United Arab Emirates

TRA هيئة تنظيم الاتصالات
TELECOMMUNICATIONS REGULATORY AUTHORITY

Guideline

Smart Government

Version 1.0

Issue Date: 1 August 2013

P O Box 26662, Abu Dhabi, United Arab Emirates (UAE)
www.tra.gov.ae

Revision control:

Version:	Issue Date:	Reason for Revision:
1.0	1 August 2013	

Table of Contents

1 Introduction

This document is to serve as a set of guidelines for the government entities to prepare themselves in transforming eGovernment to mGovernment (Smart 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 application and services.

1.1 Scope and the Organization of the document

This document covers what considerations should be made when planning & 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 smart-phones.

As such the scope of the current document is limited and in its existing form **does not** cover guidelines to 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 guidance is provided to help government entities to 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.

1.2 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 smart government, offering seamless, interactive and intelligent applications and services. The expectation to implement smart government should be based on realistic assessment of resources and capabilities that each of the entities possesses. Nevertheless, it is always positive to think about the ultimate goal, what is possible and could be done given the advances in mobile technologies and mGovernment practices.

1.2.1 Stages of mGovernment (Smart 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, Fees Enquiry etc…)
    - G2G Mobile Services (Patient's Medical History Sharing)
    - G2E Mobile Services (BYOD, Hot Desk etc.)

- mGovernment employs 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 below shows these stages of evolution of mGovernment in relation to advances in mobile (ICT) technologies and level maturity in eGovernment and data / services and integration among the government entities. The examples used in the below table are hypothetical examples and not real examples.

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 inform between government entities: Gra business license and updating records at Ministry of Labor and Dubai Economic Departmen
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	

Figure (1)

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

1.2.2 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 should be considered for mobile services development.

Below are four different types of enhancements that mGovernment brings about 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 portal 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 using “hot desks”.

The types of enhancements suggested does 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).

1.2.3 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 just mobile phones but to all mobile and intelligent devices (this may include machine to machine communications).

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

- Technology and services development are at the core but are the simplest element in adopting smart 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.

2 Prioritising Mobile Services

One of the first steps and perhaps a very critical step for government entities in transforming their eServices to mServices is evaluating & 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 as 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 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 or one eServices may be broken down to 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.

2.1 Mobile Services Definition

What constitutes a mobile service and what is an overall experience of 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, and PDAs, etc.) to serve the customer effectively and efficiently.

The Customer experience may be devided 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 receive the final and expected output.

This simple view may be shown in the figure2 below:

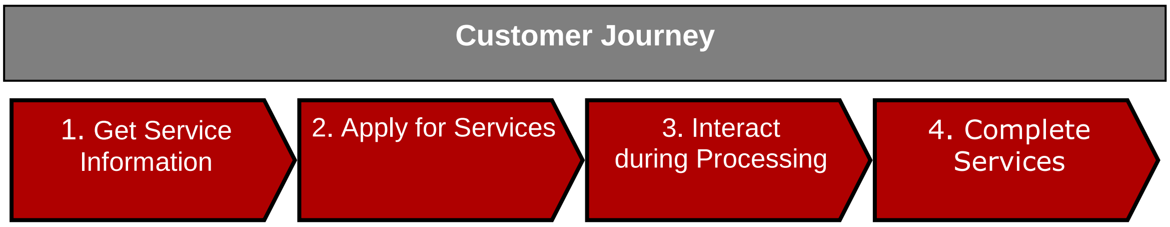

Figure2

2.1.1 Types of Enhancement 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:

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 mobile services that allow citizens to make applications, job posting, buying bus tickets, book appointments, and sign a transaction with a mobile signature 24/7. 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 nearest attraction points of interest to the users. 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.

2.1.2 Mobile Transformation Baseline:

All government entities should achieve Step1 & Step2 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.

2.2 Mobile Services Suitability

Even though mGovernance may be seen as an extension of eGovernment services, existence of eGovernance services is not a prerequisite for deployment of mGovernance services. This means that the transformation to mGovernment is not carried out only via migrating existing eServices into 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:

1. to evaluate whether services are suitable for mobility by 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 licence 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. to evaluate the complexity & 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. to take into consideration certain eServices which are core services of the government entities, but are not suitable for mainstream devices however are essential in serving the citizens. The entities may consider employing particular tailor made devices and software to enable these services. Examples include vehicle number plate identification and checking system or intelligent outdoor cameras reporting traffic information.

2.3 Mobile Service Selection & Eligibility

Choosing, which services are eligible and potentially beneficial to move to 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 method for their entities. Suitability test mentioned above is the first task. A typical set of additional considerations may include the following where a service is:

- an essential part of the operation and service quality of the entity
- used in high frequency
- high in volume of transactions
- generates new revenue streams for the entity
- easy to develop (or transform) and maintain
- adds value to the citizen happiness
- simplifies entities processes or workflow
- provides 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 above list does not suggest priorities over one another and 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 recognise that all services may not be suitable for mobile platforms, therefore entity will have to prioritise which services among a large number are the best candidates for migration.

2.4 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. Growing market for mobile devices, increasing quality of mobile networks and high demand for quality mobile applications are all together providing endless opportunities for more efficient business operations in public service and opening up new interaction possibilities with the 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 of developing mobile government applications under the light of the latest trends in mobile technology are presented.

2.4.1 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.

2.4.2 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 the 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 to enable accessing the internet over mobile wireless network. Rather small mobile devices use WAP browsers that enable Access to websites with wireless markup language.

2.4.3 Data Channel

Available in different forms of mobile messaging: Application to Person (SMS, MMS); Person to Application (enabling user 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 and smart metering etc.)

The data channel open ways to 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.

3 Guidelines for Mobile Applications

Mobile application process starts with analysing the nature of the service that will be transferred to 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 regarding how the best outcome could be achieved. 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 the information below and ask the following questions to decide how to develop the application:

- What is the current market share of the Smart Phones and operating systems?
- How much is the budget spared 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?
- Whether there is Shared API for developers use? (In case there is, it should be used)

3.1 Native Applications

Native applications development is dependent on the mobile operating systems. 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 native components such as the camera, voice recorders, GPS, etc.

3.1.1 Native Platforms:

	Apple OS	Andriod	Blackberry OS	Windows
Language	*Objective –C, C, C++*	*C, Java and C++.*	*Java*	*C#, VB, .NET*
App Store	*Apple App Store*	*Google Play*	*Blackberry App World*	*Windows Phone Market Place*

- **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, serving on the lines of '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 is already a developer account on these platforms.

3.2 Mobile Web Applications

Mobile web applications are, in fact, 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 with a 'one size fits all' approach.

Compared to native applications there are some crucial limitations:

- Native device functionalities (GPS, camera, etc.) cannot be integrated to 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.

3.3 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 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 utilizing device capabilities.

3.4 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 as 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 etc. 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 win over the 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 to 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 (i.e. PhoneGap) and Tools (i.e. Titanium Appcelerator) in order to reduce costs and efforts.

Application Life-Cycle:

- The life cycle of native application 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 device native features (i.e. camera, geo-location), mobile web applications cannot provide that. Native and hybrid applications make use of the device 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 the native applications have particular risks due to their internal data storage properties as well as utilizing the hardware sensors. In case of loss of 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 device 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 to the existing systems or very troublesome. Mobile web or hybrid applications, on the other hand, are more easily integrated to existing platforms.

Access to Service & Visibility:

- From the user 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 the applications differs from the choice of the application type. Mobile web applications are displayed in search results whilst the native applications are displayed in applications 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 creates 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 a personalized service to the users.
- Offline access to mobile web application services is not as convenient as 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 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-	Short	Long	Long
Access to Device	Yes	No	Yes
Notifications	Yes	No	Yes
Storage	Secure file	Shared SQL	Secure file system, shared
Location Awareness	Yes	Yes	Yes
Connection	Online and offline	Mostly online	Online and offline

Technical Skills	ObjectiveC, Java	HTML5, CSS,	HTML5, CSS, Javascript

4 Application Program Interfaces (APIs)

Application Program Interface (APIs), are used to make mGovernment Services or its functions available for use by other applications. Thanks to the smart-phones, 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 to the citizens thousands of mServices of public interest.

With the ability to deliver core business functionalities as APIs, a government entity transforms itself into a platform. In such 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 to succeed.

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 APIs structure, search for advice on specific data, information systems, applications or even infrastructures to expose, definition of access tiers and definition of policies of use.
- Evaluate 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, 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 specify the users and applications that will utilize the APIs. Government entity 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.

5 User Interface and Usability

Application design is not solely about the aesthetics of an application, it is also concerned with the ease and clarity when 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 UAE logo should appear as well as the Government entities 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 smart phone 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, limiting their size to certain levels to control download times and battery usage should be considered seriously. Although quality graphics definitely lead to a better user experience, the efficiency and performance issues are the priority for application users. Neat and speedy applications are mostly preferred over slow and graphics-heavy applications.
- Application size should not be too large to avoid slow download processes. It would be convenient for users if they can download applications on any type of connection be it Wi-Fi, 2G or 3G etc.
- It is advisable to keep the core application size to not more than 12-15 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 accessible Terms and Conditions page that clearly defines the usage agreements, property rights and credentials. Users should agree 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 user experience.

Navigation:

- Design intuitive architecture within the application. The application structure should be made predictable by the user and accessing each functionality should be made easy. The number of clicks to reach the desired content should be kept to a minimum.
- 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 the very least of 30-pixel size. 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 after the start-up provides 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. Avoid application information to display on the landing page.
- Allow users to be able 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 user's thinking that an application has crashed.

Offline Usage:

- Saving sessions or making use of the content for offline use functionalities should be made available to the user wherever applicable.

6 Mobile Content

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. User's interaction with the application content should be a matter of a carefully thought out design in order to enhance user experience and deliver the intended service to citizens in a seamless and convenient interface.

Easy Reach to Required Content:

- Make sure the content is delivered in a mobile friendly format, enabling users to quickly scan and find the useful information at a glance.
- Give user as much control as possible over how the content is displayed. Do not display unrequested information in detail. Allow the 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's Interaction with the Content:

- Whenever possible, allow the users to mark the content as favourite or 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 in hand and make it easy to accomplish if necessary step by step. 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 how to store the information or give feedback and comments referring to content or 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 user 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.

7 User Adoption

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.

- Make online polls or public surveys to get the opinions and suggestions from citizens on what mobile services would most benefit them.
- Analyse 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. (i.e. both SMS and Mobile Application can be utilized for the same service and users can choose from which channel they require the service).
- Promote new mobile services on government websites, entity's own website as well as in the public offices where citizens frequently visit.
- Make use of the social media and mass media to raise awareness for the offered services.
- All government entities are advised to provide incentives for using mGovernment services in order to raise adoption.

8 Mobile Security

8.1 User Related

When providing mobile services for citizens neither institution-related nor citizen-related security risks should be overlooked. Mobile services should be developed in consideration for the privacy and security of the sensitive information shared and communicated during the use of service. On the citizen end of the issue, service providers (i.e 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 preform 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 at 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 anti-virus software installed and up-to-date,
  - Windows Phones should have anti-virus software installed and up-to-date.
- For more information regarding device registration / de-registration please refer to Emirates Identity Authority (EIDA).

8.2 Mobile Application Coding Guidelines for Security

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

Sensitive Data Protection:

- Make classification of the stored data according to the sensitivity and apply security measures accordingly. Make the data processing and storage in accordance with these classifications.
- Wherever possible, store the sensitive data on the server side rather than the client's device. If the data storage in the device is necessary use file encryption APIs provided by the operating system or another trusted source.
- Sensitive data storage should always be ensured to be in encryption as well as the cached data.
- Restricting data in certain contexts might be taken as a precaution such as 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 and the rest of the data should be kept out of reach.

Password Handling:

- When passwords need to be stored in 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 application to store passwords in the application binary.

Data Protection on Transit:

- Always assume that the networks layer is not secure and put into place precautions 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 long enough keys.
- Ensure the user interface makes it clear to the user whether the certificates used are valid.

User Authentication and Session Management:

- Assist the user in choosing an appropriately secure password. (i.e. 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 (i.e. location)
- When the data is highly sensitive require another level of authentication depending on the service. (i.e. fingerprint, voice etc.)

- 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 behaviour and ask for secondary authentication when abnormal behaviour takes place. (i.e. change of location etc.)
- Keep logs of access to paid resources and make these available to the user only with authentication.

8.3 Identity Theft and Privacy Protection

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

- Make the application-specific privacy policy available to the users on the application platform in order to let users find out about the relevant issues and also provide a clear privacy policy within the application.
- Mail clear warnings to the users regarding the data practices taking place within the application that involves sensitive data interaction.
- Restrict the collection of user's personal data by the application apart from those that are 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 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 application can integrate into EIDA authentication services wherever applicable.
- Be aware that the entity is accountable on complying with the privacy laws in the country and need to always ensure that every version of the application is bound to be within the limitations of these laws. Assign a person or a department to follow the latest laws and check each version for compliance.

8.4 Testing for Security

When mobile services are designed for use, developers must understand the use cases of the services and make the application/mobile service subject 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. Systematic approach for evaluating security risks can be ensured as follows:

Analyse Usage and Risks:

- Navigate through the application to analyse 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 of the device can be utilized by the application and potential hacking of these features (camera, GPS etc.).
- Check how the payment information is secured by the application if there are any.
- Identify what other applications does the mobile service interact with. Identify those that could potentially harm the integrity and privacy.
- Ensure the source code of the application is analysed for inherent vulnerabilities.
- Check how the user authentication is performed in the application and identify potential risks.
- Analyse 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 application against “man-in-the-middle” attacks to analyse potential interference to the application.
- Check if the sensitive data is being leaked to log files.
- Also ensure server-side security is maintained with care, not just the client-side.

8.5 High-Level Security Risks

As the mobile connectivity overcomes all spatial obstacles and enables us to be connected anywhere anytime, the 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 actual workplaces and access strategic documents or applications. It becomes a key necessity to maintain confidentiality, integrity and authenticity of data in these types of networks.

Confidentiality:

Confidentiality refers to the secure way data is transmitted to the intended user and not to other interfering parties. Integrity is a measure of security to make sure no changes on the data are made during the transmission. Finally, authentication process makes sure that the sender is the trusted involved subject is the one to send the data. Confidentiality refers to the process of preventing access to information by anyone other than the intended recipient. To provide confidentiality either the data is 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 in 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 validate and authenticate itself in the device. Authentication can be enabled by a shared encryption system.

Traditional ways of working of government officers with computers had security systems of network firewalls. Nevertheless, the increasing mobility of workers of today requires the prospect of network security to be enhanced to cover more than the perimeter of the office networks to the extent the mobile services reach. Since mobile devices are likely to be used outside the security of the office firewall, administrators need to secure the data transmission by allowing only secured IP addresses to access the software and information. Certain adjustments need to be made in 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 the data security as long as each segment can suffice a level of protection for itself via own firewalls. Multiple networking enables different segments of security measures to be enabled so that application specific protection can be provided for potential threats.

8.6 Organization-Wide Risks and Mobile Security Measures

There are numerous ways of implementing 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 usage limiting needs to take place to prevent any potential security issues.

It is crucial that administrators should determine how the transmitting data is being used rather than the mobile device users. IT administrators need to have full control over the access to parameters, sensitive data and how information is being transmitted. Guidelines below will provide categorical risks 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 the 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 for personnel.
- Document several use case scenarios that is updated 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 on 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 according to the changes.

8.6.1 Application and Software Related Risks and Cautions

Mobile devices utilize many types of applications, native or system software. For additional functionalities every now and then software updates or new installations are required as it is the case with the smart phones and tablets, however, these software and applications might have vulnerabilities or malicious codes. There are numerous software and application risks that could be listed as follows.

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 for 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 to be able 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 user’s tasks.
- Use and installation of software and applications should be restricted and monitored by 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 database and networks should be enabled and users should be alerted.
- A white-list of suitable and 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 in it.

Online Threats:

When devices connect to Internet, malicious code might get in via HTML codes, JavaScript, flash or by other sources from the visited webpage. Also browser weaknesses may cause devices to be threatened by external mobile codes. Preventive action may be listed as follows:

- The chances to visit 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 entity’s security policies. It should be assured that visiting official web pages are only done with secure connections.
- Implementing policies to restrict or disable access to certain codes such as JavaScript. Limitation can allow only safe and white-listed web contents 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 visits; 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 entity network would provide extensive security and reduce risks.

8.6.2 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 emails 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.
Some measures to mitigate risks would be:

- Since the access keys are stored on the device, in case of a device loss/theft, secondary digital certificate system acts as an active revocation list 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 authentications tied to the 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.
- For identity verification in sensitive data environments two factor authentication procedures would provide high-level identity assurance.

8.6.3 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, transmitted files over the network, or the network protocol itself. Mobile devices are more exposed to network vulnerabilities since the variety and multitude of connections they can make. Wi-Fi and cellular network expose the devices that are connected to more risks than fixed line connected devices. The major risk categories and preventive mechanisms are as follows:

Collection & 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 by other devices via the same network giving access to unauthorized access to data and device.

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, encryption method should be **Federal Information Processing Standard** (**FIPS**) validated which not many devices currently have. For non-FIPS-validated devices entities should utilize FIPS 140-2 sandbox on the devices.
- Entities should give clear instructions to employees on levels of risks depending on the network types.
- The risks associated with network, though smaller when connected via entity's network, increase as the device connects 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. Users should rather look for other IP based means of messaging that provides encryption of data.
- Regular proactive training of the device users on 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 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 to make sure that it is from the authorized user should be put in place. This could be an e-mail confirmation, voice call or desktop computer verification.

GPS & Tracking Risks:

Geo-location services are available in many types of mobile devices to varying levels of capability. Applications use geo-positioning systems to track one's route, to locate places on the map and search for a nearby place. Positional data are gathered from multiple resources periodically by the device including mobile device signatures from cell nodes, Wi-Fi signatures, internal GPS receiver, etc. Combining multiple positional data provides high level of accuracy of device location, yet threats to influence some of these channels to interfere with positioning systems or illegitimately tracking 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.
- Extensive training should be given to device users on tracking issues, threats on 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 the 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 the malicious code on the device.
- Monitoring the flooding activities in real time may help reducing future attacks by filtering and limiting signal penetration.

8.6.4 Physical and User Related Threats

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

When a mobile device is lost or stolen, risk of unauthorized entities to have access to sensitive data arises. Confidentiality and integrity of the information will be a question. Moreover, sensitive data may be lost if no back up is provided. In case of device loss or theft entity policies should make sure the sensitive data will remain safe and unauthorized access to official network and information will be blocked. Malicious actions can result in entity-wide problems. Some necessary precautions are:

- 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 and 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 to hack and gather visual or audio data.

9 Mobile Payment Considerations

The availability of a mobile payment method increases the potentiality of the mServices allowing finalizing through mobile, all these mServices requiring a payment. In mobile payments a mobile operator, online payments service providers, banks and credit card operators usually are competing and imposing different models. Today the chip is included in some advanced mobile phones so using the handset as support for the electronic wallet and NFC technology to perform the payment. This system is becoming widely used in paying for 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 is the option to use a Mobile Payment Platform that acts as a payment gateway. It is composed by a client application that has to be downloaded and installed at the handset. This application allows the customer to operate with the payment gateway usually held by the online payment service provider to perform the payment. Other mobile payment systems charge the payment to a consumer's mobile account that is operated by the mobile operator that bills 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 there is no need of 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 country-wide 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 more the norm and an increasing number of companies and sites are accepting them.
- NFC payment system is a useful solution for offline citywide micropayments such as parking, public transport, newspapers and other small purchases.
- The deployment of a NFC payment system is not a matter of only one organization. It is a sizable project, which requires the co-operation with the private sector and the alignment of public sector. These projects are led by banks and the government acts as a promoter working actively hand-in-hand with the bank to engage the private sector.
- The introduction of a 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.

9.1 Mobile Payment Security:

For securing transactions on mobile platform and mobile applications 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 account or disable the payment application when they require.
- Detection mechanisms should be implemented for device loss and theft cases. System should be able to test and verify the accounts and users on a regular basis for device/user authentication. Especially after changes in the geo-location data system should require re-authentication process.
- Ensure that mobile devices do not authorize offline transactions or store transactional data for later use. Applications should require being 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 to interact with other unauthorized applications and share 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 their device and operating system security issues, which may have an outcome in terms of mobile transactions.
- When dealing with mobile government services, it should be assured that citizens only use authorized government applications for mPayments. This can be provided by the use of a government authorised logo in applications.