, etc.
  - Security requirements for the "MID SP Client" server:
    - Restricted outgoing Internet access only to PACI MID services.
    - No incoming Internet access, unless this is the same as the callback handler server.
    - Accessible only to SP's internal e-services and applications authorized by PACI.
    - Certificate Security – restrict access to the SP client certificate and limit it only to the eService/application integrating to Mobile ID.

- Security requirements for the "MID Callback Handler" server:
  - Restricted incoming internet access only to PACI MID services.
  - Callback handler service must be TLS 1.3 secure by a trusted SSL/TLS certificate.
- Security requirements for the "MID Audit Database" server:
  - The SP shall protect the MID Audit Database's integrity and availability. Data within this database is a critical evidence needed in case of claims or conflicts.
  - The SP shall ensure the MID Audit Database is regularly backed up.

2- Application Requirements

- ***User-Experience Requirements***
  - In their e-service(s) consuming Mobile ID, the SP should educate the end-user about Mobile ID as follows:
    - Provide guidance on how to get Mobile ID and where to enroll. This could be done by adding a link to Kuwait Mobile ID webpage (https://hawyti.paci.gov.kw).
    - Include hints on what the user should expect or need to do, on his Mobile ID, to authenticate a request or sign a document or transaction (provide steps).
    - Inform the user about the liability and responsibility he will take by using Mobile ID in the SP's e-service.
  - The SP e-service(s) consuming Mobile ID should explicitly inform the user how his retrieved user data will be used or processed.
  - Requirements for strong authentication scenarios:
    - For QR-based authentication, give clear instructions on how the user can use his Mobile ID to scan the QR and authenticate.
    - If the user is using a Mobile Agent (web or native), use URL-scheme approach and do not present a QR.
    - For PN-based authentication, the SP e-service must inform the user in advance that he would receive a notification and request on his Mobile ID. It should show clear instructions on how he can authenticate such request on his Mobile ID.
    - The SP e-service should instruct the user to verify that the retrieved authentication request is coming from the same SP (i.e. has the SP's logo and name).
    - It is required to include clear request details and explicit purpose in any authentication request. A recommended practice is to show the user a random challenge (composed of a few random digits) on both the eService page and include the challenge on the authentication request so that the user can be assured that he's authenticating on the right (intended) request.
    - The SP e-service should handle all possible outcomes of Mobile Authentication. This includes but is not limited to:
      - User approval.
      - User decline.
      - Timeout.
      - Error.
      - Other outcomes.

- Requirements for Digital Signature scenarios:
  - The SP e-service must show a full preview of the document, request, or transaction details which will be sent to the end-user for digital signing.
  - The SP e-service must collect user's explicit confirmations on the below before sending him/her a signing request on their Mobile ID:
    - Reviewed the entire document / data that he is required to sign.
    - Accepts to sign the document / data that he is reviewed.
      This can be done by showing the above as checkboxes that the user must check before he's able to proceed with digital signing using Mobile ID.
  - The SP e-service should give the user the option to send a copy of the document / data to his email before signing.
  - The SP e-service must give clear instructions on how the user can use his Mobile ID to digitally sign documents or transactions .
  - The SP e-service must inform the user in advance that he would receive a notification and signing request on his Mobile ID. The e-service must describe in detail what the user is required to complete the digital signing transaction.
  - The SP e-service should instruct the user to verify that the retrieved signing request is coming from the same SP (i.e. has the SP's logo and name).
  - It is required to include clear request details and explicit purpose in any signing request.
  - It is highly recommended to send the end-user the whole document or a preview of the document to his Mobile ID to review before committing the digital signature. If not, a clear text describing exactly what the user is signing on is required. Include a random number to be shown on both the e-service page and the Mobile ID signing request and ask the end-user to verify that the random number matches on the two devices (i.e. the SP client and the Mobile ID).
  - The SP e-service should handle all possible outcomes of Mobile Authentication. This includes but is not limited to:
    - User approval.
    - User decline.
    - Timeout.
    - Error.
    - Other outcomes.
  - The SP e-service must keep a copy of the document / data before signature and after signature.
  - The SP e-service must make the signed copy of the document / data available and accessible to the end-user. It is highly recommended to send the sign copy to the end-user's email to meet common legal requirements.
  - In case of incomplete signature transactions, always show a clear feedback to the user that the operation was declined or failed and no signature has taken place.

- ***Security Requirements***
  - The SP e-service or application must keep full audit log of all requests initiated against PACI Mobile ID service in the MID Audit Database.

- The SP e-service or application must keep full audit log of all callbacks received from PACI Mobile ID service in the MID Audit Database.
- The SP e-service or application should verify the following in the response or callback returned by the Mobile ID SP API:
  - Request ID – Ensure that the response belongs to a non-expired or timed-out request, and that the request has been actually initiated and logged by the SP.
  - Data Signature - This gives additional assurance to the SP that this response is originated from PACI Mobile ID System and has not been tampered with.
- In case of digital signature, the SP shall take full responsibility to utilize a secure digital signing software to:
  - Properly calculate the hash or digest for the data (document/transaction) to be signed. The hash or digest shall meet the Mobile ID API requirements.
  - Properly construct an industry compliant signed document or transaction based on the user hash/digest signature which is returned by the Mobile ID SP API. Example standards include PAdES (for PDF Documents), XAdES (for Office documents, and transactions), and CAdES.
- In case of digital signature, The SP shall ensure to meet the following security measures:
  - Assure that the hash passed to the Mobile ID API belongs to the document which is previewed to the user within the SP e-service/application and/or passed to the Mobile ID for preview.
  - The SP shall store the following evidential data items, for each digital signature transaction using the Mobile ID:
    - The original document or transaction data (i.e. before signature).
    - The calculated hash or digest which is passed to PACI Mobile ID API for signing.
    - The signed hash or digest.
    - The signed document or transaction data.

    The SP shall be able to retrieve the above data items in case needed for auditing purposes, claims, or investigation.
- The following details must be stored as part of the audit log:
  - Request Details
    - SP e-service / application identifier.
    - Transaction / operation type (auth, sign, identity verify, notification, …).
    - Request Purpose/Reason.
    - Request Description.
    - Additional Data (if present).
    - Random challenge (in case of Authentication).
    - Civil ID.
    - Data hash - passed for signature which is corresponding to document or transaction being signed (in case of Signature)
    - Preview Data / Filename (in case of Signature).
    - Notification details (in case of Notifications).
    - Request Personal Data Flag.
    - Callback URL.
    - Request Timestamp.

- Response/Callback Details:
  - MID Transaction ID (PACI Request ID).
  - QR Data (in case of QR Authentication).
  - Request Result.
  - User action.
  - User signature.
  - User certificate.
  - Personal Data Schema.
  - Response Data Stamp.
  - Response Timestamp.
  - Transaction Status.

- Whenever applicable, the SP must verify the data signature retrieved within the response or callback sent by PACI MID service.
- The SP shall ensure the integrity and availability of the audit data.
- The SP shall protect retrieved end-user data and prevent any unauthorized access to it.
- All SP services and applications must be protected with (TLS 1.2 or TLS 1.3) SSL certificates.
- The SP provider should make sure to implement OWASP's top 10 web application security considerations.

Appendix III

Mobile ID SP Subscriber Agreement

اتفاقية اشتراك مزود خدمة بمنصة تطبيق "هويتي"

شروط وأحكام الاتفاقية

الطرف الأول في هذه الاتفاقية هو الهيئة العامة للمعلومات المدنية.

الطرف الثاني في هذه الاتفاقية هو وهو مزود خدمات يرغب بالاشتراك بمنصة تطبيق "هويتي" بهدف الاستفادة منها لإضافة خدمات الموثوقية كالمصادقة والتوقيع الالكتروني والتحقق من الهوية الرقمية وغيرها.

يوافق الطرف الثاني على الشروط والأحكام التالية للاتفاقية:

1- تعريفات:

تطبيق "هويتي": هو تطبيق هاتف ذكي يحمل بطاقة مدنية رقمية(هوية رقمية) إضافة إلى شهادة توقيع إلكتروني رقمية تحتوي على معلومات المستخدم (المواطن أو المقيم) وموثقة من الهيئة العامة للمعلومات المدنية تثبت هويته عند إجراء العمليات الإلكترونية وتوقيع الملفات ويمكن التحقق من هويته باستخدامها.

منصة تطبيق "هويتي": هي مجموعة من الخدمات والأدوات التي يقوم مزود الخدمة باستخدامها والربط معها لتحقيق التكامل مع تطبيق "هويتي".

المستخدم: هو مواطن أو مقيم يحمل تطبيق "هويتي" ويستخدم خدمة مزودة من الطرف الثاني يتم من خلالها الربط مع التطبيق للمصادقة أو التوقيع الالكتروني أو التحقق من الهوية والحصول على المعلومات المدنية الخاصة به.

الشهادة الأمنية: هي شهادة رقمية تقوم الهيئة العامة للمعلومات المدنية بإصدارها للطرف الثاني عند اشتراكه وتتيح له إمكانية الوصول والربط مع خدمات منصة تطبيق "هويتي".

2- طلب وقبول الخدمة:

- يقوم الطرف الثاني بطلب الاشتراك بمنصة تطبيق "هويتي" من الطرف الأول من خلال ملء نموذج طلب الخدمة بالكامل وتقديمه للطرف الأول.
- يقوم الطرف الأول بمراجعة طلب الاشتراك ويحق له رفضه جزئيا أو كليا.
- يعتبر أن الطرف الأول قد قبل باشتراك الطرف الثاني وتقديم الخدمة له عند استيفاء الطرف الثاني ما يلي:
  - ملء نموذج طلب الخدمة بالكامل من الطرف الثاني ومراجعته وقبوله من الطرف الأول.
  - قيام الطرف الثاني بعمليات التطوير والربط مع خدمات منصة تطبيق "هويتي".
  - استيفاء الطرف الثاني كافة متطلبات الربط الفنية والأمنية التي سيحددها الطرف الأول.
  - انتهاء الطرف الأول من عمليات الفحص الفني للتأكد من استيفاء الطرف الثاني متطلبات الربط الفنية والأمنية.
  - إصدار الطرف الأول الشهادة الأمنية الخاصة ببيئة الإنتاج .

3- تعديل الاتفاقية:

فيما عدا ما ورد صراحة في هذه الاتفاقية، أية مراجعة أو تغيير لهذه الاتفاقية ستكون فعالة خلال ثلاثين (30) يوما بعد نشر التعديلات على الموقع الخاص بالهيئة العامة للمعلومات المدنية، بناء على إشعار من الطرف الأول إلى الطرف الثاني عن طريق البريد الإلكتروني أو الهاتف النقال أو كتاب رسمي، ويلتزم الطرف الثاني بالاطلاع على موقع الهيئة العامة للمعلومات المدنية الإلكتروني بشكل دوري لمتابعة أي تعديلات تطرأ على الإتفاقية.

4- إلغاء أو انتهاء الاتفاقية:

يحق للطرف الأول إلغاء الاتفاقية في أي وقت (ولا يقتصر ذلك على الآتي):

- عند قيام المشترك (الطرف الثاني) بالإخلال بأي من الشروط الواجبة في هذه الاتفاقية.
- عند حصول سوء استخدام أو تلاعب من قبل الطرف الثاني لخدمات منصة "هويتي".
- عند اكتشاف حدوث اختراق أمني أو تسريب للبيانات في أنظمة الطرف الثاني أو بنيته التحتية.
- عند استخدام أو مشاركة المعلومات المدنية للمستخدمين بشكل خارج عن أو مخالف لشروط هذه الاتفاقية أو للاستخدامات التي تم التصريح عنها من قبل الطرف الثاني في طلب الاشتراك بالخدمة.
- عند فقدان الطرف الثاني للصفة القانونية.

5- الالتزامات:

التزامات الطرف الأول:

- ضمان الدقة وعدم وجود أخطاء في بيانات الهوية الرقمية أو المعلومات المدنية للمستخدمين.
- ضمان مستوى أمني عال للتحقق من هوية المستخدم (المواطن أو المقيم) عند إصدار الهوية الرقمية له.
- ضمان مستوى أمني عال للبنية التحتية وخدمات الربط الخاصة بمنصة تطبيق "هويتي".
- ضمان مستوى عال من توفر خدمات منصة هويتي للتحقق والمصادقة والتوقيع الرقمي.
- تتوافق الهوية الرقمية والشهادة التابعة لها للمواطن أو المقيم مع اللائحة العملية للتنفيذ الخاصة بالطرف الأول.
- يوفر الطرف الأول خدمات نشر حالة الشهادة الرقمية الخاصة بالمواطن أو المقيم وتكون متاحة للطرف الثاني.
- تتوافق خدمات نشر حالة الشهادة الرقمية مع اللائحة العملية للتنفيذ الخاص بالطرف الأول.
- يلتزم الطرف الأول بألا يكشف المعلومات الخاصة بالطرف الثاني للغيرخلال فترة سريان الاتفاقية أو بعد انقضائها أو فسخها وأن يتوخى الحرص اللازم لعدم كشف هذه المعلومات، ويستثنى من ذلك الأحوال التي يجيزها القانون.
- يلتزم الطرف الأول بالاحتفاظ بنسخة من هذه الاتفاقية بعد توقيع الطرفين أو تسجيل موافقة الطرف الثاني في الأنظمة الخاصة بالطرف الأول فى حالة عدم تواجد وثيقة ورقية.
- يلتزم الطرف الأول بإبلاغ الشخص المعني من قبل الطرف الثاني عن طريق الهاتف أو البريد الإلكتروني أو عن طريق الإعلان الرسمي في وسائل التواصل الاجتماعي بعمليات الانقطاع لأعمال الصيانة الدورية.

التزامات الطرف الثاني:

- يلتزم الطرف الثاني بأن تكون جميع المعلومات التي أوردها بنموذج طلب الخدمة صحيحة ودقيقة بحيث يمكن الاعتماد عليها وأنه يتحمل المسؤولية القانونية عند عدم صحة تلك المعلومات.
- يوافق الطرف الثاني على استخدامه لخدمات منصة "هويتي" بحيث يخضع للشروط والأحكام التي اطلع عليها في نموذج طلب الخدمة واللائحة العملية للتنفيذ الخاصة بالطرف الأول.
- يقر الطرف الثاني بمسؤوليته المطلقة عن الدخول لخدمات منصة "هويتي " و استخدام الشهادة الأمنية دون أدنى مسؤولية اتجاه الغير.
- يلتزم الطرف الثاني بإخطار الطرف الأول في حال عمل أي تغيير ممكن أن يغير على الخدمات المقدمة أو البنية التحتية التابعة لها.
- يلتزم الطرف الثاني بعدم تمكين أي طرف ثالث من استخدام خدمات قنوات الربط مع منصة "هويتي" أو الشهادة الأمنية بأي شكل من الأشكال، مالم يتحصل الطرف الطرف الثاني على موافقة كتابية مسبقة من الطرف الأول.
- يلتزم الطرف الثاني باتخاذ كافة الاحتياطات الضرورية لمنع تسريب المعلومات المدنية للمستخدمين أو الدخول الغير مصرح لها.
- يلتزم الطرف الثاني بعدم مشاركة المعلومات المدنية للمستخدمين مع أي طرف آخر، مالم يتحصل الطرف الطرف الثاني على موافقة كتابية مسبقة من الطرف الأول.

- لا يجوز الكشف عن المعلومات السرية الخاصة بمنصة "هويتي" لأي استشاري أو طرف ثالث إلا إذا كان ذلك الطرف يوافق على الالتزام ببنود هذه الاتفاقية وتنفيذها وذلك بعد موافقة الهيئة العامة للمعلومات المدنية.
- يلتزم الطرف الثاني بإبلاغ الطرف الأول عند الاستعانة بخدمات أو توقيع عقد مع طرف ثالث للاستشارة أو القيام بأي أعمال تخص الربط مع منصة "هويتي"، وذلك لتوقيع اتفاقية بين الطرف الأول والطرف الثالث.
- يقوم الطرف الثاني باتخاذ كافة الاحتياطات الضرورية لمنع تعريض الشهادة الأمنية أو المعلومات المدنية للمستخدمين للسرقة أو الفقدان أو الكشف أو التعديل أو الاستخدام الغير مصرح.
- يقوم الطرف الثاني باتخاذ كافة الاحتياطات الضرورية لحماية خدماته الالكترونية والبنية التحتية الخاصة بها ومنع سوء استخدامها بأي شكل من الأشكال.
- عند حدوث اختراق أمني أو دخول غير مصرح أو سرقة للمعلومات المدنية للمستخدمين أو الشهادة الأمنية الخاصة بالطرف الثاني يلتزم بسرعة إبلاغ الطرف الأول دون تأخير لاتخاذ الإجراءات اللازمة.
- لا يجوز للطرف الثاني التدخل في الأمور الفنية لأدوات أو خدمات الربط لمنصة "هويتي" سواء بالتعديل أو التغيير إلا بعد الحصول على موافقة كتابية من الطرف الأول.
- يقر الطرف الثاني بأحقية الهيئة العامة للمعلومات المدنية في الاحتفاظ بالمعلومات الخاصة به بشكل إلكتروني والإعلان عنه كمزود خدمات مشترك بمنصة "هويتي".
- يتعهد الطرف الثاني بإبلاغ الهيئة العامة للمعلومات المدنية حال تغيّر البيانات الخاصة بالمركز القانوني له أو انتفاء الصفة.
- يقر الطرف الثاني بأحقية الهيئة العامة للمعلومات المدنية في عمل أية تعديلات على خدمات منصة تطبيق "هويتي" أو واجهات ربطها في أي وقت ولأي سبب كان مع إخطار الطرف الثاني بذلك.
- يقر الطرف الثاني بأحقية الهيئة العامة للمعلومات المدنية في فرض أو تغيير حدود الاستخدام لكافة الخدمات المتاحة على منصة تطبيق "هويتي" من قبل الطرف الثاني في أي وقت ولأي سبب كان مع إخطار الطرف الثاني بذلك.
- يقر الطرف الثاني بأحقية الهيئة العامة للمعلومات المدنية في إلغاء اشتراكه في حال الإخلال بالالتزامات التعاقدية من الطرف الثاني.
- يوافق الطرف الثاني على تحمل رسوم الخدمة في حال إقرارها وأي زيادة تقرر فيما بعد.
- لا يحق للطرف الثاني إعادة تقديم أو بيع الخدمة بأي شكل من الأشكال.
- توفير الدعم الفني الأولي للمستخدمين ضمن المؤسسة الخاصة به وفي حالة الحاجة إلى الدعم الفني من الهيئة يقوم الشخص المسؤول من الطرف الثاني بالاتصال مع الشخص المسؤول من الهيئة (الطرف الأول) خلال أيام وأوقات عمل الهيئة العامة للمعلومات المدنية الرسمية على أن يكون الشخص الفني من الطرف الثاني متواجدا خلال حل أي مشكلة.
- إبلاغ المستخدمين بأي انقطاع مبرمج أو غير مبرمج للخدمة.
- يقر الطرف الثاني بمسؤوليته الكاملة عن محتوى الرسائل المبلغة بما فيها الروابط المذكورة لأي مواقع خارجية دون أدنى مسؤولية على الطرف الأول.

6- انقطاع الخدمة غير المبرمج :

- تقوم الهيئة بالإعلان عن أي انقطاعات فجائية والوقت المتوقع لعودة الخدمة حال حدوثها ، مع إبلاغ الطرف الأول للمعني من الطرف الثاني عن طريق الهاتف أو البريد الإلكتروني بعمليات الانقطاع غير المبرمج.

7- إنهاء الاتفاقية:

- يحق لأي من الطرفين إنهاء هذه الإتفاقية أثناء مدة سريانها بعد إخطار خطي موجه للطرف الآخر قبل تاريخ الإنهاء.

8- صلاحية الاتفاقية:

- تعتبر هذه الاتفاقية سارية ابتداءً من تاريخ توقيع الاتفاقية ولمدة سنة واحدة وتجدد تلقائياً ما لم يتم إلغاؤها من أحد الطرفين.

يسري على هذه الاتفاقية كافة القوانين واللوائح الكويتية بما فيها أحكام القوانين الكويتية وأن أي نزاع أو خلاف ينشأ عن هذه الاتفاقية تختص بالفصل فيه المحاكم الكويتية.

الطرف الأول

الهيئة العامة للمعلومات المدنية

ممثله

الاسم

المسمى

الرقم المدني

التوقيع ..... التاريخ / / 20م

الطرف الثاني

ممثله

الاسم

المسمى

الرقم المدني

التوقيع ..... التاريخ / / 20م