وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Qatar e-Authentication Framework

Version: 1.2

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: June 2018

Document History:

Version	Description	Date
1.0	Published V1.0 document	May 2013
1.1	Branding Change (ICT to MOTC)	March 2016
1.2	MoTC Logo changed	June 2018

Table of Contents

Definitions

Agency	Any Government / Semi Government Agency / Organization covered in the scope of the document
Service Providers (SP)	A Service Provider (SP) is a provider of online services to the users. SPs rely on AOs to authenticate users prior to providing them services. SPs are also referred to as "*Relying Parties*".
Users	**Users** are subscribers to online services, e.g. citizens, residents, business entities. Since users are generally the initiators of online service / transaction, they are also known as a "*Claimant*" during the authentication process because the user is making a claim regarding his identity.
User Registration	**User registration** is defined as the processes involved in the initial creation of an electronic identity for a user. This encompasses the *Evidence of Identity (EOI)* or *Evidence of Relationship (EOR)* processes.
Token Issuance and Management	A **token** is something that a Claimant possesses and controls used to authenticate the Claimant's identity. A token is provided to the user for subsequent online authentication transactions. No token is perpetual, and the issuing agency is responsible for ensuring the validity of token throughout its life cycle and for any subsequent mitigation actions required, should a malfunction occur.
User Enrollment	**User enrollment** refers to the act of binding an e-Authentication credential to a known instance of a user within an IT resource context (e.g. network, website, application system) in order to enable access by the user.
Credential Verification	**Credential verification** is the verification of an enrolled token, which takes place before enabling the transaction. It encompasses the issuance of a positive identity indicator, known as an assertion, to a requesting SP. The term credential is used in this context, as opposed to token: the token would have been enrolled and bound to an identifier, prior to the need for verification. Validation is implied here, which refers to checking the status of the credential at the time of verification.

1. Legal Mandate

Emiri decision No. (8) for the year 2016 sets the mandate for the Ministry of Transport and Communication (hereinafter referred to as "MOTC") provides that MOTC has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (22) of Emiri Decision No. 8 of 2016 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

This Policy Document has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Policy Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

2. Introduction

Electronic authentication (or "e-Authentication") is the process of determining the degree of confidence that can be placed on assertions that a user is who he claims to be or an identity is what it declares to be. Assertions include identity, role, delegation and value.

The Qatar e-Authentication Framework (QeAF) is primarily concerned with the electronic authentication of assertions. Electronic transactions occur across a number of channels, including:

- ✓ Internet or web-based
- ✓ Telephone (IVR)
- ✓ Facsimile transmissions

Similar to other authentication models, e-Authentication is based on one or more of the following:

- ✓ something the user knows (e.g. password, secret questions and answers), or
- ✓ something the user has (e.g. security token), or
- ✓ something the user is (e.g. biometric)

The approach chosen to authenticate must balance the usability requirements (ease of use to the end user and the cost factor) with the acceptable level of risk.

As opposed to low-risk applications, critical applications and information systems require stronger authentication models that can accurately confirm the user's digital identity as true

3. Scope and Application

3.1. Scope

The scope of the Qatar e-Authentication Framework (QeAF) applies to:

- ✓ All government and semi government entities
- ✓ All Critical sector organizations
- ✓ Private businesses incorporated and / or operating in Qatar

Each entity should use this framework to assess and evaluate their existing e-Authentication means. They may also use this as a guideline while designing new eAuthentication controls.

3.2. Need for e-Authentication Framework

With advances in technology and increased availability of online services, citizens and residents in Qatar show a marked preference to transact online. Businesses are also realizing the benefits of extending their reach beyond conventional means of transactions.

The provisioning of online services is aimed at simplifying interactivity and transactional processes for citizens, residents and businesses to engage with the government from the comfort of their homes and offices.

Nevertheless, this convenience introduces the risk of ascertaining the online identity of the person / business to provide information assurance for the process involved.

The Qatar e-Authentication Framework (QeAF) intends to ensure that a strategic approach is adopted by entities involved to assure online identification. The framework advocates a risk based approach, balancing between the business objectives and the risks.

3.3. Roles and Responsibilities

The key to a successful e-Authentication solution is not the technology but the supporting processes, procedures, management support and an effective management of cultural issues arising out of the change.

Agencies roles and responsibilities:

- ✓ Consider the needs and expectations of individuals and business
- ✓ Provide education and awareness amongst the users
- ✓ Provide secure and reliable services
- ✓ Compliance with necessary policies, rules and regulations.
- ✓ Handling personal data in accordance to work ethics and relevant laws

User's roles and responsibilities:

- ✓ Provision of accurate evidence of identity and / or evidence of relationship information
- ✓ Ensuring security of credentials issued
- ✓ Use of credential only for the purpose issued and as per the guidelines issued

4. Policy Provisions, Articles or Proposals

4.1. e-Authentication Framework

The QeAF provides guidance on the different authentication models, various kinds of authentication tokens available, their strengths and weaknesses and identifies related risks in mitigating an Identity related threat.

It advocates the following iterative steps as part of the Agency's overall Risk management process. This will provide guidance on choosing a suitable authentication system with the desired assurance levels necessary for accessing the information it provides access to.

4.2. Determining the business requirements

This is the first step and part of requirements definition / gathering phase.

Some of the key business requirements that will govern the choice of an e-authentication solution are:

1. Information Classification: What are the services / information being accessed?
2. User Community: Identify the target users (Is it an individual or an individual acting on behalf of an entity?) and the level of skillset the user possses
3. What electronic delivery channels are available / to be used?
4. Privacy concerns / implications? This is in terms of the personal information being provided access to and also the use of personal tokens (biometric) in the authentication mechanism.
5. Legal and Regulatory obligations.
6. Any other requirements such as data integrity, confidentiality and non-repudiation.

Agencies shal conduct a risk analysis to include wide range of possible scenarios to identify potential threats associated with the process / transaction. The potential threats might result from technical failures, malicious third parties, process failure or human error amongst other things.

The following table provides an indicative level of assurances that can be used to classify various business transactions.

No Assurance	Minimal Assurance	Low Assurance	Moderate Assurance	High Assurance
Level 0	**Level 1**	**Level 2**	**Level 3**	**Level 4**
No confidence is required in the identity assertion.	Minimal confidence is required in the identity assertion.	Low confidence is required in the identity assertion.	Moderate confidence is required in the identity assertion.	High confidence is required in the identity assertion.
Publicly Available Data	General Information	Personally Identifiable Data	Financial / Government transactions	Critical Information / State Level Confidential data

Table 1: Assurance Levels

Amongst the key factors that will shape up the assurance level requirements are the data / information that is being handled / transacted and the level of confidence / integrity that is required for execution.

4.3. Determining the Assurance levels requirement

Assurance level is the minimum authentication strength (Trust) offered by an authentication process (in line with the business requirements and the potential value of the information / transaction) to mitigate against the potential impact, should an attacker be able to compromise a legitimate user's access.

To determine the required assurance levels, Agencies need to consider the strength of the components that make up the authentication solution along with associated threats and the overall risk management to mitigate or minimize these risks.

The required assurance level is a function of:

1. Strength of Authentication Mechanism
2. Strength of Registration of Entity Identity

The following table assists in computing the required assurance level.

Strength of Registration of Entity, Identity (1-4) ↑	High	Minimal (1)	Low (2)	Moderate (3)	**High (4)**
	Moderate	Minimal (1)	Low (2)	Moderate (3)	Moderate (3)
	Low	Minimal (1)	Low (2)	Low (2)	Low (2)
	Minimal	Minimal (1)	Minimal (1)	Minimal (1)	Minimal (1)
		Minimal	Low	Moderate	High
		Strength of Authentication Mechanism (1-4) →			

Table 2: Assurance Level, a function of Entity Registration process and Authentication Mechanism

4.4. Determining the e-Authentication mechanism and Credential Management System

The strength or the assurance level of a particular e-Authentication solution depends on

1. The strength of the registration process
2. The strength of the e-Authentication mechanism which in turn depends on
    a. The strength of the credential token
    b. The credential management and usage strength

An authentication token / credential is something tangible controlled by the user / subscriber that incorporates one or more of the following attributes

- Something the user / subscriber knows
- Something the user / subscriber has
- Something the user / subscriber is

These attributes are also termed as *factors*.

The management process includes the processes involved in the generation of the credential / token, its distribution to the subscriber / user, its activation and its usage within a broader authentication protocol established between the subscriber and the relying party.

The effective strength of the authentication mechanism is reliant on the effective strength of the credential token and the management processes built around it. The following factors should be considered while selecting the credential token and while building the management process around it.

Credential Tokens

1. The tokens may be
    a. Single factor, such as passwords, bio-metric code, access card etc.
    b. Multi factor , (a combination of two or more tokens) such as PIN protected smart cards, access card along with bio-metric code etc
2. The strength of a particular token as relative to the level of assurance required
3. The ease of use of the credential as related to the intended client group
4. Scalability of the solution
5. Existing credentials that may be in use
6. The capacity to meet additional requirements such as non-repudiation etc.

Management Process

1. The behavior of the credential holder has the potential to adversely affect the strength of assurance provided by the credential itself as well the management process. Due diligence shall be carried out to ensure that such threats are factored while making any decisions regarding the choice of authentication mechanism.
2. Provide adequate training and awareness to end users to minimize the risk of fraudulent use.

Following is a table illustrates the strength of Authentication Mechanism.

Strength of Credential (1-4) ↑	High	Low (2)	Moderate (3)	**High (4)**	**High (4)**
	Moderate	Low (2)	Moderate (3)	Moderate (3)	**High (4)**
	Low	Low (2)	Low (2)	Moderate (3)	Moderate (3)
	Minimal	Minimal (1)	Low (2)	Low (2)	Low (2)
		Minimal	Low	Moderate	High
	Strength of Credential Management (1-4) →				

Table 3: Strength of Authentication Mechanisms

4.5. Determining the Registration Requirement

Registration involves verifying that the subscriber's identity or other attributes are at an understood assurance level* prior to creating an e-Authentication credential.
A number of factors influence the registration requirements. These include

1. The nature of assertion to be authenticated
2. The assurance level required
3. Whether the user has been issued a credential by another Agency. In this case additional factors must be considered such as:
    a. Registration process used by that agency
    b. Credential life cycle management process employed by that agency
4. Policies and legislations impacting the overall process

The approach to registration will depend on the nature of assertion to be authenticated. These include

1. Registration of individuals (as themselves)
2. Registration of individuals as representatives of businesses

The most common approaches are
Evidence of Identity (EoI): This requires individuals to present previously authorized and verified documentation to validate their claim to an identity. These could include documents such as Birth certificates issued by valid legal entities, Citizenship documents, Passports, Physical verifications by law agencies etc.

***Assurance level here refers to the confidence provided by the registration process**

Evidence of Relationship (EoR): Also referred to as **"known customer"** basis, this requires individuals to establish they have an existing relationship with the Agency. Generally the

establishment of the original relationship would have involved an EoI process. These could include documents such Residence Permits, Driving Licenses etc.

4.6. Review the authentication solution

Once the agency has agreed upon the required assurance level and has identified the components necessary to meet the desired assurance level, an appropriate technical solution must be identified and adopted.

Considerations for technology choice are beyond the scope of this document. However technology is an important factor in the solution and due diligence shall be done to ensure that the right design / model (e.g. standalone solution, a single SIGN On solution (federated) or centralized e-Authentication solution) and an appropriate technology is chosen to complete the e-Authentication solution.

Final re-validation needs to be done after the solution is implemented to ensure that the system achieves the required assurance level and meets the necessary security requirements.

The Agency should at regular intervals reassess the solution to ensure that it continues to meet the identity authentication requirements consistently as a result of technology changes or changes in the business processes and / or objectives.

5. Recommendations

The identity management services should:

- ✓ Issue identification tokens based on sound criterion for verifying an individual's entity
- ✓ Be strongly resistant to identity fraud, tampering, counterfeiting, and any exploitation

These recommendations could be easily met using a Federated ID system.

6. Annexes

APPENDIX A: e-Authentication Model

An e-Authentication system contains the following components and supports these functions.

- ✓ Authentication Operators (AO)
- ✓ Service Providers (SP)
- ✓ Users
- ✓ User Registration
- ✓ Token Issuance and Management
- ✓ User Enrollment
- ✓ Credential Verification

The architecture for authentication system can be broadly classified into the following three models:

1. Siloed
2. Centralized
3. Federated (Single Sign ON)

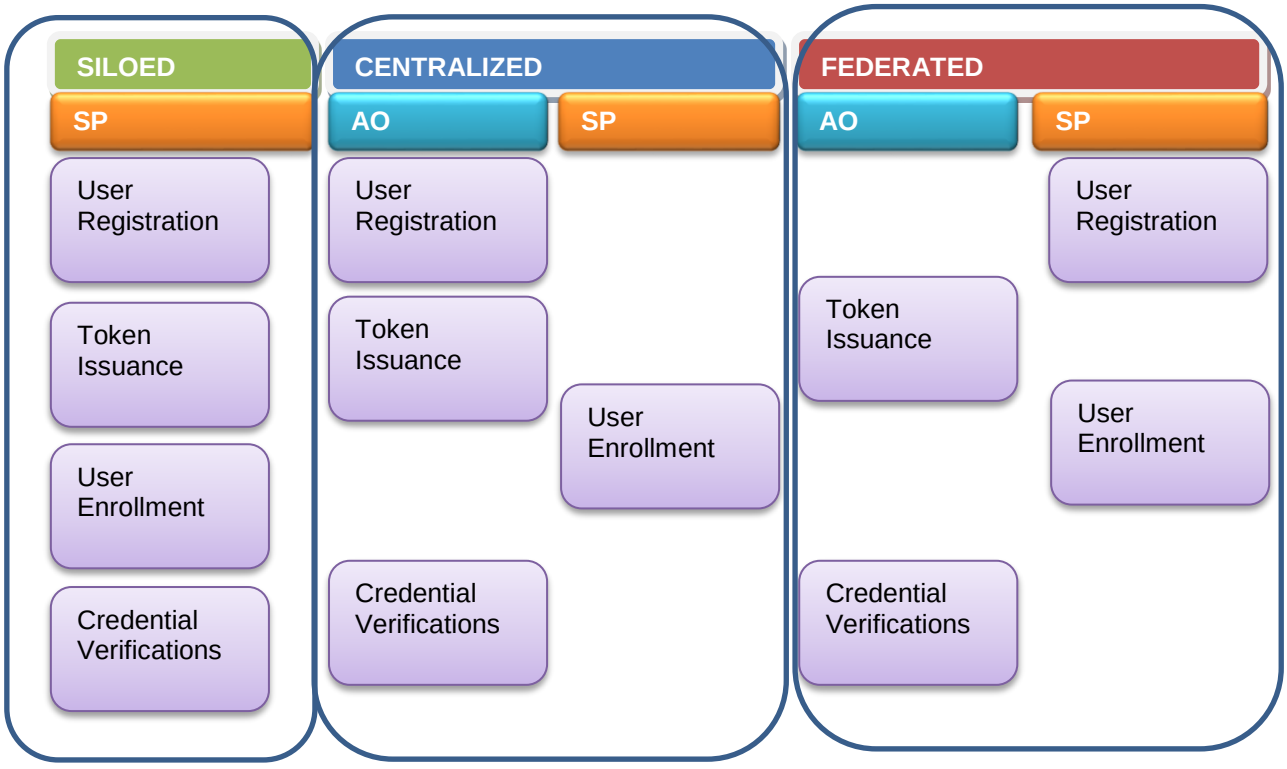

Table 4: e-Authentication Models

Siloed

This model is representative of the current authentication mechanisms being deployed by the larger segment of Agencies in Qatar. All component functions are provided by the SP. Each agency contracts the service provider separately for the purpose of procurement and establishment of in-house proprietary authentication mechanisms. This has resulted in an individual (user) possessing multiple authentication tokens, a token each for the agency with which the individual has a relationship.

As this model eliminates the need for AOs, it results in a simpler transactional process, as well as the faster transactions. The need for in-house infrastructure, though, would require high initial capital outlay, as well as continuous life-cycle maintenance costs, which may prove to be a barrier to entry for all but the largest institutions. The model does not benefit from economies of scale that can be rendered with partners and peers.

Centralized

This model sees a user registering with an AO for the provision of a global identifier and a token. The user's credentials (global identifier and token) are subsequently enrolled with each SP. When a user requires a service, the user presents his credentials to the SP, which will subsequently be redirected to the AO for verification.

As authentication services are outsourced, SPs no longer need to bear the costs involved in maintaining their in-house systems. The costs accrued to both SP and the individual is reduced by the shared infrastructure. Individuals may also have a choice in the form of factor and method of authentication. Concerns include the probability of having a single point of failure, increased transaction time, and privacy issues arising from having a global identifier registered across all SPs.

Federated (Single Sign ON)

The Federated Model differs from the centralized model in that there is no requirement for a global identifier. The AO is responsible only for the issuance of the token. The user enrolls the provided token with the SP; the token and its attributes will be associated with the user's unique identifier with the SP, resulting in a credential. Each time the user requires a service, the user presents his or her credential to the SP. The SP in turn will request a separate verification of the attached token from the AO. Positive verification is communicated back to the SP from the AO in the form of an assertion.

This mechanism serves as the basis for **Single Sign-on (SSO)**, which translates to greater user convenience as only a single authentication process is required to access multiple SPs, based on the assumption that all relying SPs have a relationship with the same AO. The Federated Model provides an additional layer of privacy to the consumer. There is no global identifier, as with the Centralized Model, resulting in lesser risk of associating content from different SPs to the same user. Initial transaction duration is expected to be longer as a result of the greater complexity of the SSO operation; but overall, performance and assurance would be greatly enhanced.

APPENDIX B: Different Types of e-Authentication Token

A token is something that the Claimant (user) possesses and controls, and is used to authenticate the Claimant's (user) identity. A token is provided to the Claimant (user) for the purpose of electronic authentication.

Listed below are some of the tokens that may be used for electronic authentication. Each of them has their own strengths and weaknesses. Furthermore, the token is perceptible to malfunction, damage and tampering either intentional or un-intentional.

The agency / authority issuing the token should take the necessary steps to ensure the validity of token throughout its life cycle.

Shared secret token

Shared token is a set of characters (alphabets, numerals and special characters used in different combinations) or a set of pre-determined prompts and answers (shared information) agreed between the Claimant (user) and the Issuer. A slight variation of the shared information is the *context specific shared information* which is based on information pertaining to the relationship between the relying party and the Claimant (user)

These kinds of tokens include passwords, PINS and shared prompts and answers.

Look Up token

Look Up token is a form of single use one-time passwords to authorize transactions. It consists of a list or database of *shared codes* provided by the Verifier to the Claimant (user). The Claimant (user) provides an un-used code from this list / database when prompted by the verifier.

Generally, Look up tokens is used as a second layer of authentication (*dual factor*) above and beyond the traditional single-password authentication. This kind of tokens include Code books, TAN cards

Out of Band token

An **Out of Band token** is a secret sent from the verifier to the user through a *pre-established secondary communication medium*; the user subsequently submits that secret in to the primary channel for authentication. Such Out of Band communication includes telephone voice channel / IVR, mobiles SMS, Email etc. A callback on a pre-registered origin i.e. IP address, telephone nos etc is also a form of Out of Band communication.

Event based OTP token

A **one-time password (OTP) token** is a password that is valid for only one login session or transaction. OTPs are difficult for human beings to memorize and therefore they require additional technology in order to work. An OTP device is a specialized hardware device that displays an OTP which is calculated within the device based on a secret shared with the credential issuer. OTP devices may require a PIN to be submitted to activate the device to generate an OTP, though not always necessary.

Cryptographic token

A persistent symmetric or asymmetric *cryptographic key* stored in or generated by means of either hardware or software is a **Cryptographic token**.

For example, a cryptographic key is used to encrypt a challenge issued by the verifier and submit the response back. The verifier in turn decrypts the response and if it matches the challenge issued by it originally, it effectively authenticates the Claimant (user) since only the user would have the correct key to encrypt the challenge in the first instance.

Biometric token

Biometric token is a distinguishing physiological or behavioral characteristic presented for verification against a database of such characteristics, and which is managed and maintained by the Verifier.

For example Retina scan, IRIS scan, Finger prints, Voice etc.

Hybrid token

The term '**Hybrid token**' is essentially not a token in itself but refers to the use of two or more of the tokens in combination, to increase the effective level of strength of the authentication process. This is also referred to as a *Multi factor authentication*.

For example, the use of Shared secret (password) or biometric token to unlock the smart card containing user's private cryptographic key.

APPENDIX C: Risk Management

A Agency's system may contain multiple categories or types of transactions and may span multiple Agencies; all of these may require different security considerations within the overall risk assessment.

A formal risk management program will help identify and mitigate risks associated with e-Authentication Management. These may include:

1. Identity Authentication: Do the electronic credentials presented belong to or identify the person he/she claims to be?
2. Integrity: Has the information been altered in transit or during processing?
3. Confidentiality: Can the Agency ensure that information remains confidential while stored or in transit?
4. Non-repudiation: Can Agency prove that a given identity has submitted or approved or signed the information received?

Agencies should conduct a thorough analysis of all possible threats including factors such as general failures and human behavior. The overall risk may be rated 'low' based on the probability of the threat being realized, however it is still recommended to include all possible threat scenarios during the analysis phase.

The risk from an authentication error is a function of two factors:

1. Potential Impact
2. Likelihood of the Impact

Possible categories of impact include

1. Loss or impact on reputation of the agency
2. Financial Impact
3. Impact on agency programs or public interests
4. Unauthorized release of sensitive information
5. Personal safety
6. Civil or criminal violations / Legal Impact

The next step is to determine the potential impact of Authentication errors.

Category	Severity Levels				
	Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
Loss of or harm to reputation of the agency / Inconvenience to any party	No Impact / No Inconvenience	No Impact / Minimal Inconvenience	Minor: Short Term damage / Minor Inconvenience	Limited Long Term damage / Significant Inconvenience	Severe or serious long term inconvenience, embarrassment to all or some or one of the involved parties
Financial Impact	No Loss	Minimal < 2% of monthly agency budget	Minor 2% to < 5% of Monthly agency budget	Moderate 5% to < 10% of Monthly agency budget	Substantial > 10% of Monthly agency budget
Harm to agency programs or public interests	No threat	No threat	Agency business or service delivery impaired in a minor way. Services affect internal users and in a small way to its external customers.	Agency business or service delivery impaired in a moderate way. Services affect its external customers in a major way.	Agency business or service delivery impaired in a severe way. Services affect other agencies and their services.
Unauthorized release of sensitive information	No Impact	Would have little impact	Measurable impact, breach of regulations or commitment to confidentiality	Release of information would have significant impact.	Would have severe consequences to a person, agency or business.
Personal safety	No risk	No risk	Minor risk of injury not requiring medical treatment	Moderate risk of minor injury or limited risk of injury requiring medical treatment	High risk of serious injury or death
Civil or criminal violations / Legal Impact	Would not assist in or hinder detection of unlawful activity.	Would not assist in or hinder detection of unlawful activity.	Prejudice investigation or facilitate commission of violations that will be subject to enforcement efforts	Impede investigation or facilitate commission of serious crime	Prevent investigation or directly allow commission of serious crime.

Table 5: Impact Assessment

It is also necessary to map the likelihood of the occurrence of these impacts in order to determine the assurance level to be applied.
An indicative mapping of impacts versus likelihood is illustrated in the table below:

Likelihood	Consequences / Impacts				
	Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
Almost Certain	Nil	Low	Moderate	High	High
Likely	Nil	Low	Moderate	High	High
Possible	Nil	Minimal	Low	Moderate	High
Unlikely	Nil	Minimal	Low	Moderate	Moderate
Rare	Nil	Minimal	Low	Moderate	Moderate

Table 6: Impact vs Likelihood (Indicative Assurance Levels)

In analyzing potential risks, the Agency must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there could be multiple failures or impact multiple persons.
The definition of potential impact contains terms such as “serious” or “minor”, where minor will depend on context. Agencies should consider the context and nature of the persons / entities affected to decide the relative significance of these impacts.

Risk Management
The risk assessments should be summarized in terms of potential impact categories (Table 5).

- ✓ Based on your analysis identify the severity level for the associated impact category.
- ✓ Identify the likelihood of the impact or threat being realized.
- ✓ The function will provide you with an risk level (Table 6).
- ✓ Choose the minimum level of risk that will cover all impact / threat categories.
- ✓ The chosen risk level will map to assurance level.

Risk	Assurance Level
Nil	Level 0
Minimal	Level 1
Low	Level 2
Moderate	Level 3
High	Level 4

Table 7: Mapping Risk level to an Assurance level

A higher assurance e-Authenitcation solution might be one way of mitigating threats, however Agencies should also consider alternative risk management approaches.

These could be in the form of enhanced security within the application, limitating information exchange or revealed and / or restricting certain “at risk” user communities etc

The Agencies should iterate the Risk analysis to ensure that existing information security strategies meet its requirements, the controls implemented are effective and functioning as required.

Such exercises should be conducted at regular intervals to manage the changing threat landscape and also whenever the business requirements change.

APPENDIX D: Legal Framework

The Qatar e-Authenitcation framework provides Agencies with an overview of principles and factors to consider while designing an e-Authentication solution.
While applying this document, the Agencies need to also consider the various national policies, directives and legislations that may have a bearing on such a solution.

Some of the notable ones are:

1. National Information Assurance Policy
2. Government e-Services Registration & Authentication Policy issued further to the Resolution of the Council of Ministers No. (18) Of 2010 on the implementation of e-Government policies
3. eCommerce Law
4. e-crime law Law

APPENDIX E: A case for Federated Identification

Today, individuals and enterprises can communicate and access critical resources more readily than ever before. The Internet allows users to connect directly with goods, services, and information, while enabling companies to link with their customers, employees, and trading partners.

Digital identity is a crucial element in the growth of sensitive data and confidential relationships online. All users create digital identities as they traverse cyberspace. At the same time, every enterprise creates identities to provide individuals with secure access to online resources and services. Without digital identities, there is no way to give certain users access to certain resources. Those resources might include a bank statement, the shipping status of an order, the email directory of co-workers, or the company intranet; the list is endless.

Multiple identities are the rule. Individuals employ different user names, passwords, and other identifying attributes in various online contexts due to practical limitations or out of a desire for anonymity. The same person may have links to many organizations. An Ooredoo customer may also be using MoI services and a KAHRAAMA account. Even within a single company, data tied to the same individual often appears in several different databases, whether by design or accident.

The proliferation of digital identities creates significant challenges. Users have trouble remembering multiple usernames and passwords. IT organizations find it increasingly difficult to manage the profusion of identity databases, even within the corporate firewall. The problem becomes worse when identities span organizational boundaries, as when providing partners access to an enterprise resources; allowing users to access online services in an enterprise with multiple databases thanks to acquisitions and legacy systems. When either the users or the companies take shortcuts, the result is increased management costs and increased security risks.

Why Federate Identity?

Federation is a standardized approach of allowing Agencies to directly provide services for trusted users that they do not directly manage. The identities of from one enterprise domain (or identity provider) are granted access to the services of another enterprise (or service provider). Within a federation, organizations play one or both of two roles: identity provider and/or service provider.

The identity provider is the authoritative entity responsible for authenticating an end user and asserting an identity for that user in a trusted fashion to trusted partners. The identity provider is responsible for account creation, provisioning, password management, and general account management. This may be achieved with existing locally accepted security mechanisms and tools. In a driver's license illustration, government is the identity provider responsible for validating the true identity of the citizen.

Those partners who offer services or share resources but do not act as identity providers are known as service providers. The service provider relies on the identity provider to assert information about a user, leaving the service provider to manage access control and dissemination based on these trusted sets of attributes.

Benefits of Federation

Federation establishes a standards-based mechanism of both sharing and managing identity information as it moves between discrete security, legal and organizational domains.
Federation enables a cost-efficient means of establishing single sign-on to cross-domain, cross-agency information. Federated single sign-on.
Federation provides Agencies managing multiple security domains with an efficient, lightweight mechanism of linking redundant identities and enabling single sign-on between security domains.

Conclusion

While today's existing identity management solutions can help increase security and reduce inefficiencies associated with managing internal users and access to internal information, increasingly the users that require access are outside of any one agency's control. Federated identity provides Agencies with an open-standards approach of enabling increased access to cross-boundary information.

Notes

Further to the Resolution of the Council of Ministers No. (18) Of 2010 on the implementation of e-Government policies, MOTC issued the Government e-Services Registration & Authentication Policy which mandates that all government e-services whether they be hosted and integrated (integrated services) or just accessed (pass-thru services) through the "Hukoomi" portal shall be authenticated through the Identity management services provided by Hukoomi.