



United Arab Emirates



الحكومة الذكية  
mgovernment

# ROAD MAP MOBILE GOVERNMENT

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



الإمارات العربية المتحدة  
وزارة شؤون مجلس الوزراء  
مكتب رئاسة مجلس الوزراء





“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

1	2	3	4	5	6	7	
<p><b>LIST OF FIGURES AND ABBREVIATIONS EXECUTIVE SUMMARY</b></p> <hr/> <p><b>INTRODUCTION AND OVERVIEW</b></p> <p>Motivation</p> <p>A View on mGovernment Ecosystem</p> <p>Approaches and Methodology</p> <p>Overview of the RoadMap</p>	<p><b>02</b></p> <p><b>03</b></p> <p><b>04</b></p> <p>04</p> <p>05</p> <p>05</p> <p>04</p> <p><b>08</b></p> <p>08</p> <p>08</p>	<p><b>TRACK 1: ESTABLISH THE ENVIRONMENT FOR mGOVERNMENT TO FLOURISH</b></p> <p>Set Up The Program Management Office</p> <p>Stakeholder Value Proposition and Involvement</p> <p>Structure and Operations Among Government Entities at Federal and Local Levels</p> <p>Development of Mobile Value Chain, and Affordable Public Access to Wireless Networks and Services</p> <p>Strengthening the Legal Base</p> <p>Capacity Building Everywhere</p>	<p><b>09</b></p> <p>09</p> <p>10</p> <p>11</p> <p>12</p> <p>13</p> <p>13</p> <p><b>16</b></p> <p>16</p> <p>17</p> <p>17</p> <p>18</p>	<p><b>TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL</b></p> <p>Mobile Identity (mobile ID) and Authentication System</p> <p>Mobile Payment (mPayment) System</p> <p>Trusted Service Manager (TSM)</p> <p>Mobile Innovation Center</p> <p>Nationwide Government Data Integration</p> <p>Government Application Store</p> <p>Develop Common Security Directives and Practices</p> <p>Set up Federal Government Network (FedNet)</p>	<p><b>20</b></p> <p>20</p> <p>22</p> <p>24</p> <p>27</p> <p>28</p> <p>31</p> <p>31</p> <p>32</p> <p><b>34</b></p> <p>34</p> <p>35</p> <p>36</p>	<p><b>IMPLEMENTATION APPROACH</b></p> <p>The Roll Out Plan</p> <p>Time Plan and Interdependencies of Milestones</p> <p>Monitoring, and Measuring the Impact Before and Beyond 2015</p> <p>Critical Success Factors</p> <p>Management of the mGovernment Program</p> <p>Ownership and Accountability</p> <p>Managerial Structure</p> <p>Managerial Processes</p> <p>Managing the Differences in the Maturity Level of Government Entities</p> <p>Managing the Risks</p>	<p><b>38</b></p> <p>38</p> <p>39</p> <p>39</p> <p>39</p> <p>39</p> <p>39</p> <p>40</p> <p>40</p> <p>40</p> <p>41</p> <p>41</p>

## LIST OF FIGURES AND LIST OF ABBREVIATIONS

### LIST OF FIGURES

Figure 2 Conceptual View of the RoadMap	05
Figure 3 RoadMap Tracks and Milestones	06
Figure 4 RoadMap Implementation Loop	38

### LIST OF ABBREVIATIONS

API	Application Programming Interface	PKI	Public Key Infrastructure
EIDA	Emirates Identity Authority	PM	Prime Minister
FedNet	Federal Network	PMO	Program Management Office
GSM	Glo Xbal System for Mobile communications	PPP	Public and Private Partnership
ICT	Information and Communications Technology	RAK	Ras al-Khaimah
ISO	International Standards Organisation	R&D	Research and Development
IT	Information Technology	RTA	Roads and Transport Authority
mGovernment	Mobile Government	SIM	Subscriber Identity Module
MIC	Mobile Innovation Center	SMS	Short Message Service
mID	Mobile ID or Mobile Identity	SSO	Single Sign On
MNO	Mobile Network Operator	SUMI	Standard Usability Measurement Inventory
mPayment	Mobile Payment	SUS	System Usability Scale
mSignature	Mobile Signature	TPP	Third-Party Payment
NESA	National Electronic Security Authority	TRA	Telecom Regulatory Authority
NFC	Near Field Communication	TSM	Trusted Service Manager
OTA	Over The Air	UAE	United Arab Emirates
		XML	Extensible Mark-up Language

## EXECUTIVE SUMMARY

This document presents a RoadMap for the UAE to move from eGovernment to mGovernment. The time span of the RoadMap covers from present to the May 2015, though most of the tasks may extend beyond 2015 in the form of improvements or natural evolution of the mGovernment. Given the existing political support, resources, determination and strategic approach, it is very likely that UAE will be creating one of the best nationwide mGovernment implementation in the world.

The scope of the RoadMap goes in parallel with the existing Federal eGovernment Strategy in that three major areas are in focus: environmental improvements, improving readiness and achieving user happiness. These focus areas are presented as four parallel tracks, first two of which correspond to improvements in the environment for the mGovernment to advance. The RoadMap Tracks are:

1. Establish the Environment For mGovernment To Flourish
2. Assess Capability And Capacity Of Government Entities
3. Establish Shared Resources Across Government Entities at The National Level
4. Achieve Citizen Happiness

Each of these tracks contains a number of milestones and each milestone is made up of a number of key tasks that needs be carried out. Some of the milestones are preparatory and focus on situation assessment and taking appropriate measures to

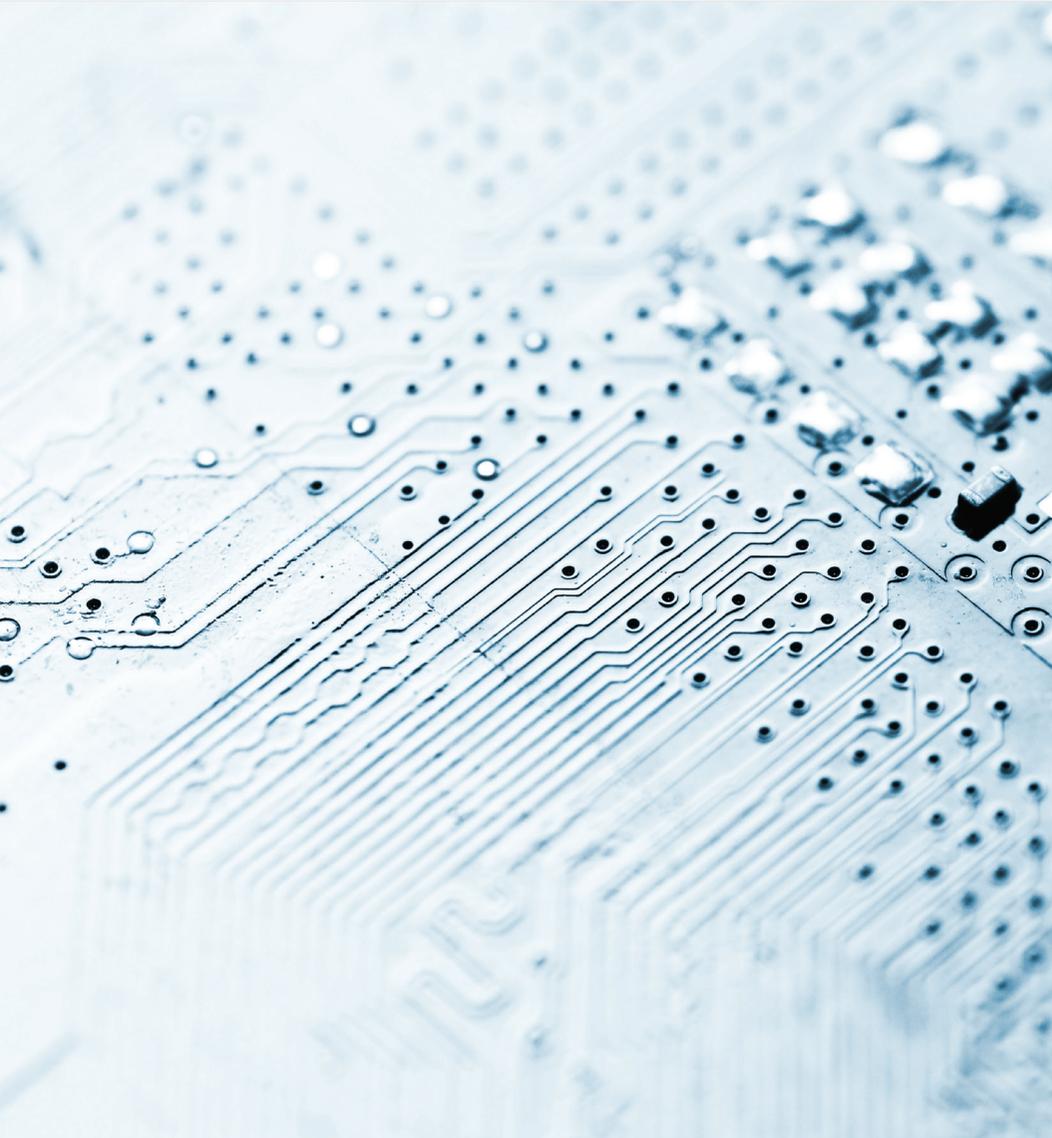
effectively carry out other milestones, especially the first two. The others contain a number of key enablers, which are essential, large scale and complex projects requiring multi stakeholder engagements. Such milestones include creation of nationwide mobile payment system, mobile ID and authentication systems, Trusted Services Manager, and shared data, application and services development.

The document contains detailed description of key activities as well as an implementation approach. As most of the milestones are large scale projects requiring heavy resources, skills and strong sustainable partnerships, an approach to creating and maintaining a competent management scheme is also discussed together with key success and failure factors.

The RoadMap should be able to support The Program Management Office, at least helping, all government entities to adopt enterprise mobility with high security concerns, to move priority eServices into mobile platform, and to create nationwide key enablers such as mobile payment and mobile ID. It should also provide support in terms of some challenging tasks such as sharing data, applications and services and be able to lead government entities to launch integrated services.

There is no doubt that mGovernment transformation is an on-going process and the RoadMap contained in this document is an essential tool to guide the core implementations in coming months until the year 2015, and create strong base and sustainability for the developments in the years to come.

## 1. INTRODUCTION AND OVERVIEW



This document contains a RoadMap for the Government of the United Arab Emirates (UAE) to transform its e-services from eGovernment to mGovernment, focusing on the use of mobile technologies covering a time frame from now till May 2015.

- Smart Government involves a strategic utilisation of advanced Information and Communications Technologies (ICT) and mobile technologies for offering public services. Although the use of mobile technologies is at the heart of any Smart Government implementation, Smart Government often refers to progressive use of such technologies to offer intelligent, interactive and context based services, which also include machine-to-human and machine-to-machine communications. Developing a countrywide Smart Government is a challenging task for any government in the world. Such effort should first go through a more foundational and core set of actions in adopting mobile technologies in public services. This RoadMap covers a limited time span, and a number of focused activities. Therefore, the Smart Government transformation efforts in this RoadMap will be referred as Mobile Government (mGovernment). This reflects a more realistic view of the mobile technologies usage given the time span until the May 2015 and the set of activities presented.
- The RoadMap proposes four parallel tracks, each of which consists of a number of milestones with a set of actions presented as key tasks. These four tracks follow closely from the existing federal eGovernment strategy. They focus on improvements on the environment, mGovernment readiness and user centric services.
- Although this document contains set of directives

on how the mGovernment transformation will be managed, it is important to note that the RoadMap assumes existence of a strong management for the mGovernment transformation. Currently, this refers to the mGov Committee formed at the Telecommunication Regulatory Authority of UAE (TRA). From now onwards, the management of the mGovernment transformation program will be referred as Program Management Office (PMO). The PMO is expected to make particular executive decisions in terms of level achievements in each milestone, time span that they take, the collaborations required and the priorities.

- Although the current RoadMap covers a time span until the 2015, the processes of mGovernment transformation are continuous and evolving. The tasks to be carried out under each milestone are expected to be mostly completed during this time, although some of the tasks are on-going and needs to be extended beyond May 2015. Such cases will be pointed out; however, the PMO needs to make specific decisions and actions when necessary. This is closely related to the question of what can be achieved until May 2015 and what should be planned for beyond 2015. The timing of the milestones will indicate the scope prior to May 2015. As mentioned earlier, any final adjustments remain as the responsibility of the PMO.

### 1.1 Motivation

The fast developments in the ICT and Mobile technologies coupled with strong penetration of mobile phones around the world has led a number of countries to seriously consider and adopt this new trend as a new channel of providing services to citizens. This has resulted in a move from good-old-fashioned eGovernment, based on fixed networks, to mGovernment where the governments can utilise mobile technologies to enhance as well as

1. INTRODUCTION AND OVERVIEW

to improve eGovernment services. The UAE is no exception. Moreover, the UAE seems to have a robust infrastructure already in place and great potential to convert mGovernment opportunities into a big success and create a global leadership in the area.

This was recently made public when Vice-President & Prime Minister of the UAE and Ruler of Dubai His Highness Sheikh Mohammed bin Rashid Al Maktoum announced the initiative for implementing mGovernment in order to improve the quality of the residents and nationals.

*"We are embracing the most modern concept in innovative government by moving towards the delivery of government services through mobile phones. We have one of the best communication infrastructures in the world today, with mobile phone subscribers in the UAE reaching 14 million, which represents an average of two mobile phones per individual."*

At a forum, organised by the UAE Government with the participation of more than 1,000 government officials, His Highness Sheikh Mohammed launched the mGovernment initiative. UAE aims not only to bring an innovative service to citizens but also reach a leading position within international practices. His Highness Sheikh Mohammed stated that all federal and local government entities are entitled to implement innovative services of mGovernment effectively within 24 months and the government is equipped with sufficient sources to enable this success.

**1.2 A View on mGovernment Ecosystem**

Mobile Government can be defined as strategic utilisation of all kinds of mobile technologies in offering public services to the citizens. A view of the mGovernment ecosystem is depicted in Figure 1.

Mobile government involves adoption of mobile business techniques and enterprise mobility in the public sector. It has three sets of stakeholders the industry, service providers and the users. In the industry the stakeholders include all businesses in the mobile value chain from Mobile Network Operators (MNOs) to solution and content producers to the device manufacturers (i.e. phones, tablet PCs, and Laptops). The service providers include the government entities and other organisations often supporting them. For example, banks may help government organisations to enable mobile payment services and a Trusted Services Manager support safe secure transactions and protection of

data. All services are directed to certain groups of users, the largest of which are the citizens. Other government entities and their employees may also be users if mGovernment services were designed for the government employees to use.

**1.3 Approaches and Methodology**

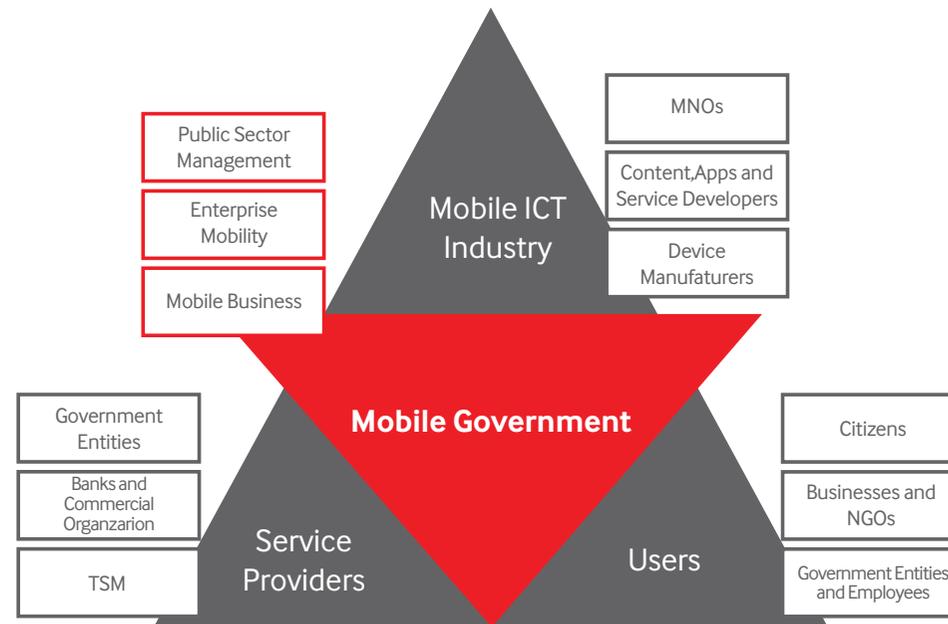
The RoadMap is drafted based on information gathered from various sources including background materials on (mobile) ICT in the UAE, eGovernment strategy and other relevant documents at the UAE's Telecommunications Regulatory Authority (TRA) as well as discussions with the mGovernment committee of the TRA and the key stakeholders of

the mGovernment transformation including key Ministries, Emirates Identity Authority (EIDA), UAE Central Bank and eGovernment authorities of Dubai, Ras al-Khaimah (RAK) and Abu Dhabi.

The RoadMap follows closely from the UAE Government's existing efforts to improve connected communications network, growth of Information Technology (IT) industry, to transform the government organisations and entities, and to implement eGovernment. It aims to be in line with overall ICT development efforts in the country. In addition, it identifies when mGovernment complements and when it offers distinctive advantages and added value to these efforts, especially to the eGovernment. In this way, a successful program of actions for mainstreaming mGovernment in the country to reach out almost all of the citizens (especially underserved communities and those living in rural areas) and business users may be possible.

Through various discussions with relevant stakeholders and workshops, the relevant information on required key tasks, the current status of eGovernment and mGovernment development, and what needs to be done in the two years ahead are gathered. During these information gathering meetings, it is observed that there a number of essential set of activities is being carried out at the TRA, which may have significant impact on the RoadMap to be developed.

The TRA is already involved in a number of key activities (such as Federal Network (FedNet), Mobile Identity, Mobile Payment (mPayment), Trusted Service Manager (TSM) and the Mobile Innovation Center (MIC) to start with the management of the



1. INTRODUCTION AND OVERVIEW

mGovernment transformation in the country. These tasks are major enablers for the nationwide success of the mGovernment. These activities could be best supported by a pragmatic RoadMap that comprises key tasks. This could have significant influence on making appropriate choices in terms of all of the activities being carried out by TRA.

Also, in line with making mGovernment transformation a nationwide project, there seems to be keen considerations to improve collaboration with, and understanding of the requirements of the various government entities in the country in terms of their level of competency, needs and approaches in transforming themselves to become an mGovernment enabled government organisation.

**1.4 Overview of the RoadMap**

Based on the information gathered and considering the current mobile ICT developments as well as the federal eGovernment strategy, a conceptual view of the RoadMap can be depicted as shown in the Figure 2 below. This is a high level view of the RoadMap, which shows essential areas in which a number of actions should be carried out. Similar to the eGovernment strategy the RoadMap also focuses on three main areas:

- Creating a environment for mGovernment (the first two steps - Figure 2)
- Enhancing the level of readiness for mGovernment (the third step - Figure 2)
- Attaining users' (i.e. citizens, government entities, and businesses) happiness (last step – Figure 2)

The first two steps in the Figure 2 are directly related to creating a favourable environment. The third step, enabling shared services, contains tasks directed for essential enhancements to the existing satisfactory

level of mGovernment readiness in the country. And the last step, attaining user happiness, requires all of the RoadMap tasks to focus on user related matters.

Although there is an urgency to carry out these activities from now until May 2015, these are core domains of activities that should be carried on through a reasonable time span. Given the scale, dependencies and the complexity of the tasks involved, some of the suggested tasks may not be fully completed by 2015. One of the significant roles of the RoadMap is to show essential milestones and tasks, which can lead to balancing and prioritization between what must be ideally done and what activities require attention before others. Furthermore, the mGovernment transformation is an on-going program for any country. For this reason, it needs to be continuously monitored, improved and sustained.

The steps that are shown in the conceptual view of the RoadMap, in fact, refer to four major tracks of the mGovernment transformation RoadMap, each of which contains a number of milestones. The Figure 3 amplifies the conceptual view of the RoadMap showing four tracks and corresponding sets of essential milestones. These four parallel tracks, although presented in detail through Sections 3 to 6, are briefly described as follows:

**1. Establish the environment for mGovernment to flourish:** This track contains milestones, which focus on creating necessary foundations for the mGovernment to exist and be sustained. This starts with establishing a strong and competent management group to plan and implement the mGovernment transformation. Other milestones deal with understanding how the government at a national level operates and the government entities are connected to one another in terms



of information and work flows; what can be done in improving stakeholder involvement and partnerships; in building capacity of the users and government entities; in creating a supportive mobile (ICT) industry and a legal framework. All of these are essential for having mGovernment to take of a countrywide program and achieve the desired goals.

**2. Assess capability and capacity of government entities:** This track mainly deals with understanding and finding out the ways for improving current situation with respect to readiness of the government entities to implement mGovernment. This track solely focuses on situation assessment with regards the government entities capabilities so that the next tracks could be implemented in a more effective and directed manner. For example, understanding capabilities of government entities in terms of their abilities to share data and applications will help to develop more realistic approaches for shared services (Track 3). Similarly, understanding

security needs will lead to development of better security directives that is part of the next track. There may be strong dependencies between this track and the other tracks.

**3. Establish shared resources across government entities at the national level:** This is the core track for improving readiness of the all government entities, especially from the point of technological view and sharing of a number of nationwide systems such as, Establishing Federal Network (FedNet) mobile payment (mPayment) and creation of mobile ID (mID).

**4. Achieve citizen happiness:** This track contains milestones that support a citizen centric mGovernment transformation especially with regards to underserved communities, citizens living in remote areas and those who form small communities such as farmers, unemployed and students. It also deals with promotion of the mGovernment services in order to speed up and assure adoption among the citizens

From Section 3 onwards a detailed description of each milestone and appropriate key tasks are discussed and summarised in a tabular form.

<b>Mobile Government Transformation RoadMap</b>	
<b>Major Tracks</b>	<b>Milestones</b>
<b>Establish the environment for the mGovernment to flourish</b>	<ul style="list-style-type: none"> <li>• Set up The Program Management Office</li> <li>• Determine Stakeholder Value Proposition and Facilitate Involvement</li> <li>• Understand Structure and Operations Among Government Entities at the Federal and Local Levels</li> <li>• Develop Mobile Value Chain in the Industry, and Facilitate Affordable Public Access to Wireless Networks and Services</li> <li>• Strengthen the Legal Base</li> <li>• Build Capacity of the Government Entities and the Users</li> </ul>
<b>Assess capability and capacity of government entities</b>	<ul style="list-style-type: none"> <li>• Assess Development and Sharing of Services and Applications</li> <li>• Assess Data / Information Sharing and Interoperability Capabilities</li> <li>• Assess Security Needs and Compliance with Security Requirements</li> <li>• Assess Resources and Skills Requirements</li> </ul>
<b>Establish Shared resources across government entities at the national level</b>	<ul style="list-style-type: none"> <li>• Set Up Mobile Identity (mobile ID) and Authentication Systems (i.e. Mobile Signature)</li> <li>• Set Up the Mobile Payment (mPayment) System</li> <li>• Set Up Trusted Service Manager (TSM)</li> <li>• Set Up Mobile Innovation Center (MIC)</li> <li>• Enable National Government Data Integration and Communication</li> <li>• Enable Hosting and Sharing Government Apps and Services</li> <li>• Create and Disseminate Commonly Shared Security Directives and Practices</li> <li>• Set Up the Federal Government Network (FedNet)</li> </ul>
<b>Achieve Citizen happiness</b>	<ul style="list-style-type: none"> <li>• Promote Convenience of Access and Usability</li> <li>• Promote Adoption of mGovernment</li> <li>• Determine Advocacy and Campaigning for mServices</li> <li>• Conduct Community Building (especially for underserved communities)</li> </ul>

## 2. ROADMAP OBJECTIVES AND OUTCOME

This RoadMap for the mGovernment transformation in the UAE sets out a number of milestones and relevant key tasks which all serve to achieve "happiness" for all citizens and residents in the country through utilisation of mobile public services. Essentially, it describes how this transformation will take place and how government entities could adopt enterprise mobility and start offering mobile services.

In this section, first, types of generic enhancements that can be expected from any implementation of mGovernment transformation will be discussed. This will set out a broader view of what can be achieved by mGovernment. Then, specific objectives and outcome of the RoadMap will be explained.

Section 2.1 provides four generic ways that mGovernment will have an influence on the transformation from eGovernment to mGovernment. These enhancements are generic and could be seen in any country and range from simply migrating selected eServices to mobile platform, to advanced levels of mGovernment implementation such as flexible working. Although mGovernment transformation in the UAE until May 2015 will be involving all of the four different enhancements suggested. The Program Management Office and all government entities should pay attention to what is possible and can ideally be implemented as part of the mGovernment transformation. The specific level that will be achieved from now to May 2015 depends on the decisions made by The Management of the Transformation and maturity level of the government entities in the UAE. In fact, one of the milestones in this RoadMap particularly focuses on this matter by working closely with all government entities and understanding their capabilities and capacities.

### 2.1 Types of Generic mGovernment Enhancements

There are four systematic ways of mGovernment enhancement in general. These enhancements might be related to the existing eServices of the government entities or totally new and unique mServices that are brought by the use of mobile technologies. In this respect, mGovernment is not a simple extension of eGovernment nor could it be viewed as just a new channel of service delivery. The four generic enhancements contributions of the mGovernment could be summarised as follows:

#### 1. 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.

**2. Citizen centric 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, mPayments for public transport and parking, and location based provisions of services.

**3. 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.

**4. 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".

It must be emphasised that these are generic enhancements that are normally expected given any mGovernment transformation within a country. How these enhancements will take place in the UAE depends on how the RoadMap will be implemented. It is evident that the mGovernment transformation in UAE until May 2015 will revolve around mostly the first two sets of enhancements.

The first enhancement is migrating fundamental eServices to become mServices. The second one is that there will be new mGovernment services that are not technologically possible to be offered via conventional wired networks as described in the second bullet point above. Given the nature of the operations of the government entities, there may be a number of mobile services concentrating around the third enhancement (mobile workforce). For example, government inspection employees, law enforcement or emergency services will be utilising most advanced mobile devices and applications to perform their tasks. At the moment, flexible working in the UAE may not be a priority. However, all government entities must keep in mind that the trend is moving towards this direction and they all have to be ready to implement remote and flexible working in the future.

### 2.2 Specific Objectives

In order to effectively implement these enhancements, this RoadMap articulates the following specific objectives, which are in line with the existing federal eGovernment Strategy in terms of its emphasis on environment, readiness and usage:

- Assess and understand the needs and requirements of the mGovernment

Transformation at the National level as a whole and at each government entity level,

- Create a favourable environment for the government entities to achieve mGovernment transformation through shared infrastructure, services, systems and appropriate guidelines and directives,
- Promote and ensure citizen adoption via convenient and personal mGovernment services delivery.

### 2.3 Expected Outcome

Accomplishing these objectives through the recommendations of this RoadMap will result in concrete outcomes, which include:

- A strong management group (i.e. mGov committee at the TRA) or agency for the whole mGovernment transformation program for now and for the future.
- A working collaborative environment among all government entities for preventing inefficiencies and promoting speed and reliability throughout the progress of the transformation.
- A reasonably well-established model of secure and trusted shared facilities, systems and services for integration and transactions. These include shared facilities for the development of apps and mServices, data centre for integration, nationwide mobile ID and mPayment systems.
- The highest level of convenience and benefits that would ensure widespread adoption of mGovernment and citizen happiness.

### 3. TRACK 1: ESTABLISH THE ENVIRONMENT FOR MGOVERNMENT TO FLOURISH

#### 3.1 Set Up The Program Management Office

The mGovernment transformation in the UAE requires a strong leadership in managing and implementing the whole program from now until May 2015 and also for the years to come. The Program Management Office will be responsible for implementing the RoadMap. Its strength should be parallel to a significant degree of accountability that is required in the implementation of the mGovernment Program.

The duties and responsibilities of the Program Management Office as it relates to implementation is given in Section 7.3 In this section, the PMO will be introduced and a discussion is presented on "what should be major roles and the responsibilities of such leadership?"

Given the complexity and the time span of the mGovernment transformation, a simplistic approach to the management may not be advisable. It is important to recognise that the management must have competencies in steering all activities detailed in this RoadMap as well as those that may come up on the way to reach out goals for 2015. This is an essential requirement for the implementation approach presented at the end of this report.

There may be two different approaches to the management of the whole program:

- A light view of management, which will have limited functionality such as only monitoring and advisory services to the government entities in their transformation to move to mGovernment. This seems very similar to existing practice where TRA is aiming to manage the program via competent mGovernment committee.

- A stronger view of management, which could be set up as a separate agency fully responsible for managing the entire mGovernment transformation for now and for the future. This agency would be involved in working very closely with the government entities in removing inefficiencies, duplication in many areas of this transformation as well as setting up and maintaining the shared infrastructure. It may even be engaged in building uniform apps or services across the government entities.

The choices between the two above should be made at the outset of the project. The appropriate structure and the role of The Program Management Office are to be clearly defined. The management should be competent and also demonstrate sustainability for the roles it performs.

#### Current Situation: The Management of mGovernment Transformation

Currently the executive management of the mGovernment program is handled by the TRA where an mGov committee is set up, members of which represents three departments namely Policies and Programs Department, Development Department and E-Government Operation Department. This committee reports to a Supreme Committee, which is composed of representations from various stakeholders such as TRA, Mobile Network Operators (Etisalat / du) etc. The current structure shows that mGovernment transformation is still the part of one of the TRA's three main functions: overlooking Information and E-Government Sector. Therefore, it is part of the existing eGovernment strategy.

#### Key Tasks:

##### KT 3.1.1 Determine core activities and the role of the management:

As discussed above it is important to analyse and decide what kind of managerial activities are needed in order to bring the mGovernment transformation to success. This will help in determining the scope and structure of the activities that the management will be involved in. Some of the typical activities that the program management unit would undertake include the followings:

- Strategically refine, organise and implement the milestones of this RoadMap.
- Through working with already established committees coordinate and implement over all mGovernment transformation such as:
  - o Provide guidelines, policies, standards and best practices across entities
  - o Enable security, data sharing, integration, enterprise mobility, application management, and device management for entities.
  - o Help entities to set priorities for their move to mGovernment.
  - o Enable collaboration and communication between different entities and promote integrated mobile services.
- Facilitate planning and developing applications to avoid inefficiencies.
- Identify and implement shared services for entity use such as mobile ID and mPayment systems.

#### Outcome:

An appropriate management approach responding to the needs of entities, where it would facilitate, coordinate and implement the key shared tasks as well as would guide the government units throughout the transformation processes.

#### Deliverable:

A competent management team responsible from implementing the RoadMap.

#### 3.1. Set up The Management of mGovernment Transformation Program

#	Key Tasks	Collaborations	Timeframe (months)
			6 12 18 24
3.1.1	Set up and determine core activities and the role of management	Program Management Office	●

**Outcome:** An appropriate management approach that will respond to the needs of entities, where it would facilitate, coordinate and implement the key shared tasks as well as guide the government units throughout the transformation processes.

3. TRACK 1: ESTABLISH THE ENVIRONMENT FOR MGOVERNMENT TO FLOURISH

**3.2 Stakeholder Value Proposition and Involvement**

The transformation to mGovernment in the UAE would not be possible without establishing strong partnership with the key stakeholders that would make some of the challenging tasks possible. In addition to the significant political mandate that exists already, the transformation program should also bring clearly identified value to all stakeholders at a wider scale in order to establish itself as a highly credible and supported initiative nationwide. This should result in valuable partnerships within government and with the private sector, contributing to various aspects of mGovernment transformation.

**Current Situation:  
Stakeholder Value Proposition and Involvement**

The present management is working closely with the following key stakeholders:

- Prime Minister Office
- Ministry of Labor
- Ministry of Finance
- Ministry of Justice
- Ministry of Interior
- Central Bank
- Emirates Identity Authority (EIDA)
- The two Mobile Network Operators (MNOs) - Etisalat and Du
- All eGovernment Programs such as Dubai eGovernment, Abu Dhabi eGovernment, etc.

In addition to these, educational institutions are also key stakeholders for capacity building programs directed to government employees.

All stakeholders seem to show sufficient eagerness to be part of the mGovernment programme. They seem to be ready to support the success of the initiative by bringing their competencies in. Emirates ID will be handling the mobile identity management (mobile ID) – device registration and authentication. Central Bank / Ministry of Finance are involved in mPayment. Ministry of Justice will be handling preparation of ICT law, as it is relevant to new mobile developments. The two MNOs (Etisalat and Du) will take part in making the overall infrastructure available to the mGovernment transformation program.

**Key Tasks:**

**KT 3.2.1. Determine and work with key stakeholders in creating favourable environment for the mGovernment transformation.**

Some of the key partners are already identified. It is also important to identify clearly what the particular roles will be, and what value each stakeholder is gaining from being part of the each of the milestones - particularly on critical nationwide projects such as mobile ID and mPayment. Potential areas that could hinder sustained cooperation should be identified and an agenda for sustaining cooperation and collaboration should be in place.

**KT 3.2.2. Identify and bring value to all stakeholders at a wider scale such as residents, visitors, and the businesses in the country.**

In addition to the key stakeholders, it is important to recognise that the success of the mGovernment transformation in the country largely depends on those stakeholders who are part of the ecosystem such as visitors, all residents from various backgrounds and the businesses. These all need to be identified and appropriate approaches to bring value to them need also to be determined from the initial phase of the project.

**Outcome:**

High-level support from all stakeholders who have strong influence on the success of the mGovernment transformation.

**Deliverable(s):**

- Identify and bring all relevant stakeholders on board.

- Determine roles and responsibilities, mutual benefits and collaboration opportunities with every stakeholder.
- Commit formally, whenever appropriate, stakeholders for their contributions to the mGovernment transformation.

**3.2. Stakeholder Value Proposition and Involvement**

#	Key Tasks	Collaborations	Timeframe (months)
			6 12 18 24
3.2.1	Set up and determine core activities and the role of management	Program Management Office	●
3.2.1	Identify and bring value to all stakeholders at a wider scale such as residents, visitors, and the businesses in the country	Program Management Office	●

**Outcome:** High level support from all stakeholders who have strong influence on the success of the mGovernment transformation.

3. TRACK 1: ESTABLISH THE ENVIRONMENT FOR MGOVERNMENT TO FLOURISH

**3.3 Structure and Operations Among Government Entities at Federal and Local Levels**

The UAE is attempting to achieve a nationwide mGovernment transformation where integration across all government entities is achieved. This nationwide view is a new and challenging approach in comparison to various successful implementations of eGovernment within each

emirate. In order to achieve this, the activities and operations of both federal government and local entities should be examined in terms of authorities and responsibilities, flow of work, processes and data sharing. This structural, procedural and interconnected view of all government organisations in the country is crucial to establish the means for government entities to share data and information, and successful integration.

**Current Situation:  
Structure and Operations Among Government Entities at Federal and Local Levels**

United Arab Emirates (UAE) is a monarchy with a president. It has seven emirates: Abu Dhabi, Dubai, Sharjah, Ajman, Fujairah, Umm Al Quwain and Ras Al Khaimah. Abu Dhabi is the capital of the Union.

The federal system of government includes the Supreme Council, the Council of Ministers (Cabinet), a parliamentary body in the form of the Federal National Council (FNC) and the Federal Supreme Court, which is representative of an independent judiciary. Prime Minister's Office is closely working with the eGovernment implementation in the country. There are also eGovernment authorities in each of the emirates such as eGovernment Dubai, eGovernment Abu Dhabi. Additionally, there are a number of eServices handled by local and federal entities. There is proven success in the implementation of federal eGovernment and eGovernment in each emirate. mGovernment programme, unlike eGovernment in each emirate, is planned to be a comprehensive and a nationwide project across the country. However, there are potential challenges in creating collaborative working environments among all government units within the UAE. For instance:

- Across all the seven emirates there are different levels of maturity of eGovernment programs.
- There is more competition among overall eGovernment implementation in the UAE than collaboration.
- There is no clear governance model for eGovernment program across the country.

These potential challenges can be solved by:

- Developing a clear Governance model for the mGov Transformation Program, which stipulates the roles and responsibilities of all stakeholders in order to construct an integrated and collaborative environment under a visionary leadership.
- Well-designed and implemented stakeholder engagement plan turning them into champions of the mGovernment success.
- Deployment of a communication plan: a detailed plan to manage internal and external communication should be developed with key stakeholders as well as an approach for management of change.

**Key Tasks:  
KT 3.3.1. Study the organisation, structure and operations of the all government entities in the UAE.**

Making mGovernment transformation a nationwide project requires a close collaboration among all government entities and especially with all eGovernment authorities of each of the emirates. This is exceptionally important for the key shared services but also for data integration and interoperability. The success of the mGovernment across the country largely depends on carefully planned design of activities and the means of communication among all government entities. It is vital to spell out clearly the lines of authorities and responsibilities, and the flow of communications and information. This may be a complex task requiring strong presence of the Management of the whole mGovernment program with its appropriate capabilities and capacities.

**Outcome:**  
Working with all government entities will help the management to assess the requirements; coordinate and plan shared services (including experiences, best practices and commonly accepted approaches to implementation) as well as improve the collaboration across government entities including data integration among government entities.

**Deliverable(s):**

- Determine and report a well-defined structure of the flow of communications and information among all government entities in the country.
- Determine and report structure of authorities and responsibilities among government entities.

- Determine and report key areas of data integration, information sharing and collaboration potential among government entities.

**3.3. Structure and Operations Among Government Entities at Federal and Local Levels**

#	Key Tasks	Collaborations	Timeframe (months)
			6 12 18 24
3.3.1	Study the organisation, structure and operations of the all government entities in the UAE	Program Management Office	

**Outcome:** Working with all government entities will help the management to assess the requirements; coordinate and plan shared services (including experiences, best practices and commonly accepted approaches to implementation) as well as improve the collaboration across government entities including data integration among government entities.

3. TRACK 1: ESTABLISH THE ENVIRONMENT FOR MGOVERNMENT TO FLOURISH

**3.4 Development of Mobile Value Chain, and Affordable Public Access to Wireless Networks and Services**

A strong mobile ICT sector is essential in supporting the countrywide mGovernment transformation.

There will be a need for presence and successful operations of companies belonging to the mobile value chain such as:

- Device manufacturers
- Content producers
- Mobile solution providers
- Mobile network operators
- Carriers

This will facilitate the development of thousands of mobile service offerings of the government. The sector also needs to be equipped with appropriate skilled labour force.

A healthy competition in the sector will also be needed for convenient and affordable public access to mobile services, which may be the key determining factor for citizen adoption and use.

**Key Tasks:**

**KT 3.4.1. Attract companies in the mobile value chain to the country:**

In order to shape these dynamics of the sector towards supporting the mGovernment initiative of the country, it is important that the sector is regulated accordingly. With the leadership of TRA, creative models of public and private partnerships should work towards assuring presence and operations of mobile (ICT) companies in the value chain in the country so that they are able to offer services to the, government entities, which are required for the technological and business aspects of the development of mGovernment. Their presence will not only support the mGovernment

transformation with close collaborations, but it will also bring in new dynamics and employment opportunities in the sector.

**KT 3.4.2. Encourage skill development and availability in the sector:**

There are already a few initiatives for skill development required by the mobile (ICT) sector and the mGovernment transformation as a whole. Such initiatives may be widened and aligned with

the mGovernment initiative. This could become a prominent part of the capacity building and Mobile Innovation Center.

**KT 3.4.3. Establish free or affordable access to government services:**

After such significant amount of effort channelled into the mGovernment transformation, it should not be slowed down or prevented due to the cost of accessing the services. There should be a plan

between MNOs and the government for providing affordable or free access to mServices both for the government entities and the citizens.

**Outcome:**

A healthy operating mobile ICT sector with sufficient support to the mGovernment transformation, plus easy and convenient access to the government services.

**Current Situation:**  
**Development of Mobile Value Chain, and Affordable Public Access to Wireless Networks and Services**

**Mobile Value Chain:** Developing mobile value chain in the UAE may be easier than thought as there may be tendencies that the private sector will follow the trend set by the government's demand for mobile solutions in the country. Currently, some of the companies in the mobile ICT industry and the relevant resources may exist as officially registered companies, and yet they may not be physically present and operating in the country. If this tendency grows, there may be more companies in the value chain actually operating and supporting the mGovernment transformation.

Most of the government entities will rely on mobile solution providers in developing their mServices. Having these companies operating in the UAE will provide opportunities for government entities to work closely with the companies in the mGovernment ICT sector, which would enable them to understand and follow the requirements better. Therefore, encouraging presence of companies in the UAE and creating strong public and private partnership (PPP) seems to be a significant opportunity that needs to be well explored.

**Skills Requirements:** According to input from TRA, a study was conducted to understand human resource requirements of the ICT sector at national level. The study showed that there was a need to improve the highly skilled human resources to the level of the pressing requirements of the ICT sector, which expands and grows fast.

In order to achieve this and enhance the ICT sector, TRA launched initiatives such as:

- The ICT Fund to achieve rapid, progressive and concrete developments within the ICT sector in the UAE; to jump start innovation within the sector - intellectual capital, technological leadership, smart research, innovative ideas, and incubating start-ups.
- Be'tha (Scholarship) Program to create a specialized and well trained ICT workforce in the country; to bridge the educational outcomes with the needs of the evolving job market, focusing on the leading scientific, telecom and IT specializations and majors.
- Sponsorship of various ICT related awards such as Mobile Awards.

There are also some academic initiatives providing ICT trainings for improving skilled labour in the industry such as Etisalat Academy.

**Public Access to Government Services:** TRA intends to regulate and facilitate availability of free or affordable public access to mGovernment services in the UAE. Both Internet providers should be part of such initiatives.

3. TRACK 1: ESTABLISH THE ENVIRONMENT FOR MGOVERNMENT TO FLOURISH

**Deliverable(s):**

- Design and put into practice appropriate policies and implementation plans for
- o Creation of dynamic mobile industry to support mGovernment transformation
- o Developing and Transformation Measurement Model
- o Skill development
- o Affordable access to mGovernment services

**3.4. Development of Mobile Value Chain and Affordable Public Access to Wireless Networks and Services**

#	Key Tasks	Collaborations	Timeframe (months)
			6 12 18 24
3.4.1	Attract companies in the mobile value chain to the country	Program Management Office, TRA	●
3.4.2	Encourage skill development and availability in the sector	Program Management Office, TRA	●
3.4.3	Establish free or affordable access to government services	Program Management Office, TRA	●

**Outcome:** A healthy operating mobile ICT sector with sufficient support to the mGovernment transformation, plus easy and convenient access to the government services.

**3.5 Strengthening the Legal Base**

Most of the eGovernment and mGovernment projects stagnate due to lack of appropriate legal framework. The presence of a strong legal base supports service offerings, transactions, building trust, protection of data and privacy of the citizens and beneficiaries.

**Current Situation: Strengthening the Legal Base**

In the UAE, the existing legal framework is based on federal eCommerce and Transactions Law enacted in 2006. In its present form, the law is not sufficient to account for new developments in mGovernment transformation such as mPayment (for example, there is a law that all government related transactions need to be conducted via e-Dirham – Law must be revised so that it will not become an obstacle) and transactions, mobile signature, and data sharing and protection. It needs to be further developed.

The TRA intends to work with relevant stakeholders (such as Ministry of Justice) to draft a comprehensive digital law.

**Key Tasks:**

**KT 3.5.1. Re-visit the ICT law to include mobile communication and provisions for mobile transactions:**

Often many countries are slow in backing up digital developments with a strong legal base. It is important that while the mGovernment transformation develops, an accompanying legal framework setup is also established to create basis for wide spreading key nationwide applications such as mobile ID and mPayment. The legal framework should also have perspectives on commercial extensions of these services as well as protection of data and privacy.

**Outcome:**

A strong legal base for mobile-based transactions, for example, using mobile ID, mPayment and acceptance of paperless communications.

**3.5. Strengthening the Legal Base**

#	Key Tasks	Collaborations	Timeframe (months)
			6 12 18 24
3.5.1	Re-visit the ICT law to include mobile communication and provisions for mobile transactions	TRA, Program Management Office, Ministry of Justice	●

**Outcome:** A strong legal base for mobile-based transactions, for example, using mobile ID and mPayment and acceptance of paperless communications.

**Deliverable(s):**

- Ensure legislations for the followings are in place
- o Supporting mGovernment transformation activities and
- o Creation and the use of mGovernment services

**3.6 Capacity Building Everywhere**

Transformation to mGovernment has crucial prerequisites regarding the existing capacity of the government institutions as well as the citizens. Success of a robust implementation of mGovernment services largely rests on the strength of the underlying composure on both the demand and the supply side. In the UAE, the required infrastructure is largely available that adds a positive implication for a successful transformation to mGovernment. Hence, key issues remaining to be

dealt with will mainly be concerning the questions of how to enhance capacity on government level as well as on public level. Following sections will analyse capacity building on these two aforementioned levels: institutional capacity building and citizen capacity building.

**Key Stakeholders:** Mobile Innovation Center, Policy Makers, Federal Government Entities and Citizens, Project Managers and IT Departments in government entities, Universities.

**Current Situation: Strengthening the Legal Base**

Government entities seem to be aware of the urgency related to mGovernment transformation. However, a general understanding of the entire process seems to be lacking and should be carefully treated. Federal and local entities are awaiting guidance and clarifications on the nature of transition in order to build capacity required for the implementation. The Mobile Innovation Center initiative, although not only a training center, may be a key organisation in order to achieve a direction for mGovernment transformation as it may bring together key players to analyse the lacking capacity and building it.

As for the citizens, mobile device usage has become a norm in the UAE whether it is mobile handsets, smart phones or tablets. Smart phone penetration is about 62%, which indicates mature level of uptake of new technology. Application usage figures are also high with the smart phone users: people on average having 27 applications installed on their smart phones and 64% connecting to internet at least once a day with their smart phones. All these imply a good base for citizen capacity.

3. TRACK 1: ESTABLISH THE ENVIRONMENT FOR MGOVERNMENT TO FLOURISH

**Institutional Capacity Building:** As is the case with all kinds of transformational processes, institutions will generally need certain adjustments, business restructuring, skills enhancements and capacity building on the path to mGovernment. Certain organisational aspects will inevitably come short in a new service strategy; human resources will need educational support for new technology and workflow; and some departments will require additional reinforcements to comply with the new demands of the transformation. In order to ensure a smooth transition towards mGovernment, policy makers should analyse the current human resource and skills capacity thoroughly and take proactive steps to enhance readiness to transforming services among the civil servants.

**Key Tasks:**

**KT 3.6.1. Raise awareness among and train the civil servants about mGovernment transformation:**

Make sure that government officials will be expecting the upcoming changes to their departments and fully understand the motivations and targets behind the mGovernment transition. Encourage all departments to pass on the planned changes in the workflow and services to their staff clearly. Encourage departments to:

- Ensure every government official has a clear understanding of the whole process;
- Foresee possible reasons for resistance to change and take the necessary measures to ensure that potential benefits to workflow, and efficiency are explained clearly;
- Involve staff to contribute to the development of ideas and best practices.

**KT 3.6.2. Analyse and improve existing human resources and skills among civil servants:**

This is the starting point to evaluate what the government entities are lacking for mGovernment transformation. The further steps will follow in accordance with the findings of the existing situation:

- Enforce Federal Government Entities to assess whether they have sufficient number of skilled IT staff to carry out the upcoming tasks that the department is intending to fulfil.
- Upon the analysis of the current level of capacity, identify the nature of the required guidance to enhance the knowledge base and technical infrastructure among all the Federal Government Entities.
- Analyse the differences and gaps between different government entities in terms of readiness.
- Formulate solutions to close the gaps and provide an efficient collaboration between entities.

**KT 3.6.3. Support Government Institutions with Education, Training and Building Technical Infrastructure:**

After a detailed study of the skills requirements of the government entities, appropriate training facilities and educational programs should take place for human resource quality enhancement.

- Organise seminars for the general matters regarding mGovernment and explain representatives the entire mobile governance transition and potential affects to the workflow and management.
- Prepare guidelines for institutional

rearrangements and discuss it with entity representatives.

- Plan nationwide training program on building technical infrastructure for Entities such as enterprise mobility. Enforce entities to take part in the programs and document each entity's transition experience provided with continuous communication.
- Provide tailor-made training facilities for government entities for institution-specific requirements for skills and capacity. (See section 5.4 Mobile Innovation Center)
- Organise IT training programs for Federal and local ministries and departments.

**Citizen Capacity Building:** Citizen readiness is as important factor as the institutional readiness for a successful mGovernment project. Gathering up-to-date information of the current usage behaviours, technical capabilities and skill requirements of the citizens are crucial in delivering them supportive services. The shortest route to achieve this is the engagement of users right from the initial stages of mGovernment transformation. Keeping close communication channels with the citizens for the development and usage of mobile services will be the key in all aspects of the mGovernment transition but specifically for capacity building of the citizens.

**KT 3.6.4. Raise awareness for the upcoming transformation in citizen services and engage citizens in the process:**

Make public aware of the transitional period of the government services. Engage them into developing ideas and taking part in the service

design. A possible way to aim for targeting citizens to engage is to ask for their opinions via feedback forms or surveys when they visit the public offices or government's official websites. Make sure you gather as much information as possible about their technical capabilities for receiving services and find out possible fields of improvement. Collect data on the usage behaviour as well as try to involve them in trainings and testing of the services.

**KT 3.6.5. Work on different segments of the society and with community organisations to build capacity:**

Different segments of the society will demand different services and, hence, the requirements for these services will vary depending on the community being dealt with. For instance, a mobile service for fishermen will require different capacity than a service for elderly people. Therefore, it is advisable to cooperate with different community organisations for capacity building. Training facilities and educational services should take part in this collaboration and reach out to targeted citizens for their exact requirements and capabilities. Community organisations will make it easier to analyse the community's usage behaviour and technical capabilities as well as to identify what kind of training would suit the best for the case in hand.

**Outcome:**

Enhanced readiness of Federal Government Entities and citizens required for mGovernment transformation regarding skills and capacities.

3. TRACK 1: ESTABLISH THE ENVIRONMENT FOR MGOVERNMENT TO FLOURISH

**Deliverable(s):**

- Design and implement awareness, training and skills development programs for government entities
- Design and implement awareness, training, adoption and skills development programs for citizens
- Design and implement awareness, training and skills development programs for businesses and other stakeholders

**3.6. Capacity Building Everywhere**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
<b>3.6.1</b>	Raise awareness among and train the civil servants about mGovernment transformation	Mobile Innovation Center, Federal Government Entities, Project Managers and IT Departments in government entities, Universities.			●	
<b>3.6.2</b>	Analyse and improve existing human resources and skills among civil servants:	Mobile Innovation Center, Policy Makers, Federal Government Entities and Citizens, Project Managers and IT Departments in government entities, Universities.			●	
<b>3.6.3</b>	Support Government Institutions with Education, Training and Building Technical Infrastructure	Mobile Innovation Center, Policy Makers, Federal Government Entities, Project Managers and IT Departments in government entities, Universities.			●	
<b>3.6.4</b>	Raise awareness for the upcoming transformation in citizen services and engage citizens in the process	Mobile Innovation Center, Policy Makers, Federal Government Entities and Citizens, Project Managers and IT Departments in government entities, Universities.				●
<b>3.6.5</b>	Work on different segments of the society and with community organisations to build capacity	Mobile Innovation Center, Policy Makers, All Government Entities and Citizens, Project Managers and IT Departments in government entities, Universities.				●

**Outcome:** Enhanced readiness of Federal Government Entities and citizens required for mGovernment transformation regarding skills and capacities.

## 4. TRACK 2: ASSESS CAPABILITY AND CAPACITY OF GOVERNMENT ENTITIES

The purpose of this track is to help the PMO to identify capabilities and capacities of the government entities. The Program Management Office must base its actions on the requirements of the government entities by surveying their capabilities and capacities according to various key areas. This will improve collaboration and cooperation among the management and the government entities. It will also allow the new mGovernment transformation to be more realistic and based on the actual situation that the government entities are in. This practice will help to create a uniform approach to developing applications, and entity-wide approaches to adopt enterprise mobility. It aims to remove repetitions and inefficiencies that will result in significant cost savings.

The milestones in this section deal with situation assessment and determining ways of supporting government entities given their capabilities and capacities rather than engaging The Program Management Office to actually implement any tasks. In this manner, the tasks in this track are different than their similar counterparts in that these are more of an essential preparation work contributing to successful implementation of the other tasks in this RoadMap.

The tasks and milestones of this track could be carried out via surveys and / or closely working with some of the selected government entities. The work accomplished in this track has strong relevance to understanding different levels of maturity of government entities and corresponding capabilities as a whole in the country. This, in turn, should lead to sound implementation approaches for the mGovernment transformation program to succeed as nationwide program.

### 4.1 Assess Development and Sharing of Services and Applications

This milestone is related to working with the government entities and understanding their capabilities and capacities in developing mobile applications and services and their ability to share and collaborate on relevant experiences. With this study, The Program Management Office understands the needs of the entities when they develop several services and assesses which of those services could be shared and could lead to integration among the entities.

#### Current Situation: Strengthening the Legal Base

Currently, the TRA is utilising its internal resources to improve communications and collaborations with the government entities. A clear communication/management of change/stakeholder engagement plan is considered essential for smooth running of the mGovernment transformation program.

As part of developing the IT Strategy for the government in 2009, the TRA conducted an IT maturity exercise for all Federal Government entities.

#### Key Tasks:

##### KT 4.1.1. Understand the needs of the entities and support the prioritization of migrating eServices:

This task focuses on understanding and supporting government entities to prioritise which of the existing eServices, primarily, to be transferred to mobile platform. It also involves an analysis of the overall needs of the government entities for managing the transformation process successfully, including development of new mobile services. Prioritization

of existing services and applications based on certain criteria is essential for starting the mGovernment transformation. A set of guidelines in this respect would help entities significantly and allow a uniform approach.

The Program Management Office (PMO) should also be fully aware of the needs of the government entities that are part of and contributing to a platform for shared services and applications. Internal structure and the culture of the organisation as well as the infrastructural differences should be carefully examined and articulated in order to form a base for finding the best approach that fits all parties.

##### KT 4.1.2. Establish a common base for knowledge sharing and collaborations

This task is related to creation of possible means for the government entities and The Program Management Office (PMO) to communicate and collaborate on the activities that each one of them is carrying out. For this task, the Management of mGovernment transformation may choose to establish a shared collaboration environment for the government entities. This environment might stimulate the re-use of existing standards, sharing best practices and lessons learnt which would eliminate re-inventing the wheel leading to cost and time efficiencies. Additionally, this may promote sharing experiences in service development.

#### Outcome:

Reduced costs, repetitions and inefficiencies and increased communications and collaboration among government entities, as it is relevant to applications and services development, which, in turn, may lead to greater user satisfaction as a result of harmonisation of services and applications.

#### Deliverable(s):

- For effective mGovernment application and services development
  - o Report on understanding of common needs and shared activities among government entities
  - o Design and put into practice policies, procedures and guidelines to promote sharing of resources and experiences and to remove inefficiencies

#### 4.1. Assess Development and Sharing of Services and Applications

#	Key Tasks	Collaborations	Timeframe (months)
			6 12 18 24
4.1.1	Understand the needs of the entities and support the prioritization of migrating eServices	Program Management Office and All Government Entities	●
4.1.2	Establish a common base for knowledge sharing and collaborations	Program Management Office and All Government Entities	●

**Outcome:** Reduced costs, repetitions and inefficiencies and increased communications and collaboration among government entities, as it is relevant to applications and services development, which, in turn, may lead to greater user satisfaction as a result of harmonisation of services and applications.

4. TRACK 2: ASSESS CAPABILITY AND CAPACITY OF GOVERNMENT ENTITIES

**4.2 Assess Data / Information Sharing and Interoperability Capabilities**

While the first milestone in the track (see Section 4.1) focused on assessment of applications and service development, this milestone is related to examining and understanding capacities and capabilities of the government entities to integrate and interoperate via sharing data and information. Interoperability refers to exchanging data in a reciprocal way. For more service-oriented and competitive public services, interoperability is inevitable. In order to achieve this, legislation harmonization and technology standardisation must be ensured. Three dimensions of interoperability need to be examined to form the basis for developing mServices in an agile manner:

- Organisational interoperability (entities having different internal structures and processes will need to collaborate to exchange information). All Government Entities determine together the requirements for common applications via a demand-driven approach (of citizens and enterprises).
- Semantic interoperability (exchanged information may be processed by any other application designed independently). For instance, Extensible Mark-up Language (XML), as mark-up language, can be the single language for the exchange of information. However, for semantic interoperability, design of XML schemas is required to integrate mobile services that are developed with different terminologies (e.g. one entity using Arabic and the other one using English as application language), etc.
- Technical interoperability (linking mobile devices and services). Front-end examples can be

interfaces, character sets, data exchange, and display. Back-end aspects may include file and message transfer protocols and security, data integration, web services, etc.

In this milestone, the job of The Program Management Office to explore possibilities of connecting government entities one another so that integrated mGovernment systems could be developed.

**Current Situation:  
Strengthening the Legal Base**

As is known, one of the biggest challenges of the mGovernment transformation is preparing government entities for data sharing and integration. Currently, among the TRA's efforts in this respect, establishing Federal Network (FedNet) is considered as a means to creating a collaborative environment among government entities. Other shared systems and components such as Trusted Service Management, Central Mobile Delivery Gateway, and shared API require integration. The efforts in building these systems should also assist in the integration. TRA already recognises that there are further crucial issues that are challenging and needs special attention. These include improving the data structures and nature of personal and business data handling and storage and having a common core data for all Federal/Local Entities.

**KT 4.2.1. Legislation harmonization, technology standardisation and interoperability:**

This is perhaps one of the most significant and the most difficult task among all milestones in the RoadMap. The Program Management Office must

involve all government entities in developing an understanding of significance of sharing data and services for successful deployment of advanced integrated mGovernment services in the country. It should articulate and communicate existing initiatives such as FedNet, and how the entities could be part of it and benefit from it. Through interactions with entities, a carefully planned course of actions should be created for achieving convergences and standardisation in various aspects of technology such as the devices management, wireless network management, application and services development and sharing. The successful implementation of this task should create a strong basis for the key milestone on data sharing data countrywide. Any legal implications of such practice should also be handled.

**Outcome:**

Better understanding of government entities as integrated service providers via mobile services and applications, which could facilitate creation of systems to be nationwide, interoperable and integrated.

**Deliverable(s):**

- For deploying integrated services
- o Report on understanding of common needs and opportunities for integration among government entities
- o Design and put into practice policies, procedures and guidelines to enable data / information harmonisation, standardization and interoperability

**4.2. Assess Data / Information Sharing and Interoperability**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
4.2.1	Legislation harmonization, technology standardisation and interoperability	Program Management Office, All Government Entities, Legal Advisors and Infrastructure Experts, and Business Analysts				

**Outcome:** Better understanding of government entities as integrated service providers via mobile services and applications, which could facilitate creation of systems to be nationwide, interoperable and integrated.

**4.3 Assess Security Needs and Compliance with Security Requirements**

mGovernment transformation requires government entities to implement enterprise mobility where security is of crucial significance. The government entities need to be supported in this process where governments' strict security policies must be communicated widely and implemented. This milestone is related to understanding existing security requirements of the government entities and providing them with support in terms of security concerns when they adopt mobile technologies in their organisations. Such support is of crucial importance for entities to smoothly deploy and manage mobile services and to prevent public data to be accessed by unauthorised third parties.

4. TRACK 2: ASSESS CAPABILITY AND CAPACITY OF GOVERNMENT ENTITIES

In this milestone The Program Management Office aims to work closely with government entities to develop a good understanding of cyber security as national priority, enterprise level security and risk mitigation approaches. Such study should also deal with privacy policies and data protection schemes in sharing and integrating data and services. Through working on this track, the results of the assessments should feed into developing such security and privacy policies (please refer to Section 5.7 milestone on Security) and these should be well articulated among the government entities in order to assure compliance.

**Key Tasks:**

**KT 4.3.1. Promote approaches for risk mitigation**

Working with the government entities closely, security risks arising from use of mobile devices, wireless networks and data transfers should be identified and the entities may be steered in order to reduce all such kind of security risks. For example, applications and services that use cloud environments for data storage rather than physically on the device can be one of the alternatives to minimise the risks.

**KT 4.3.2. Articulate and assure compliance to common security policies**

The Program Management Office and government entities should work together to develop and adhere to a common security policy and strive for its sustainability. For nationwide safe and secure mobile applications and services, based on the assessments and collaborations on this milestone, the foundations for developing a common security policy and its implementation across the government entities should be encouraged. However, creation and assuring compliance with such policies will not be

**Current Situation:  
Support Entities to Comply with Security Requirements**

In order for government entities to properly implement mGovernment, they all need to adopt enterprise mobility with appropriate wireless security provisions. Today, each government entity is working in isolation in implementing enterprise mobility. To create uniformity through a central approach is considered to be very challenging.

Initiatives or plans in guiding government entities for enterprise mobility and, in particular, for security seems to be present in each jurisdiction (Federal/ Local level) as various standards. The level of maturity, adoption varies from entity to entity. The TRA was engaged in an exercise in 2009, where the level of IT maturity was evaluated across Federal entities and an IT Security Policy was developed.

Additionally, the UAE Computer Emergency Response Team (aeCERT), established by the TRA has developed a Information Security Policy which it shares with its constituents.

In the short run, enabling enterprise mobility in all government entities is a highly demanding effort. Until this is successfully established, there is a need for contingency plans and pragmatic workable solutions.

sufficient. In addition, this milestone should open opportunities for providing the base for constant revision of activities with appropriate monitoring mechanisms as well as training key officials for performing such controls. The government entities must be made aware that a strong approach for reliability and quality assessment is fundamental

to maintain, and even strengthen, the image of the government among the citizens and the businesses.

**Outcome:**

An understanding of core issues in security and enable government entities to realise the significance of having highest standard of security in offering mobile services and applications.

**Deliverable(s):**

- Determine and Disseminate understanding of significance of mobile security in government entities.
- Design and put into practice policies, procedures and guidelines to articulate and implement compliance to mobile security measures.

**4.3. Support Entities to Comply with Security Requirements**

#	Key Tasks	Collaborations	Timeframe (months)
			6 12 18 24
4.3.1	Promote approaches for risk mitigation	Program Management Office, All Government Entities and Security Experts	●
4.3.2	Establish a common base for knowledge sharing and collaborations	Program Management Office, All Government Entities, Security Experts and Policy Advisors	●

**Outcome:** An understanding of core issues in security and enable government entities to realise the significance of having highest standard of security in offering mobile services and applications.

**4.4 Assess Resources and Skills Requirements**

This milestone is related to discovering availability or absence of technical and non-technical resources of government entities in order for them to effectively implement what is required from the mGovernment transformation. Each government entity may have different set of resources and skills. The responsibility of The Program Management Office is not only assessing the existing skills and resources but also working on resources procurement and skills improvement. This milestone may be tied to existing nationwide incentive systems based on performance. One idea is to design a performance system for government employees not only for the mGovernment transformation, but also for supporting achievements towards the year 2021 vision. The result of such assessments in this milestone will help to support other milestones in the RoadMap.

**Current Situation:  
Assess Resources and Skills Requirements**

Realistic assessment of government entities' ability to fulfil the resource and skills requirements for mGovernment transformation is not an easy task as they differ from one entity to another. The government entities are engaging in partnerships with the private sector to make up for lack of skills and resources. The TRA currently has plans in place for capacity building of the government employees throughout the country. The TRA has finalised the request for proposal and received proposals from different firms. This is in the process of evaluation. The expected timeline for the training programmes is 12 - 18 months.

4. TRACK 2: ASSESS CAPABILITY AND CAPACITY OF GOVERNMENT ENTITIES

**Key Tasks:**

**KT 4.4.1. Understand the resources and skills needed**

For successful implementation and sustainable management of mobile services and applications, for each of the government entities, a group of skilful resources must be available from organisational resources (the management team, public relations and administrative support), to technical (developers, security and infrastructure experts, testers) and specialised teams (user experience and user interface experts, strategists, legal advisors, quality control specialists, policy advisors and trainers). Government employees may need training to support the implementation of mGovernment transformation process. This may require training materials to be developed and delivered at an early stage.

The task of The Program Management Office, by working with government entities, is to identify what kinds of skills are available and which ones are typically missing. It should encourage the government entities to develop or procure skills necessary so that each entity can be part of and supportive of the mGovernment transformation.

**KT 4.3.2. Promote partnership for skills and resource development**

Understanding the skill and resource requirement naturally leads to proposing ways and steering government entities to establish partnerships in developing such resources and skills via working with partners such as other government organisations, training and educational organisations. In the long run, educational institutions, universities and private sector collaboration would be imminent such as

developing tailor-made trainings and opening new departments to match the requirements of the government entities, as the specific job profiles will be demanded to fulfill the agile mobile technology requirements. With this task The Program Management Office creates approaches to partnerships and disseminates these approaches among all government entities.

**Outcome:**

Understanding and articulation of resources and skill requirements among government entities, in order to reassure effective partnerships and a successful implementation of mGovernment transformation.

**Deliverable(s):**

- Determine and Report on common needs for resources and skills among government entities
- Design programs for meeting skills and resources requirements.

**4.4. Assess Resources and Skills Requirements**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
4.4.1	Understand the resources and skills needed	Program Management Office, technical and specialists teams, mobility consultants and All Government Entities			●	
4.4.2	Promote partnership for skills and resources development.	Program Management Office and All Government Entities				●

**Outcome:** Understanding and articulation of resources and skill requirements among government entities, in order to reassure effective partnerships and a successful implementation of mGovernment transformation.

## 5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

### 5.1 Mobile Identity (mobile ID) and Authentication System

Mobile identity is one of the key enablers for various mobile services such as mPayments, banking, voting and all sorts of services that require secure authentication. Digital fraud is escalating to unprecedented levels and users are in demand for highest security standards for the services they use. Increasing demand from mobile users for mobile services may only be provided effectively by securing transactions and using authenticated communications. A nationwide mobile ID will need to overcome authentication frauds when providing mobile identity services for citizen convenience.

Currently several entities use their own digital authentication services in the UAE such as Ministry of Interior, Roads and Transport Authority (RTA) and several banks. However, the pressing need for a secure mobile ID on a national level is emerging as a milestone not only as another form of national identity but also as a shared service that many other services may be integrated into.

**Key Stakeholders:** Emirates Identity Authority, independent TSM authority, MNOs, Service Providers, Local and Federal Government Authorities, Application Developers and Financial Institutions.

**Key Challenges Ahead:** Regardless of the way the mobile ID initiative will be unfolding itself, there are a number of key challenges that The Program Management Office and the key stakeholders should be taking into consideration:

- A strong Legal Framework should be supporting the processes where the mobile ID and mobile Signature may be used.

- The citizens should be offered a top-level convenience and ease of use.
- Security must be hand in hand with the most secure systems in the world and as such it should build trust in government operations and support the user take up.
- Mobile ID should be easy to integrate with a large number mServices that will be offered in the UAE. Technological assessment by the key partners should closely evaluate issues with interoperability.
- In many countries, the user uptake for mobile ID or mobile Signature has been very slow due to some practical reasons such as inconvenience (usability issues or difficult registration process) and competitions among the MNOs (cooperation between MNOs is a must for providing a nationwide solution, fierce competition hinders the usability and interoperability of identity services in some cases). Citizens require services that are user friendly, and that they can access with any device, via any operator and network, from anywhere, anytime. Providing secure and end-to-end services to any mobile subscriber without sacrificing from user experience is a key challenge and requires cooperation among the involved stakeholders. Mobile network operators should ensure that users would seamlessly benefit from services that utilise mobile identity without regards to which operator they subscribe.

#### **Key Tasks:**

**KT 5.1.1. Identify stakeholders and partners:** Current partners for the mobile ID involves EIDA, Service Providers and MNOs – du, Etisalat. Their roles and expectations need to be clearly identified

#### **Current Situation: Assess Resources and Skills Requirements**

Currently a physical card exists as National ID. Apart from that, different institutions have their own digital identity for their users such as Roads and Transport Authority (for road tolls and fine payments), banks (for online banking) and Internet service providers (for bill payments).

The TRA will be working with the relevant authorities (such as Ministry of Justice) to draft the required legislation.

There are several challenges regarding the data integration and interoperability within the national Mobile ID system. These challenges require enabling infrastructure such as FedNet, TSM, use of Shared Application Programming Interfaces (APIs) and data sharing platform architecture.

in order to establish a sustainable model of cooperation.

#### **KT 5.1.2. Establish a Legal Base for mobile ID:**

The use of mobile ID should be recognised as an official authentication mechanism. Any implications for its use by the citizens must be reflected to the legal framework. This may require working closely with the Ministry of Justice.

#### **KT 5.1.3. Implement Policies and Best Practices for Top Level User Security and Privacy:**

Mobile ID needs to be at least as robust and secure as the other existing authentication solutions - if not more. Subscriber Identity Module (SIM) based mobile Public Key Infrastructure (PKI) system ensures high

levels of security with all security related data is encrypted in the SIM and Global System for Mobile communications (GSM) number as the activator of the transactions.

- Ensure the mobile PKI infrastructure is unified among all the key actors involved, particularly the MNOs in order to provide a uniform security standard to the user.
- Use spam prevention codes and transaction IDs for each interaction with users in order to avoid spam requests. Users need to be sure in each transaction which parties they are interacting with.
- Ensure instant locking of mobile ID functions upon a request due to theft or loss of device.
- Implement mechanisms of detecting abnormal behaviour and add relevant secondary confirmation for the identity.

#### **KT 5.1.4. Ensure Usability and Easy Registration and Promote User Adoption:**

User uptake is dependent on many factors including ease of use and registration, the number of mPayment services that are available, security and privacy issues and awareness. Governments and the partners have a joint duty in promoting the Mobile ID.

- Enable easy registration process for mobile ID. Users should not refrain from joining these services. When registering for the services, providing proof of national ID at the branches of MNOs is sufficient in many countries that use mobile ID.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

- Upon registration, provide easiness by means of pin code authentication (request from users to only have the mobile device and pin code entry).
- Support mobile signature services as well as authentication services.
- Enable one time login for all government services in order to make it convenient for users who currently need to login to each service with different processes and passwords.
- Ensure a nationwide standard for mobile PKI and PKI infrastructure so that encryption and authentication processes will be standardised.
- Promote uniform APIs for service providers in order to enhance user experience by going through similar steps of authentication and transactions with different service providers.
- Ensure citizens have either very low-cost or free mobile ID for high adoption.
- Initiate several mobile ID services to make Mobile ID attractive to users. Start with those that are the most frequently used.
- Ensure commercial banks start using mobile ID authentication. Banks play key role in user acceptance due to broad use of banking services by citizens. Provide assistance in case banks have any reservations concerning their own system security while integrating mobile ID.
- Make mobile ID available for frequently used transactions and interactions. Especially at the initial stages this will help to increase user adoption.

- At latter stages, plan to enable enterprise subscriptions for mobile ID rather than only letting individuals have a mobile ID (e.g. businesses, companies, NGOs should also have mobile IDs).

**Outcome:**

Implementing a nationwide Mobile ID will be a baseline for the integration of various federal and local level mobile services. Citizen privacy and security will be provided on each and every service use. Payment and other transactional services will be authenticated with Mobile ID providing secure services. One time login for all government services will be possible for user convenience. Personalization of public mobile services will be possible by using contexts derived from mobile ID.

**Deliverable(s):**

- Design and implement the country-wide mobile ID system;
- Formally involve the relevant key stakeholders with clear identification of the roles and responsibilities;
- Make sure that appropriate legislations are in place;
- Design and put in practice policies/directives for the implementation and the use of the mobile ID;
- Determine and put in practice approaches to ensure user take up and adoption.

**5.1. Mobile ID and Authentication System**

#	Key Tasks	Collaborations	Timeframe (months)
			6 12 18 24
5.1.1	Identify stakeholders and partners	Program Management Office	●
5.1.2	Establish a Legal Base for mobile ID	Program Management Office, TRA, Relevant Stakeholders and Legal Experts	●
5.1.3	Implement Policies and Best Practices for Top Level User Security and Privacy	Program Management Office, TRA, Relevant Stakeholders and Security Experts	●
5.1.4	Ensure Usability and Easy Registration and Promote User Adoption	Program Management Office and Relevant Stakeholders	●

**Outcome:** Implementing a nationwide Mobile ID will be a baseline for the integration of various federal and local level mobile services. Citizen privacy and security will be provided on each and every service use. Payment and other transactional services will be authenticated with Mobile ID providing secure services. One time login for all government services will be possible for user convenience. Personalization of public mobile services will be possible by using contexts derived from mobile ID.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

## 5.2 Mobile Payment (mPayment) System

mPayment may be defined as a payment process between two parties over a mobile device. mPayment volume is peaking up around the world in the last few years, though it had been facing certain resistance from service providers and users for some time. Users are increasingly demanding convenient solutions for payment transactions - specifically for the ones that they use frequently such as road tolls, public transport, parking fees, bills and fines. Hence, mPayment services are becoming very central in public services as an enabler.

Key Challenges Ahead: A nationwide mPayment solution has various challenges with regards to:

- Security of transactions and User Authentication/ Privacy.
- Interoperability of the payments system across the MNOs, various devices and operating systems.
- Setting Legal Framework and Regulations.
- User/Service Provider Resistance to Adoption.

### Current Situation: Mobile Payment System

Currently there is no national mPayment system. There is e-Gov initiative for mPayment in Dubai that is used for topping up Salik, paying bills and fines. Legal structure needs revision and possibly certain adjustments to support national mPayment solution. Discussions are on-going with Ministry of Finance and Central Bank on creating a nationwide mPayment system.

**Key Stakeholders:** Ministry of Finance, Central Bank, Financial Institutions, MNOs, TSM entity, Service Providers.

### Key Tasks:

#### KT 5.2.1. Determine Key Stakeholders:

Identify the workflow and mutually beneficial partnerships to create an efficient and dynamic mobile commerce environment. Involve in strategic public-private partnerships as well as encourage all Federal Government Entities to join the efforts.

- Government Entities
- Mobile Network Operators
- UAE Financial Institutions
- Device Manufacturers (in the case of Near Field Communication (NFC))
- Trusted Service Manager (TSM)
- Online Payment Service Providers
- Regulatory Entities (identity management, cyber security)

#### KT 5.2.2. Identify Suitable Technologies for mPayment:

Depending on the nature of the transaction either Remote Payment solutions or Near Field Communication (NFC) systems can be used.

- For micropayment, Short Message Service (SMS) billing can be considered, which is becoming more the norm and 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.
- Deployment of a NFC payment system is not a matter of only one organisation. It's a large-scale project that requires the cooperation with private

sector and the alignment of public sector. These projects are usually led by banks. Government acts as a promoter working actively with the bank to engage private sector.

- Introduction of an NFC payment system requires planning of a gradual solution deployment. Government support for adopting the official services to new payment system is crucial. Monitoring security related issues regarding NFC and promoting the use of this technology in key public services are prominent tasks for technology adoption.

#### KT 5.2.3. Plan in advance for integrating mPayment with other public and private services:

Keep in mind that national mPayment architecture will grow in size and to various directions that are unpredictable. Several public and private initiatives will provide services that require mPayment, which will require integration with the national mPayment infrastructure. Hence, always be open for improvement with regard to integration and upgrading of the entire mPayment system.

- Provide integration with mobile ID for authentication and security. For security and privacy issues around mPayment, a central approach for identity approval is a convenient solution.
- Provide standards and guidelines for service providers using mPayment. Government entities and other entities will be able to integrate their services to the existing national payment system. They should be informed and trained about how to do so.

- Convert web-based mPayment gateways to application-based gateways. However, keep the payment process identical in each application to ensure usability.

#### KT 5.2.4. Enable Sharing of Security Standards and Policies Nationwide:

Security is the biggest challenge in mobile sector and, therefore, needs to be taken into consideration with extra care. Citizens and all the stakeholders will demand assurance on the overall security and privacy of the transactions. Otherwise, adoption rates will remain low. As outlined in section 4.3, cooperative action of government entities is required towards the risk mitigation and security standardisation.

- Establish a regulatory framework for privacy and security of transactions that are used in all of the shared mPayment services.
- Design standards for domestic and international interoperability and share it with every relevant government entity and private parties involved. Ensure international accounts can be involved in mPayment in a secure way. Ensure the services work over a range of devices and operating systems.
- Assign Trusted Service Managers (TSM) to oversee shared security elements used in nationwide mPayment transactions.

#### KT 5.2.5. Ensure nationwide implementation and adoption of mPayment Services:

Raising awareness and bringing high value to citizens, reassuring the concerns around mPayment will lead to high rates of adoption. Strategic approach

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

towards acceptance will require the efforts of all the key stakeholders in mPayment.

- Enable mPayment in all the key government transactional services and promote mPayment among government entities as well as citizens.
- Make mPayment implementations in frequently used services first such as mobile parking, transport, and small fines.
- Encourage mobile operators to take a proactive position in mPayment adoption. Ensure MNOs offer mobile devices supporting credit card or pre-paid card features.
- Involve banks in mPayment implementation and adoption. Ensure that they realise the cost benefits of mobile transactions, which can reduce the costs up to 45- times compared to face-to-face transactions.
- Involve all key actors in collaborative action plan for mPayment implementation. Incentivise active participation of financial institutions, MNOs, TPP (Third-Party Payment) providers to create a dynamic system with variety of different solutions for mPayment.

**Outcome:**

A nationwide mPayment system will provide all entities to integrate their mobile services to the national payment gateway without having to develop their own payment solutions. Transactions will be centrally secured and authenticated.

**Deliverable(s):**

- Design and implement the country-wide mobile payment system.
- Formally involve the relevant key stakeholders with clear identification of the roles and responsibilities
- Make sure that appropriate legislations are in place
- Design and put in practice policies/directives for the implementation and the use of the mobile payment
- Determine and put in practice approaches to ensure user take up and adoption.

**5.2. Mobile Payment System**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
5.2.1	Determine Key Stakeholders	Program Management Office	●			
5.2.2	Identify Suitable Technologies for mPayment	Program Management Office and Relevant Stakeholders	●			
5.2.3	Plan ahead for integrated services	Program Management Office and Relevant Stakeholders		●		
5.2.4	Establish Security Standards and Policies	Program Management Office, TRA, Relevant Stakeholders and Security Experts			●	
5.2.5	Ensure nationwide implementation and adoption of mPayment Services	Program Management Office and Relevant Stakeholders				●

**Outcome:** A nationwide mPayment system will provide All Government Entities to integrate their mobile services to the national payment gateway without having to develop their own payment solutions. Transactions will be centrally secured and authenticated.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

### 5.3 Trusted Service Manager (TSM)

TSM is a neutral independent entity serving in between service providers (government and businesses) and MNOs during mPayment transactions. It serves as a single point of contact for the service providers to reach their customer base through mobile network operators. Hence, using the networks of mobile operators, TSMs allow service providers to manage transactions in a secure way without involving in or interrupting the business model of the service providers. It is one of the key actors among many in mGovernment ecosystem. Thus, within each national environment, different models for TSMs can be implemented. It could, for instance, be managed by one MNO, a committee of different MNOs or by trusted third parties. For the UAE, a consortium was formed to govern the national TSM. It is also possible to have more than one TSM depending on the market needs. In that case, it is possible to see a combination of the above-mentioned models. However, regardless of the model being used TSMs should have following abilities:

- To involve in high-numbered partnerships and contracts.
- To maintain good reputation of service security.
- To have a trusted image within the mobile ecosystem.

The need for a TSM emerges for several reasons. First of all, any application that requires access to personal information should be handled with care. Personal information on mobile devices should be stored in a secure element rather than device's own memory. Provisioning the security of personal

information is the major role that the TSM plays. It restricts access to applications and data to only those that have authority to access it. TSM also provisions secure handling of the personal data by the financial institutions and third parties. Security of key management processes takes place for data handling. Finally, during the payment process the user should be properly authenticated so that the payment receiver/sender is verified correctly.

**Key Stakeholders:** MNOs, EIDA, Financial Institutions, Service Providers, Citizens, and TSMs.

#### Critical Role of TSM:

In the complex environment of mobile sector where numerous parties' active involvement and harmonious collaboration is essential, TSM plays a key role of coordinating the interests of different players without interfering in the business procedures and, at the same time, ensuring users' data security and privacy. An independent TSM is, thus, very central in the whole mobile sector platform. The first key role is that TSM connects service/application providers with the mobile operators allowing each of them to access the other's customers in its safe environment.

Second key role is that TSM provides a platform of trust where service providers, citizens and mobile operators as well as software developers can pursue their interest keeping their relations with each other on stable grounds. TSM can provide consultancy, security checks, testing and evaluation for the new applications and at the same time may mediate the user transactions in a secure way. It may also handle customer support and data storage facilities required in these activities.

Third key role TSM can take on is to manage applications/service platforms such as setting standards for eligible applications, activation of payment applications as well as securing personal data in case of software threats and device loss (deactivation).

Typical activities of TSM may include but not limited to the list below. These tasks are related to MNO, Service Provider, Over the Air (OTA) Provisioning and Handset and Application Management:

- TSM should get into contractual relationship with all the available mobile operators (Du, Etisalat and service providers) in order to reach out to broadest target population. Hence, a service provider (e.g. public transport tickets) that wants to reach out to the majority of the citizens should be able to do so regardless of which mobile subscription citizens may have.
- Administrative functions such as billing, reporting and reconciliation for the services provided to the mobile network operators should also be carried out by TSM.
- Customer relations with regards to TSM activities should be handled by TSM as well.
- Contractual relationships should also be set and maintained with the service providers. Service Provider profiles may vary from government entities to banks, shopping centres to transport authorities.
- Administrative functions to the Service Providers should be similar to the ones to MNOs.
- TSM should maintain data staging for all types of applications.

- TSM must ensure network connection security through authentication management without causing any drawback on business rules for customer conformity.
- Service provider application lifecycle management is also a responsibility of TSM. Therefore, activation, registration and cancellation should all be handled by the TSM itself.
- Application security keys should be managed by the TSM for specific secure element configurations.
- TSM should ensure all the security standards used in the systems conform to the security standards imposed by the regulatory body.
- TSM should provide a platform that enables integration with different stakeholders and allow interoperability among them.

#### Current Situation: Trusted Service Manager (TSM)

There are on-going negotiations with TSM companies and a main consortium involving MNOs (Etisalat and du), Ministry of Finance and Central Bank, EIDA, and National Electronic Security Authority (NESA) will be managed by TRA. The workflow will also necessarily include other financial institutions, retailers and merchants as well as payment gateways. The intention is to have a central and national TSM provisioning mobile payments and mobile identification as an independent institution. MNOs may have their own TSM agreements with other companies in loyalty to the national TSM. Stakeholders are willing for a centralised solution in order to reduce duplicate efforts and save costs. Centralised TSM is expected to solve integration issues as well. A legal base is to be developed based on required laws and policies.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

**Key Tasks:**

**KT 5.3.1. Identify objectives and key stakeholders; define an initial business plan:**

The environment that TSM will be operating in is a very complex one and the most crucial task is to position the TSM centrally among all the stakeholders as an independent provisioning body that keeps each and every stakeholder's interest beyond any conflict.

- Work on a roundtable (a consortium is formed already) of the main key players that will be involved in the business case namely: MNOs (Etisalat, Du), EIDA and NESAF, Financial Institutions (Banks including Central Bank), Ministry of Finance. Identify clear objectives on a timeframe.
- Benchmark with other TSM models being implemented in similar environments. Identify key differences and special requirements in the UAE mobile commerce eco-system.
- Study what sort of collaboration between these key players will be necessary in the mobile sector. Define a generic workflow and improve that. Keep in mind that TSM will be the core of the relationship and communication between these institutions as well as the warrantor of each party's interests.
- Report on the current financial background in the UAE and potential influence of mobile commerce to the key sectors.
- Analyse what existing systems, technologies and partnerships can be a base for setting up a TSM such as the National ID, on-going security systems the banks may have, SIM Card capacities of different MNOs.

- Identify an initial business model and determine what other players will need to be involved for a properly working model.

- Setup contractual agreements among different stakeholders involved in the National TSM.

**KT 5.3.2. Identify secure services that need to be part of the TSM solution:**

The TSM model will be set to follow the scope of the planned secure services. Available infrastructure, demand for services, requirements of the market as well as the innovative initiatives will define the secure services needed in the UAE.

- Determine the scope of the TSM regarding the services that it will be handling as well as the position it will be taking among the other stakeholders.
- Determine which secure services will initially be taking place under the provision of the TSM.
- Identify what outsourcing arrangements are required for technology, service management, software development and seek for potential partnership where relevant.
- Analyse the technology infrastructure for the planned secure services and set a timeframe for implementation of these services.

**KT 5.3.3. Assess and Evaluate TSM Solution and Services Providers:**

Determining tasks and assigning roles and liabilities will provide a feasible working model.

- Examine how the precise relation between TSM and the EIDA will be set. Assign clear roles and tasks to TSM with regards to national identity

policies.

- Assess the possible role for a central private TSM company and how it would fit in the unique UAE environment.
- Define the relationship between the central TSM and the private TSMs working within the eco-system. Determine the scope of the liabilities and authorities in the complex environment. Provide clear guidelines on the communication between different TSMs and workflow.

**KT 5.3.4. Proceed with Legal Framework Adjustments:**

Due to the changing roles and new tasks emerging, legal base should be supported with relevant legislations towards the TSM model. Complex legal issues will arise regarding the sensitive data protection and privacy as well as accountability issues related to potential flaws and misuse of the system. As discussed in Section 3.5, legislative work should include adjustments as new legal questions emerge for the TSM.

- Make sure the legal framework includes issues that will define the responsibilities and liabilities of the TSM and the other stakeholders. Also present those to the legislative bodies to finalise the required laws.
- Determine the actions of the TSMs operating in the UAE and include them in the regulatory framework.

**KT 5.3.5. Pilot and Implement the TSM Solution**

Initial pilot programs would prove useful to see what peculiar cases arise within the given context of the UAE. Pilot programs should be monitored and

analysed by all the key stakeholders. Improvement decisions should be constantly considered and implemented. It is, however, important to consider that the nationwide TSM solution will raise different issues to deal with than the pilot program. Therefore, stakeholders should bear in mind of the possible different case scenarios that may arise during the nationwide implementation of TSM. What is most important is that piloting of such complex and large project may take some time. Therefore, it is crucially important to make choices, especially about the technology, that will not be obsolete within a short time. The same applies to partnerships resting on sustainable models of cooperation's and win-win cases.

**KT 5.3.6. Develop policies and procedures around the tasks of TSM:**

As TSM will be in the core of a complex mobile sector environment, the tasks and functions of the TSM should be clearly defined and relationships and accountability issues between TSM and other stakeholders should be determined and documented. Various types of functions and relationships of TSM will require peculiar set of arrangements as, for instance, contractual relations with MNOs will differ from those with financial institutions.

- Define accountabilities and tasks regarding the contractual relations with mobile network operators (Du, Etisalat). Set interoperability standards and security standards that will be in place. Determine a convenient user registration procedure for citizens subscribed with either of the MNOs.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

- When certain mobile devices or applications are used for services, defining standards, equipment and applications in order to ensure security and operability within the TSM environment. Implement procedures for testing devices and applications and provide consultancy and support to technology providers.
- Define the nature of the relationships with different types of service providers. Define accountabilities and tasks with the contracts and identify entire set of tasks of TSM regarding the service providers. Ensure secure integration of service providers to the TSM ecosystem without interfering with the business plans of the service providers.
- Ensure secure storage and transmission of sensitive data in all transactions taking place and for all the parties involved. Document necessary preventive mechanisms against fraud and ensure high levels of security and privacy to users.
- Define the role of TSM regarding end-customer life cycle management as well as service provider application management. Identify and manage all the procedures of interactions with the end-user from beginning to end of processes including user registration, account activation and deactivation, opting in/out of services, logging in the application etc.
- Set up a call-centre with several departments of customer support related to all the services provided. Define what types of customer support roles the TSM will undertake and identify tasks regarding customer care – from users to service providers as well as MNOs and technology providers.

**Outcome:**

Security, authentication and privacy of the transactions of citizens will be provisioned by the independent body TSM that will mediate the operations among the service providers, MNOs and financial institutions on the background without getting involved in the business processes.

**Deliverable(s):**

- Design and implement the TSM
- Formally involve the relevant key stakeholders with clear identification of the roles and responsibilities
- Make sure that appropriate legislations are in place
- Design and put in practice policies/directives for the implementation and the use of the TSM and its services
- Determine and put in practice approaches to ensure the expected performance from TSM will be realised.

**5.3. Trusted Service Manager**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
5.3.1	Identify objectives and key stakeholders; define an initial business plan:	Program Management Office	●			
5.3.2	Identify secure services that need to be part of the TSM solution:	Program Management Office and Relevant Stakeholders		●		
5.3.3	Assess and Evaluate TSM Solution and Services Providers:	Program Management Office		●		
5.3.4	Proceed with Legal Framework Adjustments:	Program Management Office,	●			
5.3.5	Pilot and Implement the TSM Solution	Program Management Office and Relevant Stakeholders		●		
5.3.6	Develop policies and procedures around the tasks of TSM:	Program Management Office and Relevant Stakeholders			●	

**Outcome:** Security, authentication and privacy of the transactions of citizens will be provisioned by the independent body TSM that will mediate the operations among the service providers, MNOs and financial institutions on the background without getting involved in the business processes.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

**5.4 Mobile Innovation Center**

Mobile Innovation Center (MIC) plays a vital role towards achieving mGovernment targets as well as maintaining high quality standards of mobile services through planning, innovation, training and knowledge dissemination, consultancy, testing, and Research and Development (R&D).

**Key Stakeholders:** Universities, MNOs (du and Etisalat), Supporting partners (Google, Apple, Nokia, Microsoft, Emirates Group) and government entities.

**Mission of MIC:** The main role of Mobile Innovation Center is to keep mGovernment transformation smooth and innovative at each stage of maturity. MIC should keep track of the latest developments in mobile technology, evaluate feasible directions in mGovernment for the short and long term within local context, constantly analyse usage and adoption behaviour and assist all the entities with providing guidelines and best practices. Some of the activities of MIC may be listed as follows:

- Conduct R&D to foster innovation in mobile service implementation
- Usability and security testing for mobile applications and devices
- Enhancing the quality of existing applications
- Provide learning facilities for government entities, schools and universities (training, seminars, conferences, etc.)
- Keep track of latest developments and trends in mobile governance and mobile technologies as well as new security issues and use cases

- Enhance collaboration between entities, service providers, citizens and other stakeholders
- Define service and security standards and guidelines for mobile applications
- Provide consultancy to government entities

**Current Situation:  
Mobile Innovation Center**

Several meetings will take place with potential partners for building Mobile Innovation Center including: Google, Microsoft, Appcelerator, Khalifa University, Zayed University and Emirates Group. MIC is planned to function as an institution that constantly pushes for improvements and innovation in mGovernment. It is planned to increase know-how and collaboration within the government entities as well as the other key players around mGovernment by R&D, consultancy, training and testing. Key partnerships are being sought at the moment to serve to the best of its abilities towards these goals.

**Key Tasks:**

**KT 5.4.1. Identify Partnerships and Suitable Revenue Models:**

Identify which actors may play important role in keeping the mGovernment transformation innovative and robust. Engage private sector in various projects and encourage government entities to take active roles.

- Define the scope of the mutual relationship between MIC and the government entities. Establish communication channels with entities' project managers, application developers and IT departments.

- Establish strong connections with national mobile sector's key players: mobile application developers, service providers, device manufacturers, software engineers as well as mobile network operators.
- Involve relevant university departments in research projects, develop initiatives among academic personnel and students to contribute to mobile service innovation.
- Keep close contact with key global actors such as Google, Apple, and Blackberry. Seek possible partnerships for the general management of the MIC as well as for different projects carried out within MIC. Keep global players informed of MIC's activities and encourage proposals for new projects.
- Set a revenue model that may include partnerships, public/private sponsorships, service charges and membership fees.

**KT 5.4.2. Define Service Strategy and Technical Requirements:**

Analyse what tasks are awaiting MIC and what the requirements are.

- Identify the scope of MIC and offered services. Analyse the technology infrastructure required for the operations.
- Provide potential partners with parallel directions regarding the form of relationship they will set with MIC.
- Define technical standards and policies for operational and innovation framework, security, testing and evaluation framework.

**KT 5.4.3. Reap the Benefits of Collaboration and Partnerships:**

Make the most out of the key strategic partnerships and collaboration. Keep communication between the stakeholders alive at all times and create an inclusive environment where each stakeholder can contribute more and benefit more.

- Organise periodic meetings and seminars with government entities and other stakeholders. Present them MIC's recent findings on mGovernment implementations; discuss best practices and challenges of the previous period in terms of mobile development and implementation.
- Encourage certain service providers to join efforts under the provision of MIC in order to achieve innovative solutions for integrating services and take part in building goal-oriented partnerships among different government entities.
- Communicate local and federal challenges and achievements to relevant partners and stakeholders in order to acquire potential improvements in mobile services and bring in new ideas.
- Provide consultancy and recommendations to entities seeking solutions and involve them in partnerships that MIC established.
- Engage citizens in testing and using government mobile services and include them in innovation process.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

**Outcome:**

The centre will function to constantly improve mGovernment services by conducting researches, promoting good practices among the entities, testing new applications, providing consultancy to demanding government entities, and managing an innovative environment around mGovernment.

**Deliverable(s):**

- Set up the MIC with desired functionalities
- Formally involve the relevant key stakeholders with clear identification of the roles and responsibilities
- Design and put in practice policies/directives for the implementation and the operations of the MIC

**5.4. Mobile Innovation Center**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
5.4.1	Identify Partnerships and Suitable Revenue Models	Program Management Office			●	
5.4.2	Define Service Strategy and Technical Requirements	Program Management Office			●	
5.4.3	Reap the Benefits of Collaboration and Partnerships	Program Management Office and Relevant Partners				●

**Outcome:** The centre will function to constantly improve mGovernment services by conducting researches, promoting good practices among the entities, testing new applications, providing consultancy to demanding government entities, and managing an innovative environment around mGovernment.

**5.5 Nationwide Government Data Integration**

This milestone is perhaps one of the most influential ones on achieving a properly functioning mGovernment program in the country where all government entities work together, especially for offering integrated services. Ideally this could have been based on a one nationwide government data centre - whether private (solely owned and managed by the government) or hybrid with some of data handled by known third party offerings. The complexity and scale of the tasks involved in this milestone seems to lead to more practical approaches where all the data may be connected via secure network among government entities called FedNet. FedNet seems to be one of the core activities already initiated by the TRA having mGovernment needs in mind. FedNet is also aiming to improve communications and collaborations among all government units. This may also be extended supporting digital communications with the citizens with the help of authentication systems such as mobile signature.

Resolving data connectivity is only one of the major parts of the requirements for data integration among all government entities. Other key activities, as referred in Section 4.2, include conducting data harmonisation, facilitating interoperability, and integration of services and exchange of data / information.

While this milestone is crucial and has a significant impact on the success and advancement of the mGovernment transformation, it requires huge amount of efforts and dedication on the side of The Program Management Office and all government entities.

Each government entity handles several types of information related to citizens, finances, employees, historical statistics as well as information about the entity itself. The information is stored and used for certain services for one entity. However, this institutional information may also be required in other use cases, for example, by other departments of the same entity, by other entities or even by citizens. Hence, there is an increasing need to treat every piece of data handled by government entities as categorical and systematic information that may be used and re-used by other parties. Data integration among all government entities in the UAE aims to make information accessible, interoperable and meaningful for any party that uses it. In this manner, integration can be viewed as the capability to make information re-usable by other parties and leverage this information for various other entities' procedural or operational purposes. Data integration is a key enabler for national and local governments in many aspects of their service delivery including but not limited to:

- Enable integrated services delivery to citizens by allowing data to flow seamlessly across entities and making collaboration between entities convenient
- Transform the various types of strategic data in each entity into organised, searchable and meaningful information for various use cases
- Improve operational efficiency by eliminating duplications and manual data processing
- Enhance government responsiveness to new service design with new conditions by enhancing monitoring and execution capabilities

- Provide institutional transparency by making certain data available to public upon request

The UAE's mGovernment transformation is a nationwide program, however, data integration at that scale is not an easy task due to a number of technical, cultural and operational barriers. This milestone will be achieved for the desired outcome if several key success factors are taken into considerations:

- **Strong Leadership:** A strong top-down political will and support is a key ingredient to foster a collaborative approach within and across government entities. This will ensure each government entity shares and commits to the fact that mGovernment transformation is a nationwide program.
- **Demonstration of Institutional Benefits:** Potential gains, benefits and efficiency improvements should be made clear to all government entities in order to gain support and enable a collaborative environment among the entities.
- **Information Governance:** The Program Management Office needs to clearly organise the shared information, access rules to information, conditions of use, accountability and ownership arrangements, setting standards and processes, privacy issues and legislative alignment. The coordinating and monitoring information and data sharing require clear governance of the procedures and architectures entirely.
- **Information Standards and Interoperability:** Relevant standards should be developed and

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

applied to creation, storage and transmission of data in order to enable intra-entity sharing and re-using data.

- **Ensuring Data Quality:** Data quality, security and re-usability need to be ensured.
- **Security and Privacy:** The Management of the transformation program needs to assure that appropriate security and privacy conditions are met during information sharing and this should be applied to all the sensitive data owned by the entities.

**Current Situation:  
Mobile Innovation Center**

Apart from the existing individual data centres of different government entities, FedNet is on the planning stage, which, as one of its functions, will provide Federal Government Entities hosting for the servers/systems and efficient communication channels.

One to one data integrations exist between some entities (e.g. Banks with Central Bank; Ministry of Finance with other ministries; Ministry of Interior with Ministry of Labor). Otherwise, various parts of data required for one transaction resides in different locations in general. Data integrity implementation plans are underway starting with FedNet project that will provide connectivity between all government entities. Intention for building a data warehouse exists.

**Key Tasks:**

**KT 5.5.1 Plan and Organise for best utilisation of data resources for mGovernment:**

One of the key activities of this milestone is related to the preparation of the data given various established data centres and databases that already exist. This is a challenging task when it comes to, for example, harmonisation and standardisation across the government entities. Perhaps, this could be done within the framework of FedNet, supporting already existing plans and executions.

**KT 5.5.2. National Data Governance:**

Nationwide data integration is a complex task with several different layers. A top down authority to coordinate government entities on the path to data sharing and service integration will be necessary. Initial tasks of National Data Governance Body will be to:

- Analyse the current data architecture and structure
- Identify the degree of data readiness for interoperable data sharing and processing
- Investigate potential interoperability opportunities within the existing data handling systems
- Define a strategy for national data integration
- Define the business value of costs and benefits of data integration
- Initiate a platform to discuss what data can be shared and how it can be shared among the government entities (e.g. wiki, forum and seminars).

- Define the technology infrastructure required for data integration. Initially a cutting-edge data warehouse needs to be set up as well as a common transaction language should be implemented via Web APIs.

**KT 5.5.3. Create Nationwide Data Policy covering key components of data integration:**

Standardising the information management process will enhance collaboration between entities and bring efficiency in sharing strategic data and integrated service delivery. Clear data policy papers, directives and standards should be delivered for entities in order to be engaged in nationwide data integration.

- Provide entities policies for entity-wide data management and ensure their current data management practices are reviewed and adapted to new policies within a certain timeframe.
- Provide policies for access to data and sharing data including security and privacy issues as well as property rights and licences for the use of data.
- Provide policies on data archiving, and provisions for re-usable data design for entities.
- Deliver a RoadMap for entities towards data integration. Clearly describe priority tasks regarding reengineering data management procedures, change management issues as well as restructuring the current key data sets in hand.

**KT 5.5.4. Assist Entities towards Data Integration:**

In order to attain standards in data handling, storing and sharing, all the government entities will require

assistance in business process re-engineering, implementing standards and securely sharing information within and across entities.

- Endorse entities to publish their own key information catalogues that will be maintained by them and be re-usable by other entities. By aggregating all the data inventories of each entity, document an index of all available data sets that are available for sharing with other entities.
- All government entities should be provided with detailed implementation guidelines including standards for data, metadata and technology being used.
- Encourage setting up departments to handle entity-wide information management that will ensure all new key data to be sharable with other parties and convert existing key data sets to standard forms in order to make them available for re-use.
- Enforce institutional restructuring to share tasks related to data creation, processing, storing and sharing. Ensure there will be accountability within entities on crucial issues like data quality, accuracy, interoperability and security.
- Set directives for data categorization for each piece of data in order to enable searchable information for other parties' re-use of data.

**KT 5.5.5. Move onto Open Data Policy for Transparent Government:**

Making government data publicly available is a big step forward towards government transparency, gaining public trust and citizens engagement. The

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

case for data integration is never accomplished unless citizen's integration is also provided. Government entities cannot shift all their data to be publicly available in a short time, however, it should be provided that the new data complies with open data policies and the existing data sets should gradually be converted for public use given the priority to the most relevant ones first.

- Encourage government entities to cooperate with citizens and businesses in order to identify what government data should be made public and which ones to prioritise.
- Enforce entities to release certain types of information within limited timeframe.
- Enable central display of the available public data on government web portals or specially designed listings.
- Aim for non-discriminatory, accessible and free public data and remove all types of restrictions for the use and re-use of the publicly available data.
- Enforce gradual distribution of the entities' archived information regardless whether it is digital or on paper.
- Ensure data quality by setting standards in open public data and implementing a monitoring mechanism.
- Restrict distribution of sensitive and private data that are included in the publicly available information.

**KT 5.5.6 Align FedNet with the requirements of**

**mGovernment Transformation:**

As it is planned, FedNet aims to create a network among the government entities providing high capacity and high-speed connectivity and various services over this connectivity such as IP telephony, email exchange. mGovernment transformation could benefit from this connectivity if FedNet is aligned with data, and perhaps, service-sharing requirements among government entities. A network across the UAE by means of cloud technology could connect all government entities creating an invaluable infrastructure for sharing services. This, of course, should be accompanied by well-designed governance policy and standardisation as well as security monitoring.

**Outcome:**

An integrated and connected government entities via a network allowing secure sharing facilities as well as efficient communication and decision making processes that reduce costs, increase security of data, enhance service delivery and improve business processes to allow new integrated service opportunities.

**Deliverable(s):**

- Design a nationwide government data integration plan
- Set up a management unit for the government data integration
- Formally involve the relevant key stakeholders with clear identification of the roles and responsibilities
- Design and put in practice policies/directives for the implementation of government data integration

**5.5. Nationwide Government Data Integration**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
5.5.1	Plan and Organise for best utilisation of data resources for mGovernment:	Program Management Office, all government entities	●			
5.5.2	Set up a National Data Governance Body	Program Management Office, all government entities		●		
5.5.3	Create Nationwide Data Policy covering key components of data integration	Program Management Office, all government entities		●		
5.5.4	Assist Entities towards Data Integration	Program Management Office, all government entities	●			
5.5.5	Move onto Open Data Policy for Transparent Government:	Program Management Office, all government entities		●		
5.5.6	Align FedNet with the requirements of mGovernment Transformation:	Program Management Office, all government entities			●	

**Outcome:** An integrated and connected government entities via a network allowing secure sharing facilities as well as efficient communication and decision making processes that reduce costs, increase security of data, enhance service delivery and improve business processes to allow new integrated service opportunities.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

**5.6 Government Application Store**

Making public services applications available in popular platform stores (e.g. Apple Store, Android Market and Blackberry) and having a government portal that displays all the approved government applications provides significant convenience for users to find applications they need, give feedback or make suggestions. In this way, they will also know what are the authorised mobile applications for certain services and be able to install them to their mobile devices.

**Key Stakeholders:** Government entities, Service Providers, Application Developers.

**Current Situation:  
Government Application Store**

Currently no such portal exists, however, a decision is made to have a Government App Store that will host applications and assess eligibility of the applications to the extent that they meet store standards. Eligible applications will only be those that pass the required tests regarding usability, security and other standards that are previously set. Hence, the government application store will function not only as a displaying unit for the applications but also as a promoter and evaluator of certain quality standards that need to be met by the mobile service designers.

**Key Tasks:**

**KT 5.6.1. Define Standards for mGovernment Services, Establish Services Portal and Evaluate Entities:** Define requirements for eligible mGovernment services and enforce standards of mobile services to the Federal Government Entities.

- Engage government entities to promote their applications via the portal.

- Define standards for applications that are eligible for publishing on government portal with regards to relevancy, security, integration and ease of use. Ensure users are acknowledged of the security of applications on the portal.
- Evaluate entities in accordance with the quality and quantity of the applications they present in the government application store.
- Provide regular statistical feedback to entities on what they achieved so far in terms of their presence in government application store as well as tips for improvement.

**KT 5.6.2. Enable Users to access the Services**

**Categorically:** Ensure that mobile services are categorised so that they can be easily located and searched for on the portal by citizens

- Display users categorised applications of mobile public services: classifications could be according to operating system (e.g. iOS, Android), channels of communication (e.g. SMS, Voice, NFC), area of service (e.g. tourism, health, education, transport), locality (e.g. Dubai, Abu Dhabi).
- Ensure presence of government application store in social media for gaining adoption.
- Work closely with Mobile Innovation Center for application evaluations, testing for quality and enhancements.

**Outcome:**

Having a government application store that is hosting applications and mobile services will provide citizens easy access to authorised applications. The

portal will showcase categorical government services as well as information on standards and guidelines for application and service development.

**Deliverable(s):**

- Design and implement services enabling hosting and sharing of mGovernment applications and services
- Design and put in practice policies/directives for the implementation and the use of hosting and sharing applications and services among government entities
- Design and put in practice policies/directives to promote user access and adoption of hosted and shared applications and services

**5.6. Hosting and Sharing Government Apps and Services**

#	Key Tasks	Collaborations	Timeframe (months)
5.6.1	Define Standards for mGovernment Services, Establish Services Portal and Evaluate Entities	Program Management Office, MIC and All Government Entities	6 12 18 24
5.6.2	Enable Users to access the Services Categorically:	Program Management Office and All Government Entities	

**Outcome:** Having a government portal hosting applications and mobile services will provide citizens easy access to authorised applications. The portal will showcase categorical government services as well as information on standards and guidelines for application and service development.

**5.7 Develop Common Security Directives and Practices**

In section 4.3, a milestone and key tasks for assessing the security needs of the government entities were presented. In this section, primarily based on that assessment, a number of key tasks will be presented and, as a result The Program Management Office needs to come up with a set of security directives and facilitation plans for sharing experiences to deal with security risks. Mobile services bring new challenges with regards to security and necessitate new risk mitigation measures to be taken for the security of government data regardless of where it is stored, how it is transmitted and which devices are used. Moreover, citizens' private information must be secured in each of the interaction via mobile services. The security requirements evolve together with the mobile technologies and government entities should adapt to new threats and take up-to-date precautions proactively.

**Key Stakeholders:** Software Developers, Application, Developers, Government entities.

**Current Situation:  
Develop Common Security Directives and Practices**

Currently, there is a certain need for adapting digital security policies to include new threats and risks introduced as a result of the mGovernment transformation. TRA has established a Computer Emergency Response Team to deal with the problems around digital security including perspectives for legislation, raising awareness, national expertise building and to establish a centre to gather and disseminate information about potential threats, observed vulnerabilities and cyber security incidents, etc. There are challenges ahead regarding implementation of security standards across all entities as well as monitoring it.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

**Key Tasks:**

**KT 5.7.1. Prepare detailed policies on federal, local and entity-wide mobile security:**

Ensure Federal Government Entities are informed of the security threats and delivered common guidelines for security instructions for risk mitigation.

- Identify potential risks for entities and users.
- Receive reports from entities on the experienced security issues, analyse and share them with other entities for reference and precaution.
- Ensure citizen privacy and data security is the focus of the security policies.

**KT 5.7.2. Ensure All Government Entities Follow Standard Security Guidelines and Directives:**

Guide entities on how to implement security measures and enforce the government wide security standards to be implemented.

- Keep entities aware of the potential risks in new technology.
- Provide training and guidelines to entities about security regarding device management, application management, network security and data security.
- Do not let the security policies and guidelines cause performance and efficiency drawbacks on the workflow of the government entities. Consider the working environment and usage patterns in designing the directives.
- Ensure safe adoption of new technologies each time a change occurs. Guide the entities on any improvements on the network structure,

application upgrade or device configuration. This may need to be accompanied by necessary security checks, and if required, new security measures will need to be introduced.

**Outcome:**

New threats introduced by mGovernment adoption will be mitigated by standard security procedures and constant monitoring of the potential threats appearing with the evolving technology.

**Deliverable(s):**

Design and put in practice policies/directives for the implementation and the compliance to mobile security among government entities

**5.7. Develop Common Security Directives and Practices**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
5.7.1	Prepare detailed policies on federal, local and entity-wide mobile security	Program Management Office and TRA		●		
5.7.2	Ensure All Government Entities Follow Standard Security Guidelines and Directives	Program Management Office, TRA and All Government Entities			●	

**Outcome:** New threats introduced by mGovernment adoption will be mitigated by standard security procedures and constant monitoring of the potential threats appearing with the evolving technology.

**5.8 Set up Federal Government Network (FedNet)**

Establishing a federal network is a fundamental milestone in order to integrate institutional operations and government data. Interconnected government institutions is a prerequisite to efficient data handling, integrated public services, and interoperable systems for information sharing and efficient decision making processes.

**Current Situation:  
Set up Federal Government Network (FedNet)**

Currently, federal government entities are not connected together and they have independencies in performing ICT related tasks. The plan for FedNet, which aims to create a robust network connection among the government entities, has been around sometime and now is expected to be put in practice soon. In this way, FedNet is a significant component of this RoadMap and the mGovernment transformation in the UAE. According to the existing plan, existing integrations between entities are either bilateral or involving more than two parties (i.e. Ministry of Finance with other Ministries, Banks with Central Bank, Ministry of Interior with Ministry of Labor etc.). Data sharing culture between institutions seems to be a crucial factor to improve, in order to flourish FedNet. Some of challenges are around building a collaborative approach for a data sharing culture.

**KT 5.8.1. Identify the Goals, Available Resources, Business Case and System Requirements:**

Government entities should work together to define the purpose of interconnection via the federal network; analyze the data structure to be shared and what is the most cost effective and efficient

way of realizing the project. Resource distribution among different Federal Government entities should be analyzed in order to close the gaps. As some of the minimum setup requirement for connectivity to FedNet may be missing within some entities.

- Define the goal of FedNet and identify key milestones for Government Entities to follow.
- Determine the scope of the services that will be provided under FedNet. Include the details to what extent the planned Data, Voice, Video and Internet services will be provided by FedNet, what investments are required and feasible.
- Identify the level of interconnection that will be setup between Federal Government entities. Explore how institutions will integrate their data into FedNet and what standards and procedures will be in use. (i.e. whether a certification or accreditation method will be put in place to test the data quality, usability and security )
- Examine whether Federal Government Entities' existing infrastructure is sufficient for planned interconnection. Determine additional requirements taking varying levels of progress among different entities into account.
- Identify hardware and software requirements for the system that will be used for interconnectivity. Determine what products will best serve the purpose and consider the security implications of each possible soft/hardware solutions.
- Agree on the business case of the FedNet project. Examine how FedNet will support the workflow of each government entity, how privacy issues will be resolved and what formats of data sharing will be in place.

5. TRACK 3: ESTABLISH SHARED RESOURCES ACROSS GOVERNMENT ENTITIES AT THE NATIONAL LEVEL

**KT 5.8.2 Analyze the Data to be Shared as well as Access & Security Issues:**

Analyzing the nature of the data used/stored by all government entities will set the procedures of interconnection and data sharing. Sensitivity of the data to be shared as well as the authorization to access the data should carefully be studied and best practices should be documented for the use of all federal government entities.

- Determine the format of data sharing and storage and familiarize government entities to gradually processing and keeping data in reusable format.
- Define specific security requirements that the overall interconnectivity between institutions will cause. Identify mitigation measures to be taken for potential threats and misuse of the system.
- Identify the data sensitivity that will be shared and stored within FedNet system. Hierarchically classify the data with regards to the sensitivity levels and determine the security measures to be implemented for varying levels of sensitivity. Determine which data will be accessible without any restriction.
- Define the user profiles that will be authorized to access, exchange and backup data.
- Determine what information services will be provided over the FedNet by each Federal Government Entity and identify what security measures need to be taken for unique cases of usages so as to protect the integrity and confidentiality of the overall system.

**KT 5.8.3. Set up or Select from existing Data Centre:**

Data centre is an important component of the Federal Network infrastructure. Data centre will be

the main platform where the inter-agency network will be served and the hardware and applications will be hosted. Physical equipment required includes computing equipment, servers, disk storage and backup storage systems and power conditioners to keep the data centre running at all times. Decisions on what hardware and software products to use, where to set the data centre, what existing technologies can be used as the building blocks are to be cooperatively taken by the agreement of the project management and all government entities.

**KT 5.8.4. Put FedNet in Practice Involving All Government Entities:**

Once the infrastructure and institutions are ready FedNet project should be tested with initial pilot and a launch plan should be put in action. Management and ownership of the data should be set to certain directives, and services within FedNet should clearly be defined. Task division should be handled by the FedNet management, and all Federal Government entities should comply with the standards and rules set by the FedNet management.

- Identify the procedures and key milestones in implementation of FedNet and what procedures to follow.
- Identify tasks and responsibilities for Federal Government Entities and enforce assigning of personnel that will maintain interconnection in each entity.
- Enforce security rules and guidelines to prevent any damage to integrity and confidentiality of data.
- Test procedures and workflow to ensure that interconnection gives desired results.
- Organize training sessions, forums and seminars for government employees in order to build capacity

and ensure best practices nationwide.

- Determine data backup policy (i.e. which data to backup, whether the data in transmission is to be stored, access to backups etc.)
- Document a service catalogue that FedNet offers and make it publicly available.
- Monitor how the change management in business operations due to data integration affects the data handling and processing procedures. Discuss with entity representatives to achieve best practices.
- Involve all Federal Government Entities to develop a Service Level Agreement to document interconnection arrangements.

**Outcome:**

FedNet will provide a solution to efficient and cost effective information sharing, data storing and processing across all Federal Government Entities. It will also provide services such as Voice, Data, Video and Internet services between various locations in the UAE. Another key outcome is the enabling feature of FedNet for new integrated public services that will bring together efforts from different government entities in its own platform.

**Deliverable(s):**

- Report on the scope, mission and responsibilities of FedNet.
- Establish the Federal Network and onboard government entities.
- Document available resources and required infrastructure for setting up FedNet
- Design a catalogue of services that will be provided by FedNet.
- Report on what institutional data will be shared

between Federal Entities and what format will be used.

- Report on potential security threats against FedNet system, and mitigation measures.
- Train government employees and deliver guidelines to government entities on best practices.

**5.8. Set up Federal Government Network (FedNet)**

#	Key Tasks	Collaborations	Timeframe (months)
			6 12 18 24
5.1.1	Identify the Goals, Available Resources, Business Case and System Requirements	Program Management Office, TRA and All Federal Government Entities	●
5.1.2	Analyze the Data to be Shared as well as Access & Security Issues:	Program Management Office, TRA and All Federal Government Entities	●
5.1.3	Set up or Select from existing Data Centre:	Program Management Office, TRA and All Federal Government Entities	●
5.1.4	Put FedNet in Practice Involving All Government Entities:	Program Management Office, TRA and All Federal Government Entities	●

**Outcome:** Implementing a nationwide Mobile ID will be a baseline for the integration of various federal and local level mobile services. Citizen privacy and security will be provided on each and every service use. Payment and other transactional services will be authenticated with Mobile ID providing secure services. One time login for all government services will be possible for user convenience. Personalization of public mobile services will be possible by using contexts derived from mobile ID.

## 6. TRACK 4: ACHIEVE CITIZEN HAPPINESS

### 6.1 Mobile Accessibility and Usability

Technology is at the core of mGovernment transformation, however, it is not sufficient to ensure widespread adoption in the country. Technologically, the most advanced mobile services may be offered but this is not useful at all if citizens do not adopt it. Therefore, provisions for accessibility and usability of mGovernment services are essential.

Clear policies regarding the convenience of access and usability of the services by citizens should be delivered to each party involved in mobile service offerings. Service design process should always take into account who will actually be using the service. This should include necessary functionalities to attract each and every targeted user to easily take up the service regardless of their location, device or platform.

**Mobile accessibility:** This generally refers to making mobile services widely available, free or at a low cost, and convenient to those that the services are intended. In Section 3.4, a milestone on creating affordable access to mServices was discussed. In this section, accessibility is viewed from a wider and user's perspective where the cost is only part of the factors for accessibility. Another accessibility factor is the availability of services anywhere any time and to all of the citizens.

When designing a mobile service, it is important to think that the citizens may differ in terms of their demographics, income, location and even some may have certain disabilities. Thus, in order to reach out to almost all citizens, special accessibility conditions, design features (e.g. text to voice capability), affordable pricing and wide coverage of the network services may need to be taken into consideration.

Accessibility may require partnerships among several organisations in order to eliminate any possible but unintended discrimination in providing public services.

#### Current Situation: Mobile Accessibility and Usability

mGovernment Education and Training Project will be targeting to raise awareness and improve technical ability of all the stakeholders in mGovernment transformation. Training and education programs as well as initiating a new service culture and better citizen interactions are all the key tasks of these projects. Universities will be playing a key role in these programs, which will involve UAE Government officials, Government IT staff, students and the general public.

Mobile network infrastructure is developed to a high degree and all regions of the UAE are covered. There is a project called "Echo of Silence" aiming inclusion of people with hearing and speech disabilities into the society with advanced technological assistance as well as training programs.

#### Key Tasks:

##### KT 6.1.1. Improve general accessibility throughout the country:

Include accessibility issues, as described at the beginning of this section, in telecommunications policies as well as recommend best practices to government entities for accessible services design. Involve mobile operators and service providers to promote special tariffs/packages for citizens, especially for underserved communities, in order to increase their mobile device usage.

##### KT 6.1.2. Focus on special requirements for people with disabilities:

Get feedback on policy improvements and best practices from organisations dealing with disabilities as well as from directly disabled people. Promote availability of assistive technologies that are affordable for the disabled and elderly.

##### KT 6.1.3. Revise accessibility provisions:

Make periodic surveys and analyse the usage behaviours and adoption of mobile technologies among the people with disabilities and keep track of their requirements.

**Usability:** Accessibility alone is not sufficient for wider adoption of mGovernment services. In the UAE, there is a high expectancy for having government services to be convenient and easy to use. Therefore, a special focus on usability issues would attain high level of citizen satisfaction and improvements in the government reputation. As it is the case with accessibility, usability must also be accounted for the citizens regardless of the device they use or the background they have. Policy makers and project managers should provide clear directives and provide best practices to enhance the user experience for those who are involved in mobile services development process. A part of the success in mGovernment services rests with the degree of quality that they bring to users' life. Some of the usability criteria should be set around efficiency, effectiveness and citizen satisfaction.

##### KT 6.1.4. Identify target groups and define usability standards and design guidelines:

Study the target audience thoroughly: what devices are common, what the technical capabilities are, what operating systems are mostly being used,

what functionalities they find more practical. Ensure the entities follow certain rules when developing applications and mobile services regarding ease of use and design issues. Provide clear guidelines on how to and how not to develop mobile services.

##### KT 6.1.5. Create and Promote usability resources and make them available:

Gather already existing documentation for usability. For instance, there are already a number of usability standard questionnaires such as System Usability Scale (SUS), Standard Usability Measurement Inventory (SUMI) in addition to International Standards Organisation (ISO). Make these resources online available by means of an appropriate website as well as best practices, templates, checklists, tips, etc.

#### Outcome:

mGovernment services targeted to every citizen eliminating any discriminations as well as enhancing user experience for all users.

#### Deliverable(s):

- Design and put into practice accessibility and usability plans

6. TRACK 4: ACHIEVE CITIZEN HAPPINESS

6.1. Mobile Accessibility and Usability

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
6.1.1	Improve general accessibility throughout the country	Program Management Office and MNOs	●			
6.1.2	Focus on special requirements for people with disabilities	Program Management Office, MNOs, Civil Society Organisations and NGOs		●		
6.1.3	Revise accessibility provisions	Program Management Office, MNOs, Civil Society Organisations and NGOs		●		
6.1.4	Identify target groups and define usability standards and design guidelines	Program Management Office, MNOs, Civil Society Organisations and NGOs	●			
6.1.5	Create and Promote Usability resources and make them available	Program Management Office, MNOs, Civil Society Organisations and NGOs		●		

**Outcome:** mGovernment services targeted to every citizen eliminating any discriminations as well as enhancing user experience for all users.

6.2 Promoting, Adoption and Advocacy for mGovernment Services

In Section 3.6, a milestone on capacity building was presented, which mostly concentrated on technical capacity building of government entities and citizens as part of creating a favourable environment for the mGovernment transformation. This section, although closely related to the capacity building, focuses on user centric (both citizens and employees of the government entities) issues when it comes to the adoption of mGovernment. In general, promotion of adoption and campaigning for mGovernment services may normally be part of the capacity planning activities. However, due to the extreme significance of adoption as most eGovernment and mGovernment projects fail due to the lack thereof, it deserves a different milestone, which is more directed to non-technological and user centric issues.

The promotion of the mGovernment services is a collective effort where all stakeholders should join to be part of the mGovernment transformation and contribute to adoption. Some of the tasks related to stakeholder involvement presented in Section 3.2 should include support for the promotion and campaigning for the mServices. This milestone primarily focuses on two of the key stakeholders as user: government entities and citizens.

Creating mGovernment services and making them available through mobile access alone are not sufficient for mainstreaming mGovernment in the country and attaining widespread adoption among the citizens. Scrupulous effort is essential to raise awareness, promote services and conduct advocacy campaigns. Governments may implement the most intelligent, informative and practical mobile services. However, without citizens and entities using them,

these efforts may remain to be inefficient use of resources.

Adoption of mGovernment has certain barriers on both the citizens' side and the government entities' side. These barriers vary from cultural structures to technical capacities and from lack of awareness to resistance to change. Thus, planning an efficient campaign to raise awareness and engage users, is as crucial as developing the mobile services. There may be two perspectives on adoption of mGovernment services: entity-wide adoption and citizen adoption.

**Entity-Wide Adoption:** As mGovernment requires a certain level of organisational re-structuring and business process management, the workflow may necessarily be subject to change. This may not always be welcomed or easily accepted by the government employees. It is very common to see resistance to change or reluctance to adopt the new ways of performing tasks. In order to eliminate potential resistance, employees should be given chances to see clear advantages of using mobile technologies.

**Current Situation:  
Promoting Adoption and Advocacy for  
mGovernment Servicesa**

The obvious need for a good campaign and adoption policy is widely recognised by all the stakeholders and awaiting the actual mGovernment transformation to flourish.

**Key Tasks:**

**KT 6.2.1. Introduce change gradually:** Gradual implementation of mobile services generally gives better results in terms of acceptance. Initial implementations can be kept as pilot programmes in order to test the applications and devices and to get employees familiar with the technology. The results of the piloting should be communicated to all employees in order to show the benefits of mGovernment transformation.

**KT 6.2.2. Communicate benefits of mGovernment transformation:**

Training and education of the employees is a very central task. Practical and in-class training is key to improve acceptance of mobile technologies in government organisations. Training programmes should clearly demonstrate productivity benefits and usability features to the employees (see below for citizens). Employees should be given encouragement to suggest improvements on the services and give technical and usability feedback. This will engage them in the service design and improve service quality.

**Citizen Adoption:** Expecting citizens to take any mServices offered quickly and in large numbers is often a very optimistic approach. While some citizens need simply to be notified about the services, the others may need more campaigning and support as they may be on the less privileged side of the digital divide where they may have difficulties in terms of accessibility and usability. Therefore, citizen adoption depends on a number of issues such as awareness, perceived convenience, security and privacy implications, usefulness of the applications and trust. Demonstrating potential benefits to the users and gaining their trust is as important as designing

6. TRACK 4: ACHIEVE CITIZEN HAPPINESS

mobile services. Meeting and exceeding the expectations is the way to achieve citizen satisfaction from the services provided.

**KT 6.2.3. Use various channels and promotional campaigns:** Use mass media (TV, newspapers, magazines) extensively to raise awareness for the provided mobile services. Encourage government authorities to promote their mobile services through these channels. Get important and respected public figures to promote mobile services (sportsmen, singers, influential artists, etc.). Promote mobile services also via the entities' websites and in the offices where citizens visit.

**KT 6.2.4. Create quick wins and popularity:** To generate a culture around mobile service usage, it is best to start with the services that are most frequently used such as transport and education. When mobile services become part of daily life, more citizens will be engaged in using these services. Whenever possible, provide the services via several channels in order to engage every type of users (smart phone users, simple mobile handset users). For instance, SMS version of a notification service may be more useful for some users whilst native applications are more convenient for the others. Let users choose the channels they prefer to receive the services. Ensure the mobile version of the services actually make processes easier for the users. Mobile services should be designed to complete all the processes end to end in one go.

**KT 6.2.5. Involve citizens, build trust and provide secure and personal services:** Involve citizens in the design process of the mobile services. Know their expectations and gather their

suggestions. Users will be more inclined to use the services that they actively participated in the design. Personalise the services. Ensure citizens can login once for all government services and get personalised information and service by using the mobile services. Integrate services with the social media whenever relevant. Build trust among the citizens that their privacy and security is protected.

**Key Stakeholders:** Mass media, MNOs, Government entities (federal and local), Service Providers, Community Organisations.

**Outcome:** Promoting mGovernment adoption will increase user involvement and enhance the reach of government to its citizens. Citizens will be informed of the availability and benefits of the mobile services and encouraged to use them.

**Deliverable(s):**

- Design and put into practice policies/directives for government entities to adopt mGovernment services
- Design and put into practice campaigns for improving user's adoption and the spread of mGovernment in the country

**6.2. Promoting, Adoption and Advocacy for mGovernment Services**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
6.2.1	Introduce change gradually	Program Management Office and All Government Entities	●			
6.2.2	Communicate benefits of mGovernment transformation	Program Management Office and All Government Entities		●		
6.2.3	Use various channels and promotional campaigns	Program Management Office and All Government Entities		●		
6.2.4	Create quick wins and popularity	Program Management Office and All Government Entities	●			
6.2.5	Involve citizens, build trust and provide secure and personal services	Program Management Office, TRA and All Government Entities		●		

**Outcome:** Promoting mGovernment adoption will increase user involvement and enhance the reach of government to its citizens. Citizens will be informed of the availability and benefits of the mobile services and encouraged to use them.

**6.3 Community Building**

Local and federal governments should always be on the lookout for reaching more citizens and bringing quality services to all the segments of the society. Identifying unique needs of each segment and designing services that are tailor-made to their requirements is the key to citizen satisfaction.

It is highly advised that governments should pay special attention to extending mobile services to underserved communities. Definition of 'underserved' varies depending on the context but can be explained as a group who has more disadvantages in receiving certain public services over the other groups. For instance, mobile healthcare force for the elderly is considered as a public service for those who cannot commute to hospital as conveniently as the younger people. Another case could be informative services for tourists or expatriates to overcome their disadvantage of access to local information due to

language barriers. Mobile job notification services for the unemployed may be another example. In some other cases, low-income groups may not have advanced devices or technological infrastructure to be able use the mServices. Therefore, services should be made available on the devices they use and the environment they live.

**Key Stakeholders:** Community Organisations, Unions and Occupational Organisations, MNOs, Government entities, Service Providers and Application Developers.

**Current Situation: Community Building**

There are a few initiatives focusing on elderly people and people with disabilities. The analysis of different communities' requirements and technology use is awaiting more attention.

6. TRACK 4: ACHIEVE CITIZEN HAPPINESS

**Key Tasks:**

**KT 6.3.1. Identify and prioritise crucial segments of the society and those who are underserved:** Analyse different segments of society with regards to occupation, nationality, economical background, physical capability, settlement region and other possible unique characteristics. Identify what mobile services would benefit these communities by working closely with the representatives of these groups. Prioritise bringing service to certain communities that happened to be underserved in comparison.

**KT 6.3.2. Assess service and capacity building needs for different community groups:**

Analyse the readiness of the community for the intended services. Analyse mobile usage behaviour and special requirements of the case; investigate technical requirements and how capacity building among the users as well as infrastructure will take place; communicate with the communities in order to determine the best fit for the needs and discuss feasible options with the service and technology providers.

**KT 6.3.3. Develop and innovate mobile services for various communities:**

Decide for the most urgent services to be implemented. Finalise the decisions as a result of the feedback from the communities and other stakeholders and follow a clear rollout plan that takes into account the adoption of the services. Efforts should be directed to find solutions to multiple communities at once by providing certain level of integration within the service structure.

**Outcome:**

Targeted communities will have mobile services and applications tailor-made for their requirements. Government will have a better reach to communities that are underserved.

**Deliverable(s):**

- Design and implement a plan for inclusive and community oriented mGovernment service provisions.

**6.3. Community Building**

#	Key Tasks	Collaborations	Timeframe (months)			
			6	12	18	24
6.3.1	Identify and prioritise crucial segments of the society and those who are underserved	Program Management Office, Universities, NGOs and Civil Society Organisations		●		
6.3.2	Assess service and capacity building needs for different community groups	Program Management Office, Universities, NGOs and Civil Society Organisations			●	
6.3.3	Develop and innovate mobile services for various communities	Program Management Office, All Government Entities, Universities, NGOs and Civil Society Organisations				●

**Outcome:** Targeted communities will have mobile services and applications tailor-made for their requirements. Government will have a better reach to communities that are underserved.

## 7. IMPLEMENTATION APPROACH

The existing infrastructure and ICT readiness in the UAE, owing to the successful development in eGovernment, is at a level that could support one of the world's most advanced mGovernment implementation. With this ambition in mind, the RoadMap recommends more realistic goals to be achieved from now until May 2015. The essence of the mGovernment program involves utilisation of frontiers of mobile technologies and related know-how to offer services to citizens, where either the government organisations or the users are supported to be reasonably ready to take up these services.

The implementation of the mGovernment requires significant amount of preparations, planning and capacity building even before mGovernment program starts. These should be followed by adaptive monitoring, evaluation and impact measurement while services are gradually wide spreading in the country. It is a countrywide program that requires full attention and creative solutions for success, which may also face a number of potential risks.

There may be two critical and practical understanding, with which it would be easier to lead the implementation of the mGovernment program to a successful one:

- Viewing implementation of mGovernment across the country (a nationwide program) as one of a significant contribution to the over all socio-economical development of the country in gaining customer happiness, and hence there may be a number of partners who may share the same objective and their support must be gained.

- Working with strength and endurance with the recognition that mainstreaming mGovernment in the UAE as a nation wide project will be very challenging in some ways, including existing management structure and different levels of maturity among existing eGovernment implementations, data integration, required capacity building efforts in government and among users.

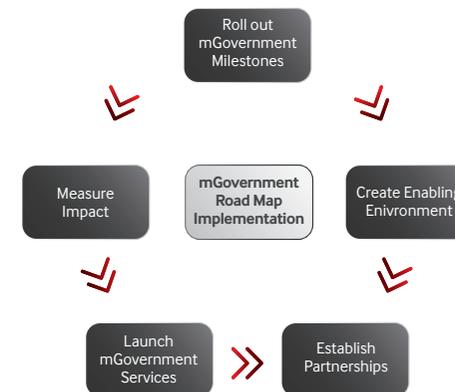
Approaching the implementation of the mGovernment RoadMap with these two pragmatic understandings would better prepare the mGovernment leaders for the tough job ahead. Our suggested implementation plan includes work on four major areas:

1. Management decides actions and preferences on particulars of roll out plan for each of the milestones.
2. Key Success factors are identified and benefited to the most.
3. Management of the mGovernment program in terms of structure and processes are established.
4. Essential risk factors are identified and avoided.

### 7.1 The Roll Out Plan

The RoadMap has four parallel tracks to it and each track contains a number of milestones, under which there are key tasks to be carried out. Each key task has its own responsible entity or statement of any partnerships required as well as the timeline to be completed. The Program Management Office has to decide how to phase out each of the milestone and relevant key tasks in accordance with the introductory discussions on the milestones in Section 1.4 and the guidance on the implementation here.

Figure 4 below shows that each of roll out scheme for the milestones are continuous processes with appropriate preparations and check points for impact and revisions. In the figure the box showing "launching mServices" are only relevant to those milestones where particular milestone contains such services – in some cases it may not be relevant. However, each milestone has its relevant key tasks in terms of building capacity or preparations, checking out and making sure that the context or the environment for the milestone to have appropriate settings for it to be successful are in place, establishing collaboration terms with key partners, launching mServices –if any -, and monitoring and measuring impact. This loop may be applied to all of the milestones in general. However, some of the milestones are actually large scale projects with their extensive resource requirements and complex tasks such establishing the mobile payment, TSM, data integration or mobile ID. There may also be close links and interdependencies among them.



### 7.1.1 Time Plan and Interdependencies of Milestones

This RoadMap is designed having a time span from now until 2015. There are a number of issues to take care about while managing the time and implementation of the RoadMap.

- The RoadMap contains four parallel tracks and they all must start more or less at the same time. However the first two tracks are more like a set of preparation work and there are strong dependencies among milestones of first two tracks and this may be true for other milestones of the other two tracks. The timing for starting and completion should be decided accordingly.
- The time to complete each of the key tasks in the RoadMap is given in each of the table of the milestones. Suggesting exact timings for these key tasks is not easy as there are a number of factors that could affect these timings. Some of these factors include goals and competencies of The Program Management Office, available resources and partnership dynamics and external factors such situations affecting government entities etc. Therefore, one of the core tasks of The Program Management Office is to review and decide best estimates of the times indicated in the tables for each of key tasks and accordingly create visual time plan for the RoadMap. It is very likely that this will not be as precise as it should and will need revisions. It is probably more realistic to have detailed time plans for each of the milestones depending of the scale and complexity of the projects relevant to a milestone. In this way, after knowing the details of the task activities, it may be possible to make a more realistic estimate of how long each milestone would take.

## 7. IMPLEMENTATION APPROACH

- The dependencies among the milestones could also be identified in similar way. Although some of the dependencies are easy to identify (such as the ones in Track 1 and 2 and the rest of the RoadMap), some others need a detailed study as in time plan of the activities.

### 7.1.2 Monitoring, and Measuring the Impact

At the beginning of this section a generic approach to monitoring and impact measurement (see Figure 4 RoadMap Implementation Loop) is presented for each of the milestones. Setting up feedback and revision channels for conducting monitoring and measuring directly influences the structure of the Management of the mGovernment program. It is crucial that such procedures are carried out with competent human resources within the Management. Depending on the scale and the complexity of the milestone, detailed monitoring and impact measurement could be delegated to those who are responsible from specific projects such as setting up a TSM or mobile ID.

### 7.1.3 Before and Beyond 2015

Although the RoadMap is designed until the year 2015, some of the milestones may not be fully completed and some of the milestones that are completed will need to be managed and sustained after the year 2015. One of the key implications for these facts is that The Program Management Office should be set up having a sustainable and long-term future of the mGovernment transformation in the UAE. It cannot simply be a unit set up to manage the transformation until a certain time and for just certain tracks, or milestones. It is a management unit that will remain for the years to come in order to support advances, revisions and all required changes of mGovernment.

It is not very easy to exactly determine what will be accomplished before the year 2015 and what will remain to be worked upon after that. However, it is possible to set out a number of desired level performance goals until year 2015:

- As it is discussed in Section 2.1 it is expected that the RoadMap implementation will have enhancement on eGovernment in terms of moving at least a specific number of existing eServices per government entity to the mobile platform. This may also include a number of new and unique mServices, especially those that are part of the core businesses of a given government entity (such as law enforcement units using mobile devices when doing their jobs in the field).
- Achieving full integration is a long term and very challenging tasks. It is advisable to have a strong ambition on this matter while being realistic. IT may be possible that some government entities, which are ready or already sharing data and services, may do the mobile counterparts, perhaps with limited improvements.
- Implementations requiring full-fledged enterprise mobility adoption for all of the government entities are also challenging. Practices involving flexible and remote working including Bring Your Own Device may be those that are yet to be seen after the year 2015 for most of the government entities.
- It is important that the first track and the second track are made priorities and all effort is done for the high-level completion within the time pan of the RoadMap.
- Similarly, key enabling and shared systems such

mobile ID, mobile Payment are also completed before the year 2015.

Having these points in mind, The Program Management Office may chose set up specific goals within the guidelines of the RoadMap such as "every government entity should priorities and implement at least 20 mServices" or "80 per cent of the government's all IT related personnel will be trained on Enterprise mobility" or "Adoption rate for mGovernment services should reach to 80 per cent of the population". In summary, as the RoadMap is not based on an mGovernment strategy, it may be difficult to spell out detailed goals to achieve given a specific time span.

### 7.2 Critical Success Factors

There are a number of critical success factors that may influence the implementation of the mGovernment RoadMap, and therefore, they deserve a special care:

- Political leadership, support and willingness, is sustained ideally at all times, at all levels and stages of the program
- Establishing the required capacity at the coordination and implementation centre (i.e. TRA) to lead and manage all milestones successfully to the end.
- Managing a balanced pace between the capacity, change and transformation required in government organisations; and the speed of mGovernment services development, both locally and centrally.
- Creation of well-planned and sustainable

partnership models required for all of the milestones, and beyond may 2015.

- Understanding the advancement of mGovernment to highest potential can only be achieved via intra and inter governmental data and services integration and interoperability, and therefore taking appropriate action to achieve that.
- Realising the essential role of local governments and local community building in for capacity building and spreading the mGovernment in the country.
- The success of the shared services such as mobile ID and mPayment to be a countrywide system has direct and the most significant influence on the success of the mGovernment overall.
- Establishing evaluation mechanisms and impact measurements for the implementation and doing adaptive revisions based on feedback.

### 7.3 Management of the mGovernment Program

Section 3.1 introduced the millstone and key tasks related to setting up Program Management Office which is responsible from managing the mGovernment transformation program. It is also responsible for implementing this RoadMap. A successful management approach to the mGovernment RoadMap requires institutionalising the mGovernment program in the government by establishing the appropriate managerial structure and the processes. This section presents particulars of such institutionalising.

### 7.3.1 Ownership and Accountability

Clearly, the management of the of the mGovernment transformation program, with its structure established and the processes put in place will be the major unit owning the implementation of the RoadMap. It is accountable to the committees established at the higher level. The Management will naturally be distributing responsibilities for implementing various milestones and their tasks to project groups within and will work closely with relevant partners and stakeholders. This delegation of responsibilities and authorities needs to be managed with stressed accountability measures.

The management of the certain milestones may prove especially difficult in this respect such as those related to mobile payment, the TSM and mobile ID. The tasks belonging to these milestones require working closely with a number of stakeholders. The performance expectation of stakeholders, and those from them need to be clearly identified and communicated. The milestone on stakeholder management in Section 3.2 could be very much helpful in this respect. It is important that such partnerships and measures of accountability are set having sustainability in mind. There are evidences of poorly managed partnership in a number of significant projects in eGovernment and mGovernment domain as there are well managed ones, too.

### 7.3.2 Managerial Structure

At the moment the mGovernment program in the UAE is being led by the mGov committee established in the TRA. The management's capacity must respond to the complex requirements of each of the milestone implementations both in terms of required technical skills as well as

managing potential collaborations with external organisations and consultants. One of the pressures might come from supporting the milestones that require close communications and collaborations with a large number of government entities for understanding their requirements and supporting these requirements for the entities to successfully implement mGovernment.

In addition to the above, a strong, and perhaps a centralised management, is required as the implementation may need to be distributed like a network allowing cooperation and collaborations in many ways among a number of core stakeholders:

- **Central management of the mGovernment Program:** The mGov Committee in TRA is responsible from carrying out all milestones. This committee needs sufficient capacity to carry out program management tasks with various projects involving planning, coordination, and leading execution of RoadMap key tasks, such as mobile ID, mPayment, integration, capacity building, creating the enabling environment and partnership building.
- **Distributed leaders of mGovernment across the government organisations central or local at the emirates level:** These may be units (i.e. eGovernment authorities or representations of government organisations, or units at local governments of the emirate), who are champions of mGovernment and are responsible from contributing to the program within their area or jurisdictions. These are all connected to each other within the network for collaborations and cooperation.

- **Local communities:** As described in the community building section (6.3), these are distributed communities of user groups such as farmers, unemployed etc. They may have two roles: 1) enabling wider adoption of mGovernment services through referrals and social networking and 2) providing data and information with respect to how mGovernment services are doing at the user level –what is going right and what needs improvement?

- **Stakeholders in the industry, NGOs and Academia:** these are sometimes users of mGovernment services but often are contributing partners to the program implementation in terms of capacity building, healthy operations in the mobile business and creation of the enabling environment.
- **National and international partners:** These are all organisations that have a stake in the socio-economical development of country via mGovernment transformation from MNOs to companies in the mobile value chain, from Government organisations to wealthy and charitable organisations and individuals.

### 7.3.3 Managerial Processes

One of the best ways to implement mGovernment RoadMap countrywide is to see the implementation process as a combination of a top-down and bottom-up building of properly run set of projects within the framework developed.

- **Top-down processes:** It is important that there is a strong leadership and visionary unit planning, initiating executions and monitoring implementation to go in the right direction. Top

down processes are often related to goal setting and action plans with respect all milestones and creation of enablers and solving bottlenecks during the implementation. It is not a hierarchical system but rather a loose but always present managerial style facilitating achievements of the goals. A good example to this is the generation of guidelines that are fed with input from various government entities and eGovernment authorities in the country.

- **Bottom-up processes:** If mGovernment services are mostly directed to the citizens, and for it to spread around the country, the dynamics should be expected to be bottom-up – from citizens and local government entities towards central government entities. All around the world local mGovernment services are more successful and spread than the central ones. The distributed government entities as mGovernment service providers will initiate and run a number of mGovernments services that are relevant to the local communities. These has to be managed locally but monitored centrally as they constitute and significant part of the overall mGovernment development in the country. A good example for this would be parking fee payment across the cities in the country.

The processes whether they are top-down or bottom are all part of and exist within a network structure where all central and distributed mGovernment implementers collaborate, share resources and know-how from one to another wherever they be geographically in the country.

Managing the processes in this way is not an easy task. Therefore, the implementation of the

## 7. IMPLEMENTATION APPROACH

mGovernment RoadMap may be phased and focused on certain milestones initially. In any case, however, The Program Management Office must carry out preparations and planning activities to move mGovernment services to various parts of the country, to numerous government entities and to reach to the whole population progressively.

### 7.3.4 Managing the Differences in the Maturity Level of Government Entities

The picture of the accomplishments in eGovernment domain in the UAE clearly presents differences in achievements and level of readiness of the various government entities. These differences will reflect themselves when it comes to implementing mGovernment transformation. In similar projects around the world there are tendencies to assume that all government entities will react and perform in a similar way. However, this is not completely true and the government entities differ in terms of their resources, competencies, goals and degree and speed of performance. In order to understand this issue better, Track 2 in Section 4 is designed.

This track will help both The Program Management Office and also the government entities to reconcile the differences to the extend possible. The implications of such differences for the Management of the mGovernment program may be significant. Phasing out implementation of the RoadMap time-wise might be helpful but perhaps levelling (i.e. a stepwise or incremental) degree of implementations according to regions and government entities may also be an option too. The sound basis for such decisions may be obtained during and after some of the milestones, especially those belonging Track 2, are implemented.

### 7.3.5 Managing the Risks

There is no doubt that a proper implementation of mGovernment in the UAE will set one of the best examples in the world with its strong resources, readiness and political support. Currently, there may be a few areas, which present a great risk to this endeavour:

- In time, the current management of the program may not be sufficient to handle the growing complexity and technicality of the mGovernment transformation.
  - Data integration and interoperability among government entities may not be at a level of quality that facilitates advanced mGovernment services, such as intelligent and interactive location based services.
  - The collaboration and cooperation required among the government entities and eGovernment authorities may fall short of what is required from the nationwide implementation of the mGovernment transformation.
  - The shared services are at the core of the overall success of the mGovernment program and they are interdependent. Failure or a substandard implementation in one may lead to a domino effect of failures in other parts of the mGovernment transformation.
- Lack of user take up – not being able to onboard users by encouraging them to adopt mGovernment services.
  - Losing the political support and the support of the government organisations
  - Inability to improve capacity of the government entities and the users
  - Loss of sustainable financing
  - Lack of or insufficient number of national and international strong partners

Most of the risks related to the implementation of the RoadMap may be avoided with the improvements of the capacity by endorsing the mGovernment unit under TRA to be the Government Chief Information Officer so that it can plan ahead, develop standards & policies, invest in shared core services, design of capacity building programs in government and for the citizens and manage communication and cooperation channels among government entities.

In addition to those risks, which are integral part of the ecosystem in which the mGovernment program will be implemented, a significant attention should also be paid to: