United Arab Emirates

UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمارات العربية المتحدة
وزارة شـــؤون مجلـــس الـــوزراء
مكتب رئاسة مجلس الوزراء

هيئة تنظيم الاتصالات TRA
Telecommunications Regulatory Authority

"All initiatives are launched for the benefit of the people and for achieving their aspirations. So, all entities shall work to achieve these initiatives promptly. All obstacles shall be removed in order to translate these initiatives into concrete projects that positively change the life of people."

His Highness Sheikh Khalifa Bin Zayed Al Nahyan,
President of the UAE


"I want UAE Government services to be delivered to the public through mobile phones."
His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice-President and Prime Minister of the UAE and Ruler of Dubai

CONTENTS

INTRODUCTION

This document serves as a set of guidelines for government entities to prepare themselves in transforming eGovernment to mGovernment (Mobile Government). It will assist the entities in meeting some of the challenges of exploiting the benefits that may be gained from mGovernment. It contains a set of guidelines for making entities "m-ready" to the requirements of developing and implementing advanced mobile ICT-based applications and services.

SCOPE AND THE ORGANIZATION OF THE DOCUMENT

This document covers considerations that should be made when planning and implementing mobile services. It covers the technical and usability issues, how they should be handled and what security measures should be taken into account. The focus is more on mGovernment services development to be provided by the government entities in the UAE via mobile technologies and relevant devices including but not limited to smartphones.

As such the scope of the current document is limited and in its existing form does not cover guidelines for setting up entity level wireless networks, use of wide area networks nor the use of devices for offering services as part of a typical enterprise mobility adoption.

An exception is made in the security section, which covers a range of risks such as high-level generic security concerns, risks associated with local wireless networks, communications, applications, data and devices.

The organisation of the document is as follows:

- In the next section a set of guidelines is provided to help government entities decide how to select and prioritize which services should be offered as part of the mGovernment. These decisions are based on understanding what mobile service is and what kinds of criteria should be followed in determining mGovernment services and appropriate technologies.

- Then, the document covers in detail mobile application development considerations including various platforms, APIs, user and usability issues, the mobile content and assuring user adoption.

- A wider view on security is given including a complete consideration of enterprise-wide mobility.

- The document finally ends with guidance on developing and maintaining a secure payment system for the mGovernment services.

This document is intended for the use of mobile service designers, IT departments and project managers within government entities.

BACKGROUND

The government entities in the UAE are mandated to improve their services via a strategic utilization of mobile technologies by May, 2015. This entails primarily moving eServices to mServices via adoption of mGovernment. Ideally this should result in practices of Mobile Government, offering seamless, interactive and intelligent applications and services. The expectation to implement Mobile Government should be based on the realistic assessment of resources and capabilities that each of the entities possesses. Nevertheless, it is always positive to think about the ultimate goal, the possibilities and what could be done given the advances in mobile technologies and mGovernment practices.

STAGES OF MGOVERNMENT (MOBILE GOVERNMENT) EVOLUTION

The mGovernment evolution focuses on the strategic utilization of the most advanced ICTs, particularly mobile technologies, in transforming the ways government organizations work, in order to best satisfy the needs of the citizens through seamless intelligent and interactive communications anytime, anywhere, with any device, working effectively with all relevant stakeholders.

- mGovernment involves at least two distinctive enhancements in the public sector:
  - Structural improvements of business processes and the way employees work.
  - The most convenient services offered according to citizens' needs.

- Mobile service delivery, although not easily segmented as below, can typically be deployed as follows:
  - G2C Mobile Services (Notification, Live Traffic SMS, Nearest Hospitals etc.)
  - G2B Mobile Services (Business Registration, Fee Enquiry etc.)
  - G2G Mobile Services (Patient's Medical History Sharing)
  - G2E Mobile Services (BYOD, Hot Desk etc.)

- mGovernment employs the most advanced mobile technologies transforming eGovernment to Mobile Government:
  - It is available 24/7 regardless of place, platform or device.
  - It employs the most advanced intelligent mobile technologies such as location based and context-aware applications and services.
  - It is seamless to the users due to its effective integration and the use of intelligent X2X communications – X maybe a machine or a human.

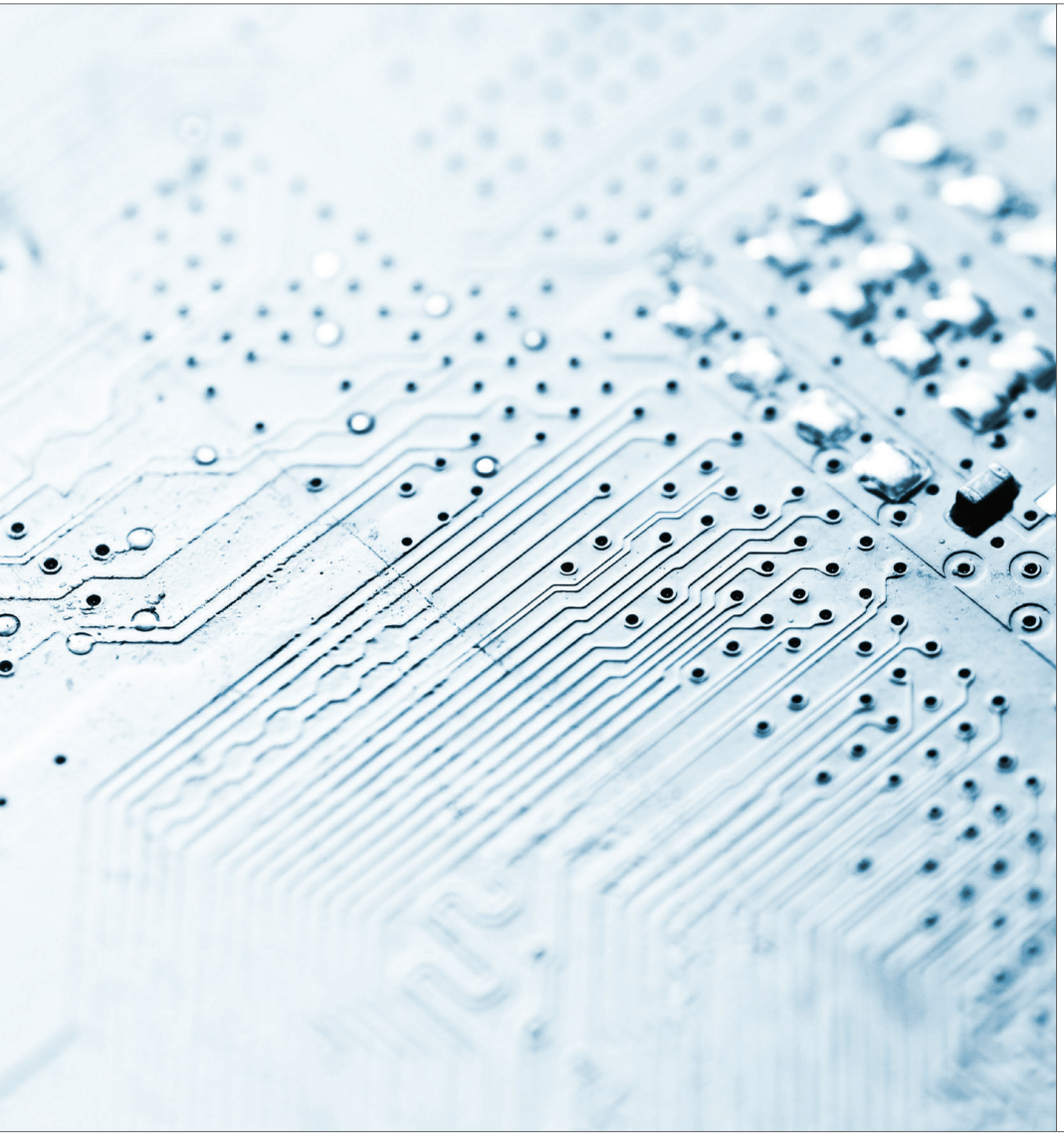
- mGovernment is most effective when it creates partnerships among Public Sector organizations, with the Private Sector, NGOs and Civil Society organizations whenever there are commonly shared objectives.

The table to the right shows these stages of evolution of mGovernment in relation to advances in mobile (ICT) technologies and the level of maturity in eGovernment and data/services and integration among the government entities. The examples used in the table are purely hypothetical.

Thus, Mobile Government is at the core of transforming eGovernment to mGovernment (Mobile Government) via approaches to use mobile technologies at various stages and levels. mGovernment enhances eGovernment in various ways by creating a favourable working environment by allowing government employees to work mobile, and improving lives of citizens through high quality government services, which allow efficient interactions using mobile devices.

A spectrum of mGovernment service delivery formats

	SMS (INFORMATION/ PUSH SERVICE)	SMS (INTERACTIVE/ PUSH & PULL SERVICE)	MOBILE VERSION OF ESERVICES	TRANSACTIONAL MOBILE APPS	INTEGRATED MOBILE APPS
G2C*	Vaccination alerts	Receiving school exam results upon demand	Applying for a birth certificate	Paying traffic fines	Doing multiple complementary services: changing home address and updating National ID card and employment record at Ministry of Labor
G2B	Business license renewal reminders	Query on business license application	Applying for business license	Business license renewal and payment	Sharing and exchanging information between government entities: Granting business license and updating records at Ministry of Labor and Dubai Economic Department
G2G	N/A	N/A	N/A	Sharing and exchanging information between government entities: Patients' records across all hospitals and medical centres.	
G2E	N/A	N/A	N/A	Providing tools and information access to government employees: Accessing the traffic department to issue a fine for illegal vehicle parking and updating records in relevant departments	



TYPES OF GENERIC MGOVERNMENT ENHANCEMENTS OVER EGOVERNMENT

Understanding the enhancements of mGovernment is crucial to understanding what kind of services are suitable as well as relevant and which should be considered for mobile services development.

Below are four different types of enhancements that mGovernment brings to the conventional way of offering services in public sector organisations.

- Direct Conversion from eGovernment portal: This is transforming suitable services from among existing eGovernment portals into suitable mGovernment services. These are conventional web based services, which are also made available on the mobile platform.

- Citizen-centric new mobile services: These are distinctive mGovernment services that may not be available in conventional eGovernment but are made possible due to mobile technologies. For instance, mobile payments for public transport and parking as well as location-based provisions of services.

- Services for mobile workers: This is field force automation where government employees working outside the offices (such as employees of emergency services and inspection services; patient care at home are equipped with mobile devices and technologies.

- Flexible working: This is about government entities promoting remote working such as working from home and allowing its employees to use mobile devices in the office and "hot desks".

The types of enhancements suggested do in no way imply a complete set of tasks that each government entity should be implementing. The primary implementations in mobile government may necessarily be converting eServices to mServices and focussing on citizen-centric applications (G2C).

A FEW CONCEPTUAL CLARIFICATIONS ON MGOVERNMENT

A few critical points that have always been somehow confusing or not clear in the minds of mGovernment implementers since the idea of the mGovernment had first been articulated:

- mGovernment does not replace the eGovernment but it complements and enhances the existing systems and services.

- mGovernment is not limited to mobile phones, but extends to all mobile and intelligent devices (this may include machine-to-machine communications).

- mGovernment has two broad and distinctive objectives:
  - Improving citizen interactions by offering services to citizens via mobile or intelligent technologies and
  - Improving public sector organisations, process engineering and public sector modernisation, and interactions within government entities.

- Technology and services development are at the core, but are the simplest element in adopting Mobile Government. However the soft issues are of significant importance, such as strategic approaches to mGovernment, capacity building in government, change management, building mobile society, assuring user adoption and use.

One of the first steps and perhaps a very critical step for government entities in transforming their eServices to mServices is evaluating and deciding which services should be migrated and how they should be prioritised in this process. This requires careful consideration of at least four significant issues:

1. Defining what constitutes a mobile service
2. What is suitable for mobility
3. Who are in the target audience
4. What are the selection criteria for choosing services to migrate
   - Citizen requirements (surveys/online polls)
   - Adds value (i.e. increases efficiency in completing a task)
   - Volume of transactions
   - Frequency of use
   - Ease of transformation
   - Potential for revenue stream

It should be noted that migration from eGovernment to mGovernment is not a one-to-one processes. There are eServices, which may require that they be aggregated into one mService. At the same time there may be one eService that may be broken down into a few mServices. It is also very likely that the entities will have to offer completely new mServices in order to exploit the benefits on mobility and improve their services via this new channel, offering new services that are not normally possible via conventional means.

MOBILE SERVICES DEFINITION

What constitutes a mobile service and what is an overall experience of a user with a mobile service? Mobile Government is the extension of eGovernment so that government services are provided from anywhere and at any given time through smart devices (mobile phone applications, laptops, PDAs etc.) to serve the customer effectively and efficiently.

The customer experience may be divided into four distinct interactive steps.

Steps 1 – Get Service Information: The customer finds out what kind of service is required and how, when and where to get it.
Step 2 – Apply for Services: The customer initiates the interaction with the Federal Entity to obtain the desired services.
Step 3 – Interact during Processing: The customer starts using the service and pays for it, if applicable, and receives the services.
Step 4 – Complete Services (End-to-end): The customer completes the service interaction and receives the final and expected output.
This simple view is shown in Figure 2 below:

TYPES OF ENHANCEMENTS OF MOBILE SERVICE

mGovernement enhancements may be simply viewed as four different categories of mobile services, which can be summarized as follows:

Informational Services

Users may access current government information, vote or make a request, register and report. This is mostly true for the static information that does not require extensive interaction with the citizens i.e. weather, regulation, emergency, exam results, road closures, events, schedules, fee changes information and notifications. SMS is broadly used in these applications. Interactive Voice Response (IVR) or Interactive Video Response (IVVR) may also be used. Informational and educational services tend to use SMS or distribute information via mobile web or WAP.

Interactive Services

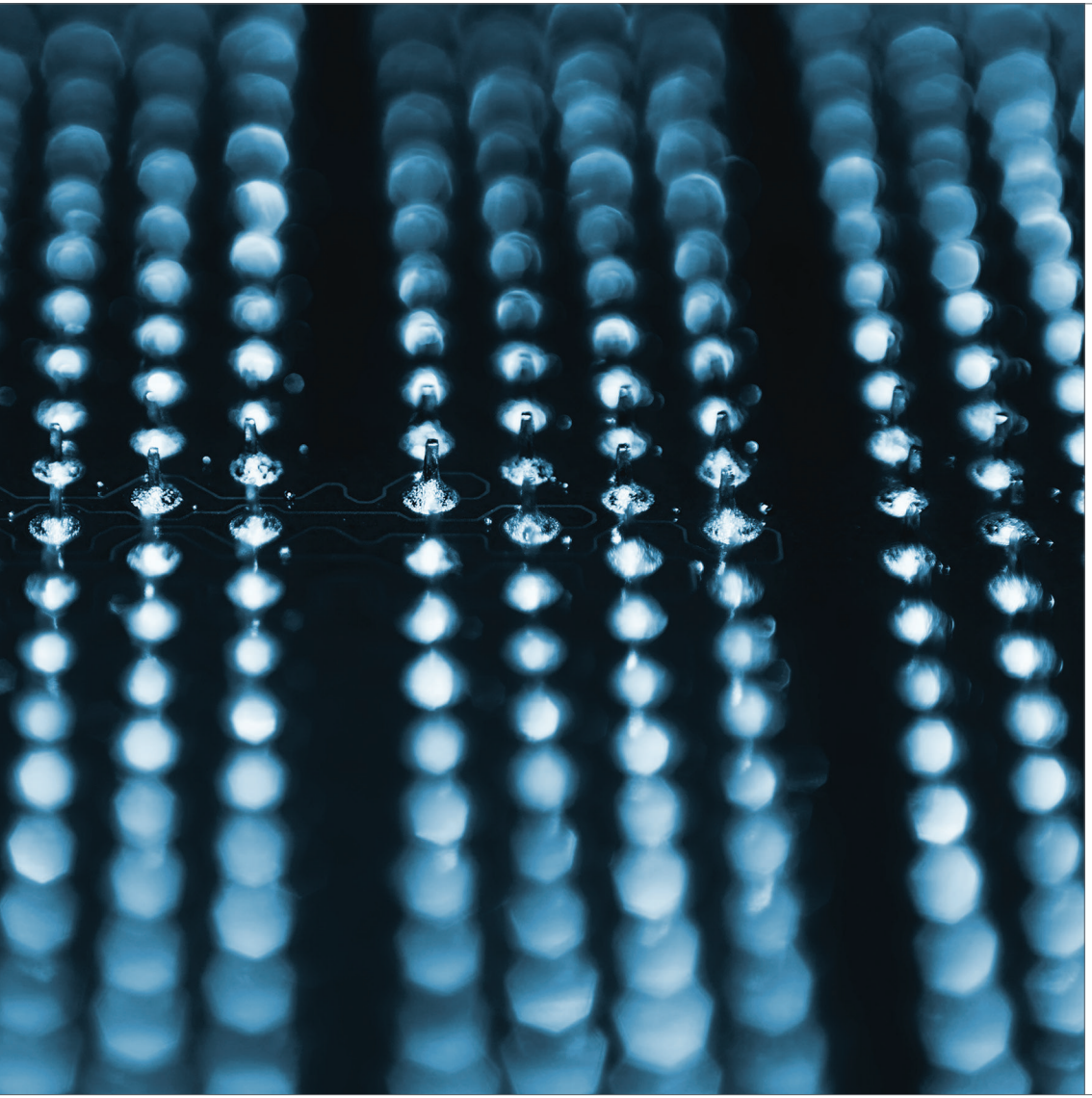
This constitutes applications which enable citizens to engage in dialogue with the government. Interaction is often conducted on a personal level, which involves sharing personal data, applications, access to certain databases and specific service areas. Location-based technologies, such as, photo/video capabilities and mapping tools act to increase the possibilities of available services. More recently, there is evidence of an increase in the use of social media tools in the capacity to communicate urgent news and 'real time' information sharing. Interactive services such as health (monitoring, tests, and screening), education (admissions and exam results), information inquiries (live traffic info, account information) and law enforcements are but a few of the wide scope of possibilities open to the use of interactive applications.

Transactional Services

These are 247/ mobile services that allow citizens to make applications, post jobs, buy bus tickets, book appointments, and sign a transaction with a mobile signature. Arising from these types of services are security and privacy issues, which require specialized technology initiatives for secure transactions and storing sensitive information in a secure way. Mobile signature technologies and NFC payments all require uniquely designed security systems.

Integrated Services

These are mobile services that combine services and/or data from different departments of the same entity or different entities. These generally make it more convenient for the citizens by allowing the integration of different services. A live traffic update service, for instance, may integrate the services of the Road and Transport Authority (RTA) along with mapping services to suggest different routes and to inform users of nearest points of interest. Integrated services are generally those which bring the most value to the citizens and are the main focus of mobile development in the UAE. Government entities are encouraged to collaborate with other entities and develop solutions for integrated services.



MOBILE TRANSFORMATION BASELINE

All government entities should achieve Step 1 and Step 2 as a minimum baseline in order to be considered mobile enabled.

As a first phase, all government entities should focus on Citizen-centric (G2C) services as an immediate priority for mobile transformation.

MOBILE SERVICES SUITABILITY

Even though mGovernment may be seen as an extension of eGovernment services, the existence of eGovernment services is not a prerequisite for the deployment of mGovernment services. This means that the transformation to mGovernment is not carried out only via migrating existing eServices onto the mobile platform. However, typically an entity would start by evaluating its existing eServices. In most cases, informational and transactional services will be the ones that entities will be starting with.

Before making any selection for migration of eServices, it is necessary to:

1. Evaluate whether services are suitable for mobilityby mapping between the requirements of a service, the constraints of the capacity and use of mobile technologies to offer such services. For example, services requiring attachment of documents for the user to apply for a business license may not be highly appropriate for its mobile version. This also applies, to complex maps or visual content, which require detailed examination and perhaps memory and processing requirements when it is migrated to mobile. Such applications may not even be required to be on the mobile platform.
2. Evaluate the complexity and viability of the required change on the workflow and process engineering This may be an additional principle in implementing services on a mobile platform. Services that lead to process re-engineering that simplifies the business processes and eliminates unnecessary steps taken by the user are relatively more suitable for implementation in the mobile.
3. Take into consideration certain eServices which are core services of the government entities essential in serving citizens, but which are not suitable for mainstream devices. Entities may consider employing particular tailor-made devices and software to enable these services. Examples include vehicle number plate identification and checking systems or intelligent outdoor cameras reporting traffic information.

MOBILE SERVICE SELECTION AND ELIGIBILITY

Choosing which services are eligible and potentially beneficial to move to the mobile platform is neither an easy nor a straightforward task. Each entity must develop and run its own set of evaluation mechanisms. However, there are certain principles, which may guide entities to develop such selection methods for their entities. The suitability test mentioned above is the first task. A typical set of additional considerations may include whether a service is:

- An essential part of the operation and service quality of the entity
- Used in high frequency
- High in volume of transactions
- Generating new revenue streams for the entity
- Easy to develop (or transform) and maintain
- Adding value to citizens' lives
- Simplifying an entity's processes or workflow
- Providing efficiencies such as cost and time
- Improves the reputation of the government
- Suitable for the target audience
- Demanded by the citizens (based on surveys and polls)

The list above does not suggest that any of the considerations take priority over another. A particular entity may find its own unique set of criteria, as these may not be applicable to all entities. What is important is to recognize that all services may not be suitable for mobile platforms, therefore each entity will have to prioritise which services among a large number are the best candidates for migration.

OVERVIEW OF MOBILE APPLICATION CHANNELS

Mobile strategies involve considerations on several key points: the available ICT infrastructure; technology requirements of the intended service; accessibility and usability of the services by citizens. The growing market for mobile devices, increasing quality of mobile networks and high demand for quality mobile applications are together providing endless opportunities for more efficient business operations in public service and opening up new interaction possibilities with citizens. Therefore, it becomes a very critical issue to have a solid vision on what goals are targeted with the public service and what options are available in terms of technology. In this section, channels for developing mobile government applications under the light of the latest trends in mobile technology are presented.

VOICE CHANNEL

Voice channel is still a viable option in mobile communication owing to its:

- Applicability on all devices
- Simplicity of use (no literacy needed)
- Higher capacity for communication and information sharing
- Familiarity

Innovative voice applications have been developed for interactive voice dialogues with computers allowing numerous applications such as voice access for driving directions, processing telephone calls, speech recognition, voice based web access etc.

SIGNALING CHANNEL

SMS: Due to its ease of use and popularity, SMS is still being used for many applications such as notifications, news and weather updates, emergency situation management, healthcare and medical reminders, voting, donation and payments etc. Voice SMS and Video SMS channels also provide ease of use for the end users and provide new ways to deliver information both to mobile public workers and citizens.

Unstructured Supplementary Service Data (USSD): Transfer of messages take place directly over network signaling channels so it is free and highly accessible. Good usage areas are secure mobile banking, news and submission services, and voting.

WAP (Wireless Application Protocol): WAP is a protocol that enables access to the Internet over mobile wireless network. Rather small mobile devices use WAP browsers that enable access to websites with wireless markup language.

DATA CHANNEL

Available in different forms of mobile messaging: Application to Person (SMS, MMS); Person to Application (enabling users to upload content: popular usage in voting and photo upload etc.); Person to Person and finally Machine to Machine (asset management, tracking, remote maintenance, POS/payment, healthcare security, smart metering etc.)

The data channel opens significant opportunities for developing applications processing data. Better data coverage and advancing mobile devices make data applications and mobile web a convenient solution for data mobility and access to rich content anywhere, anytime.

The mobile application development process starts with analyzing the nature of the service that will be transferred to the mobile platform. Each and every service will require particular functions to be utilized by the application without compromising user convenience and design related priorities. Choosing the platform and mobile channel to develop the application is a fundamental step in achieving the best outcome. There are both advantages and disadvantages to each delivery system and the nature of the services will be the decisive factor. The information below is intended to guide government entities to decide which type of application is more suitable for their project.

Please refer to the information below and ask the following questions to decide how to develop the application:

- What is the current market share of smartphones and operating systems?
- How much is the budget set aside for the project?
- How often does the application content need to be updated?
- How quickly should the application be developed and made available?
- What is the expertise level in the entity to develop the mobile service?
- Who are the targeted users and what are their expectations?
- What is the security level required?
- What is the level of simplicity targeted in the service?
- Is there Shared API for developers' use? (In case there is, it should be used)

NATIVE APPLICATIONS

Native application development is dependent on the mobile operating system. Different platforms require different tools and programming languages to be used for application development. Hence, each application requires expertise on the platform, devices, several programming languages and coding. In terms of usability, there are several features that are only available in native applications:

- Multi-touch Gestures: Several types of customizable gestures that aim to enhance user experience and usability. Functionalities can be customized for double-tap on the screen, swipe and spread pinch for intuitive usage of the applications.
- Advanced Animation and Graphics: In applications requiring extensive data and fluid animations, native applications provide the best functionality with fast graphic API.
- Integration with Device Features: Native applications make seamless use of the mobile device's native components such as the camera, voice recorders, GPS etc.

NATIVE PLATFORMS

- Android: Google's operating system for mobile devices.
- iOS: Developed by Apple Inc. iOS operating system is known for its intuitive features and enormous application market called Apple Store.
- Blackberry: Designed and operated by Research in Motion as a 'personal digital assistant' capable of internet browsing, e-mails, and media.
- Windows Phone: Operating system developed by Microsoft. Targeted mainly at the customer market rather than entities.

For each of the operating systems or platforms, there is an application store review process for each application registered. Entities should have a developer account in these platforms to register. It should be noted that the review process takes approximately two weeks after submission, given that there already is a developer account on these platforms.

	LANGUAGE	APP STORE
Apple OS	Objective C, C, C++	Apple App Store
Android	C, Java and C++	Google Play
Blackberry OS	Java	Blackberry App World
Windows	C#, VB, .NET	Windows Phone Market Place

MOBILE WEB APPLICATIONS

Mobile web applications are websites that are designed for mobile device use typically using standard web technologies like HTML5, JavaScript and CSS. These applications are compatible with different browsers, platforms and operating systems through a 'one size fits all' approach.

Compared to native applications there are some crucial limitations to mobile web applications:

- Native device functionalities (GPS, camera etc.) cannot be integrated into mobile web applications as with the native applications
- Session management remains an issue as opposed to native applications
- Offline use and storage of data functionalities cannot be provided with mobile web applications.

HYBRID APPLICATIONS

The issue that mobile web applications cannot utilize mobile device functionalities brings us to hybrid applications that are basically mobile web applications written with standard web programming languages, e.g. JavaScript and HTML5, and that are wrapped in a native container. In many ways this combines the best of mobile web and native application features such as the ease of development, offline usage and utilization device capabilities.

WHICH APPROACH TO CONSIDER?

To develop a decision-making framework for choosing which type of applications to use for the services, a number of conditional guidelines, depending on the nature of the service, are listed below:

Analyze Targeted Audience

- Understand the unique requirements of your audience. Know your target audience and analyze what types of devices they are more likely to use, what preferences they have, what are the latest trends among them If possible:
  - conduct surveys or online polls to understand their expectations.
  - check the web statistics to find out the types of devices and platforms on which users are currently using your application.

Development Costs

- If financial cost and technical resources are major concerns, mobile web applications beat native applications. Native applications require separate application development and expertise for each platform.

Cross-compatibility

- Cross-compatibility is frequently imperative in public services. Rather than developing several different applications on different platforms for the same service, it might be more efficient to invest in a mobile web hybrid application to reach out to citizens.
- When developing native applications it is recommended for all government entities to use Cross Platform Framework (e.g. PhoneGap) and Tools (e.g. Titanium Appcelerator) in order to reduce costs and efforts.

Application Life Cycle

- The life cycle of native applications is considerably short. If life cycle management decisions favor long-term applications, native applications are not always the best choice.

Utilizing Device Features

- If the nature of the mobile service requires integration with a device's native features (e.g. camera, geo-location), mobile web applications cannot provide that. Native and hybrid applications make use of the device's capabilities and hardware sensors.
- Native applications provide a better user experience in many ways by utilizing special gestures, graphics, device sensors etc.

Security

- When security is a question, it might be argued that native applications have particular risks due to their internal data storage properties as well as utilizing the hardware sensors. In case of loss of a device, native applications might let unauthorized people access sensitive data stored on the device whereas, in the case of mobile web, the data storage is safe out of the device. Utilization of device features might also cause security problems as in the case of tracking of a device's location by interfering entities via the application.

Integration

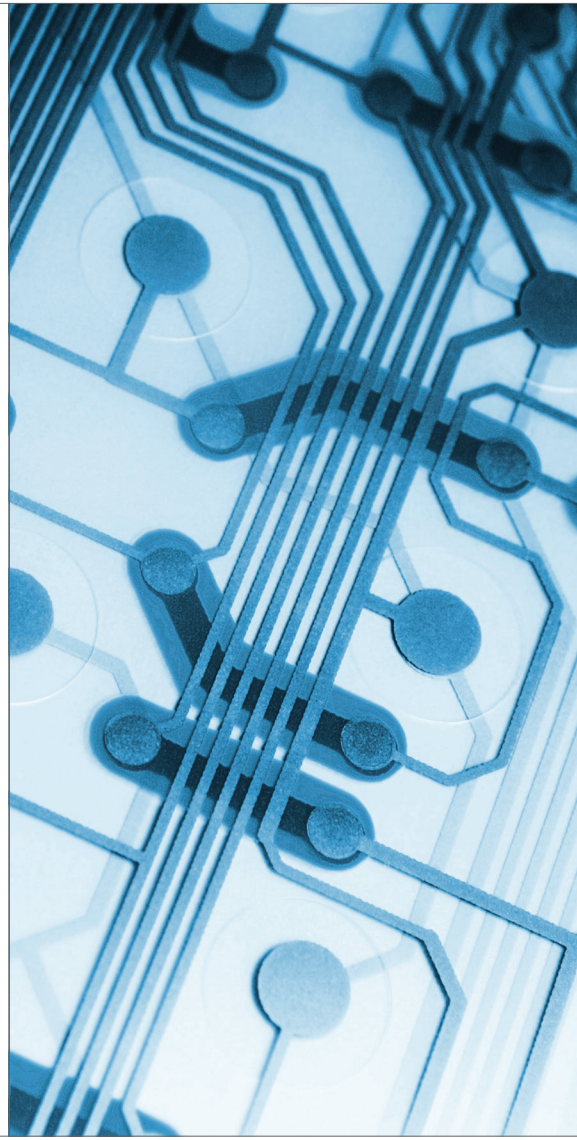
- When applications need to access the current systems or existing databases integration is crucial. Native applications are mostly either impossible to integrate into the existing systems or very troublesome. Mobile web or hybrid applications, on the other hand, are more easily integrated into existing platforms.

Access to Service & Visibility

- From the user's perspective, if the application is intended for immediate and fast access, mobile web applications should be considered. In order to be used, native applications have to be searched and downloaded first. However, mobile web applications are easily accessible from any device.
- Visibility of an application depends on the application type. Mobile web applications are displayed in search results, whilst native applications are displayed in application stores. Hence, mobile web reaches out to a wider community than native applications.

User Experience

- When the application requires interactivity with the user, native applications are the alternative to follow. Touch gestures and ease of navigation create a better user experience that is hard to achieve with mobile web applications.
- Native applications also provide user configurability to personalize the application to their own likes, in particular for the applications that are used on a regular basis; native applications will give users a personalized service.
- Offline access to mobile web application services is not as convenient as with native applications. Native applications can store data within the device for offline use, which works better from the user's perspective considering that access to the Internet is sometimes not possible.



Summary Comparison of Mobile Service Delivery Options

	NATIVE	HTML5	HYBRID
Graphics	Native APIs	HTML, Canvas, SVG	HTML, Canvas, SVG
Performance	Fast	Slow	Slow
Native Look and Feel	Native	Emulated	Emulated
Distribution	Application Store	Web	Application Store
Application Life Cycle	Short	Long	Long
Access to Device Equipment (GPS, Camera)	Yes	No	Yes
Notifications	Yes	No	Yes
Storage	Secure File Storage	Shared SQL	Secure File System, Shared SQL
Location Awareness	Yes	Yes	Yes
Connectivity Requirement	Online and Offline	Mostly Online	Online and Offline
Technical Skills Requirement	ObjectiveC, Java	HTML5, CSS, Javascript	HTML5, CSS, Javascript

Application Program Interface (APIs) are used to make mGovernment services or its functions available for use by other applications. Thanks to smartphones, traditional applications and even web applications are being substituted by new mServices.

New apps are being built quickly by mashing up existing services and capabilities in creative ways. An application no longer has a single user interface, but many interfaces. These interfaces can be built on different technologies, can target different types of users, and can be built by various interested parties. To enable these multiple interfaces, the Application Program Interface (API) has become the primary interface for applications both old and new. APIs are the new distribution channel for government services.

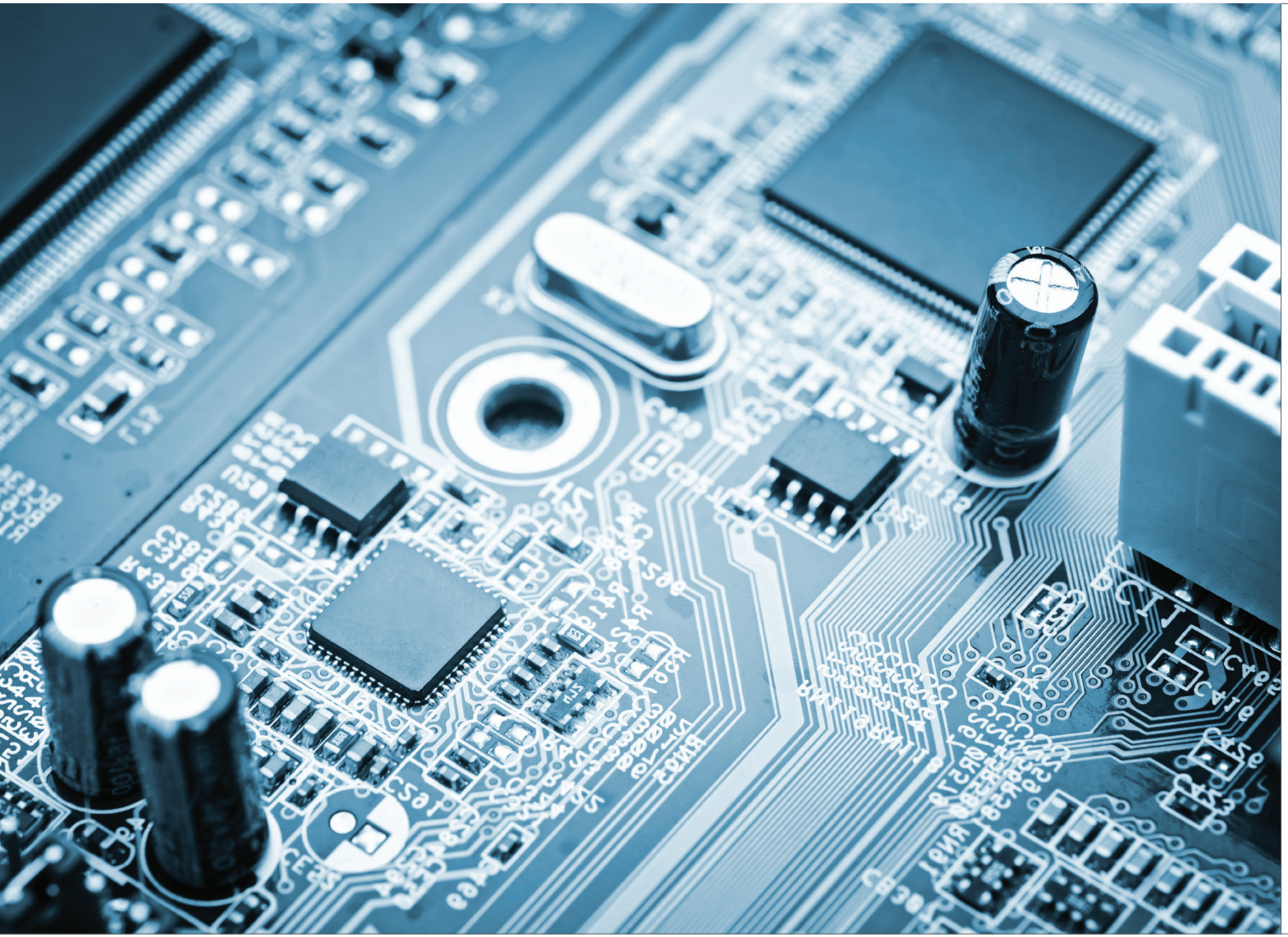
Government entities should embrace this trend that will bring thousands of mServices of public interest to citizens.

With the ability to deliver core business functionalities as APIs, a government entity transforms itself into a platform. In such a scenario, it's not enough to offer a set of APIs; this offer needs to be reliable, scalable, and secure. APIs should be offered with the same security and service level as their governmental applications. The secured and scalable delivery of APIs requires the use of an enterprise API management platform.

When implementing a successful API program some key questions should be observed. The adoption of standards de facto, the harmonization of the different government entities' APIs and the ability to create a common ecosystem to drive the innovative development of apps are key factors for success.

Government entities should:

- Define an API program and consider services which could be shared across the UAE government leading to an integrated ecosystem.
- Target the right developers mix you are interested in (internal, partner, third-party).
- Build the right APIs for your business. Define the APIs structure, search for advice on specific data, information systems, applications or even infrastructures to expose, define access tiers and policies of use.
- Evaluate the viability of Open Authorization (OAuth) Standard as its gaining support as an open protocol to allow secure authorization for clients to access server resources in a simple and standard method. It is being adopted in web, mobile and desktop applications.
- Identify top success metrics and measurement methodology. Monitor API traffic and use against set objectives.
- Build a modern developer portal to accelerate adoption of your APIs. It will help to attract and on-board external developers. The portal should offer browse and search APIs and access to the selected APIs.
- Ensure the developer's portal includes interactive API documentation, from which developers can execute live API calls.
- The developer portal should include self-service developer registration, key sign-up and account management.
- Establish a process for requesting developers to specify the users and applications that will utilize the APIs. Government entities should set up and enforce policies for approval to use the APIs.
- Developers should be notified about changes in APIs. You can create a list of favourite APIs to track and receive notifications on any event that impacts them. These events could be life cycle events, such as when a new version of the API is available.
- Offer community tools and content like blog, apps examples, sample code and a forum. Socialize the new ideas, apps, concerns and suggestions.
- Engage developers with support including ideas of what kinds of applications can be created with the APIs, and who the prime targets for app uses are.



Application design is not solely about the aesthetics of an application, it is also concerned with the ease and clarity of using an application. The user-centric design considers all aspects of the interaction with the application from installation/access to personalization of features.

There are a number of key points to pay attention to with regards to usability and interface:

Font Size

- While considering text font size, consider the target user's device screen sizes. As with many mobile devices it is the case that the screen sizes are not comparatively sized; therefore, the font size should not be too large. At the same time, keeping the font too small creates readability issues. Compromise should be found in considering the user experience and mobile device properties.

User Interface

- Make sure the User Interface (UI) buttons are indicating clear functionality and make sense to the users. If the application is using custom buttons rather than default ones, users should intuitively know what function the button serves and where it will take the user.
- In all stages of transaction completion the UAE logo should appear in conjunction with the government entity's own logo appropriately placed in the reserved place in accordance with government communication standards.
- The unnecessary crowding of buttons makes the navigation inconvenient. Icons or links should have enough space in between in order to avoid tap errors.
- When considering smartphone users, pay

attention to ergonomics within the application and design for convenient one-handed use.
- When visual icons are used rather than text, make sure they are logical to the user. Graphics should be clear and self-explanatory.
- Wherever possible, avoid forcing users to scroll.
- Be descriptive, brief and precise, especially on the alert screens.

Display Resolution
- Screen resolution choice should be made with consideration depending on the mobile device screen size and the amount of content to be displayed. In general, it is best to use large resolutions and less content on the screen, creating a more user friendly device.

Application Size Considerations
- If graphics are utilized in the application, seriously consider limiting their size to certain levels to control download times and battery usage. Although quality graphics lead to a better user experience, efficiency and performance issues are the priority for application users. Neat and speedy applications are mostly preferred over slow and graphics-heavy applications.
- To avoid slow download processes, application size should not be too large. It would be convenient for users if they can download applications on any type of connection be it Wi-Fi, 2G, 3G etc.
- It is advisable to keep the core application size to no more than 1215- MB. Additional features can be served as an add-on or in-application data download so as to avoid irrelevant use of device memory.
- In case of image usage within the applications, always use Alternative text (ALT text). This will be descriptive in cases where the image cannot be viewed due to download issues etc.

Battery Life
- Application properties should take into account the battery consumption and should not cause any drawback on mobile device battery life.

Terms of Use
- Applications should have an accessible Terms and Conditions page that clearly defines the usage agreements, property rights and credentials. Users should agree to the Terms and Conditions at least once within the application. It can be provided after the initial installation as a Terms of Use agreement page and allow the user to access the application only after agreeing to the stated terms. .

Clear Language
- Make sure all the text-based communication is done with an understandable terminology. According to the targeted users' profile, choice of words and terms should be considered. Complex sentences or excessive use of unfamiliar terms diminish the user experience.

Navigation
- Design intuitive architecture within the application. The application structure should be predictable for the user and accessing each functionality should be made easy.
- Deliver the information on a hierarchical basis sorting the most relevant as the easiest to access. The purpose of the application should be clearly identified and it should be assured that the user would find the intended functionality in just a few steps.
- Links to the main features of the application should be displayed in the main page of the application and users should be able to see the overall functionality of the application. Inner pages should have secondary links displayed clearly wherever applicable.
- Titles and links should clearly identify the purpose of the material. For each piece of content, applications should use clear and descriptive titles and links.
- Provide navigational buttons on each screen the user might get to. Considering the screen size, in many cases it can be more convenient to just display 'back' and 'home' buttons and navigate to other pages via home screen. Relevant in-content links may also help users navigate seamlessly within the application.
- Navigation icons and buttons should be designed to a minimum size 30-pixels. It should be clear where the navigation would take the user.

Integration with Device Features
- Make appropriate use of the device features when necessary, especially in cases where user interaction is applicable.

Performance
- Initial start-up of the application should not be time consuming. Delaying heavy process functions until after the start-up provides a better user experience.
- Application should crosscheck available Internet connections and use the wireless connection as a default wherever available. When excessive data usage will take place, users should be notified in case of a mobile broadband connection (2G, 3G etc.)
- Upon leaving the application the user should be able to return to the same page he or she had left the application from. It should be avoided to follow the same steps to get to the same page.

User Guidance
- Provide a 'help' button to instruct the user on how to use the application. Don't display application information on the landing page.
- Allow users to search within the application wherever necessary. Search results should be filtered and narrowed down by the user to get precise results.
- Let users know of the on-going activity within the application during processing periods to prevent users from thinking that an application has crashed.

Offline Usage
- The capability to save sessions or make use of the content for offline use functionalities should be made available to the user wherever applicable

Fundamentally, content is at the core of the use of a mobile service. Content could be delivered to the user with, for example, text, images, video, voice or a map. A user's interaction with the application content should be a matter of a carefully thought out design in order to enhance user experience and to deliver the intended service to citizens in a seamless and convenient interface.

Easy Reach of Required Content

- Make sure the content is delivered in a mobile friendly format, enabling users to quickly scan and find useful information at a glance.
- Give users as much control as possible over how the content is displayed. Do not display unrequested information in detail. Allow users to get in-depth content only when requested.
- Always design the content architecture for impatient users. Mobile device users tend to require quicker access to relevant content and tend to be easily distracted by interfering details.

Organization of User Interaction with the Content

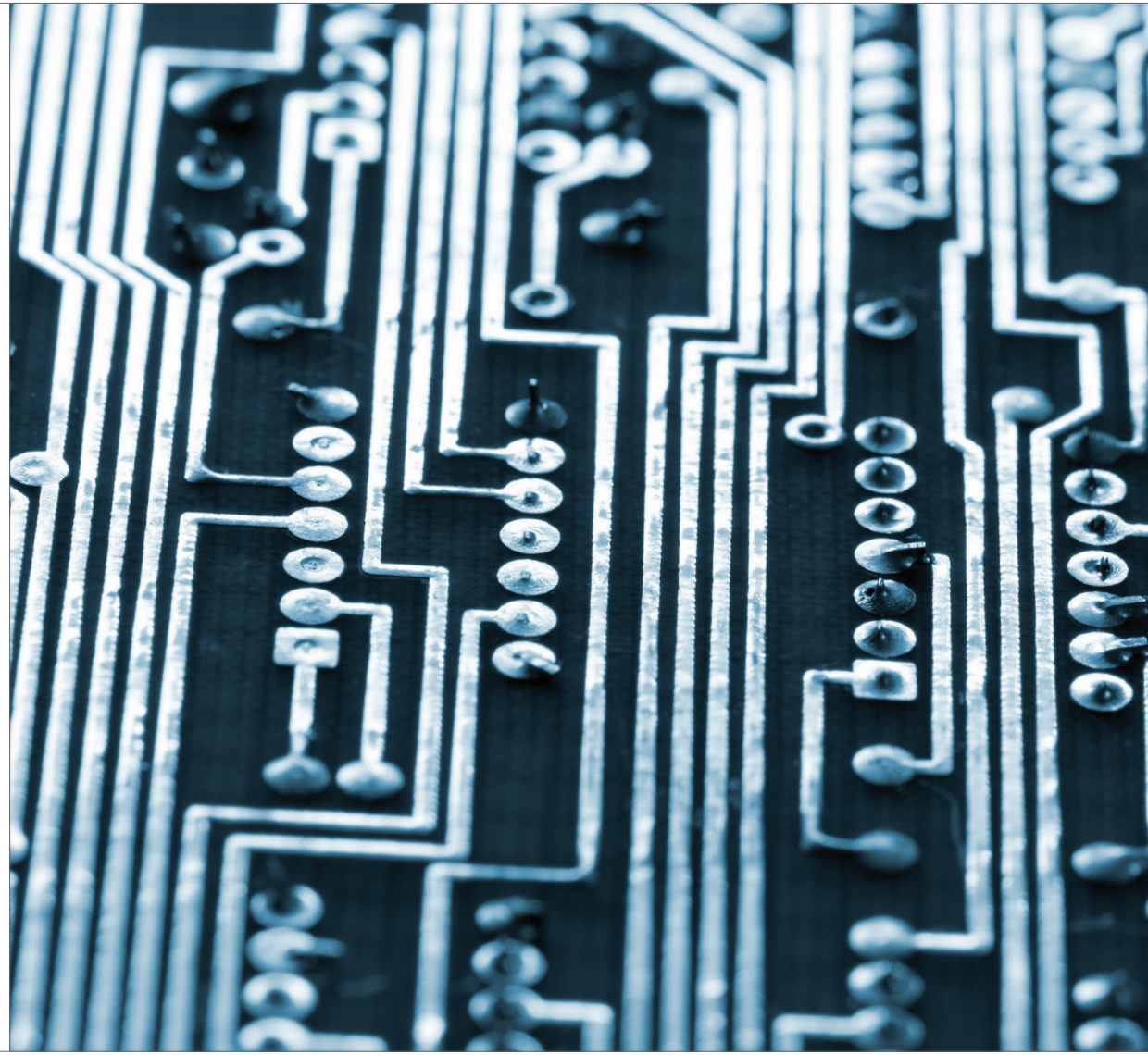
- Whenever possible, allow users to mark the content as favourite or to organize content in user-defined folders for later use.
- Users visit the application with a purpose. Present the tools and information with consideration for the user's task at hand and guide them step by step if necessary. For all the stages of the user-content interaction, allow users to know what the next step will be.
- Ensure that the content allows user interaction wherever relevant and possible. Certain services may need users to get involved in storing the information, to give feedback and comments, or to personalize and share it.
- Enable and encourage informational content to be shared via social networks or mail within the application without leaving the screen.

Content Structure and Variety

- Make use of inbound links within the application content to provide seamless access to categorical information.
- Present users with extra content other than the initial purpose of use. Unexpected bonuses within the application increase user engagement and satisfaction.
- Update the content regularly and also on every information change occurrence. Check the relevancy of the content for present use on a regular basis and omit expired content.
- When simplicity is not the main concern, provide the user with a mixed balance of content such as videos maps, texts and images.
- Consider language options depending on your target audience. Make English content available wherever necessary.

Implementing mobile services only is not the full task in government entities hands. Getting the citizens and government employees to use these mobile services may be a bigger challenge in some cases. Involving citizens in mobile service design, raising awareness and promoting adoption are crucial tasks of government entities.

- Conduct online polls or public surveys to get opinions and suggestions from citizens about which mobile services would most benefit them.
- Analyze your target audience via polls and surveys especially on how they use mobile technologies, what devices and operating systems they use etc.
- Implement desired mobile services via more than one mobile channel to ensure it reaches out to a broader group e.g. both SMS and a mobile application can be utilized for the same service and users can choose from which channel they would like to access the service.
- Promote new mobile services on government websites, the entity's own website as well as in the public offices frequented by citizens.
- Make use of social media and mass media to raise awareness of the offered services.
- All government entities are advised to provide incentives for using mGovernment services in order to raise adoption.



USER RELATED

When providing mobile services to citizens, neither institution-related nor citizen-related security risks should be overlooked. Mobile services should be developed with consideration for the privacy and security of the sensitive information shared and communicated during the use of service. Government entities should ensure the safe use of services by the users.

Mobile Service Authorization

- Implemented mobile services should be announced in the Government Application Directory (http://government.ae/en/web/guest/mobile-government) and users/citizens should be able to check if the mobile service they are using is actually authorized by the government via the directory.
- Citizens should be warned against unauthorized mobile services making spam requests from the users. Users should be encouraged to use only the government authorized applications and services for the mobile public service.
- It is advisable to show the government logo in each mobile government services offered to citizens.

Testing

- Government entities should perform security and usability tests prior to making mobile services available to the public.
- In future, the mGovernment Innovation Center will offer a spectrum of services which will include mGov Lab where various tests (e.g. security, usability, efficiency etc.) will be conducted to ensure that they meet acceptable government standards.
- More information about the mGovernment Innovation Center will be provided in due course.

User Registration

- Depending on the context of the application or mobile service, user authentication should be utilized whenever applicable. Entities should decide what type of authentication is more suitable for their services:
  - SIM card
  - Two-way authentication
  - Digital certification
- Government entities should contact Emirates Identity Authority (EIDA) for all matters related to user registration.

Device Registration & Device Security

- Device registration should be checked to ensure the service is being used by a device registered via Emirates Identity Authority (EIDA).
- Device deregistration steps should be set clearly and published to users in order to secure citizens in case of device loss/theft.
- When mobile government applications are being installed by the users, the device being used should comply with the following security requirements depending on the operating system:
  - iOS operating systems should not be jail broken
  - Android devices should have up-to-date anti-virus software installed
  - Windows Phones should have up-to-date anti virus software installed
- For more information regarding device registration de-registration please refer to Emirates Identity Authority (EIDA).

MOBILE APPLICATION CODING GUIDELINES FOR SECURITY

When developing mobile applications the usage characteristics, the existence of sensitive data or issues of sharing of private information should be considered and security measures should be put in place from the development phase onwards depending on the security level needed for the special case. The following guidelines will introduce several critical security issues related to mobile application development.

Sensitive Data Protection

- Classify stored data according to sensitivity and apply security measures accordingly. Make data processing and storage in accordance with these classifications.
- Wherever possible, store sensitive data on a server rather than the client's device. If data storage on the device is necessary use file encryption APIs provided by the operating system or another trusted source.
- Sensitive data storage should always be encrypted, as does cached data.
- Restricting data in certain contexts might be necessary as a precaution e.g. usage in a different location.
- For secure action, disclose data minimally for the user, that is, identify which data will be of use to the user. The rest of the data should be kept out of reach.

Password Handling

- When passwords need to be stored on the device, always ensure operating systems encrypt the passwords and authorization tokens. Do not use a device which stores passwords without encryption.
- When devices are utilizing secure elements, make sure the application makes use of these secure elements to store passwords and authorization tokens.
- Ensure that the option for changing the passwords is enabled.
- Ensure that passwords cannot be accessed via logs and cache files.
- Do not allow the application to store passwords in the application binary.

Data Protection on Transit

- Always assume that the network's layer is not secure and put precautions into place accordingly.
- When an application is sending sensitive data over the air/wire, enforce the use of end-to-end secure channel (SSL/TLS).
- Use strong encryption algorithms and keys that are long enough.
- Ensure the user interface informs the user whether the certificates used are valid.

User Authentication and Session Management

- Assist the user in choosing an appropriately secure password. (e.g. the length, use of uppercase and lowercase letters, symbols, numbers etc.)
- Use dual-factor authentication via SMS or email, if appropriate.

- If necessary, use context data to add further security to authentication (e.g. location)
- When the data is highly sensitive, put an added level of authentication in place depending on the service. (e.g. fingerprint, voice)
- User appropriate security protocols for session management after the initial authentication.
- Choose session identifiers with high entropy to avoid predictability.

Prevent Unauthorized Access to Pay-For Resources (mWallet, SMS etc.)

- Check for abnormal usage behavior and ask for secondary authentication in the case of abnormal behaviour (e.g. change of location)
- Keep logs of access to paid resources and make these available to the user only with authentication.

IDENTITY THEFT AND PRIVACY PROTECTION

One of the biggest challenges in mobile computing is ensuring user privacy and security. Transportability of mobile devices, which use increasing amounts of personal information, makes them vulnerable to identity theft by loss/theft of the device. Mobile service development requires strict security measures against potential threats of identity theft and privacy breach. Here follow specific guidelines that apply to identity management issues, some of which have already been discussed before in 'application security', but needs emphasis with respect to privacy concerns.

- Make the application-specific privacy policy available on the application platform so users can find out about the relevant issues. Also provide a clear privacy policy within the application.
- Mail clear warnings to users regarding the data practices taking place within the application that involves sensitive data interaction.
- Restrict the collection of users' personal data to information required by the service being used.
- Assign permissions to users to configure privacy settings within the application and let them know potential consequences of certain configurations. Ensure that the default settings are restrictive in terms of private information usage.
- Use complex encryption to store and transmit sensitive information.
- Ensure privacy controls and password operations are easily accessible by the user and that they are transparent. Allow users to change their passwords and provide secure ways to renew forgotten passwords.
- When a Mobile Identity system is implemented by EIDA, ensure mobile applications can integrate into EIDA authentication services wherever applicable.
- Be aware that the entity is accountable for complying with the privacy laws of the country and need to always ensure that every version of the application is within the limitations of these laws. Assign a person or a department to keep up to date with the latest laws and check each version for compliance.

TESTING FOR SECURITY

Developers should subject the application/mobile service to various tests to ensure secure usage. Entities should be aware of potential risks and check the vulnerabilities of the mobile services and mitigate threats with preventive measures. A systematic approach to evaluating security risks can be ensured as follows:

Analyze Usage and Risks

- Navigate through the application to analyze the basic functionality and workflow. Identify networking interfaces used by the application. Identify the protocols and security standards used by the application.
- Identify what hardware from the device can be utilized by the application and the potential hacking of these features (camera, GPS etc.).
- Check how the payment information, if any, is secured by the application.
- Identify what other applications the mobile service interacts with. Identify those that could potentially harm the integrity and privacy.
- Ensure the source code of the application is analyzed for inherent vulnerabilities.
- Check how user authentication is performed in the application and identify potential risks.
- Analyze data storage within the application. Consider the algorithms used in encryptions if they are vulnerable to known issues.
- Check what kind of data are subject to caching. Is there any sensitive information being kept in cache?
- Test the application against "man-in-the middle"attacks to analyze potential interference with the application.
- Check if sensitive data is being leaked to log files.
- Ensure security is maintained with care on the server-side, not just on the client-side.

HIGH-LEVEL SECURITY RISKS

As mobile connectivity overcomes all spatial obstacles and enables us to be connected anywhere and anytime, data transfer and access becomes a ubiquitous activity. Mobile devices connect via mobile networks, Wi-Fi, GPS, NFC or Bluetooth; however, these networks do not always provide the essential security. It is very common that mobile workers use these insecure networks outside the workplace and access strategic documents or applications. It becomes a key necessity to maintain confidentiality, integrity and authenticity of data on these types of networks.

Confidentiality

Confidentiality refers to the secure way in which data is transmitted to the intended user and no other interfering parties. Integrity is a measure of security to make sure no changes are made to the data during transmission. Finally, an authentication process makes sure that the sender is the trusted involved subject to send the data. Confidentiality refers to the process of preventing access to information by anyone other than the intended recipient. To provide confidentiality, the data is either encrypted or the data is sent through an encrypted tunnel.

Integrity

Integrity enables a recipient to detect whether a message has been modified by a third party while in transit, and authentication allows the recipient to identify the sender and trust that this sender actually sent the message. Strong data confidentiality and

integrity are especially critical for wireless traffic, as data can be more easily intercepted – and potentially compromised – by virtually anyone in the vicinity of the wireless network.

Integrity involves validating the trustworthiness of the data by using preventive measures. Encryption solves the problem on both the sender's and receiver's end by checking the validity of the decryption process while sending, transmitting and recognition.

Authentication
For authentication security, the devices should be capable of authenticating itself to the network systems and the server in return should be able to validate and authenticate itself on the device. Authentication can be enabled by a shared encryption system.

Traditionally government officers with office computers had security systems of network firewalls. The increasing mobility of today's workers demands enhanced network security that extends beyond the perimeter of office networks to cover mobile services as well. Since mobile devices are likely to be used outside the security of the office firewall, administrators need to secure data transmission by allowing only secured IP addresses to access the software and information. Certain adjustments need to be made to any inbound and outbound initiated connections. In some cases allowing only outbound connections might reduce the risks since the network will recognize the IP addresses. In this sense, push services are safer than pulling information from the mobile device as it does not need to grant access to the sensitive database.

Segmenting the network architecture in the workplace might improve data security as long as each segment can enforce a sufficient level of protection for itself via its own firewalls. Multiple networking enables different segments of security measures to be enabled so that application specific protection can be provided for potential threats.

ORGANIZATION-WIDE RISKS AND MOBILE SECURITY MEASURES

There are numerous ways of implementing an organization-wide wireless security policy depending on the nature of the technology being used. In most cases, following certain basic security measures will provide enough security for attempted data breaches. Security measures should be well instructed to the employees to not let any vulnerability create problems in case of insecure use of the system. Additionally, in most cases, a monitoring mechanism or some limitation of usage is required to prevent any potential security issues.

The onus lies with administrators and not mobile users to determine how the transmitted data is being used. IT administrators need to have full control over the access to parameters, sensitive data and how information is being transmitted. The following guidelines provide categorical risk assessments and preventive mechanisms.

- Clearly define which information is available to certain users and what type of data is allowed to be circulated within the official networks.
- Ensure the organization-level infrastructure is sufficient to implement relevant security policies. Detect the technology and skills required for overall security and plan ahead for use case scenarios.
- Define use case scenarios for general workflow with regards to application and device usage. Consider user and device access permissions for each security level of data and document it for internal training purposes of personnel.
- Document several use case scenarios and update on a regular basis. Cover potential risks, mitigations and best practices for each scenario and make it available to users.
- Identify security cautions with regards to performance and efficiency throughout the organization. Assess security risks in a hierarchical structure and document preventive mechanisms accordingly without excessive interruption to the execution of the tasks. Security should not be provided at the expense of the efficiency and ease of use.
- Ensure creation of logs for security issues faced categorized for the devices and operation types. Make the logs available to the technical personnel to identify peculiar risks and threats for future reference.
- Schedule regular security-based trainings on the security issues faced by the employees and devices in order to keep users up to date on new threats and risks.
- Ensure continuous monitoring of the changes in the organization-level infrastructure and update the security policies and practice accordingly.

APPLICATION AND SOFTWARE-RELATED RISKS AND CAUTIONS

Mobile devices utilize many types of applications, native or system software. Every now and then software updates or new installations are required to add functionality, as is the case with smartphones and tablets. However, these software and applications might have vulnerabilities or malicious codes. Here follows a list of numerous software and application risks.

Threats from Applications, Software Code and Operating Systems

The software on the mobile device may contain codes written to perform unauthorized actions. These codes can come via installed/updated software, downloaded applications, instant messages or mail and may interfere with normal operation of the device or cause risks of data theft and loss. Operating systems are subject to similar risks, yet they might cause greater trouble due to their capacity on the device and data is greater than the applications.

Preventive steps are necessary for potential software and operating system risks:

- Entities should choose the most protective hardware and operating systems. Upgrading these may make the overall system safer due to new protections provided for recently discovered potential threats. Operating system security should be compared with the other versions in order to choose the most secure option.
- Device users should be given proper training on potential threats and impose certain guidelines to avoid unauthorized installations and downloads.
- Firewalls should be utilized as far as they do not cause major performance drawbacks. They can detect the malwares in 'real time' and take the necessary, immediate preventive action.
- Scheduled virus scans should be periodically applied without interfering with users' tasks.
- Use and installation of software and applications should be restricted and monitored by the entity's own policies and procedures.
- When the devices are connected to entity-wide networks, internal firewalls should be activated in the device.
- Mobile devices should be controlled centrally to enable entity-wide configurations, remote data management, remote data recovery and data wipe.
- Precautions should be taken in case of operating system disorders such as jail breaking. In the case of detection of compromised devices, device access to databases and networks should be enabled and users should be alerted.
- A white-list of suitable, safe applications and software should be published within the entity and centrally imposed on all devices. These lists should be regularly reviewed to include or exclude items.

Online Threats

When devices connect to the Internet, malicious code might be transferred via HTML codes, JavaScript, flash or by other sources from the web pages visited. Browser weaknesses may also cause devices to be threatened by external mobile codes. The following serves as examples of preventive action:

- The possibility of visiting untrusted pages can be avoided by using entity-wide security checks or certificates. Users also can use web proxies to utilize entity filters and firewalls on their own devices.
- It is far safer to use the latest versions of web browsers. Additional configurations should be made to align with the entity's security policies. It should be assured that visiting official web pages are only done with secure connections.
- Implement policies to restrict or disable access to certain codes such as JavaScript. Limitation can allow only safe and white-listed web content to activate certain codes.
- In cases where there are high risks and highly sensitive data, strict measures might be put in place as long as they do not cause performance issues such as turning JavaScript off except the official page visits; verifying website certificates on each page visit; turning off tracking properties on the browsers or applications wherever possible; clearing cookies on every browser session or disabling them; disabling direct internet connections and requiring use of the entity's network would provide extensive security and reduce risks.

DEVICE-RELATED RISKS AND CAUTIONS

As it is the case with the network security of organizations, a mobile device that gives access to any kind of organizational data needs to be secured with similar firewalls. Thus, device security becomes as important as the network security. For instance, in the case of an unauthorized access of device issue, identity theft may arise and cause sensitive data loss or misuse.

To some extent, security of the sensitive data can be provided through authentication with a password. Certain syntax for the password choice is necessary many times to make sure only the authorized persons access the information. Password expiration schedules might be put in place to make regular changes in the passwords.

More advanced solutions of multiple authentication procedures are also applicable in certain situations such as smart cards or biometrics that ensure not only the password is known but also another security measure is carried by the user (finger print or a smart card).

Device security management is very crucial for the entire security architecture within the entities. Device-based risks also threaten desktop computers, databases as well as e-mails and network servers and could lead to unauthorized access to sensitive data or system downturn. The mobility of the devices makes them vulnerable to data loss or theft. Here follow some measures to mitigate risks:

- Since the access keys are stored on the device, a secondary digital certificate system acts as an active revocation list in the case of device loss or theft, so that the authentication is blocked for the unauthorized parties. Additional passwords may also be utilized for authorization.
- Application filters against access to device hardware should be utilized. Only relevant and authenticated applications should have access to device resources (camera, microphone etc.)
- To prevent potential dangers from lost devices or theft, strict authentication mechanisms should be

put in place. Depending on the sensitivity of the data architecture, several layers of authentication tied to system authorization or encryptions should be utilized. Remote access to mobile devices can also impose security measures in case of device loss or theft by data wiping, data recovery etc.
- Two-factor authentication procedures would provide high-level identity assurance for identity verification in sensitive data environments.

NETWORK-RELATED RISKS AND PRECAUTIONS

Network vulnerabilities can be exploited in several ways via applications, data documents or mobile device control and configuration plane. The threats may stem from the connected devices, files transmitted over the network, or the network protocol itself. Mobile devices are more exposed to network vulnerabilities due to the variety and multitude of connections they can make. Wi-Fi and cellular networks expose the devices to more risks than fixed line connected devices. The major risk categories and preventive mechanisms are as follows:

Collection and Manipulation of Data/Voice via the Network and Over the Air:
Mobile devices utilize IEEE 802.11 standards to connect to Wi-Fi networks. They can connect to hotspots and entity access points. Devices may be interfered with by other devices via the same network, giving unauthorized access to data and devices.

Similarly, mobile devices connecting over a cellular network may be vulnerable to interception. Bluetooth connections also have several known issues on hijacking attacks during system initialization, although using encryption and authentication mechanisms. Similar issues arise in Near Field Communications (NFC) as well as infrared communications with mobile devices.

To minimize these risks:
- Data encryption on each transmission will reduce risks wherever applicable. However, the encryption method should be validated by Federal Information Processing Standard (FIPS), which few devices currently have. For non-FIPS-validated devices entities should utilize FIPS 1402- sandbox on the devices.
- Entities should give clear instructions to employees on the level of risk depending on the network type.
- The risk associated with networks is smaller when the device connects via the entity's network. Risks increase for devices connected via cellular networks. So setting a security policy is not always practical.
- 3G and 4G networks should be disabled in high risk environments to prevent dangerous exposure. Bluetooth, NFC and 802.11 connections can also be disabled when virtual private connections cannot be accessed.
- Virtual Private Network (VPN) services should provide strong authorization mechanisms when connecting the official networks.
- Connecting to multiple connections from the same device should be prohibited by the entity's policies.
- MMS/SMS communications may be unreliable due to the fact that they can be observed and manipulated on transmission. Instead, users should consider other IP-based means of messaging that provide encryption of data.
- Regular proactive training of device users exposed to risky networks and environments should be in every entity's policies.
- Use of VPN connections should be made available and encouraged in high-risk situations to connect to the official network. Authentication, encryption, confidentiality and integration of the data will be secured via VPNs.
- File verification should be enabled for all the content transmitted to the mobile device.
- In case of data submissions by users, a secondary confirmation should be put in place to ensure it comes from the authorized user. This could be an e-mail confirmation, voice call or desktop computer verification.

GPS and Tracking Risks
Geo-location services are available on many types of mobile devices to varying levels of capability. Applications use geo-positioning systems to track one's route, to locate places on a map and to search for nearby places. The device periodically gathers positional data from multiple resources including mobile device signatures from cell nodes, Wi-Fi signatures, the internal GPS receiver etc. Combining various positional data provides a high level of accuracy of device location, yet threats to influence some of these channels and interfere with positioning systems or illegitimately track the device are issues to be considered in terms of security and precision.

- Exposure of tracking data should be disabled if it is not absolutely necessary. Device positioning and retrievable data loss, however, might necessitate using these applications.
- When GPS is required by the nature of the task, it is best to disable third party applications to use geo-location.
- Device users should receive extensive training on tracking issues, threats to location data precision and encryption of location data on devices.

Jamming and Flooding Risks
Mobile devices, whether they connect via Bluetooth, cellular, Wi-Fi or GPS, are vulnerable to blockage of reception or transmission via a process called 'jamming'. Flooding, on the other hand, is to load the device with more data transmission than it can process.

To deal with these threats
- For Wi-Fi networks, jamming threats should be prevented by wireless intrusion detection and prevention systems, which alert network administrators in case of jamming.
- Use of malware scanners and alert systems are helpful to minimize flooding threats that are caused by malicious code on the device.
- Monitoring flooding activities in real time may help reduce future attacks by filtering and limiting signal penetration.

PHYSICAL AND USER-RELATED THREATS

Mobility of the devices makes them vulnerable to some physical and user-related risks such as loss of the device, extreme physical conditions, user errors and misuses of devices.

When a mobile device is lost or stolen, the risk arises of unauthorized entities accessing sensitive data. Confidentiality and integrity of the information will be in question. Moreover, sensitive data may be lost if no backup is provided. In case of device loss or theft, entity policies should ensure the sensitive data will remain safe and that unauthorized access to the official network and information will be blocked. Malicious actions can result in entity-wide problems. Here follow some necessary precautions:

- Strong passwords should be required for all devices.
- Device purchases should only be made from trusted sources. Devices from untrusted suppliers should be restricted. A white list of products and suppliers can be prepared to guide purchasing activities.
- Regular backups of the data should be scheduled, with data stored centrally. Depending on the workload and flow, additional manual backups should be encouraged to avoid data loss.
- Central control over data wiping should be enabled for all devices so that access to entity-wide information can be prevented remotely.
- Remote controls should also be able to lock screens protected by passwords until data is recovered or wiped.
- Timely reporting of lost or stolen devices should be deemed necessary and be instructed to device users.
- Geo-location services, if they can be enabled remotely, should be activated to locate the devices.
- Disabling data encryption should be prohibited.
- Users should be trained to be very careful about the physical control of the device and they should be instructed about the potential dangers of device loss.
- Tamper-proof features in the mobile devices should be enabled wherever available in order to prevent malicious codes and software to be installed on the device.
- Built-in capabilities of the devices should be turned off if it is not part of the functionality being used (e.g. camera and microphone) to avoid third parties from hacking and gathering visual or audio data.

The availability of a mobile payment method increases the potential of allowing finalizing through mobile for all mServices requiring a payment.
In mobile payments a mobile operator, service providers of online payments, banks and credit card operators usually are competing and imposing different models. Today the chip is included in some advanced mobile phones allowing support for electronic wallet and NFC technology to perform the payment. This system is becoming widely used for the payment of small purchases made in physical stores or transportation services, but cannot be used to perform online payments.

For online mobile payments in general, there are different solutions on the market that are quite similar to those developed for web payment. One option is a Mobile Payment Platform that acts as a payment gateway. It is composed by a client application that has to be downloaded and installed on the handset. This application allows the customer to perform the payment through a payment gateway usually held by the online payment service provider. Other mobile payment systems charge the payment to a consumer's mobile account that is operated by the mobile operator, billing the customer using the regular billing service of the operator.

The below should be taken into consideration by all government entities:

- Mobile payment will be a national-wide integrated service throughout the UAE, hence keep in mind a possible integration with the national mobile payment system when offering transactional services.
- Clearly identify the requirements of the mobile payment system you need. Do you need online payments or is there no need for performing online payments?
- Clarify the scope of the mobile payment system. Are you looking for a mobile payment system for local mGovernment transactions or planning to establish a countrywide payment system?
- Think about whether mobile payment is your core business or not.
- If you need to solve a need for micropayment consider using SMS billing, which is becoming the norm and an increasingly accepted by number of companies and sites.
- NFC payment system is a useful solution for offline citywide micropayments such as parking, public transport, newspapers and other small purchases.
- The deployment of an NFC payment system is not a matter of only one organization. It is a sizable project, which requires co-operation with the private sector and the alignment of the public sector. These projects are led by banks and the government acts as a promoter working actively hand-in-hand with the banks to engage the private sector.
- The introduction of an NFC payment system requires planning a gradual deployment of the solution. In that project, the government entity should not only be the promoter, but also the best supporter adapting the official services to the new payment system.

MOBILE PAYMENT SECURITY

For securing transactions on the mobile platform and mobile applications, the following guidelines are the most relevant:

- Unauthorized device access should be prevented with features such as PIN, password or biometric systems.
- On the server-side, keep logs of unsuccessful attempts of login, report abnormal patterns of usage.
- Users should have remote control capability over the transactions in order to deactivate accounts or to disable the payment application when they require.
- Detection mechanisms should be implemented for device loss and theft cases. The system should be able to test and verify the accounts and users on a regular basis for device/user authentication. Changes in the geo-location data especially should require re-authentication.
- Ensure that mobile devices do not authorize offline transactions or store transactional data for later use. Applications should require devices to be online for transactions.
- In order to secure mobile devices and applications, manage patch updates for new versions with regards to new types of threats and risks.
- Avoid payment applications from interacting with other unauthorized applications and sharing data.
- Provide additional user information on security to ensure that users are aware of the potential threats and possible outcomes. Users should also be aware of the security issues associated with their device and operating system, which may affect the outcome of mobile transactions.
- When dealing with mobile government services, it should be ensured that citizens only use authorized government applications for mPayments. Using a government authorized logo in applications will aid in this.