United Arab Emirates

هيئة تنظيم الاتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

الدليل الإرشادي

للحكومة الذكية

إصدار رقم 1

تاريخ الإصدار: 1 أغسطس 2013

ص.ب 26662، أبو ظبي، الإمارات العربية المتحدة (أ.ع.م.)
www.tra.gov.ae

قائمة التعديلات:

رقم الإصدار	تاريخ الإصدار	سبب التعديل
1.0	1 أغسطس 2013	

المحتويات

1 مقدمة

تهدف هذه الوثيقة إلى توفير مجموعة من الإرشادات للجهات الحكومية من أجل تهيئتها للتحول من الحكومة الإلكترونية إلى الحكومة الذكية، كما تهدف إلى مساعدة تلك الجهات على تخطي بعض التحديات التي ستواجههم أثناء محاولتهم الاستفادة من مميزات الحكومة الذكية. وتتضمن كذلك مجموعة من الإرشادات التي تهدف إلى جعل الجهات الحكومية "جاهزة للتحول الذكي" (m-ready) من حيث متطلبات تطوير وتنفيذ أحدث التطبيقات والخدمات الذكية التي تعتمد على تقنيات المعلومات والاتصالات.

1.1 نطاق وترتيب الوثيقة

تغطي هذه الوثيقة الأمور الواجب أخذها بعين الاعتبار عند التخطيط للخدمات الذكية وتنفيذها، وتشمل الأمور الفنية وسهولة الاستخدام (usability)، وكيفية التعامل معها والتدابير الأمنية الواجب اتخاذها. تركز الوثيقة بشكل أساسي على كيفية اختيار خدمات الحكومة الذكية التي سيتم تقديمها من قبل الجهات الحكومية في دولة الإمارات العربية المتحدة عبر التقنيات والأجهزة الذكية بما في ذلك الهواتف الذكية.

ومن هنا، فإن نطاق هذه الوثيقة محدود، وهي بشكلها الحالي **لا تغطي** الإرشادات المتعلقة بإنشاء شبكات لاسلكية على مستوى الجهات الحكومية، أو استخدام شبكات واسعة المدى أو استخدام الأجهزة من أجل تقديم الخدمات كجزء من النهج العام الذي تتبعه أي مؤسسة في سياق تحولها إلى تقديم الخدمات الذكية.

هناك استثناء واحد في القسم المتعلق بالأمن، إذ إنه يغطي طيفاً واسعاً من المخاطر؛ مثل: المخاوف العامة المتعلقة بمسألة الأمن، والمخاطر المتعلقة بالشبكات اللاسلكية الداخلية، والاتصالات، والتطبيقات، والبيانات، والأجهزة.

أما طريقة تنظيم هذه الوثيقة، فهي كالآتي:

- يتناول القسم التالي مجموعة من الإرشادات العامة التي وضعت بهدف مساعدة الجهات الحكومية على اتخاذ قراراتها بشأن اختيار الخدمات التي سيتم إطلاقها كجزء من الحكومة الذكية، ووضع سلم أولويات لها. تعتمد تلك القرارات على فهم ماهية الخدمة الذكية والمعايير الواجب اتباعها في تحديد الخدمات التي ستتضمنها الحكومة الذكية واختيار التقنيات المناسبة لها.
- القسم الذي يليه يتناول بالتفصيل اعتبارات تطوير التطبيقات الذكية بما في ذلك تطويرها للعمل عبر منصات متعددة، وواجهات برمجة التطبيقات (APIs)، والمسائل المتعلقة بالمستخدم، وسهولة الاستخدام، والمحتوى الذكي، إضافةً إلى كيفية ضمان تبني المستخدم للخدمات الذكية.
- بعد ذلك، تلقي الوثيقة نظرة أشمل على الإجراءات الأمنية بما في ذلك اعتبارات التحول الذكي على نطاق المؤسسة ككل.
- في نهاية الوثيقة، تم وضع إرشادات عامة حول تطوير وصيانة نظام دفع آمن لخدمات الحكومة الذكية.

تم وضع هذه الوثيقة ليستخدمها مصممو الخدمات الذكية، وإدارات تقنية المعلومات، ومديرو المشاريع العاملين في الجهات الحكومية.

1.2 فكرة عامة

تم تكليف الجهات الحكومية في دولة الإمارات العربية المتحدة بتطوير خدماتها عبر الاستفادة بشكل استراتيجي من التقنيات الذكية، وذلك بحلول شهر مايو 2015، ما يعني بشكل أساسي تحويل الخدمات الإلكترونية إلى خدمات ذكية عبر التحول إلى الحكومة الذكية. ينبغي أن يؤدي هذا إلى تحقيق ممارسات عملية للحكومة الذكية عبر تقديم تطبيقات وخدمات تتسم بالسلاسة والتفاعلية والذكاء. غير أن تطبيق الحكومة الذكية يجب أن يعتمد على تقييم واقعي للموارد والإمكانات التي تمتلكها كل جهة حكومية. ومع ذلك، فإنه من الجيد دائماً التفكير في الهدف النهائي الذي يتمثل في استشراف ما يمكن القيام به في ظل التقدم الكبير في مجال التقنيات الذكية وتطبيقات الحكومة الذكية.

1.2.1 مراحل التحول إلى الحكومة الذكية

يركّز التحول إلى الحكومة الذكية على الاستخدام الاستراتيجي لأحدث تقنيات المعلومات والاتصالات، وعلى رأسها التقنيات الذكية، بهدف إجراء تحوّل نوعي في الطريقة التي تعمل وفقها المؤسسات الحكومية، وذلك لتحقيق رضا المستخدمين، وبالتعاون الفعال مع جميع الجهات ذات الصلة. ويتم ذلك عبر توفير وسائل تواصل سلسة وتفاعلية وذكية تعمل في أي وقت وأي مكان، عبر العديد من الأجهزة.

- تتضمن الحكومة الذكية إجراء تحسينات مميزة لاثنين من المجالات المتعلقة بالعمل الحكومي على الأقل:
  - تحسينات هيكلية على إجراءات العمل وطريقة عمل الموظفين
  - توفير الخدمات الأكثر ملاءمة للجمهور وفقاً لاحتياجاتهم

- على الرغم من أن تصنيف الخدمات الذكية ليست عملية بسيطة، إلا أنه يمكن تقديمها على النحو الآتي:

- خدمات من الجهة الحكومية إلى المواطنين **(G2C)** (مثل الإشعارات، رسائل نصية قصيرة توضح حالة المرور، أقرب المستشفيات إلى الموقع الجغرافي، إلخ).
- خدمات من الجهة الحكومية إلى الشركات **(G2B)** (مثل تسجيل الشركات، الاستفسار حول الرسوم، إلخ).
- خدمات من الجهة الحكومية إلى جهات حكومية أخرى **(G2G)** (مثل تبادل المعلومات حول حالة المريض وتاريخه الصحي).
- خدمات من الجهة الحكومية إلى الموظفين **(G2E)** (مثل "أحضر جهازك معك" **(BYOD)**، وأسلوب التشارك في الحيز المكتبي **(hot desking)**، إلخ).

- تطبق الحكومة الذكية أحدث التقنيات لتحويل الحكومة الإلكترونية إلى حكومة تمتاز بالآتي:

- متوافرة على مدار الساعة في أي مكان وعبر أي منصة تشغيل أو جهاز ذكي.
- توظف أحدث التقنيات الذكية مثل التطبيقات والخدمات التي تعتمد على تحديد الموقع الجغرافي أو البيئة المحيطة.
- السلاسة وسهولة الاستخدام بفضل التكامل الفعّال الذي تمتاز به إضافةً إلى استخدام التواصل الذكي بين الطرفين **(X2X)** حيث يمكن أن تشير **(X)** إلى جهاز أو إلى إنسان.

- تكون الحكومة الذكية أكثر فعالية عندما تؤسس شراكات بين المؤسسات الحكومية من جهة، ومؤسسات القطاع الخاص، والمؤسسات غير الحكومية ومؤسسات المجتمع المدني من جهة أخرى، وذلك حيثما توافرت أهداف مشتركة.

يبين الجدول أدناه مراحل التحوّل إلى الحكومة الذكية المتعلقة بالتطورات الحاصلة في تقنيات المعلومات والاتصالات **(ICT)**، ومستوى جاهزية الحكومة الإلكترونية للتحول إلى الحكومة الذكية من حيث البيانات والخدمات وعملية التكامل بين الجهات الحكومية وبعضها البعض، علماً أن الأمثلة المستخدمة في الجدول أمثلة افتراضية وليست حقيقية.

بعض طرق تقديم خدمات الحكومة الذكية

	رسائل نصية قصيرة (خدمات معلوماتية/ خدمات إشعار)	رسائل نصية قصيرة (خدمات تفاعلية/ خدمات إشعار واستعلام)	النسخة الذكية من الخدمات الإلكترونية	تطبيقات ذكية إجرائية	تطبيقات ذكية متكاملة
إلى الجمهور* (G2C)	تذكير بمواعيد التطعيمات	الحصول على نتائج الامتحانات المدرسية عند الطلب	تقديم طلب للحصول على شهادة ميلاد	تسديد رسوم المخالفات المرورية	إجراء عدة خدمات تكميلية مثل: تغيير عنوان المنزل، وتحديث بيانات بطاقة الهوية وسجل التوظيف لدى وزارة العمل.
إلى الشركات (G2B)	التذكير بموعد تجديد الرخصة التجارية	الاستفسار عن حالة طلب الرخصة التجارية	طلب الحصول على رخصة تجارية	تجديد الرخصة التجارية ودفع الرسوم	تبادل المعلومات بين الجهات الحكومية: منح ترخيص تجاري، وتحديث البيانات لدى وزارة العمل والدائرة الاقتصادية بدبي.

إلى الجهات الحكومية (G2G)	غير قابل للتطبيق	غير قابل للتطبيق	غير قابل للتطبيق	تبادل المعلومات بين الجهات الحكومية: سجلات المرضى في جميع المستشفيات والمراكز الطبية على مستوى الدولة.
إلى الموظفين (G2E)	غير قابل للتطبيق	غير قابل للتطبيق	غير قابل للتطبيق	توفير الأدوات اللازمة للموظفين الحكوميين، والسماح لهم بالوصول إلى المعلومات: الدخول إلى إدارة شرطة المرور من أجل تحرير مخالفة صف سيارة، وتحديث البيانات لدى الدوائر المختصة.

شكل رقم (1)

وهكذا، فإن الخدمات الذكية تقع في صلب عملية تحول الحكومة الإلكترونية إلى حكومة ذكية (mGovernment or Smart Government)؛ وذلك عبر استخدام التقنيات الذكية في مراحل ومستويات مختلفة. ومن شأن الحكومة الذكية أن تعزّز الحكومة الإلكترونية بطرق متعددة، فهي تسهم في خلق أجواء عمل مناسبة لموظفي الحكومة للعمل الذكي، وتساعد في تحسين حياة المواطنين من خلال تقديم أرقى مستويات الخدمات الحكومية التي تتيح تواصلاً فعالاً باستخدام الأجهزة الذكية.

1.2.2 أنواع التحسينات العامة التي تدخلها الحكومة الذكية على الحكومة الإلكترونية

فهم التحسينات التي تميز الحكومة الذكية أمر ضروري لتحديد نوعية الخدمات التي يجب أخذها بعين الاعتبار عند تطوير الخدمات الذكية.

في ما يأتي أربعة أنواع من التحسينات المختلفة التي تدخلها الحكومة الذكية على الطريقة التقليدية التي تتبعها الجهات الحكومية عند تقديم خدماتها:

- **تحويل مباشر لبعض خدمات بوابة الحكومة الإلكترونية:** تحويل خدمات مناسبة من بين الخدمات القائمة التي توفرها بوابة الحكومة الإلكترونية إلى خدمات الحكومة الذكية، وهذه خدمات إلكترونية تقليدية يتم توفيرها على المنصة الذكية.
- **خدمات ذكية جديدة يتم توفيرها للجمهور:** وهي خدمات مميزة قد لا تكون متاحة في الحكومة الإلكترونية التقليدية وأصبحت ممكنة بسبب التقنيات الذكية. من أمثلة هذه الخدمات: دفع رسوم وسائل المواصلات العامة ومواقف السيارات باستخدام الهاتف المتحرك، إضافةً إلى الخدمات التي تعتمد على تحديد الموقع الجغرافي.
- **خدمات للموظفين الميدانيين:** وتعني أتمتة القوى العاملة الميدانية؛ حيث يتم تزويد الموظفين الحكوميين الذي يعملون خارج مكاتبهم (مثل موظفي خدمات الطوارئ والتفتيش، ومن يعملون على رعاية المرضى في المنازل) بأجهزة وتقنيات ذكية.
- **ساعات العمل المرنة:** وتتعلق بتشجيع الجهات الحكومية للعمل عن بعد؛ مثل العمل من المنزل والسماح للموظفين باستخدام الأجهزة الذكية داخل المكتب، علاوةً على استخدام أسلوب التشارك في الحيز المكتبي (hot desking).

لا تنطوي تلك التحسينات المقترحة بأي حال من الأحوال على مجموعة كاملة من المهام التي ينبغي على كل جهة حكومية القيام بها، وإنما قد تتطلب الإجراءات الأولية لتطبيق الحكومة الذكية، تحويل الخدمات الإلكترونية إلى خدمات ذكية، مع التركيز على التطبيقات المتعلقة بالمواطنين (G2C).

1.2.3 بعض الأفكار الخاطئة حول مفهوم الحكومة الذكية

منذ نشأة المفهوم، دائماً ما يرتبك القائمون على تنفيذ الحكومة الذكية في فهم بعض النقاط الأساسية، وأحياناً تكون تلك المفاهيم غير واضحة بالنسبة لهم، ونحاول في ما يأتي توضيحها:

- الحكومة الذكية ليست بديلاً عن الحكومة الإلكترونية، إنما تكملها وتعمل على تعزيز الأنظمة والخدمات القائمة.

- لا تقتصر الحكومة الذكية على الهواتف المتحركة، وإنما تشمل جميع الأجهزة المحمولة والذكية (قد يشمل ذلك الاتصالات بين الأجهزة وبعضها البعض).

- للحكومة الذكية هدفان متميزان وبعيدا المدى:
  - تقديم الخدمات إلى الجمهور عبر التقنيات الذكية ـ توفير خدمات تفاعلية مع الجمهور.
  - تطوير مؤسسات القطاع الحكومي - إعادة هيكلة الإجرءات العملية وتحديث القطاع العام ـ التفاعلات داخل الجهات الحكومية.

- في حين يشكل تطوير التقنيات والخدمات جوهر التحول إلى الحكومة الذكية، إلا أنه في ذات الوقت أسهل عناصرها، فأمور مثل المناهج الاستراتيجية المتبعة في عملية التحوّل إلى الحكومة الذكية، وبناء القدرات الحكومية، وإدارة التغيير، والتأسيس لمجتمع "ذكي"، وتبني الجمهور للخدمات الذكية... جميعها تنطوي على أهمية كبيرة في هذا السياق.

2 تحديد أولويات الخدمات الذكية

أولى الخطوات - وقد تكون أكثرها أهمية - التي يجب على الجهات الحكومية اتخاذها عند تحويل خدماتها الإلكترونية إلى خدمات ذكية تكمن في إجراء تقييم شامل للخدمات وتحديد أي منها سيتم تحويله وكيفية وضع الأولويات خلال عملية التحويل. وهو ما يتطلب دراسة متأنية لأربع مسائل مهمة على الأقل هي:

1. تعريف وتحديد مكوِّنات الخدمة الذكية
2. تحديد الخدمات المناسبة التي يمكن تحويلها إلى خدمات ذكية
3. تحديد الجمهور المستهدف لكل خدمة
4. تحديد معايير اختيار الخدمات التي سيتم تحويلها، وفيما يأتي بعض هذه المعايير:
   - احتياجات الجمهور (ويجري تحديدها من خلال الاستبيانات واستطلاعات الرأي عبر الإنترنت)
   - القيمة المضافة (أي زيادة كفاءة إنجاز المهام)
   - حجم المعاملات
   - معدلات الاستخدام
   - سهولة التحويل
   - إمكانية المساهمة في زيادة الإيرادات

تجدر الإشارة إلى أن الانتقال من الحكومة الإلكترونية إلى الحكومة الذكية لا يعني تحويل كل خدمة إلكترونية إلى خدمة مقابلة ذكية، فقد يتطلب الأمر تحويل مجموعة من الخدمات الإلكترونية إلى خدمة ذكية واحدة. وفي المقابل، قد يتم تجزئة خدمة إلكترونية واحدة إلى عدة خدمات ذكية. ومن المرجح أيضاً أن تضطر الجهات الحكومية إلى استحداث خدمات ذكية جديدة تماماً للاستفادة من التقنيات الحديثة، وتحسين خدماتها عبر هذه القنوات المبتكرة لطرح خدمات جديدة لا يمكن توفيرها عادةً عبر الوسائل التقليدية.

2.1 تعريف الخدمات الذكية

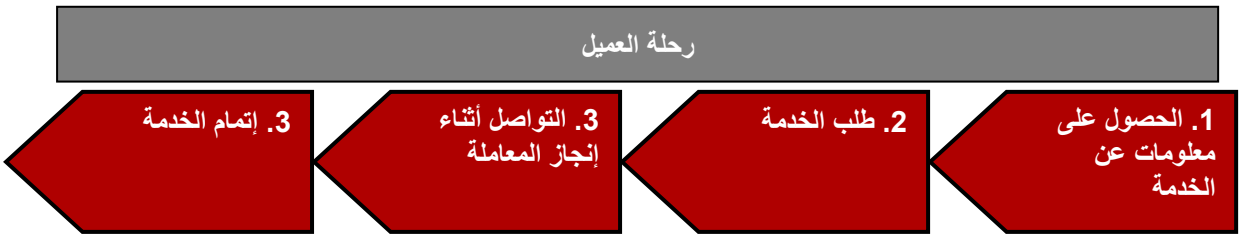
ما هي الخدمة الذكية؟ وكيف يمكن تعريف تجربة المستخدم مع الخدمات الذكية بشكل عام؟ تشكل الحكومة الذكية امتداداً للحكومة الإلكترونية، حيث يتم تقديم الخدمات الحكومية من أي مكان وفي أي وقت عبر الأجهزة الذكية (مثل تطبيقات الهاتف المتحرك، والحاسب المحمول، وأجهزة المساعد الرقمي الشخصية، إلخ).

أما تجربة المستخدم، فيمكن تقسيمها إلى أربع خطوات تفاعلية متميزة:

الخطوة الأولى - الحصول على معلومات عن الخدمة: يتعرف العميل من خلالها إلى الخدمة المطلوبة وكيف ومتى وأين يمكن الحصول عليها.

الخطوة الثانية – طلب الخدمة: يبدأ العميل عملية التفاعل مع الجهة الحكومية للحصول على الخدمة المبتغاة.
الخطوة الثالثة – التواصل أثناء إنجاز المعاملة: يبدأ العميل في إجراءات استخدام الخدمة ويسدد الرسوم، إن وجدت، وكنتيجة لتواصله مع الجهة الحكومية يحصل على الخدمات التي تساعده.
الخطوة الرابعة – إتمام الخدمة (من البداية إلى النهاية): يكمل العميل عملية التفاعل الخاص بالخدمة المطلوبة ويحصل على النتائج المرجوة.

ويمكن اختصار ما ذكر أعلاه من خلال الشكل رقم 2 أدناه:



شكل رقم (2)

2.1.1 أنواع التحسينات التي تدخلها الخدمات الذكية

يمكن تقسيم التحسينات المترافقة مع الحكومة الذكية إلى أربع فئات مختلفة من الخدمات الذكية يمكن تلخيصها كالآتي:

تحسين جودة الخدمات المعلوماتية:

بإمكان المستخدمين الوصول إلى المعلومات الحكومية الحالية، والتصويت على موضوع معين، وتقديم الطلبات والبلاغات، والتسجيل. وينطبق هذا على المعلومات الثابتة التي لا تحتاج إلى تفاعل مكثف مع الجمهور(مثل المعلومات، والإشعارات المتعلقة بحالة الطقس، والقوانين، وحالات الطوارئ، ونتائج الامتحانات، وإغلاق الطرقات، والفعاليات، والجداول الزمنية، والتعديلات على الرسوم، الخ). في مثل هذه الحالات، تفي الرسائل النصية القصيرة (SMS) بالغرض، حيث يجري استخدامها على نطاق واسع، كما يمكن أيضاً استخدام وسائل الاستجابة الصوتية التفاعلية (IVR) أو الاستجابة التفاعلية بالصوت والصورة (IVVR). أما الخدمات المعلوماتية والتعليمية فتميل إلى استخدام الرسائل النصية القصيرة، أو تنشر المعلومات عبر الإنترنت للهواتف المتحركة (mobile web) أو نظام التطبيقات اللاسلكية (WAP).

تمكين الخدمات لتصبح أكثر تفاعلاً:

وهي عبارة عن التطبيقات التي تمكّن المواطنين من إجراء حوار تفاعلي مع الحكومة. وغالباً ما يجري التفاعل على المستوى الشخصي، حيث يتم تبادل البيانات الشخصية، والتطبيقات، والوصول إلى قواعد بيانات ومجالات خدماتية معينة. وتعمل التقنيات التي تعتمد على تحديد الموقع الجغرافي مثل التصوير، وتسجيل مقاطع الفيديو، والخرائط، على زيادة إمكانيات الخدمات المتاحة. وقد ثبت في الآونة الأخيرة زيادة التوجه إلى استخدام وسائل التواصل الاجتماعي من أجل بث الأخبار العاجلة أو تبادل المعلومات بشكل فوري. ويمكن استخدام التطبيقات الذكية في طيف واسع من الاحتمالات الكبيرة المفتوحة لتقديم العديد من الخدمات التفاعلية في مجالات مختلفة مثل الخدمات الصحية (المراقبة، والاختبارات، والفحوصات) وخدمات التعليم (نتائج القبول والامتحانات) وخدمات الاستفسارات (حركة السير، ومعلومات الحساب)، وخدمات الجهات المسؤولة عن تطبيق القوانين، وغيرها.

تطوير الخدمات الإجرائية:

وهي الخدمات الذكية التي تتيح للجمهور تقديم الطلبات، أو الإعلان عن شاغر وظيفي، أو شراء تذاكر الحافلات، أو حجز موعد، أو التوقيع على المعاملات رقمياً، وذلك على مدار الساعة. ولكن تصاحب خدمات من هذا النوع قضايا تتعلق بالأمن والسرية تتطلب مبادرات لتطوير تقنيات خاصة تضمن إجراء المعاملات وتخزين المعلومات الحسّاسة بطريقة آمنة؛ إذ إن تقنيات التوقيع الرقمي وعمليات الدفع عن طريق تقنية التواصل قريب المدى (NFC) تتطلب أنظمة أمنية مصمَّمة بشكل خاص.

تحقيق التكامل بين مختلف الخدمات

وهي خدمات ذكية تجمع خدمات أو بيانات من أقسام مختلفة داخل الجهة الحكومية الواحدة أو من جهات حكومية أخرى، ما يجعلها أكثر ملاءمة للجمهور عبر إتاحة التكامل بين خدمات متنوعة. فعلى سبيل المثال، يمكن لخدمة تحديث الحالة المرورية أن تربط بين خدمات هيئة الطرق والمواصلات مع خدمة الخرائط من أجل اقتراح طرق بديلة للمستخدمين، وكذلك إعلامهم عن أقرب المواقع في محيطهم الجغرافي التي قد تكون محل اهتمام بالنسبة لهم. بشكل عام، الخدمات المتكاملة هي تلك الخدمات التي تحقق القيمة الأفضل للمستخدم، والتي تشكل مركز اهتمام تطوير الخدمات الذكية في دولة الإمارات العربية المتحدة. لذا على الجهات الحكومية أن تتعاون مع غيرها من المؤسسات لتطوير حلول تتيح تقديم خدمات متكاملة.

2.1.2 القاعدة الأساسية للتحول الذكي

ينبغي على الهيئات الحكومة جميعها إنجاز الخطوتين الأولى والثانية كحد أدنى كي يمكن اعتبارها مؤهلة لتقديم الخدمات الذكية.

في المرحلة الأولى، يجب على جميع الجهات الحكومية التركيز بشكل أساسي على الخدمات الموجهة للجمهور (G2C) في عملية التحول إلى الحكومة الذكية.

2.2 كفاءة الخدمات الذكية

على الرغم من أنه يمكن اعتبار الحكومة الذكية امتداداً للحكومة الإلكترونية، إلا أن وجود الخدمات الحكومية الإلكترونية ليس شرطاً مسبقاً للتحول إلى الحكومة الذكية؛ ما يعني أن التحول إلى الحكومة الذكية لا يتم فقط عن طريق ترحيل الخدمات الإلكترونية إلى منصة الخدمات الذكية. ولكن تبدأ عملية التحول في العادة، بتقييم الخدمات الإلكترونية القائمة لدى الجهة الحكومية. وفي معظم الحالات، تكون الخدمات المعلوماتية والإجرائية هي أولى الخدمات التي تبدأ الهيئة الحكومية بتحويلها إلى خدمات ذكية.

من الضروري قبل اتخاذ أي قرار بشأن اختيار الخدمات الإلكترونية التي سيتم تحويلها إلى خدمات ذكية، القيام بما يأتي:

1. إجراء تقييم للخدمات لمعرفة إذا ما كانت تصلح لتحويلها إلى خدمات ذكية أم لا، وذلك عبر دراسة متطلبات الخدمة، والقيود على السعات المتاحة، وإمكانية استخدام التقنيات الذكية لتقديم تلك الخدمات. فقد لا يكون من المناسب تحويل الخدمات التي تتطلب من المستخدم إرفاق مستندات معينة (التقديم للحصول على رخصة تجارية على سبيل المثال)، إلى خدمات ذكية. وينطبق ذلك أيضاً على الخرائط المعقدة أو المحتويات المرئية التي تحتاج إلى مراجعة مفصلة أو معالجة، أو قد تتطلب حجم ذاكرة كبير عند ترحليها إلى خدمات ذكية.

2. تقييم درجة التعقيد في التغيير المطلوب إجراؤه على طريقة سير العمل، والجدوى من إجرائه في ذات الوقت. ويمكن اعتباره أحد الأمور الأساسية التي تضاف إلى أسس تنفيذ الخدمات عبر المنصات الذكية. تُعتبر الخدمات التي تؤدي إلى إعادة هيكلة طريقة العمل من أجل تبسيطها والتقليل من الخطوات غير الضرورية التي على المستخدم اتخاذها أكثر ملاءمة نسبياً لتحويلها لخدمات ذكية.

3. الأخذ بعين الاعتبار الخدمات الإلكترونية التي تعد جوهرية بالنسبة للجهات الحكومية وتساعد في خدمة الجمهور بشكل كبير، ولكنها غير مناسبة للأجهزة الذكية الشائعة الاستخدام، حيث بالإمكان أن تدرس تلك الجهات استخدام أجهزة وبرامج يتم تعديلها للمساعدة في تحويل تلك الخدمات إلى خدمات ذكية. من بين الأمثلة التي يمكن إدراجها هنا: أنظمة التعرف إلى رقم لوحة السيارة والكشف عليها، وكاميرات خارجية ذكية توفر معلومات عن حركة المرور، الخ.

2.3 اختيار الخدمات الذكية وتحديد قابليتها للتحول

ليس من السهل تحديد أي من الخدمات التي تتوافر فيها شروط التحول إلى خدمات ذكية وفي ذات الوقت يعود تحويلها بالنفع، إذ ينبغي على كل جهة تطوير واستخدام آلياتها الخاصة من أجل تقييم تلك الخدمات واتخاذ القرارات بشأنها. غير أن هناك بعض المبادئ التي من شأنها توجيه وإرشاد الجهات الحكومية إلى تطوير مثل تلك الوسائل للقيام بعملية الاختيار، و يعتبر اختبار الملاءَمة المذكور أعلاه أحد تلك الوسائل. وفي ما يأتي مجموعة من الأمور النموذجية الإضافية التي يمكن أخذها بعين الاعتبار في ما يخص الخدمة المراد تحويلها:

- أن تشكل عنصراً أساسياً من عناصر سير العمل وجودة الخدمات التي تقدمها الجهة الحكومية
- أن تكون معدلات استخدامها كبيرة
- أن يكون حجم المعاملات فيها كبيراً
- أن توفر مصدراً إضافياً لإيرادات الهيئة
- من السهل تطويرها (أو تحويلها) وصيانتها
- أن تحقق قيمة مضافة تسعد الجمهور
- أن تساعد على تسهيل إجراءات الجهة الحكومية أو طريقة سير العمل فيها
- أن توفر كفاءة في التكلفة والوقت.
- أن تساهم في تحسين النظرة العامة إلى الحكومة
- أن تكون مناسبة للجمهور المستهدف
- أن تكون مطلوبة من قبل الجمهور (وفقاً لاستبانات واستطلاعات رأي يتم إجراؤها)

القائمة أعلاه لا تعطي أولوية لعنصر على الآخر، ويمكن لكل جهة وضع مجموعة المعايير الخاصة بها؛ فقد لا تكون هذه القائمة مناسبة لجميع الجهات الحكومية. ما يهم اعتباره في هذا السياق هو أن الخدمات ليست جميعها مناسبة للترحيل إلى المنصات الذكية، لذا ينبغي على كل جهة أن تضع أولوياتها في ما يتعلق بتحديد الخدمات الأكثر ملاءمةً للتحول الذكي.

2.4 لمحة عامة عن قنوات التطبيقات الذكية

تتضمن استراتيجيات الخدمات الذكية عدة نقاط جوهرية مثل: بنية تقنية المعلومات والاتصالات المتاحة، والمتطلبات التقنية للخدمة المراد تحويلها، وإمكانية وصول الجمهور للخدمة وسهولة استخدامها. توفر عوامل مثل سرعة انتشار الأجهزة الذكية، وارتفاع جودة شبكات الهاتف المتحرك، وزيادة الطلب على التطبيقات الذكية عالية الكفاءة، فرصاً لانهائية للارتقاء بكفاءة العمليات التشغيلية في القطاع الحكومي، وتفتح الباب أمام وسائل تفاعل جديدة مع الجمهور. ومن هنا، أصبح من الضروري امتلاك رؤية واضحة حول الأهداف المبتغاة من الخدمات الحكومية والخيارات التقنية المتاحة. نستعرض في هذا القسم لمحة عن قنوات تطوير تطبيقات الحكومة الذكية في ضوء آخر المستجدات على نطاق التقنيات الذكية.

2.4.1 القنوات الصوتية

ما تزال قنوات الاتصال الصوتية تشكل خياراً قابلاً للتطبيق في مجال الاتصالات الذكية لعدة عوامل منها:

- إمكانية تطبيقها على جميع الأجهزة الذكية
- سهولة استخدامها (ليست هناك حاجة للتدرُّب على استخدامها)
- توفيرها قدرة أعلى للاتصال وتبادل المعلومات
- كونها مألوفة لدى الجميع

وقد تم تطوير الكثير من التطبيقات المبتكرة المتعلقة بالتواصل الصوتي التفاعلي مع أجهزة الحاسب الآلي، ما أتاح توفير العديد من التطبيقات في هذا الإطار مثل: الإرشادات الصوتية للاتجاهات أثناء القيادة، وإجراء المكالمات الهاتفية، والتعرف إلى الأصوات، والدخول إلى الإنترنت عن طريق الإرشادات الصوتية، الخ.

2.4.2 قناة إرسال الإشارات (Signaling Channel)

الرسائل النصية القصيرة (SMS): نظراً لسهولة استخدام الرسائل النصية القصيرة وانتشارها الواسع، ما تزال تستخدم في العديد من التطبيقات مثل: الإشعارات، والأخبار، وأحوال الطقس، وإدراة حالات الطوارئ، ورسائل التذكير المتعلقة بالرعاية الصحية والطبية، والتصويت، والتبرع، والدفع، الخ. كما تعد قنوات الرسائل الصوتية ورسائل الفيديو سهلة الاستخدام بالنسبة للمستخدمين، وتوفر وسائل جديدة لإيصال المعلومات سواء لموظفي الحكومة الميدانيين أو للمستخدمين العاديين.

بروتوكول بيانات الخدمات التكميلية غير المنظمة (USSD): وهنا يتم تحويل الرسائل مباشرة عبر قنوات إشارة الشبكة ، لذا تكون مجانية والوصول إليها متاح بشكل كبير. ومن المجالات التي يمكن استخدام هذه التقنية فيها: التعاملات البنكية الآمنة، والأخبار، وتقديم الطلبات، والتصويت.

بروتوكول التطبيقات اللاسلكية (WAP): وهو بروتوكول عالمي وظيفته تمكين الدخول إلى شبكة الإنترنت عبر الشبكة اللاسلكية للهاتف المتحرك. وتستخدم الأجهزة المتحركة الصغيرة متصفحات الواب **(WAP)** التي تمكِّنها من الدخول إلى شبكة الإنترنت باستخدام لغة ترميز لاسلكية.

2.4.3 قناة البيانات (Data Channel)

وتتوافر في أشكال متعددة من الرسائل المتحركة: رسالة من تطبيق إلى شخص (مثل SMS, MMS)، و رسالة من شخص إلى تطبيق (مثل السماح للمستخدم بتحميل المحتويات المراد إرسالها. من الاستخدامات الشائعة لهذا التطبيق: التصويت على مسألة معينة، وتحميل الصور، الخ)، و رسالة من شخص إلى شخص، وأخيراً رسالة من آلة إلى آلة (إدارة الأصول، المتابعة، الصيانة عن بعد، الدفع لدى نقاط البيع، أمن الرعاية الصحية والعدادات الذكية، الخ).

وتتيح قناة البيانات العديد من الفرص المهمة لتطوير تطبيقات تُعنى بمعالجة البيانات، فتوفير تغطية أوسع للبيانات مع وجود الأجهزة الذكية المتطورة، يجعل من تطبيقات البيانات مع توافر الإنترنت عبر الأجهزة الذكية حلاً مناسباً لتنقل البيانات والوصول إلى محتويات ثرية في أي وقت ومن أي مكان.

3 إرشادات حول التطبيقات الذكية

تبدأ عملية التحويل إلى تطبيقات ذكية بتحليل طبيعة الخدمة المراد نقلها إلى منصة ذكية. وتتطلب كل خدمة خصائص وظيفية معينة لاستعمالها ضمن التطبيق دون المساس براحة المستخدم أو الأمور المتعلقة بالتصميم. ويشكّل اختيار المنصة والقناة الذكية اللتين سيتم تطوير التطبيق من خلالهما خطوة أساسية يجب اتخاذها للحصول على أفضل النتائج، فلكل نظام مزاياه وعيوبه، وهنا تشكّل طبيعة الخدمات العامل الحاسم في عملية الاختيار. تهدف المعلومات الآتية إلى توجيه الجهات الحكومية لاتخاذ القرار المناسب بشأن نوع التطبيق الأكثر ملاءَمة لمشروعاتها.

يرجى الاطلاع على المعلومات الواردة أدناه والإجابة على الأسئلة المطروحة من أجل التوصل إلى قرار بشأن كيفية تطوير التطبيق:

- ما هي حصة السوق الحالية من الهواتف وأنظمة التشغيل الذكية؟
- ما هي الميزانية المخصصة للمشروع؟
- ما معدل تحديث محتوى التطبيق؟
- ما هي الفترة الزمنية التي يجب خلالها تطوير التطبيق وإتاحته للاستخدام؟
- ما مستوى الكفاءات داخل الهيئة القادرة على تطوير الخدمة الذكية؟
- من هم المستخدمون المستهدَفون؟ وما هي توقعاتهم؟
- ما هي مستويات الأمن التي يجب اتخاذها؟
- ما مدى البساطة المبتغى تحقيقه في الخدمة؟
- هل هناك واجهة برمجية مشتركة **(Shared API)** يمكن للمبرمجين استخدامها؟ (يجب استخدامها إن وجدت).

3.1 التطبيقات الأصيلة (Native Applications)

يعتمد تطوير التطبيقات الأصيلة على أنظمة التشغيل الذكية، إذ تتطلب كل منصة استخدام أدوات ولغات برمجية مختلفة من أجل تطوير التطبيقات؛ وبالتالي يحتاج كل تطبيق إلى خبرات معينة تتعلق بالمنصة والأجهزة، وإتقان العديد من لغات البرمجة والترميز. أما من حيث سهولة الاستخدام، فهناك العديد من الميزات التي لا تتوافر إلا في التطبيقات الأصيلة، وهي:

- **نقاط اللمس المتعدد** (Multi-touch Gestures)**:** وهي أنماط متعددة من الحركات التي يمكن تخصيصها والتي تهدف إلى تعزيز تجربة المستخدم وتحقق سهولة الاستخدام. ويمكن تعديل الخصائص الوظيفية لإتاحة خاصية النقر المزدوج على الشاشة وخاصية التصغير والتكبير ما يحقق سهولة تامة في استخدام التطبيقات.
- **مستوى متقدم من الرسومات والغرافيك:** في التطبيقات التي تحتاج إلى كمية كبيرة من البيانات والرسوم الديناميكية، توفر التطبيقات الأصيلة أفضل الخصائص الوظيفية التي تحتوي على واجهة برمجة للتطبيقات توفر رسوم غرافيك سريعة.
- **التكامل مع خصائص الجهاز:** تستفيد التطبيقات الأصيلة بسهولة من المكونات الأساسية للجهاز الذكي مثل: الكاميرا، ومسجل الصوت، ونظام تحديد المواقع الجغرافية، الخ.

3.1.1 المنصات الأصيلة (Native Platforms)

	نظام تشغيل آبل Apple OS	أندرويد Android	نظام تشغيل بلاك بيري Blackberry OS	ويندوز Windows
اللغات المستخدمة	*Objective –C, C, C++*	*C, Java and C++.*	*Java*	*C#, VB, .NET*
اسم متجر التطبيقات	**متجر آبل للتطبيقات**	**غوغل بلاي** *Google Play*	**عالم بلاك بيري للتطبيقات**	**سوق ويندوز فون**

- **أندرويد:** نظام تشغيل غوغل للأجهزة الذكية.
- **iOS:** تم تطويره من قبل شركة "آبل"، ويعرف نظام تشغيل **iOS** بخواصه التي تتميز بالسهولة، وبكم التطبيقات الهائل في متجر آبل **(Apple Store)**.
- **بلاك بيري:** تم تصميمه وتشغيله من قبل شركة ريسيرتش إن موشن (Research in Motion)، ويقدم خدماته على غرار "المساعد الرقمي الشخصي" ويتيح تصفح الإنترنت والبريد الإلكتروني، ووسائط الإعلام.
- **ويندوز فون:** عبارة عن نظام تشغيل تم تطويره من قبل شركة مايكروسوفت، ويتوجه بشكل أساسي إلى سوق المتعاملين من الأفراد وليس المؤسسات.

هناك آلية لمراجعة وتقييم التطبيقات قبل رفعها على متجر التطبيقات الخاص بكل نظام تشغيل أو منصة. ولتسجيل التطبيقات، يتعين على المؤسسة امتلاك حساب كمطّور تطبيقات على تلك المنصات. تجدر الإشارة إلى أن عملية التقييم تستغرق حوالي أسبوعين بعد تقديمها؛ هذا في حال كانت المؤسسة المتقدمة تمتلك حساب مطوِّر على تلك المنصات.

3.2 تطبيقات الويب الذكية

تطبيقات الويب الذكية هي في الواقع مواقع إلكترونية مصممة للاستخدام عبر الأجهزة الذكية والتي عادة ما تستخدم تقنيات الويب المعيارية مثل HTML5، جافا سكريبت، CSS. وتتوافق تلك التطبيقات مع مختلف المتصفحات والمنصات والنظم التشغيلية؛ متبعة منهج "قياس واحد مناسب للجميع".

بالمقارنة مع التطبيقات الأصيلة (Native Applications)، هناك بعض القيود الجوهرية على تطبيقات الويب منها:

- لا يمكن إجراء تكامل بين الخصائص الوظيفية الأصيلة للجهاز (مثل نظام تحديد المواقع، والكاميرا، إلخ) مع تطبيقات الويب كما هو الحال لدى استخدام التطبيقات الأصيلة.
- لا تزال إدارة جلسات الاستخدام (session management) تواجه صعوبات على عكس الأمر في التطبيقات الأصيلة.
- لا توفر تطبيقات الويب خصائص الاستخدام من غير اتصال بالإنترنت (offline) أو تخزين المعلومات.

3.3 التطبيقات الهجينة (Hybrid Applications)

للتغلب على مشكلة عدم إمكانية استفادة تطبيقات الويب الذكية من خصائص الأجهزة الذكية، يمكن اللجوء إلى التطبيقات الهجينة، وهي عبارة عن تطبيقات ويب ذكية تمت كتابتها باستخدام اللغات البرمجية القياسية (مثل جافا سكريبت وhtml5) ووضعت في قالب التطبيقات الأصيلة. ويجمع هذا في نواح كثيرة بين أفضل خصائص تطبيقات الويب الذكية والتطبيقات الأصيلة مثل: سهولة التطوير والاستخدام من غير الاتصال بالإنترنت (offline) والاستفادة من خواص الأجهزة الذكية.

3.4 كيف تختار المنهج المناسب؟

نورد في ما يأتي بعض الإرشادات والشروط التي تعتمد على طبيعة الخدمة، والتي يمكن أن تساعد في وضع إطار لاتخاذ القرار بشأن اختيار نوع التطبيق الأنسب للخدمات:

تحليل وفهم الجمهور المستهدف:

- تعرّف إلى المتطلبات الخاصة بالمستخدمين، وذلك عبر فهم الجمهور المستهدف وتحليل أنواع الأجهزة التي يفضلون استخدامها، والتوجهات الحديثة السائدة، إلخ. إذا كانت الفرصة متاحة، يمكن إجراء الآتي:
  - استبيانات أو استطلاعات رأي عبر الإنترنت بهدف فهم توقّعات الجمهور المستهدف.
  - الاطلاع على إحصاءات الإنترنت لمعرفة أنواع الأجهزة والمنصات التي يستخدمها العملاء للوصول إلى التطبيق الخاص بك.

تكاليف التطوير:

- إذا كانت التكلفة المالية وقلة الموراد الفنية من الأمور التي قد تعيق تطوير التطبيقات الذكية، ينصح باللجوء إلى تطبيقات الويب الذكية وليس التطبيقات الأصيلة؛ إذ إن التطبيقات الأصيلة تتطلب القيام بعملية تطوير منفصلة وتحتاج إلى كفاءات متخصصة بالتطوير لكل منصة على حدة.

التوافق مع منصات متعددة (Cross-compatibility):

- من الضروري أن تتوافق الخدمات الحكومية مع منصات متعددة، فبدلاً من تطوير تطبيقات متعددة لتوفير نفس الخدمة عبر منصات مختلفة، يمكن اللجوء إلى طريقة أكثر كفاءة عبر استخدام تطبيق ويب ذكي هجين للوصول إلى الجمهور.
- عند تطوير تطبيقات أصيلة، من المستحسن أن تستخدم جميع الجهات الحكومية إطار متعدد المنصات (مثل PhoneGap) وأدوات مثل (Titanium Appcelerator)؛ وذلك بهدف تخفيض التكاليف والجهود اللازمة لعملية التطوير.

دورة حياة (عمر) التطبيق:

- تعتبر دروة حياة التطبيق الأصيل قصيرة نسبياً. وإن كانت اللجنة المختصة باتخاذ القرار بشأن تحديد عمر التطبيق تفضل تطبيقات ذات عمر طويل، لا تمثل عندها التطبيقات الأصيلة دائماً الخيار الأفضل.

الاستفادة من خواص الجهاز:

- إذا كانت طبيعة الخدمة الذكية تتطلب تكاملاً مع الخواص الأصيلة للجهاز (مثل الكاميرا، ونظام تحديد الموقع الجغرافي)، فلا تستطيع تطبيقات الويب الذكية توفير ذلك. وهنا يمكن اللجوء إلى التطبيقات الأصيلة والهجينة إذ يمكنها الاستفادة من خواص الجهاز، وأجهزة الاستشعار (الحساسات) التي يوفرها.
- توفر التطبيقات الأصيلة تجربة أفضل للمستخدم في نواح كثيرة من خلال الاستفادة من الحركات الخاصة، والرسومات، والحسّاسات، وغيرها من الخواص التي يوفرها الجهاز.

الاعتبارات الأمنية:

- عند التطرق إلى مسألة الأمن، يمكن القول إن التطبيقات الأصيلة تنطوي على مخاطر معينة نظراً لخصائص تخزين المعلومات داخلها، فضلاً عن استخدامها للحسّاسات الخاصة بالجهاز. وفي حال فقدان الجهاز يمكن أن تسمح التطبيقات الأصيلة لأشخاص غير مخوّلين بالدخول إلى معلومات حسّاسة تم تخزينها على الجهاز، بينما يكون تخزين المعلومات آمناً في حالة تطبيقات الويب الذكية. إضافةً إلى ذلك، يمكن أن يسبب استخدام الخواص التي يوفرها الجهاز مشكلات تتعلق بالأمن، حيث يمكن لجهات دخيلة تتبع موقع الجهاز من خلال التطبيقات نفسها.

التكامل:

- عندما تحتاج التطبيقات الدخول إلى النظم أو قواعد البيانات القائمة يكون التكامل أمراً حتمياً. ويُعتبر التكامل إما أمراً مستحيلاً أو معقداً للغاية في حال استخدام التطبيقات الأصيلة، بخلاف تطبيقات الويب الذكية أو التطبيقات الهجينة التي يكون تكاملها مع المنصات القائمة أكثر سهولة.

الوصول إلى الخدمة والبحث عنها:

- إن كانت الغاية هي تمكين المستخدم من الوصول الفوري والسريع إلى التطبيق، عندئذ ينصح بتطبيقات الويب الذكية؛ إذ إن التطبيقات الأصيلة تحتاج لأن يقوم المستخدم بالبحث عنها وتنزيلها أولاً، بينما يمكن الدخول إلى تطبيقات الويب الذكية مباشرة من أي جهاز.
- تختلف عملية الوصول إلى التطبيق حسب نوعه، فتطبيقات الويب الذكية تظهر ضمن نتائج البحث، أما التطبيقات الأصيلة فيتم عرضها في متاجر التطبيقات فقط، ما يجعل تطبيقات الويب قادرة على الوصول إلى شريحة أكبر من المستخدمين مقارنة بالتطبيقات الأصيلة.

تجربة المستخدم:

- تعتبر التطبيقات الأصيلة البديل الذي يمكن استخدامه عندما يتطلب التطبيق تفاعلاً مع المستخدم؛ إذ إن خاصية اللمس وسهولة التنقل عبر الصفحات تساهم في جعل تجربة المستخدم أفضل وهو ما يصعب تحقيقه في حالة تطبيقات الويب الذكية.
- كما تتيح التطبيقات الأصيلة للمستخدم إمكانية تعديل الإعدادات لتخصيص التطبيقات بالشكل الذي يناسبه، وخاصة التطبيقات التي تستخدم بشكل منتظم. بمعنى آخر، توفر التطبيقات الأصيلة خدمة ذات طابع شخصي للمستخدمين.
- لا يشكل الدخول إلى خدمات تطبيقات الويب الذكية دون الاتصال بالشبكة أمراً مريحاً كما هو الحال في التطبيقات الأصيلة التي تستطيع تخزين البيانات داخل الجهاز من أجل استخدامها دون الاتصال بالشبكة؛ وهو ما يفضله المستخدم، حينما لا يكون الاتصال بالإنترنت متاحاً.

مقارنة تلخيصية لخيارات تقديم الخدمات الذكية			
	التطبيقات الأصيلة	**HTML5**	**التطبيقات الهجينة**
الرسومات	واجهات برمجة تطبيق أصيلة	HTML, Canvas, SVG	HTML, Canvas, SVG
الأداء	سريع	بطئ	بطئ

الشكل والانطباع العام	أصيل	محاكى (Emulated)	محاكى (Emulated)
التوزيع	متجر التطبيقات	الإنترنت	متجر التطبيقات
دورة حياة التطبيق	قصيرة	طويلة	طويلة
الدخول إلى الجهاز	ممكن	غير ممكن	ممكن
الإشعارات	ممكن	غير ممكن	ممكن
التخزين	ملفات محمية	SQL مشترك	نظام ملفات آمن ومشترك
التعرف إلى الموقع	نعم	نعم	نعم
الاتصال بالإنترنت	باتصال ومن دون اتصال	غالباً يتطلب اتصالاً	باتصال ومن دون اتصال
المهارات الفنية	ObjectiveC, Java	HTML5, CSS,	HTML5, CSS, Javascript

4 واجهات برمجة التطبيقات (APIs)

تستخدم واجهات برمجة التطبيقات (APIs) لجعل الخدمات الحكومية الذكية أو وظائفها متاحةً للاستخدام من قبل التطبيقات الأخرى. وبفضل الهواتف الذكية، تحل الخدمات الجديدة محل التطبيقات التقليدية وتطبيقات الويب.

يتم تطوير التطبيقات الجديدة بسرعة عن طريق مزج الخدمات والقدرات القائمة بطرق إبداعية، فلم يعد للتطبيق واجهة مستخدم واحدة، بل عدة واجهات. هذه الواجهات يمكن بناؤها باستخدام تقنيات مختلفة، لتستهدف أنواع مختلفة من المستخدمين، ويمكن أيضاً بناؤها من قبل عدة جهات مهتمة بالقيام بذلك. ومن أجل تمكين الواجهات المتعددة، أصبحت واجهة برمجة التطبيق (API) الواجهة الأساسية للتطبيقات سواء القديمة أو الجديدة. كما أصبحت واجهات برمجة التطبيق قناة التوزيع الجديدة للخدمات الحكومية.

يجب على الجهات الحكومية تبني هذا التوجّه الذي سيوفر للجمهور آلاف الخدمات الذكية التي يحتاجونها.

من خلال القدرة على تقديم الخواص الوظيفية الأساسية للعمل كواجهات برمجة للتطبيقات، تتحول الجهة الحكومية نفسها إلى منصة. وهنا لايكفي تقديم مجموعة من واجهات برمجة التطبيقات، بل يجب أن تكون تلك الواجهات موثوقة، وقابلة للتطوير وآمنة في آن معاً. يتحتم توفير واجهات برمجة التطبيقات تلك وفق مستويات من الأمن والجودة تتطابق مع مستويات تطبيقاتها الحكومية. ويتطلب تقديم واجهات برمجة التطبيقات الآمنة والقابلة للتطوير استخدام منصة مؤسسية لإدارة واجهة برمجة التطبيق (enterprise API management platform).

لتنفيذ واجهة برمجة تطبيق ناجحة، هناك بعض المسائل الأساسية التي يجب مراعاتها والتي تشكّل عوامل جوهرية للنجاح وتشمل: تطبيق المعايير القائمة، وتحقيق الانسجام بين مختلف واجهات برمجة التطبيقات الخاصة بالجهات الحكومية، والقدرة على إيجاد نظام مشترك صديق للبيئة ليقود عملية تطوير مبتكرة للتطبيقات.

ويتعين على الجهات الحكومية أن تقوم بما يأتي:

- تحديد برنامج واجهة برمجة التطبيق وتحديد الخدمات المشتركة بين الجهات الحكومية في دولة الإمارات العربية المتحدة والتي من شأنها أن تقود إلى تطبيق نظام متكامل صديق للبيئة.
- استخدام مجموعة مناسبة من المبرمجين (داخلي، شريك، جهة خارجية).

- بناء واجهات برمجة التطبيقات المناسبة لطبيعة عملها، وتحديد هيكل واجهات برمجة التطبيقات، وطلب المشورة بشأن بعض البيانات أو أنظمة المعلومات أو التطبيقات أو حتى البنى التحتية الممكن إتاحتها للجمهور، وكذلك تعريف مستويات الدخول إلى التطبيق وتحديد سياسات الاستخدام.
- تقييم الجدوى من استخدام الجهة الحكومية لمعيار التفويض المفتوح (OAuth) لتدعم مكانتها بصفتها تقدم بروتوكولاً مفتوحاً يسمح بتفويض آمن للعملاء للدخول إلى مصادر الخادم (server) بطريقة بسيطة وقياسية. ويجري اعتماد هذا المعيار في تطبيقات الإنترنت والأجهزة الذكية وأجهزة الحاسب المكتبية.
- تحديد أعلى معايير النجاح وآليات القياس من خلال رصد حركة واجهة برمجة التطبيق واستخدامه ومقارنة النتائج بالأهداف الموضوعة لذلك.
- إنشاء بوابة تطوير إلكترونية حديثة بهدف تسريع عملية اعتماد المستخدمين لواجهات برمجة التطبيقات التابعة للجهة الحكومية، إذ يساعد ذلك على جذب وتشغيل مطوِّرين خارجيين. ويجب أن توفر البوابة إمكانية التصفح والبحث عن واجهات برمجة تطبيقات محددة والدخول إلى الواجهة المطلوبة.
- التأكد من توافر مستندات توثيق تفاعلية لواجهة برمجة التطبيق على بوابة المطوِّرين تتيح لهم إنشاء مكالمات حية تتعلق بواجهة برمجة التطبيق.
- ينبغي أن تحتوي بوابة المطوِّرين على خدمة تسجيل ذاتية للمطوِّرين وإمكانية تسجيل الدخول وإدارة الحساب.
- إنشاء آلية لإرسال طلب إلى المطوِّرين من أجل تحديد المستخدمين والتطبيقات التي ستستخدم واجهة برمجة التطبيقات. على الهيئة الحكومية وضع وتنفيذ سياسات للسماح باستخدام واجهات برمجة التطبيقات.
- يجب إخطار المطوِّرين بالتغييرات التي تتم على واجهة برمجة التطبيقات. يمكن إنشاء قائمة بواجهات برمجة التطبيقات المفضَّلة من أجل متابعة واستلام الإخطارات حال حدوث أي أمر يمكن أن يؤثر عليها. قد تتعلق تلك الأمور بدورة حياة التطبيقات، مثل توافر نسخة حديثة من واجهة برمجة التطبيق.
- توفير أدوات التواصل الاجتماعي ومحتوياتها؛ مثل: المدوَّنات، ونماذج عن التطبيقات، ونموذج الرموز البرمجية، والمنتديات؛ بحيث تجعل كل ما هو جديد من الأفكار والتطبيقات والمخاطر والاقتراحات متاحة للمجتمع.
- إشراك المطوِّرين بالأمور المتعلقة بالدعم بما يشمل تقديم أفكار حول أنواع التطبيقات الممكن إنشاؤها مع واجهات برمجة التطبيقات، وماهية الجماهير المستهدفة لاستخدام التطبيقات.

5 واجهة المستخدم وسهولة الاستخدام

لا يتعلق تصميم التطبيق بالشكل الجمالي فقط، إنما يجب أن يراعي مسألتي السهولة والوضوح عند استخدامه. فالتصميم الذي يجعل من المستخدم محوراً له يهتم بجميع النواحي التفاعلية مع التطبيق بدءاً من تنزيله أو الدخول إليه وانتهاءً بإعداد الميزات الخاصة.
هناك عدد من النقاط الجوهرية التي ينبغي مراعاتها في ما يتعلق بسهولة الاستخدام وواجهة المستخدم:

حجم الخط

- ينبغي وضع حجم شاشة الجهاز الذي يعمل عليه المستخدم في الاعتبار عند تحديد حجم الخط المستخدم في النصوص، إذ إن شاشات الكثير من الأجهزة الذكية ليست كبيرة؛ لذا، لا ينبغي أن يكون حجم الخط كبيراً جداً. وفي الوقت ذاته، يؤدي تصغير حجم الخط بشكل كبير إلى مشكلة في قراءته. ومن هنا يتحتم إيجاد حل وسط يراعي تجربة المستخدم وخصائص الجهاز على حد سواء.

واجهة المستخدم:

- ينبغي التأكد من أن أزرار واجهة المستخدم تحمل دلالات واضحة على وظيفتها بما يؤدي المعنى المطلوب بالنسبة للمستخدم. فإن كان التطبيق يستخدم أزراراً معدَّلة غير الأزرار المتعارف عليها، عندها ينبغي أن تكون مصمَّمة بشكل يتيح للمستخدم معرفة وظيفتها وإلى أين ستأخذه.
- ينبغي أن يظهر شعار دولة الإمارات العربية المتحدة والشعار الخاص بالجهة الحكومية في جميع مراحل المعاملة وأن يتم عرضهما في المكان المناسب بما يتماشى مع المعايير المتّبعة في المراسلات الحكومية.
- يؤدي استخدام عدد كبير من الأزرار من دون داعٍ إلى تجربة تصفح غير مريحة بالنسبة للمستخدم، إذ ينبغي ترك مساحات كافية بين الأيقونات (الرموز) والروابط لتفادي الضَغط على الأيقونة أو الرابط غير المقصودين.

- عند التوجه لمستخدمي الهواتف الذكية، يجب مراعاة العامل البشري في التطبيق وتصميمه بحيث يكون مناسباً للاستخدام بيد واحدة.
- عند استخدام الرموز البصرية عوضاً عن النص، ينبغي الحرص على أن تكون منطقية بالنسبة للمستخدم، بحيث تكون الرسومات واضحة وتعبر عن الوظيفة المبتغاة منها بشكل تلقائي.
- العمل قدر المستطاع على تجنيب المستخدم التمرير إلى أسفل الصفحة (scrolling).
- كن وصفياً وموجِزاً ودقيقاً؛ خاصةً في ما يتعلق بشاشات عرض التنبيه.

دقة العرض

- ينبغي عند اختيار دقة الشاشة مراعاة حجم شاشة الجهاز الذكي وحجم المحتوى المعروض. عموماً، يُفضل استخدام دقة عالية ومحتوى أقل على الشاشة، ما يجعل الجهاز أكثر ملاءمة للمستخدم.

أمور يجب أخذها بالاعتبار في ما يتعلق بحجم التطبيق:

- إن كان التطبيق يحتوي على رسومات، ينبغي الحرص على جعل حجم تلك الرسومات محدوداً بحيث لا يستغرق تنزيلها وقتاً طويلاً ولا يستهلك أيضاً جزءاً كبيراً من البطارية. ورغم أن جودة الرسومات تؤدي إلى تجربة أفضل للمستخدم، إلا أن أداء التطبيق هو الأهم بالنسبة للمستخدم؛ فالتطبيقات الأنيقة والسريعة غالباً ما يتم تفضيلها على تلك البطيئة والتي تحتوي على كم كبير من الرسومات.
- يجب الحرص على ألا يكون حجم التطبيق كبيراً جداً لتفادي البطء في عملية التنزيل؛ فالمستخدم يفضل التطبيقات التي يمكن تنزيلها باستخدام أي من أنواع الاتصال بالإنترنت سواء أكان واي فاي (Wi-Fi) أو 2G أو 3G أو غيرها.
- ينصح بألا يزيد حجم التطبيق الأساسي عن 12-15 ميغا بايت، أما الخواص الأخرى فيمكن توفيرها كإضافات أو بيانات ضمن التطبيق يمكن تنزيلها اختيارياً لاحقاً، وذلك لتفادي استنفاد ذاكرة الجهاز في أمور غير ضرورية.
- إذا كان هناك ضرورة لاستخدام الصور ضمن التطبيقات، ينصح دائماً باستخدام النص البديل (ALT text) بحيث يؤدي مهمة الوصف لدى تعذر عرض الصورة بسبب صعوبات في التنزيل أو غير ذلك من مشكلات.

عمر البطارية:

- عند إعداد خصائص التطبيق، ينبغي مراعاة نسبة استهلاك البطارية والحرص على أن لا تؤثر تلك الخواص على عمر بطارية الجهاز المستخدم.

شروط الاستخدام:

- ينبغي أن تحتوي التطبيقات على صفحة لشروط وأحكام الاستخدام يسهل الوصول إليها بحيث تشرح بشكل واضح اتفاقيات الاستخدام وحقوق الملكية والاعتمادات. على المستخدم الموافقة على تلك الشروط والأحكام لدى الدخول إلى التطبيق مرة واحدة على الأقل. يمكن عرض اتفاقية شروط الاستخدام بعد تثبيت التطبيق لأول مرة، وعدم السماح للمستخدم بالدخول إلى التطبيق إلا بعد الموافقة على تلك الشروط.

اللغة الواضحة:

- ينبغي الحرص على أن تكون جميع المصطلحات الواردة في النصوص المستخدمة للتواصل واضحة ويمكن فهمها من قبل المستخدم، حيث يُنصح باختيار المفردات والمصطلحات بعناية وبعد دراسة متأنية، إذ إن استخدام الجمل المعقدة أو الكثير من المفردات غير المألوفة يؤثر سلباً على تجربة المستخدم.

التنقُّل داخل التطبيق (الملاحة):

- ينبغي تصميم الهيكل الداخلي للتطبيق بحيث يكون واضحاً وسهلاً وسهل التوقُّع من قبل المستخدم، وبما يتيح الدخول إلى كل خاصية وظيفية بسهولة تامة، والوصول إلى المحتوى المبتغى بأقل عدد ممكن من النقرات.
- الحرص على تقديم المعلومات على أساس هرمي متسلسل وفرزها بشكل يساعد على الوصول إلى المعلومات الأكثر أهمية بسهولة. يجب تعريف الغاية من وراء التطبيق بشكل واضح والتأكد من أن المستخدم سينجح في الوصول إلى الوظيفة المطلوبة عبر أقل عدد ممكن من الخطوات.

- ينبغي عرض الروابط المؤدية إلى خواص التطبيق الأساسية على الصفحة الرئيسية بما يسمح للمستخدم رؤية مجمل الخصائص الوظيفية له على الصفحة ذاتها. أما الصفحات الداخلية فيجب أن تحتوي على روابط ثانوية معروضة بشكل واضح حيثما دعت الحاجة.
- ينبغي أن تدل العناوين والروابط بشكل واضح على الغاية من الموضوع؛ حيث يتحتم أن تستخدم التطبيقات عناوين وروابط وصفية واضحة لكل جزء من المحتويات.
- ينبغي توفير أزرار ملاحية في كل صفحة يمكن أن يزورها المستخدم. وبالنظر إلى حجم الشاشة، من المستحسن عرض زرّي "الرجوع" و"الصفحة الرئيسية" فقط، وأن يتم التنقّل بين الصفحات عبر الصفحة الرئيسية فقط. يمكن أيضاً للروابط ذات الصلة بالمحتويات الداخلية مساعدة المستخدم على التنقّل بشكل أسهل ضمن التطبيق.
- ينبغي أن تكون أيقونات (رموز) وأزرار التنقل (الملاحة) مصممة بحجم (30 بيكسل) على الأقل، وأن تدل بشكل واضح عن المسار الذي سيذهب إليه المستخدم لدى النقر عليها.

التكامل مع خواص الجهاز:

- ينبغي الاستفادة من مميزات الجهاز إلى أقصى حد عند الضرورة، وخاصة في الحالات التي يكون فيها تفاعل المستخدم متاحاً.

الأداء:

- لا ينبغي أن يستغرق التشغيل الأولي للتطبيق وقتاً طويلاً، فتأجيل الوظائف التي تحتاج إلى معالجة كبيرة إلى ما بعد التشغيل الأولى يساهم في توفير تجربة أفضل للمستخدم.
- ينبغي أن يتمتع التطبيق بالقدرة على التحقق من الوسائل المتوفرة للاتصال بالإنترنت واستخدام الاتصال اللاسلكي كإعداد افتراضي في حال توفره. وعند وجود كم كبير من البيانات يجب إخطار المستخدم عندما يكون الاتصال بالإنترنت قائماً عبر وسائل الاتصال الذكية الواسعة المدى (2G أو 3G... إلخ).
- لدى الخروج من التطبيق، ينبغي أن يتمكن المستخدم من العودة إلى نفس الصفحة التي ترك عندها التطبيق دون الحاجة إلى تكرار الخطوات نفسها للوصول إلى الصفحة ذاتها.

توجيه المستخدم:

- ينبغي توفير زر "المساعدة" لتعريف المستخدم على كيفية استخدام التطبيق وتجنب عرض المعلومات حول التطبيق في الصفحة الرئيسية التي يصل إليها المستخدم.
- إتاحة الفرصة للمستخدم للبحث ضمن التطبيق حيثما دعت الحاجة، وتمكينه أيضاً من فرز نتائج البحث وتضييق نطاقه من أجل الحصول على نتائج دقيقة.
- الحرص على معرفة المستخدم لما يجري ضمن التطبيق أثناء إنجاز المهام حتى لا يظن أن التطبيق قد توقف عن العمل.

الاستخدام دون الاتصال بالإنترنت (offline):

- ينبغي إتاحة إمكانية حفظ جولات الاستخدام، أو الاستفادة من المحتويات في حال العمل دون الاتصال بالإنترنت حيثما كان ذلك ممكناً.

6 المحتوى الذكي

يعد المحتوى جوهر استخدام أي خدمة ذكية. ويمكن أن يصل المحتوى للمستخدم في صورة نصوص، أو صور، أو مقاطع فيديو، أو خدمات صوتية، أو خرائط، وغير ذلك من وسائل. ولتعزيز تجربة المستخدم وتقديم الخدمات المطلوبة للجمهور عبر واجهة سلسة ومريحة، ينبغي تصميم عملية تفاعل المستخدم مع محتوى التطبيق بعناية فائقة.

سهولة الوصول إلى المحتوى المطلوب:

- ينبغي الحرص على أن يكون المحتوى بصيغة تتناسب مع الأجهزة الذكية، لمساعدة المستخدمين على العثور على المعلومات المفيدة بنظرة سريعة.
- اجعل التحكم في كيفية عرض المحتوى بيد المستخدم قدر الإمكان، ولا تعرض تفاصيل غير ضرورية. اسمح للمستخدم بالحصول على محتوى أكثر تفصيلاً فقط عندما يرغب في ذلك.

- احرص دائماً على تصميم بنية المحتوى لتناسب المستخدم غير الصبور، فمستخدمو الأجهزة الذكية في العادة يرغبون في الوصول إلى المحتوى المطلوب بسرعة، وتعمل التفاصيل غير اللازمة على تشتيت انتباههم.

تنظيم عملية تفاعل المستخدم مع المحتوى:

- اسمح للمستخدم، كلما كان ذلك ممكناً، أن يضيف المحتوى لقائمة "المفضلة"، أو أن ينظم المحتوى في مجلدات يحددها هو لاستخدامها لاحقاً.
- يزور المستخدم التطبيق لغرض معين، لذا، يجب وضع هدف المستخدم في الاعتبار، وتوفير الأدوات والمعلومات اللازمة وجعل تحقيقه سهلاً خطوة بخطوة إذا لزم الأمر. اجعل المستخدم على دراية بالخطوة التالية في كافة مراحل التفاعل بين المستخدم والمحتوى.
- تأكد من أن يتيح المحتوى التفاعل مع المستخدم كلما كان ذلك مناسباً وممكناً، إذ قد تتطلب بعض الخدمات أن يختار المستخدم الكيفية التي يود تخزين المعلومات وفقها، أو أن يبدي رأيه في المحتوى، أو أن يخصصه ويشاركه.
- اجعل من الممكن مشاركة المحتوى المعلوماتي عبر شبكات التواصل الاجتماعي أو البريد الإلكتروني ضمن التطبيق نفسه من دون مغادرة الشاشة، وشجع المستخدم على القيام بذلك.

هيكلة المحتوى وتنوعه:

- استفد من الروابط الداخلية (inbound links) ضمن محتوى التطبيق، وذلك لتوفير وصول سلس للمعلومات الخاصة بكل فئة.
- قدم للمستخدم محتوى إضافياً زيادة عن الاستخدام الأساسي للتطبيق. المكافآت غير المتوقعة داخل التطبيق تزيد من تفاعل المستخدمين وكذلك درجة رضاهم.
- قم بتحديث التطبيق بشكل منتظم، وكذلك عند حدوث أي تغيير في المعلومات. راجع ملاءَمة المحتوى للاستخدام الحالي بشكل دوري، وقم بحذف المحتوى عند انتهاء صلاحيته.
- عندما لا تكون البساطة هي الهاجس الأكبر، وفر للمستخدم محتوى متنوعاً متوازناً يضم الفيديو، والخرائط، والنصوص، والصور.
- ادرس مسألة توفير المحتوى بلغات أخرى اعتماداً على الجمهور المستهدف، وقم بتوفير المحتوى باللغة الإنجليزية حيثما كان ذلك ضرورياً.

7 استخدام الجمهور للخدمات الذكية

لا تنتهي مهمة الجهة الحكومية عند تحويل خدماتها إلى خدمات ذكية، ففي بعض الحالات، قد يكون تشجيع الجمهور وموظفي الجهة الحكومية على استخدام تلك الخدمات الذكية هو التحدي الأكبر. ويُعتبر إشراك المواطنين في تصميم الخدمات الذكية، ورفع الوعي والتشجيع على تبني تلك الخدمات من المهام الجوهرية للجهات الحكومية. وفي هذا السياق يمكن القيام بالخطوات الآتية:

- استطلاع آراء الجمهور واقتراحاتهم عبر الاستبيانات واستطلاعات الرأي الإلكترونية حول أكثر الخدمات الذكية التي يمكن أن يستفيدوا منها.
- تحليل الجمهور المستهدف عبر استطلاعات الرأي والاستبيانات، وبشكل خاص من حيث كيفية استخدامهم للتقنيات الذكية، والأجهزة وأنظمة التشغيل التي يستخدمونها، الخ.
- طرح الخدمات الذكية المرغوبة عبر أكثر من قناة لضمان وصولها إلى أكبر شريحة (على سبيل المثال، يمكن توفير نفس الخدمة عبر الرسائل النصية القصيرة والتطبيقات الذكية، وإتاحة المجال أمام المستخدمين لاختيار القناة التي تناسبهم للحصول عليها).
- الإعلان عن الخدمات الذكية الجديدة عبر الموقع الإلكتروني للجهة الحكومية، والمواقع الإلكترونية الأخرى، وكذلك في المكاتب الحكومية التي يزورها الجمهور بشكل متكرر.
- الاستفادة من قنوات التواصل الاجتماعي ووسائل الإعلام الجماهيري لرفع مستوى الوعي بالخدمات المقدمة.
- يفضل أن تقدم الجهات الحكومية حوافز لمستخدمي خدمات الحكومة الذكية بهدف رفع نسبة تبني الجمهور لهذه الخدمات.

8 أمن الخدمات الذكية

8.1 التدابير الأمنية المتعلقة بالمستخدم

عند توفير الخدمات الذكية للجمهور، لا يجب إغفال أي من المخاطر الأمنية سواء المتعلقة بالمؤسسة أو بالمستخدم، فعند تطوير الخدمات الذكية، يجب الأخذ في الاعتبار أمور الخصوصية والأمن المتعلقة بمشاركة معلومات حساسة أثناء استخدام تلك الخدمات. وفي ما يتعلق بالمستخدم، يجب على مقدم الخدمة (الجهة الحكومية، على سبيل المثال) ضمان الاستخدام الآمن للخدمة من قبل الجمهور.

اعتماد الخدمات الذكية:

- يجب الإعلان عن الخدمات الذكية التي يتم تنفيذها في دليل التطبيقات الحكومية (http://government.ae/ar/web/guest/mobile-government). كما يجب أن يتمكن الجمهور/المستخدمون من التأكد أن الخدمة الذكية التي يستخدمونها معتمدة من قبل الحكومة وذلك عبر الدليل نفسه.
- يجب تحذير الجمهور من الخدمات الذكية غير المعتمدة والتي ترسل طلبات مزعجة إلى المستخدمين، ويجب تشجيعهم على استخدم التطبيقات الحكومية والخدمات الذكية المعتمدة فقط.
- من المستحسن وضع شعار حكومة الدولة في كل خدمة حكومية ذكية يتم توفيرها للجمهور.

الاختبارات:

- على الجهات الحكومية إجراء اختبارات الأداء وسهولة الاستخدام قبل طرح الخدمات الذكية للجمهور.
- سيوفر مركز ابتكار الحكومة الذكية في المستقبل مجموعة من الخدمات ستشمل مختبراً للحكومة الذكية يتم فيه إجراء الاختبارات المختلفة (مثل الأمن، وسهولة الاستخدام، والكفاءة، الخ) لضمان أن تتوافق هذه الخدمات مع المعايير الحكومية المقبولة.
- سيتم توفير المزيد من المعلومات حول مركز ابتكار الحكومة الذكية في الوقت المناسب.

تسجيل المستخدمين:

- تبعاً لسياق التطبيق أو الخدمة الذكية، يجب اللجوء إلى اعتماد آلية المصادقة على المستخدم عندما يتطلب الأمر، وعلى الجهات تحديد نوع المصادقة الأنسب لخدماتها:
  - شريحة الهاتف المتحرك (SIM)
  - المصادقة ثنائية الاتجاه (Two Way Authentication)
  - المصادقة الرقمية
- يجب على الجهات الحكومية التواصل مع هيئة الإمارات للهوية لكافة الأمور المتعلقة بتسجيل المستخدمين

تسجيل الأجهزة وأمنها:

- يجب التحقق من تسجيل الأجهزة لضمان أن يتم استخدام الخدمة عن طريق جهاز مسجل عن طريق هيئة الإمارات للهوية.
- يجب وضع خطوات واضحة لشطب الأجهزة وإعلان تلك الخطوات للمستخدمين لضمان أمنهم في حالة فقدان أو سرقة الأجهزة الخاصة بهم.
- عندما يقوم المستخدم بتنزيل التطبيقات الحكومية الذكية، يجب أن يتوافق الجهاز المستخدم مع الشروط الأمنية التالية، وذلك حسب نظام التشغيل المستخدم:
  - الأجهزة التي تعمل بنظام تشغيل **iOS**: يجب ألا يكون قد تم كسر حمايتها (**jailbroken**).
  - الأجهزة التي تعمل بنظام أندرويد: يجب أن يكون قد تم تثبيت برنامج مضاد للفيروسات عليها وأن يتم تحديثه.
  - هواتف ويندوز يجب أن يكون قد تم تثبيت برنامج مضاد للفيروسات عليها وأن يتم تحديثه بشكل مستمر.
- لمزيد من المعلومات حول تسجيل/شطب الأجهزة، يرجى التواصل مع هيئة الإمارات للهوية.

8.2 إرشادات الأمن الخاصة بتشفير التطبيقات الذكية:

يجب أخذ العديد من المسائل بعين الاعتبار عند تطوير التطبيقات الذكية مثل: خصائص الاستخدام، ووجود بيانات حساسة، ومشاركة المعلومات الخاصة. وينبغي اتخاذ التدابير الأمنية في هذا الخصوص ابتداءً من مرحلة التطوير تبعاً لمستوى الأمن اللازم لكل حالة على حدة. وتستعرض الإرشادات أدناه عدداً من القضايا الشائكة المتعلقة بالأمن عند تطوير التطبيقات الذكية.

حماية البيانات الحساسة:

- تأكد من تصنيف البيانات المخزنة وفقاً لدرجة حساسيتها، وقم باتخاذ التدابير الأمنية طبقاً لذلك. نفذ عمليات معالجة وتخزين البيانات وفقاً لتلك التصنيفات.
- قم بتخزين البيانات الحساسة على الخادم (server) بدلاً من تخزينها على جهاز العميل، كلما كان ذلك ممكناً. إذا كان من الضروري تخزين البيانات على جهاز العميل، استخدم واجهة التطبيق البرمجية (API) لتشفير الملفات والتي يوفرها نظام التشغيل، أو عبر مصدر موثوق آخر.
- يجب التأكد دائماً من تشفير البيانات الحساسة المخزنة، وكذلك البيانات في ذاكرة التخزين المؤقت (cached).
- في بعض الحالات، يمكن وضع القيود حول البيانات كإجراء احترازي (الاستخدام في موقع جغرافي مختلف على سبيل المثال).
- لدواعي الأمان، اكشف عن الحد الأدنى من البيانات للمستخدم؛ أي قم بتحديد البيانات التي ستكون ذات فائدة للمستخدم، واحجب بقية البيانات.

التعامل مع كلمات المرور:

- عندما يتطلب الأمر تخزين كلمات المرور في الجهاز، تأكد دائماً من أن أنظمة التشغيل تعمل على تشفير كلمات المرور ورموز إعطاء الإذن بالاستخدام (Authorization tokens).
- لا تستخدم أجهزة تقوم بتخزين كلمات المرور من دون تشفيرها.
- إذا كانت الأجهزة تستخدم العناصر الآمنة (secure elements)، تأكد من أن يستفيد التطبيق من هذه العناصر الآمنة لتخزين كلمات المرور ورموز إعطاء الإذن بالاستخدام.
- تأكد من توفير إمكانية تغيير كلمات المرور.
- تأكد من عدم إمكانية الوصول إلى كلمات المرور عن طريق السجلات أو الملفات في ذاكرة التخزين المؤقت.
- لا تسمح للتطبيق بتخزين كلمات المرور في الواجهة الثنائية للتطبيق (application binary)

حماية البيانات أثناء نقلها:

- افترض دائماً عدم أمان طبقة الشبكات، وعلى هذا الأساس، اتخذ الاحتياطات اللازمة.
- عندما يقوم تطبيق معين بإرسال بيانات حساسة سلكياً أو لاسلكياً، اجعل استخدام قناة آمنة لنقل البيانات بين طرفين (SSL/TLS) شرطاً لازماً.
- استخدم لوغاريتمات تشفير قوية ومفاتيح طويلة.
- تأكد من أن واجهة المستخدم توضح للمستخدم ما إذا كانت الشهادات المستخدمة صالحة أم لا.

المصادقة على المستخدمين وإدارة الاستخدام:

- ساعد المستخدم على اختيار كلمة مرور آمنة مناسبة (على سبيل المثال، طول الكلمة، استخدام الأحرف الكبيرة والصغيرة، والرموز، والأرقام، الخ)
- استخدم المصادقة الثنائية عبر الرسائل النصية القصيرة والبريد الإلكتروني، إذا كان ذلك مناسباً.
- إذا دعت الحاجة، استخدم بيانات البيئة المحيطة لإضافة مستوى آخر من المصادقة (الموقع الجغرافي على سبيل المثال).
- في حالة البيانات الحساسة للغاية، اطلب مستوى آخر من المصادقة وفقاً للخدمة (مثل البصمة، الصوت، الخ).
- استخدم بروتوكولات الأمن المناسبة لإدارة الاستخدام بعد المصادقة الأولية.
- اختر بطاقات تعريف لجلسات الاستخدام تتمتع بدرجة عالية من العشوائية (entropy) لتجنب القدرة على التخمين.

امنع الوصول غير المصرح به للمصادر المستخدمة في عمليات الدفع المالي (المحفظة الذكية، الرسائل النصية القصيرة، الخ):

- تحقق من سلوكيات الاستخدام غير الطبيعية واطلب مصادقة ثانوية عندما يتم رصد ممارسات غير معتادة (مثل تغيير الموقع الجغرافي، الخ).
- احتفظ بسجلات الوصول إلى الخدمات المدفوعة واجعلها متاحة للمستخدم فقط بعد المصادقة.

8.3 سرقة الهوية وحماية الخصوصية

أحد أكبر التحديات التي تواجه الحوسبة الذكية هي ضمان خصوصية وأمن المستخدم. وتساعد سهولة حركة الأجهزة الذكية التي تستخدم معلومات شخصية بشكل متزايد على أن تكون عرضة لسرقة الهوية عن طريق فقدان أو سرقة الجهاز. يتطلب تطوير الخدمات الذكية اتخاذ تدابير أمنية مشددة ضد التهديدات المحتملة لسرقة الهوية واختراق الخصوصية. وفي ما يأتي إرشادات معينة تتعلق بمشاكل إدارة الهوية، بعضها تمت مناقشتها سابقاً تحت بند "أمن التطبيقات" ولكنها بحاجة إلى إعادة التأكيد عليها في ما يخص المخاوف المتعلقة بالخصوصية.

- اجعل سياسة الخصوصية الخاصة بالتطبيق متاحة للمستخدمين على منصة التطبيق لكي تساعدهم على التعرف إلى القضايا ذات الصلة، وكذلك لتوفير سياسة خصوصية واضحة ضمن التطبيق.
- حذِّر المستخدمين بشكل واضح في ما يتعلق بممارسات البيانات التي تحدث ضمن التطبيق والتي تتضمن بيانات حساسة.
- امنع جمع التطبيق لبيانات المستخدم الشخصية ما عدا البيانات المطلوبة للخدمة التي يجري استخدامها.
- اسمح للمستخدمين بتغيير إعدادات الخصوصية ضمن التطبيق وعرفهم بالعواقب المحتملة جراء استخدام إعدادات معينة. كما يجب التأكد من وجود قيود على الإعدادات الافتراضية في ما يتعلق باستخدام المعلومات الخاصة.
- استخدم طرق تشفير معقدة لتخزين ونقل المعلومات الحساسة.
- تأكد من أن يتمكن المستخدم من الوصول إلى ضوابط الخصوصية وإعدادات كلمات المرور بسهولة ووضوح. اسمح للمستخدم بتغيير كلمة المرور الخاصة به ووفر له وسائل آمنة لتغيير كلمة المرور عند نسيانها.
- عندما تقوم هيئة الإمارات للهوية بتطبيق نظام الهوية الذكية، تأكد من قدرة التطبيق الخاص بك من التكامل مع خدمات المصادقة التي توفرها الهيئة حيثما ينطبق ذلك.
- يرجى ملاحظة أن الجهة الحكومية مسؤولة عن الامتثال لقوانين الخصوصية في الدولة ويجب عليها أن تتأكد من التزام كافة إصدارات التطبيق بهذه القوانين. قم بتعيين شخص أو قسم لمتابعة أحدث القوانين والتحقق من امتثال كل إصدار لهذه القوانين.

8.4 اختبارات الأمن

عند تصميم الخدمات الذكية، يجب على المطوِّرين فهم مجالات استخدام هذه الخدمات وإخضاع التطبيق أو الخدمة الذكية للعديد من الاختبارات لضمان الاستخدام الآمن. وعلى الجهات الحكومية أن تكون على دراية بالمخاطر المحتملة وأن تتحقق من نقاط الضعف في الخدمة الذكية وتعمل على اتخاذ التدابير الوقائية للتقليل من آثار هذه التهديدات. وفيما يأتي بعض الخطوات الممنهجة التي يمكن اتخاذها لتقييم المخاطر الأمنية:

تحليل الاستخدام والمخاطر:

- قم بالتنقل عبر التطبيق لتحليل الوظائف الأساسية وطريقة العمل فيه. قم بتحديد واجهات الشبكات التي يستخدمها التطبيق، وحدد البروتوكولات ومعايير الأمن التي يستخدمها.
- حدد خواص الجهاز الذي يمكن أن يستخدمها التطبيق وفرص القرصنة المحتملة لها (مثل الكاميرا، تحديد المواقع، الخ)
- تحقق من الكيفية التي يؤمن بها التطبيق معلومات الدفع إذا كان يوفر هذه الخاصية.
- حدد التطبيقات الأخرى التي تتفاعل معها الخدمة الذكية، وحدد التطبيقات التي قد تضر بمعايير السلامة والخصوصية.
- تأكد من تحليل الشيفرة المصدرية (source code) للتطبيق وذلك لتحديد مواطن الضعف فيها
- تحقق من الكيفية التي تتم بها عملية المصادقة على المستخدم في التطبيق، وحدد المخاطر المحتملة.
- قم بتحليل عملية تخزين البيانات ضمن التطبيق. راجع الخوارزميات المستخدمة في التشفير وإذا ما كانت عرضة لمشكلات معروفة.
- تحقق من نوع البيانات التي يتم تخزينها في الذاكرة المؤقتة، وإذا ما كان يتم تخزين معلومات حساسة في تلك الذاكرة.

- اختبر التطبيق ضد هجمات "اختراق المحادثات" الذي يتسلل فيه المهاجم بين متحاورين في شبكة دون علم أيّ منهما (man-in-the-middle) لتحليل التدخلات المحتملة في التطبيق.
- تحقق إذا كانت البيانات الحساسة يتم تسريبها لملفات السجلات (log files).
- تأكد من الحفاظ على الأمن من جهة الخوادم وليس من جهة العميل فقط.

8.5 المخاطر الأمنية العالية

كما يتغلب الاتصال عبر الأجهزة الذكية على كافة العوائق المكانية ليبقى المستخدم على اتصال في أي وقت ومن أي مكان، أصبحت عملية نقل البيانات والوصول إليها واسعة الانتشار لتغطي هي كذلك كافة الأماكن. تتواصل الأجهزة الذكية عبر شبكات الهاتف المتحرك، والواي فاي، وأنظمة تحديد المواقع الجغرافية (GPS)، وتقنيات التواصل قريب المدى (NFC)، والبلوتوث، وغيرها. إلا أن هذه الشبكات لا توفر دائماً الأمن المطلوب؛ فمن الشائع جداً أن يستخدم العاملون الميدانيون هذه الشبكات غير الآمنة خارج أماكن العمل الفعلية للوصول إلى وثائق أو تطبيقات استراتيجية. لذا، أصبح الحفاظ على سرية وسلامة وصحة البيانات في مثل هذه الشبكات من الضرورات الأساسية.

سرية البيانات:

تشير "السرية" إلى الطريق الآمن الذي يتم من خلاله نقل البيانات للمستخدم المقصود وليس إلى أطراف أخرى دخيلة. السلامة هي إحدى معايير الأمن للتأكد من عدم إجراء أي تغييرات على البيانات أثناء نقلها. أما "المصادقة"، فيتم التأكد عن طريقها من أن المرسل هو الطرف الموثوق به الذي يقوم بإرسال البيانات. تشير السرية إلى عملية منع الوصول إلى المعلومات من قبل أي شخص بخلاف الطرف المقصود. ويتم توفير السرية إما عن طريق تشفير البيانات أو إرسال البيانات عبر قنوات مشفرة.

سلامة البيانات:

تمكِّن سلامة البيانات المستلم من أن يكتشف إذا ما تم تعديل الرسالة بواسطة طرف آخر أثناء عملية النقل، وتسمح عملية المصادقة للمستلم أن يحدد المرسل وأن يثق أن المرسل هو بالفعل من أرسلها. أمن البيانات وسلامتها أمران مهمان جداً في عملية النقل اللاسلكي، حيث يمكن بسهولة لأي شخص في محيط الشبكة اللاسلكية، اعتراض البيانات، وتعريضها للخطر.

تتضمن عملية السلامة التحقق من مصداقية البيانات عبر اتخاذ تدابير وقائية. وتحل عملية التشفير المشكلة لدى كل من المرسل والمستقبل عبر التحقق من صحة فك التشفير خلال عمليات الإرسال، والنقل، والتمييز.

المصادقة:

بهدف ضمان أمن عملية المصادقة، ينبغي أن تكون الأجهزة نفسها قادرة على إجراء عمليات المصادقة لأنظمة الشبكات، وأن تكون الخوادم، بدورها، قادرة على مصادقة أنفسها في الأجهزة. ويتم تمكين عملية المصادقة عبر نظام تشفير مشترك.

كانت عمليات الحماية للموظفين الحكوميين الذين يعملون على أجهزة الحاسب الآلي تتم عبر أنظمة أمن الجدران النارية (firewalls)، إلا أنه مع زيادة عدد الموظفين الذين يحملون الأجهزة الذكية، يجب تعزيز عملية أمن الشبكات لتمتد إلى الخدمات الذكية وألا تقتصر على شبكات المكاتب. ونظراً لاحتمال استخدام الأجهزة الذكية خارج نطاق جدران الحماية في المكاتب، يتعين على إداريي الشبكات تأمين نقل البيانات عبر السماح لعناوين بروتوكول الإنترنت (IP) الآمنة فقط من الوصول إلى البرامج والمعلومات. يجب إجراء تعديلات معينة على أي اتصالات واردة أو صادرة. وفي بعض الحالات، السماح بالاتصالات الصادرة فقط قد يقلل من المخاطر؛ حيث ستتعرف الشبكة على عنوان بروتوكول الإنترنت. وهكذا، فإن خدمات الإشعار (push services) أكثر أماناً من خدمات الاستعلام عبر الأجهزة الذكية حيث أنها لا تحتاج إلى منح حق الوصول لقاعدة البيانات الحساسة.

قد تساعد تجزئة بنية الشبكة داخل مكان العمل في تحسين أمن البيانات طالما استطاع كل قطاع أن يوفر مستوى من الحماية عبر جدران الحماية الخاصة به. ويساعد استخدام الشبكات المتعددة على تمكين قطاعات مختلفة من التدابير الأمنية، ليتم توفير حماية خاصة بالتطبيق ضد التهديدات المحتملة.

8.6 المخاطر على مستوى المؤسسة وتدابير أمن الخدمات الذكية

هناك العديد من الطرق لتنفيذ سياسة أمنية لاسلكية على مستوى المؤسسة ككل، وذلك اعتماداً على طبيعة التقنية المستخدمة. في معظم الحالات، يساعد اتباع تدابير أمنية أساسية معينة إلى توفير الأمن الكافي ضد محاولات اختراق البيانات. لذا، يجب توضيح التدابير الأمنية للموظفين بشكل جيد حتى لا تتسبب أية نقاط ضعف في خلق مشكلات في حالات الاستخدام غير الآمن للنظام. إضافة إلى ذلك، يتعين في معظم الحالات وضع آلية للرصد أو للحد من الاستخدام لمنع أية مشكلات محتملة تتعلق بالأمن.

من المهم أن يحدد المسؤولون - وليس مستخدمو الأجهزة الذكية - الكيفية التي يتم بها استخدام البيانات التي يتم نقلها. يتعين على مسؤولي تقنية المعلومات السيطرة التامة على عملية الوصول إلى المتغيرات (parameters)، والبيانات الحساسة، والكيفية التي يتم بها نقل البيانات. توضح الإرشادات التالية آليات تقييم لبعض المخاطر العامة وسبل الوقاية منها:

- حدد المعلومات التي تتوافر لمستخدمين محددين ونوع البيانات المسموح بنشرها وتداولها في الشبكات الرسمية للجهة الحكومية.
- تأكد من وجود بنية تحتية كافية في الجهة الحكومية لتنفيذ السياسات الأمنية ذات الصلة. حدد التقنيات والمهارات المطلوبة للأمن بشكل عام وخطط مسبقاً لسيناريوهات حالات الاستخدام.
- حدد سيناريوهات حالات الاستخدام لسير العمل العام في ما يتعلق باستخدام كل من التطبيق والجهاز. ابحث مسألة حصول المستخدم والجهاز على إذن قبل الوصول إلى كل من مستويات أمن البيانات وقم بتوثيق ذلك لأغراض التدريب الداخلي للموظفين.
- وثق سيناريوهات استخدام مختلفة يتم تحديثها بشكل منتظم. قم بتغطية المخاطر المحتملة، وطرق التخفيف من المخاطر، وأفضل الممارسات لكل سيناريو واجعلها متاحة للمستخدمين.
- قم بتحديد التحذيرات الأمنية المتعلقة بالأداء والكفاءة على مستوى المؤسسة ككل. قم بتقييم المخاطر على أساس هرمي ووثق آليات الحماية على هذا الأساس، من دون التسبب في مقاطعة تنفيذ المهام بشكل كبير، حيث لا يجب توفير الأمن على حساب الكفاءة وسهولة الاستخدام.
- تأكد من وجود سجلات للقضايا الأمنية التي يتم مواجهتها وأن يتم تصنيفها وفقاً لنوع الجهاز ونظام التشغيل المستخدم. وفِّر هذه السجلات للفنيين لتحديد المخاطر والتهديدات الغريبة للرجوع إليها مستقبلاً.
- وفر تدريبات منتظمة في المسائل المتعلقة بالأمن التي يواجهها الموظفون وكذلك التهديدات التي تواجه الأجهزة، لإبقاء المستخدمين على اطلاع بالمستجدات المتعلقة بالتهديدات والمخاطر.
- تأكد من وجود مراقبة مستمرة للتغييرات في البنية التحتية على مستوى المؤسسة ككل وقم بتحديث السياسات والممارسات الأمنية وفقاً لتلك التغييرات.

8.6.1 المخاطر والتحذيرات المتعلقة بالتطبيقات والبرامج

تستخدم الأجهزة الذكية أنواعاً متعددة من التطبيقات، والبرامج الأصيلة أو الخاصة بالأنظمة. من حين لآخر، تطلب هذه التطبيقات والبرامج إجراء تحديثات أو تنزيل برامج من أجل إضافة وظائف جديدة لها كما هو الحال في الهواتف الذكية والأجهزة اللوحية. ولكن، قد تحتوي هذه البرامج والتطبيقات على نقاط ضعف أو شيفرات خبيثة. وهناك العديد من المخاطر المتعلقة بالبرامج والتطبيقات يمكن سردها على النحو التالي:

تهديدات من التطبيقات، والشيفرات البرمجية، وأنظمة التشغيل

قد تحتوي البرامج المثبتة على الأجهزة الذكية على شيفرات معينة تمت كتباتها لتقوم بإجراءات غير مصرح بها. ويمكن أن تخترق هذه الشيفرات الأجهزة عن طريق البرامج التي يتم تحديثها أو تثبيتها، أو التطبيقات التي يتم تنزيلها، أو الرسائل الفورية، أو البريد الإلكتروني. وقد تتعارض هذه الشيفرات مع التشغيل العادي للجهاز أو تتسبب في مخاطر تتمثل في سرقة أو فقدان البيانات. أنظمة التشغيل كذلك عرضة لمخاطر مشابهة، إلا أنها قد تتسبب في مشكلات أكبر نظراً لأن تأثيرها وقدرتها على الجهاز والبيانات أكبر بكثير من تأثير التطبيقات.

لذا، من الضروري اتخاذ خطوات وقائية ضد المخاطر المحتملة للبرامج وأنظمة التشغيل منها:

- يتعين على المؤسسات اختيار أجهزة وأنظمة تشغيل ذات حماية عالية جداً. تحديث هذه الأجهزة قد يساعد على أن يكون النظام أكثر أمناً بسبب الحماية الجديدة التي يتم توفيرها ضد التهديدات المحتملة الحديثة التي يتم اكتشافها. ينبغي مقارنة الإصدارات المختلفة لأمن أنظمة التشغيل لاختيار أكثرها أمناً.
- ينبغي توفير التدريب المناسب لمستخدمي الأجهزة على التهديدات المحتملة وفرض قيود معينة لمنع تثبيت وتنزيل برامج غير مصرح بها.

- ينبغي استخدام جدران الحماية طالما أنها لا تتسبب في إعاقة الأداء بشكل كبير. هذه الجدران يمكنها كشف البرمجيات الخبثية في الحال واتخاذ الإجراءات الوقائية اللازمة حيالها.
- يجب جدولة إجراء مسح ضد الفيروسات (virus scan) بشكل دوري من دون التدخل في مهام المستخدم.
- يجب تقييد ومراقبة استخدام وتثبيت البرامج والتطبيقات وفقاً للسياسات والإجراءات الخاصة بالمؤسسة.
- ينبغي تنشيط جدران الحماية الداخلية في الأجهزة عند توصيلها في الشبكات على مستوى المؤسسة ككل.
- ينبغي التحكم في الأجهزة الذكية مركزياً حتى يمكن ضبط إعدادات الأجهزة على مستوى المؤسسة ككل، وكذلك لإدارة البيانات، واستعادتها أو مسحها عن بعد.
- يجب اتخاذ الاحتياطات في حالة حدوث خلل في نظام التشغيل مثل كسر الحماية (jailbreaking). في حالة رصد أجهزة تتعرض للخطر، يجب منع وصول تلك الأجهزة للبيانات والشبكات، وتنبيه المستخدمين.
- يجب توزيع قائمة بيضاء داخل المؤسسة بالتطبيقات والبرامج الآمنة والمناسبة ويتم فرضها مركزياً على جميع الأجهزة. وينبغي مراجعة هذه القوائم بشكل منتظم لإضافة برامج وتطبيقات جديدة أو حذف عناصر منها.

تهديدات عبر الإنترنت:

عندما تتصل الأجهزة بشبكة الإنترنت، قد تصل إليها شيفرات خبيثة عبر تطبيقات HTML، أو جافا سكريبت، أو فلاش، أو مصادر أخرى عن طريق صفحات الويب التي يتم زيارتها. كما قد يتسبب ضعف المتصفحات في تعريض الأجهزة لخطر شيفرات خارجية. وهنا، يمكن اتخاذ الإجراءات الوقائية على النحو الآتي:

- يمكن تجنب دخول المستخدمين إلى مواقع غير موثوقة عن طريق استخدام فحوصات أو شهادات أمنية على مستوى المؤسسة ككل. يمكن كذلك للمستخدمين استعمال مخدمات الويب الفرعية (web proxies) للاستفادة من المرشحات (filters) وجدران الحماية الخاصة بالمؤسسة في الأجهزة الخاصة بهم.
- استخدام الإصدارات الحديثة من متصفحات الويب يوفر درجة أمان أكبر. يجب تعديل الإعدادات لتتناسب مع سياسات الأمن في المؤسسة. يجب التأكد من عدم الدخول إلى المواقع الإلكترونية الرسمية إلا عبر وسائل اتصال آمنة.
- تنفيذ سياسات تهدف إلى تقييد أو تعطيل الوصول إلى شيفرات معينة مثل جافا سكريبت، والسماح فقط لمحتوى المواقع الآمنة والمواقع المتضمنة في القائمة البيضاء من تفعيل شيفرات معينة.
- في الحالات التي توجد بها مخاطر عالية وبيانات حسّاسة للغاية، يمكن اتخاذ إجراءات صارمة طالما أنها لا تتسبب في تعطيل الأداء، مثل إيقاف تشغيل جافا سكريبت عند زيارة المواقع غير الرسمية، والتحقق من شهادات الموقع في كل صفحة يتم زيارتها، وإيقاف خصائص التتبع في المتصفحات أو التطبيقات كلما أمكن، ومسح ملفات تعريف الارتباط (cookies)، بعد كل زيارة أو تعطيلها تماماً، ومنع الاتصال المباشر بالإنترنت وفرض استخدام شبكة المؤسسة. هذه الإجراءات من شأنها توفير درجة أمن عالية والحد من المخاطر بشكل كبير.

8.6.2 مخاطر ومحاذير تتعلق بالأجهزة

كما هو الحال مع أمن الشبكات في المؤسسات، لا بد من تأمين جميع الأجهزة الذكية، التي تسمح بالوصول إلى أي من بيانات المؤسسة، عبر جدران حماية مشابهة. فلا بد أن تكون مسألة أمن الأجهزة على نفس درجة أهمية أمن الشبكات. فعلى سبيل المثال، الوصول غير المصرح به للجهاز، قد يتسبب في العديد من المشكلات مثل سرقة الهوية أو فقدان بيانات حساسة أو سوء استخدامها.

يمكن تأمين البيانات الحساسة إلى حد معين من خلال المصادقة باستخدام كلمة مرور. ومن الضروري وضع قيود متعددة أمام المستخدم عند اختيار كلمة المرور للتأكد من حصول الأشخاص المخولين فقط على المعلومات. يمكن كذلك ترتيب وقت معين تنتهي فيه صلاحية كلمات المرور ليتم تغييرها بشكل دوري.

هناك العديد من الحلول الأكثر تعقيداً لإجراءات تصديق متعددة المراحل يمكن تطبيقها في حالات معينة مثل استخدام البطاقات الذكية، أو القياسات البيولوجية (مثل بصمة الإصبع) لضمان قيام المستخدم بإجراء أمني آخر بخلاف معرفة كلمة السر.

إدارة أمن الأجهزة أمر بالغ الأهمية للبنية الأمنية بأكلمها في المؤسسات، فالمخاطر المتعلقة بالأجهزة تهدد كذلك أجهزة الحاسب المكتبية، وقواعد البيانات، والبريد الإلكتروني، وخوادم الشبكات، كما قد تتسبب في وصول أشخاص غير مصرح لهم إلى بيانات حساسة، أو قد تتسبب في بطء الأنظمة. علاوةً على ذلك، فبسبب طبيعتها المتنقلة، فإن الأجهزة الذكية عرضة لضياع أو سرقة البيانات.

بعض التدابير التي يمكن اتخاذها للحد من هذه المخاطر تتضمن ما يأتي:

- حيث أن مفاتيح الوصول يتم تخزينها على الجهاز نفسه، يمكن تنشيط نظام الشهادة الرقمية الثانوية ليعمل كقائمة نقض الشهادات (revocation list) في حالة فقدان أو سرقة الجهاز؛ وبهذا يتم حظر مصادقة الأطراف غير المصرح لها. كما يمكن استخدام كلمات مرور إضافية للمصادقة.
- ينبغي استخدام مرشحات للتطبيقات (application filters) للوصول إلى مكونات الجهاز، بحيث يسمح فقط للتطبيقات ذات الصلة والمصرح لها بالوصول إلى خواص الجهاز (مثل الكاميرا، والميكروفون، الخ).
- ينبغي وضع آليات مصادقة صارمة للوقاية من الأخطار المحتملة المتعلقة بفقدان أو سرقة الأجهزة؛ حيث يجب أن تمر عملية الوصول إلى النظام بعدة مراحل من المصادقة أو التشفير طبقاً لحساسية بنية المعلومات. كما يمكن أن تشكل آلية الوصول إلى الأجهزة الذكية عن بعد (remote access) إحدى التدابير الأمنية التي يمكن اتخاذها في حالات فقدان أو سرقة الأجهزة وذلك عبر تسهيل عمليات مسح البيانات، واسترجاعها.. الخ.
- في حالة البيانات الحساسة، يمكن التحقق من الهوية عبر إجراءات مصادقة ذات عاملين لتوفير درجة عالية من إثبات الشخصية.

8.6.3 مخاطر ومحاذير تتعلق بالشبكات

يمكن استغلال نقاط الضعف في الشبكات بعدة طرق عبر التطبيقات أو وثائق البيانات أو التحكم في الأجهزة الذكية وإعدادتها. قد تنبع التهديدات من الأجهزة المتصلة بالشبكة، أو من الملفات التي يتم إرسالها عبرها، أو من بروتوكول الشبكة نفسها. الأجهزة الذكية تكون عرضة أكثر من غيرها لنقاط الضعف في الشبكة حيث إن تنوع وكثرة طرق الاتصال مثل الواي فاي والشبكات الخلوية، تعرض الأجهزة المتصلة بتلك الشبكات إلى مخاطر أكثر من الأجهزة المتصلة عبر الأسلاك.

ويمكن تصنيف فئات المخاطر الرئيسية وآليات الوقاية كما يأتي:

جمع البيانات المقروءة/ الصوتية والتلاعب بها عبر الشبكة وعبر الأثير:

تستخدم الأجهزة الذكية معايير IEEE 802.11 للاتصال بشبكات الواي فاي، ويمكنها الاتصال بالنقاط الساخنة (hotspots) ونقاط الوصول التابعة للمؤسسة. وهكذا، يمكن لأجهزة خارجية أن تتداخل مع تلك الأجهزة عبر نفس الشبكة ما يتيح الوصول غير المصرح به للجهاز والبيانات المخزنة عليه.

وبالمثل، فإن الأجهزة الذكية التي تتصل عبر شبكة الهاتف المتحرك قد تكون عرضة للاختراق. وللاتصال عبر تقنية البلوتوث كذلك العديد من المشكلات المعروفة عبر اختراقه أثناء تهيئته على الرغم من استخدام آليات التشفير والمصادقة. كما توجد مشكلات مشابهة خلال اتصال الأجهزة الذكية عبر تقنيات الاتصال قريب المدى (NFC) والأشعة تحت الحمراء.

للحد من هذه المخاطر، يجب اتخاذ التدابير الآتية:

- يساعد تشفير البيانات في كل عملية إرسال على تقليل المخاطر كلما كان ذلك قابلاً للتطبيق. إلا أن أسلوب التشفير يجب أن يكون متوافقاً مع نظام Federal Information Processing Standard (FIPS) الأمر الذي لا تمتلكه الكثير من الأجهزة في الوقت الحالي. وبالنسبة للأجهزة غير المتوافقة مع نظام FIPS، يجب على المؤسسات أن تستخدم آلية FIPS 140-2 sandbox للأمن.
- ينبغي على المؤسسات إعطاء تعليمات واضحة لموظفيها عن مستويات المخاطر اعتماداً على أنواع الشبكات التي تستخدمها.
- تزداد المخاطر المرتبطة بالشبكات عند اتصال الأجهزة عبر شبكة الهاتف المتحرك أكثر من ارتباطها بالشبكة الداخلية للمؤسسة؛ لذا، لا يُعدُّ وضع سياسة أمنية حلاً عملياً دائماً.
- يجب تعطيل شبكات الجيل الثالث والجيل الرابع (3G & 4G) في البيئات عالية المخاطر لمنع التعرض للخطر. كما يمكن كذلك تعطيل الاتصال عبر تقنيات البلوتوث والاتصال قريب المدى (FNC) وبروتوكول 802.11 للاتصال اللاسلكي عند تعذُّر الاتصال بشبكة افتراضية خاصة (virtual private connections).
- ينبغي أن توفر الشبكات الافتراضية الخاصة (VPN) آليات قوية للتصريح بالاتصال مع الشبكات الرسمية.
- ينبغي على سياسات المؤسسة حظر الاتصال المتعدد من نفس الجهاز.

- قد يكون الاتصال عبر الرسائل النصية القصيرة (SMS) أو رسائل الوسائط المتعددة (MMS) غير آمن حيث يمكن تعقبها والتلاعب بها أثناء عملية الإرسال. يجب على المستخدم بدلاً من ذلك البحث عن وسائل أخرى لإرسال الرسائل تعتمد على بروتوكول الإنترنت (IP based) وتعمل على تشفير البيانات.
- يجب أن تحتوى سياسات جميع المؤسسات على تدريبات استباقية منتظمة لمستخدمي الأجهزة التي تعمل ضمن شبكات أو بيئات تتعرض للمخاطر.
- يجب توفير وتشجيع استخدام الاتصال بالشبكة الرسمية عبر الشبكات الافتراضية الخاصة (VPN) في الحالات عالية المخاطر، حيث تكون عمليات المصادقة، والتشفير، والسرية، وتكامل البيانات آمنة عبر هذه الشبكات.
- يجب توفير آلية التحقق من الملفات (file verification) بالنسبة لكافة المحتويات التي يتم إرسالها إلى الأجهزة الذكية.
- في حالة إرسال المستخدم للبيانات، يجب وضع آلية ثانوية للتحقق وللتأكد من أن البيانات تم إرسالها من المستخدم المصرح له. هذه الآلية قد تكون عبر البريد الإلكتروني، أو مكالمة صوتية أو التحقق عبر سطح مكتب الحاسب الآلي.

مخاطر أنظمة تحديد المواقع والتتبع:

تتوافر خدمات تحديد الموقع الجغرافي في العديد من الأجهزة الذكية بمستويات وقدرات متفاوتة. وتستخدم التطبيقات أنظمة تحديد المواقع الجغرافية لتتبع مسار المستخدم، أو لتحديد الأماكن على الخريطة والبحث عن مكان قريب. يقوم الجهاز بشكل دوري بجمع بيانات الموقع الجغرافي عبر مصادر متعددة تشمل بصمة الجهاز الذكي في شبكة الهاتف المتحرك، وبصمة الواي فاي، وجهاز استقبال نظام تحديد المواقع (GPS) الداخلي.. إلخ. جمع بيانات الموقع الجغرافي من عدة مصادر يوفر مستوى عالٍ من الدقة في تحديد موقع الجهاز، إلا أن التأثير على بعض هذه القنوات لتتداخل مع أنظمة تحديد المواقع، أو تتبع الجهاز بشكل غير قانوني تشكل تهديدات يجب أخذها بعين الاعتبار من حيث الأمن ودقة الأداء.

-
- ينبغي تعطيل إمكانية تتبع البيانات إذا لم يكن ذلك ضرورياً، إلا أن آليات تحديد مكان الجهاز واستعادة البيانات المفقودة، قد تتطلب استخدام هذه الإمكانيات.
- عندما تتطلب طبيعة المهمة استخدام نظام تحديد المواقع (GPS)، من الأفضل منع التطبيقات الخارجية من استخدام نظام تحديد الموقع الجغرافي.
- ينبغي توفير تدريب مكثف لمستخدمي الأجهزة حول موضوعات التتبع، والتهديدات الخاصة ببيانات الموقع، وتشفير بيانات الموقع على الجهاز.

مخاطر التشويش والإغراق:

عند اتصال الأجهزة الذكية عبر تقنية البلوتوث أو شبكة الهاتف المتحرك أو الواي فاي أو نظام تحديد المواقع (GPS)، تكون هذه الأجهزة عرضة لإعاقة الاستقبال أو الإرسال عن طريق عملية تسمى "التشويش" (jamming). من جهة أخرى، "الإغراق" (flooding) هو تحميل الجهاز بكمية بيانات أكبر من أن يستطيع معالجتها. وللتعامل مع هذه التهديدات يمكن اتخاذ التدابير الآتية:

- بالنسبة لشبكات الواي فاي، ينبغي منع التهديدات عبر أنظمة كشف ومنع التسلل اللاسلكي، التي تقوم بإخطار مسؤولي الشبكات عند حدوث تشويش.
- يساعد استخدام ماسحات البرمجيات الخبيثة (malware scanners) وأنظمة الإنذار على الحد من تهديدات الإغراق التي تسببها الشيفرات الخبيثة في الجهاز.
- رصد أنشطة الإغراق حال حدوثها قد يساعد على تقليل الهجمات المستقبلية من خلال تصفية عمليات اختراق الإشارات والحد منها.

8.6.4 تهديدات تتعلق بالجهاز وبالمستخدم

الأجهزة الذكية عرضة لمخاطر مادية وأخرى تتعلق بالمستخدم مثل: فقدان الجهاز، وظروف الاستخدام القاسية، وأخطاء المستخدم، وسوء استخدام الأجهزة.

عندما يتم فقدان أو سرقة جهاز، هناك مخاطر في أن تقوم جهات غير مصرح لها بالوصول إلى بيانات حساسة، وعندها تكون سرية وسلامة المعلومات في خطر، وقد تفقد بيانات مهمة ما لم توجد نسخة احتياطية منها. يجب على سياسات المؤسسات أن تتأكد من أمن البيانات الحساسة ومنع الوصول للشبكة الرسمية والمعلومات عند فقدان أو سرقة الأجهزة، فالأنشطة الضارة قد تؤدي إلى مشكلات على مستوى المؤسسة ككل. في ما يأتي بعض الاحتياطات الضرورية التي يجب اتخاذها:

- ينبغي فرض استخدام كلمات مرور قوية في جميع الأجهزة.
- لا ينبغي شراء الأجهزة إلا من مصادر موثوق بها. يجب حجب الأجهزة المشتراة من موردين غير موثوقين، ويمكن إعداد قائمة بيضاء بالمنتجات والموردين للاهتداء بها في عمليات الشراء.
- يجب جدولة إجراء نسخ احتياطية من البيانات وتخزينها مركزياً. اعتماداً على طريقة سير العمل وحجمه، كما ينبغي اتخاذ إجراءات إضافية للتخزين الاحتياطي منعاً لفقدان البيانات.
- ينبغي تفعيل إمكانية التحكم المركزي في عملية مسح البيانات من جميع الأجهزة حتى يمكن منع الوصول إلى المعلومات عن بعد على مستوى المؤسسة ككل.
- يجب أن يكون التحكم عن بعد كذلك قادراً على قفل الشاشات باستخدام كلمة مرور حتى يتم استعادة البيانات أو مسحها.
- يجب اعتبار عملية سرعة الإبلاغ عن الأجهزة المفقودة أو المسروقة أمراً ضرورياً، وتعميم ذلك على مستخدمي الأجهزة.
- إذا أمكن تفعيل خدمات تحديد الموقع الجغرافي عن بعد، يجب تشغيلها لتحديد مكان الجهاز المفقود أو المسروق.
- يجب منع تعطيل عملية تشفير البيانات.
- يجب تدريب المستخدمين على أن يكونوا حذرين جداً بالنسبة لسيطرتهم الفعلية على الأجهزة وأن يتم إعطاءهم تعليمات حول الأخطار المحتملة لفقدان الأجهزة.
- ينبغي تفعيل الخواص التي تمنع العبث بالجهاز الذكي كلما أمكن ذلك لمنع تثبيت الشيفرات الخبيثة والبرامج على الجهاز.
- يجب إيقاف عمل بعض الخواص الداخلية للأجهزة ما لم تكن جزءاً من الوظائف المستخدمة (مثل الكاميرا والميكروفون) لتجنب أن تقوم أطراف خارجية باختراق الجهاز وجمع بيانات مرئية أو مسموعة.

9 أمور يجب أخذها بالاعتبار في ما يتعلق بالدفع عبر الأجهزة الذكية

مع توافر عدة طرق للدفع، تزداد فرص تنفيذ الخدمات الذكية المدفوعة بشكل كامل عبر الأجهزة الذكية. في العادة، تتداخل عدة أطراف في عملية الدفع عبر الأجهزة الذكية مثل مشغل الهاتف المتحرك، ومزود خدمة الدفع الإلكتروني، والبنك، وشركة بطاقة الائتمان، ويفرض كل طرف من هذه الأطراف نموذجاً خاصاً به. تتضمن بعض أجهزة الهاتف المتحرك الحديثة شريحة تدعم المحفظة الإلكترونية وتقنية الاتصال قريب المدى (NFC) تساعد على إتمام عملية الدفع. وقد انتشر هذا النظام بشكل واسع في عمليات الشراء البسيطة في المتاجر أو في المواصلات، ولكن لا يمكن استخدامه للشراء عبر الإنترنت.

بالنسبة للدفع الإلكتروني عبر الأجهزة الذكية بشكل عام، هناك حلول متعددة متاحة في السوق، وهي مشابهة إلى حد كبير للحلول التي تم تطويرها للدفع عبر شبكة الإنترنت. أحد هذه الحلول هو استخدام منصة ذكية خاصة بالدفع (Mobile Payment Platform) تعمل كبوابة تساعد على إتمام عمليات الدفع، وتتألف من تطبيق خاص بالعميل يقوم بتنزيله وتثبيته على الجهاز. يسمح هذا التطبيق للعميل أن يتعامل مع بوابة الدفع التي عادة ما تكون لدى مزود خدمة الدفع الإلكتروني من أجل إتمام عملية الدفع. بعض أنظمة الدفع الذكية الأخرى تضيف المبلغ إلى حساب الهاتف المتحرك الخاص بالعميل، ويقوم مزود الخدمة بإضافة المبلغ المدفوع إلى فاتورة المستهلك.

يجب على جميع الجهات الحكومية أخذ النقاط التالية بعين الاعتبار:

- خدمة الدفع عبر الأجهزة الذكية ستكون خدمة متكاملة في جميع أنحاء دولة الإمارات العربية المتحدة. لذا، عند توفير خدمات إجرائية، يجب وضع إمكانية التكامل مع نظام دفع وطني في الاعتبار.
- حدد بوضوح متطلبات نظام الدفع عبر الأجهزة الذكية التي تحتاجها. هل تحتاج إلى نظام للدفع عبر الإنترنت؟ أم أنه لا توجد حاجة لإجراء عملية الدفع عبر الإنترنت؟
- حدد نطاق نظام الدفع الذكي. هل تبحث عن نظام للدفع الذكي لمعاملات الحكومة الذكية المحلية؟ أم تخطط لتأسيس نظام للدفع على مستوى البلد؟
- هل يشكل الدفع الذكي جوهر طبيعة عملك أم لا؟
- إذا كنت بحاجة لحل يلبي احتياجات دفع مبالغ مالية بسيطة، فكر في اعتماد الدفع عبر الرسائل النصية القصيرة (SMS billing)، والتي أصبحت شائعة ويعتمدها عدد متزايد من الشركات والمواقع الإلكترونية.
- نظام الدفع عبر تقنية الاتصال قريب المدى (NFC) حل مناسب لتسديد المبالغ المالية البسيطة من دون اتصال بالإنترنت مثل دفع رسوم المواقف، والمواصلات العامة، وشراء الصحف وغير ذلك من مشتريات بسيطة.

- انتشار نظام الدفع عبر تقنية الاتصال قريب المدى، لا يتعلق بمؤسسة واحدة فقط، فهو مشروع كبير يتطلب التعاون مع القطاع الخاص والمواءمة مع القطاع الحكومي. هذه المشروعات يقودها القطاع المصرفي وتعمل الحكومة كمروج للخدمة جنباً إلى جنب مع البنك لإشراك القطاع الخاص.
- إدخال نظام الدفع عبر تقنية الاتصال قريب المدى يتطلب التخطيط لنشر تدريجي للنظام. في هذا المشروع، يجب على الجهة الحكومية أن لا تعمل كمروج فقط ولكن كأفضل داعم عبر تكييف الخدمات الحكومية مع نظام الدفع الجديد.

9.1 أمن الدفع الذكي

الإرشادات التالية مهمة لتأمين المعاملات في منصات الدفع الذكي والتطبيقات الذكي:

- ينبغي منع وصول الأجهزة غير المصرح بها باستخدام خواص مثل رقم التعريف الشخصي (PIN)، أو كلمة مرور، أو أنظمة القياسات الحيوية (biometric systems).
- من جهة الخادم، احتفظ بسجلات محاولات الدخول غير الناجحة، وأبلغ عن أنماط الاستخدام غير المعتاد.
- ينبغي أن يكون للمستخدمين القدرة على التحكم عن بعد في المعاملات من أجل غلق الحساب أو تعطيل تطبيق الدفع عند الحاجة.
- يجب وضع آلية لرصد حالات فقدان أو سرقة الأجهزة. ويجب أن يكون النظام قادراً على اختبار الحسابات والتحقق منها ومن المستخدمين بشكل دوري من أجل المصادقة على الجهاز والمستخدم. بشكل خاص، عند حدوث تغيير في بيانات الموقع الجغرافي، يجب على النظام إعادة إجراء عملية المصادقة.
- تأكد من أن الأجهزة الذكية لا تسمح بإجراء المعاملات إذا لم تكن متصلة بشبكة الإنترنت (offline) أو أن تقوم بتخزين بيانات المعاملات لاستخدامها لاحقاً. يجب على التطبيقات أن تشترط اتصالها بالإنترنت لإتمام المعاملات.
- لتأمين الأجهزة والتطبيقات الذكية، تأكد من تنزيل تحديثات الإصدارات المتعلقة بأنواع التهديدات والمخاطر الجديدة.
- تجنب أن تتعامل تطبيقات الدفع مع تطبيقات أخرى غير مصرح لها أو أن تتبادل البيانات معها.
- وفر معلومات إضافية خاصة بالأمن للمستخدم لضمان أن يكون على دراية بالتهديدات المحتملة والنتائج الممكنة. يجب أن يكون المستخدمون كذلك على دراية بقضايا الأمن الخاصة بالأجهزة التي يستخدمونها وأنظمة التشغيل، والتي قد يكون لها تأثير في ما يتعلق بالمعاملات الذكية.
- عند التعامل مع خدمات الحكومة الذكية، يجب أن يستخدم الجمهور التطبيقات الحكومية المعتمدة فقط لعمليات الدفع الذكي. ويمكن تطبيق ذلك بأن تحتوي التطبيقات على شعار حكومي معتمد.