إطار عمل للحكومة الالكترونية باعتماد منهجية الخدمات الموجهة

*م. عبد الرزاق ياسين المحمد المحمود **د. وسيم ياسين جنيدي

(الإيداع: 15 نيسان 2019 ، القبول: 24 آيلول 2019)

الملخص:

نظراً لأهمية الإجراءات الحكومية وإنعكاسها على مختلف القطاعات، فإن كل الحكومات – في العقدين الأخرين– قد تبنت مفهوم الحكومة الالكترونية والذي يعني دمج وتكامل أنظمة المؤسسات الحكومية ضمن إطار عمل موحد يحقق تبادل البيانات بطريقة آمنة، بهدف تقديم خدمات إلكترونية تشاركية للمؤسسات الحكومية فيما بينها (G2G) أو لقطاع الأعمال (G2B) أو للمواطنين (G2C)، طُورت عدة منهجيات لتنفيذ مشاريع الحكومات إلالكترونية مثل (e–Gif, EA, CORBA, SOA)، في السنوات الأخيرة أثبت منهجية الخدمات الموجهة (SOA) كفاءتها العالية في تحقيق تكامل واندماج التطبيقات الموزعة، في هذا البحث نجري سبر لمنهجية الخدمات الموجهة والدراسات التي اعتمدت هذه المنهجية، كمقدمة للحل المقترح لتفعيل مبادرة الحكومة الإلكترونية السورية التي تواجه مجموعة من التحديات تعيق استثمارها بشكل فعال.

الكلمات المفتاحية: هيكلية الخدمات الموجهة، الحكومة الإلكترونية، ممر الخدمات الاحترافي، لغة توصف خدمات الويب، بروتوكول الوصول إلى الكائن البسيط، أمن خدمات الويب.

*طالب ماجستير (علوم ويب) – الجامعة الافتراضية السورية.

**باحث في مركز البحوث العلمية ومدرس في الجامعة الافتراضية السورية.

E-Government framework based on SOA

Eng. AbdulRazzak Yassin Almohamad Almahmoud **Dr. Wassim Yassin Aljuneidi**

(Received: 15 April 2019, Accepted: 24 Septemper 2019)

Abstract:

Referring to the importance of government procedures and their impact on various sectors, all governments - in the last two decades - have adopted the concept of e-government, which means integration of various stand-alone governmental systems into interoperability framework to exchange data securly and provide e-services for the governmental participants (G2G), for business sector (G2B) or for citizens (G2C). Several methodologies have been developed to implement e-government projects such as (e-Gif, EA, CORBA and SOA).In the last few years, service-oriented architecture (SOA) has proven its efficiency in integrating distributed applications.

In this paper, we will review the methodology of service-oriented architecture (SOA) and the related works that adopted this methodology, asa preface to the proposed solution to activate the Syrian e-government initiative, which faces a range of challenges hindering its effective implementation.

Keywords: E-government, Syria,Web Services Description Language, Simple Object Access Protocol, Service Oriented Architecture, Virtual Private Network, Enterprise Service Bus, WS-Security

1-المقدمة

رغم التزام الحكومة السورية بدعم تنفيذ الحكومة الإلكترونية، واطلاق مبادرة مشروع الحكومة الالكترونية السورية سنة 2009، إلا أن مؤشر تنمية الحكومة الالكترونية حسب المسح الذي قامت به إدارة الشؤون الاجتماعية والإقتصادية بالإمم المتحدة للحكومات الالكترونية لعام 2014 وعام 2018 يشير إلى تراجع الترتيب من (135) لعام 2014 إلى (164) لعام 2018، بينما تقدم مؤشر المشاركة الالكترونية والاستفادة منه وفقاً للمراحل من الترتيب (164) لعام 2014 إلى الترتيب (152) لعام 2018 [1] [2]، تدل هذه المؤشرات بوضوح لواقع متأخر للحكومة الالكترونية السورية، رغم أن معظم الوزارات تمتلك أنظمة معلوماتية وقواعد بيانات، إلا أن هذه الأنظمة معزولة عن بعضها البعض بسبب ضعف البنية التحتية للإتصالات وعدم وجود شبكة حكومية شاملة تربط جميع الوزارات لتنفيذ عملية دمج وتكامل هذه الأنظمة، وكذلك الأمر لا يوجد قاعدة بيانات حكومية مركزية، بمعنى آخر أنه لا وجود لإطار عمل مشترك ما بين الوزارات، يضاف إلى ذلك عوامل لوجستية مؤثرة (الحاجة لكوادر بشرية مؤهلة تقنياً، التمويل، ضرورة متابعة الخطط بشكل فعال) هذه التحديات تقتضي إيجاد حل رشيق يتمتع بالمرونة وسهولة الإدارة، لتجاوز مجمل هذه العوائق.

في هذا البحث نقدم حلاً مقترحاً يتبنى منهجية الخدمات الموجهة لما تتمتع به من مرونة عالية وقابلية للتوسع واستيعاب المستجدات، فمنهجية الخدمات الموجهة تتيح إمكانية العمل بطريقة تزايدية خطوة–خطوة ومع تكرار الأعمال تتزايد الخدمات دونما أن يكون لذلك تأثير ملحوظ على ما تم إنجازه في مراحل سابقة، يضاف إلى ذلك أنها لا تحتاج لأي مفاهيم معقدة قد تشكل عبئاً إضافياً على الجهات المشتركة بالحكومة الالكترونية، وبهدف التخفيف من المتطلبات المادية والبشرية وضمان توافقية مكونات اطار العمل ، يتبنى الحل المقترح استخدام المعايير القياسية ويتجنب استخدام المنتجات التجارية، يتكون الحل المقترح من خمس مكونات أساسية (خزان الخدمات، الوسيط، المراقبة، المصادقة، التدقيق)، ويتكون الوسيط من أربع مكونات (قائمة التحكم بالوصول، العراب، مولد الواجهات، مركب الخدمات) ترتبط هذه المكونات مع باقي طبقات الحكومة الالكترونية باستخدام البروتوكولات المعتمدة وشبكة خاصة آمنة لتشكل بمجموعها ممر خدمات إحترافي يحقق تكامل وإندماج الخدمات الالكترونية.

2-المواد وطرائق البحث:

اتبع البحث سلسة من الخطوات المترابطة للوصول إلى النتائج المرجوة :

1-حدد المنهجية المستهدفة بالدراسة (SOA) باعتبارها الأكثر ملاءمة لواقع ومتطلبات تفعيل الحكومة الالكترونية السورية.
2-أجرى سبراً دقيقاً لهذه المنهجية وأهتم بأفضل الممارسات الموصى بها عالمياً.
3-أجرى دراسة للمعايير القياسية العالمية ذات الصلة.
4-أجرى مراجعة للدراسات العالمية المشابهة.
5-أجرى مراجعة لواقع الحكومة الالكترونية السورية ولوثائقها المنشورة.
6-بالاعتماد على النقاط السابقة، اقترح البحث دراسة تصميمة لإطار العمل، ومن ثم قدم نسخة تنفيذية للمقترح.

2-1-منهجية الخدمات الموجهة وأفضل الممارسات

منهجية الخدمات الموجهة (Service Oriented Architecture) SOA هي استراتيجية لترابط واندماج العمليات الموزعة على شبكات واسعة وأنظمة تشغيل مختلفة، تعتمد هذه المنهجية ثلاثة مفاهيم تقنية أساسية هي: (الخدمة، الاقتران الفضفاض، التخاطب البيني) [3].

- **الخدمة**: هي وظيفة مستقلة بذاتها، تختص بأداء مهمة بسيطة (كتخزين البيانات) أو مهمة معقدة (كمعالجة طلب شراء) ، وتتمتع الخدمة بمجموعة من الخصائص: الإستقلالية، التجريد ، إمكانية اكتشافها عند البحث عنها في مخزن الخدمات

العام ، اللازدواجية بمعنى أنه يمكن إعادة طلب الخدمة دون أن يتسبب الطلب الثاني بأية مشاكل، إمكانية إعادة استخدامها من أي جزء كان في المنظومة، إمكانية إنشاء خدمات مركبة باستدعاء خدمات أخرى ، امكانية إستدعاء الخدمة من أي نظام تشغيل كان، إمكانية تبادل البيانات فيما بين الخدمات بغض النظر عن منصة العمل، إمكانية تنفيذ الخدمة من خلال الويب، كل المعلومات اللازمة للاستفادة من الخدمة يتم توفيرها من خلال عقد الخدمة.

– **الاقتران الفضفاض:** هو مبدأ يهدف إلى التقليل من ارتباط الخدمات الموزعة بالأنظمة التي تعمل فوقها، بهدف تخفيف أثر تغيرات نظام التشغيل على الخدمات، وله أشكال مختلفة تتيح لمصمم هيكلية الخدمات الموجهة أن يعتمد الخيارات المناسبة التي تخدم أهدافه، من أهم أشكال الاقتران الفضفاض: تبادل الرسائل بشكل غير متزامن، تبادل أنماط بيانات غير المتجانسة، نقل طلبات الخدمة وإجراء موازنة الحمل من خلال وسيط، التحقق من نوع البيانات باستخدام واجهات مجردة، ربط البيانات ديناميكياً، استقلالية الاقتران عن منصة العمل، استخدام أنماط البيانات البسيطة، تنفيذ المناقلة بالتعويض بشكل غير متزامن، التحكم بمنطق العمليات بشكل لامركزي لتجنب حالات الفشل (عنق الزجاجة)، نشر التحديثات بشكل غير متزامن وهذا الأمر يرتبط بمفهوم الاصدارات التي يجب على المستفيد أن يراعيها لترقية برمجياته لتتوافق مع الإصدارات المستحدثة، بالعموم أشكال الاقتران هذه، ليست إلزامية وإنما هي خيارات لإعتماد المناسب منها حسبما تقتضيه الضرورة.

– **التخاطب البيني:** هو تبادل البيانات بين الخدمات الموزعة على أنظمة تشغيل متنوعة باستخدام ممر الخدمات الاحترافي (ESB)الذي يشكل البنية التحتية لمنهجية الخدمات الموجهة ويؤمن الاتصال ما بين المستفيد ومزود الخدمة بالإضافة لمهام أخرى مثل: نقل البيانات، التوجيه الذكي، الإجراءات الأمنية، الوثوقية، إدارة الخدمات، المراقبة، يتبع ممر الخدمات في عمله منهجيتين مختلفين:

1) استخدام البروتوكول وفي هذه الحالة يفويض الكثير من مهامه إلى مزود الخدمة والمستفيد، وفي هذه الحالة يلتزم كل من المزود والمستفيد بالأدوات القياسية الموصى بها لتوليد البرمجيات القادرة على التخاطب مع هذه البروتوكولات ولعل أفضل مقاربة لهذا النمط هي استخدام بروتوكول (SOAP) مع خدمات الويب.

2) استخدام واجهة التطبيقات البرمجية (API) وفي هذه الحالة يشغل ممر الخدمات العديد من البرمجيات (المركزية أو اللامركزية) ويوفر البروتوكولات الشفافة لكل من المزود والمستفيد لإستخدامها في نشر وتنفيذ الخدمات.

يمكن لممر الخدمات أن يوفر أشكال إقتران مختلفة:

1) اقتران محكم (نقطة إلى نقطة) وهذا النوع معرض للفشل في حالة عدم توفر مزود الخدمة.

2) الاقتران الفضفاض عندئذ يتولى ممر الخدمات مهمة البحث عن مزود الخدمة المناسب ويوجه إليه طلب المستفيد، وفي هذه الحالة يلعب ممر الخدمات دور الوسيط الذي يتحكم بتوزيع الحمل ومعالجة التغيرات الديناميكية في هيكلية الخدمات الموجهة.

أوصت الطبعة الزرقاء للحكومة الالكترونية الصادرة عن الخدمات العامة لتكنولوجيا المعلومات والاتصالات في بلجيكا بمجموعة من الإرشادات باعتبارها أفضل الممارسات التي تلبي المعايير القياسية لتطبيقات الحكومة الإلكترونية [4]:

1) يجب استخدام (*SSL*) لضمان أمن إستداعاء الخدمة واستخدام ***(SAML)*** في عملية التحقق.

2) في إجراء التكامل أوصت باستخدم (وسيط) يتضمن إدارة سهلة للخدمات، لتوحيد أسلوب تزويد الخدمات والسياسة التي يجب أن يلتزم بها المستفيد.

3) يجب أن تستوفي وظائف ممر الخدمات مجموعة من المتطلبات:

– دعم أساليب المصادقة المختلفة Federation، ID، token based، SAML

– تدقيق وتوثيق الأحداث، الخصوصية، الأداء، الوفرة

– منح تفويض الوصول إلى الموارد، بناءاً على السياسة العامة للمنظومة

- استخدام معيار التوجيه (CBR) أو توزيع الحمل لتوجيه طلب الخدمة إلى المزود المناسب
- توفير خدمة تحويل تنسيق الرسالة لتجاوز التغييرات التي تطرأ على واجهة الخدمة
- توفير خدمة مراقبة بهدف جمع مؤشرات عن المزود والمستفيد والتحقق من تنفيذ عقد مستوى الخدمة (SLA)
- توفير خدمة معالجة الأخطاء وإشعار المسؤول عنها
- استخدام التخزين المؤقت لتحسين زمن الاستجابة
- استخدام الفلترة لإزالة معلومات الخصوصية من الرسائل لحماية المستخدمين
- تخفيف التعقيدات الفنية لتسهيل إجراءات التكامل.

4) يجب أن تراعي الاوركسترا (الخدمات المركبة) عدة مفاهيم: التنفيذ غير المتزامن، التعويض، التفرع الشرطي، التنفيذ المتوازي للأنشطة غير المترابطة، المؤقتات والإنتظار المشروط، التعامل مع الإصدارات المتعددة، مراقبة الأداء.

5) يجب تسجيل معلومات الخدمات بمخزن مركزي، وتوفير انماط بحث مختلفة لتسهيل اكتشافها، يمكن استخدام المعيار (UDDI) أو أي تقنيات أخرى لتخزن المعلومات الوصفية للخدمات والبحث عنها.

6) يجب تفعيل وظائف مراقبة حالات الفشل لكل الأنظمة المستخدمة، لتسهيل تحديد جذر المشكلة.

7) يجب معيرة أسلوب تسجيل الأحداث كون أن هذا الأمر يتقاطع مع كل التطبيقات مما يقتضي أن يتمتع مكون التدقيق بمرونة كافية لاستيعاب المستجدات وأن يكون قابل لإعادة الاستخدام مع أكثر من تطبيق.

8) يجب أن توفر البوابة للمستفيد الخصوصية والتخصيص، استنادًا إلى السماحيات الممنوحة، باعتبارها نقطة الوصول للخدمات المراقبة أمنياً.

2-2-معايير تقنية ذات صلة

1) WS-Security يهتم هذا المعيار بأمن الرسائل التي تسلك مسارات متعددة النقاط وتستخدم مفاتيح تشفير مختلفة، لم يقم المعيار بإيجاد مفاهيم جديدة وإنما وفر إمكانية استخدم المعايير الأمنية المعتمدة مثل: PKI، Kerberos، X.509، XML Signature، XML Encryption بطريقة سهلة من خلال تضمين هذه المعايير في ترويسة رسالة الـ SOAP دون أن يتدخل بنمط التشفير أو التوقيع الرقمي فاستخدم العنصر BinarySecurityToken لهذا الغرض واستخدم العنصر UsernameToken لنقل اعتماد المستخدم [5].

2) WSDL لغة نصية تعتمد الـ XML لتوصيف واستكشاف خدمات الويب ومعرفة أنواع البيانات والوظائف التي تقوم بها الخدمة، ولإستدعاء وظائفها يمكن استخدام البروتوكول (SOAP) لهذا الغرض [6].

3) UDDI يتولى مهمة تسجيل المعلومات الوصفية لمزودي الخدمة وشروط استخدام الخدمة، ويوفر هذه المعلومات للمستفيدين لاستكشاف الخدمات والاستفادة منها [7]، في عام 2005 أعلنت مجموعة المعايير الدولية OASIS عن إصدار جديد للمعيار UDDI 3.0.2 يدعم البنى التحتية المتنوعة ليصبح معياراً قياسياً مفتوحاً يحقق التخاطب البيني على نطاق أوسع ويلبي متطلبات هيكلية الخدمات الموجهة (SOA) [8]، في 2018 قامت شركة Microsoft بإزالة خدمة UDDI من مخدم ويندوز 2008، لتجعلها كأحد مكونات مخدم التكامل BizTalk مبررةً هذا الإجراء بأنه إعادة ترتيب لمنتجاتها بهدف تقديم خدمة أفضل لسوق هيكلية الخدمات الموجهة (SOA) [9].

4) VPN يوفر آلية لتشفير وتغليف الحزم المتبادلة ما بين الأجهزة المتصلة عبر الانترنت باستخدام البروتوكول (IP) وارسالها ضمن نفق خاص، فيبدو الاتصال وكأنه اتصال ما بين نقطتين بغض النظر عن طبيعة الشبكة الوسيطة، يتفق الطرفان على نظام تشفير، فيقوم منشيء النفق بتشفير الحزمة لضمان أمنها، ثم يقوم مُبدِّل VPN بتغليف الحزمة المشفرة

بالكامل في حزمة IP وإرسالها عبر الإنترنت، عند نقطة النهاية تستلم الطرفية الأخرى من نفق الشبكة الافتراضية، الحزمة وتزيل منها معلومات الـ IP وتفك التشفير وفقًا لنظام التشفير المتفق عليه، ومن ثم ترسل الحزمة الناتجة إلى الجهاز المستهدف، الفائدة الرئيسية لهذا النوع من الإتصال هو التكلفة المنخفضة مقارنة بالخط المؤجر عالي السرعة، استمرارية العمل كون أن خطوط الاتصال بين أجهزة التوجيه تسلك مسارات منطقية يمكن تغيرها بكل بساطة وشفافية، إمكانية اتصال مستخدمي الهواتف المحمولة مع شبكة الـ VPN، إمكانية مراقبة المعلومات التي يصل إليها المستخدم، إمكانية تأسيس اتصال VPN بنطاق ترددي منخفض وزيادة عرض النطاق الترددي عند الحاجة [10].

2-3-الدراسات المشابهة

(1) إطار التشغيل المشترك لخدمات الحكومة الالكترونية في الفلبين: قدم "ريغالادو وماريفيك" دراسة لإطار عمل، للتخاطب البيني باعتماد الخدمات الموجهة باعتبار أنها تغطي الأبعاد الثلاثة للتخاطب البيني (التنظيم والدلالة والترابط التقني)، يتكون المقترح من تسع طبقات (معالجة الأعمال، الحوكمة، جودة الخدمة، التكامل، هيكلة المعلومات، التشغيل، الكائنات الخدمية، الخدمات، وطبقة العرض) المقترح واضح ومنظم من الناحية النظرية، إلا أنه لم يقدم أفكار تقنية جديدة [11].

(2) تطوير هيكلية حكومة الكترونية باعتماد الخدمات الموجهة لتحقيق التخاطب البيني: قدم "الخنجري وآخرون" هيكلية للحكومة الالكترونية باعتماد الخدمات الموجهة (SOA) معتبرين أن هذه المنهجية ستشكل الحل المستقبلي للحكومات الالكترونية، قسموا الهيكلية إلى ثلاثة أقسام رئيسية: القسم الأول الحكومة الالكترونية ذات الخدمات الموجهة ويتكون من خمس طبقات (طبقة العرض، طبقة العمليات، طبقة الخدمات، طبقة التشغيل، الطبقة الدلالية)، القسم الثاني خزانات التخاطب البيني ويتكون من خزان معالجة العمليات ويرتبط بطبقة العمليات، خزان الخدمات ويرتبط بطبقة الخدمات، خزان دلالي يرتبط بالطبقة الدلالية، القسم الثالث البنية التحتية لضمان الجودة والتطوير ويتكون من مركز التميز الحكومي لضمان الجودة، فريق تطوير خدمات الدولة، نظام المعلومات لتزويد فريق التطوير بأفضل الممارسات في مجال التخاطب البيني، ونظام الاكتشاف ويتولى البحث عن أفضل الخدمات المتعلقة بمهمة معينة والتوصية بها، الدراسة جيدة أعطت وصف لمقترح واضح، أغفلت بعض التفاصيل مثل: الإجراءات الأمنية ، دور ممر الخدمات، المقاربة التطبيقية للمقترح [12].

(3) تكامل بيانات الحكومة الإلكترونية بالاعتماد على منهجية الخدمات الموجهة: قدم "مادوخ وبركة" نموذجاً لإطار عمل بالاعتماد على الخدمات الموجهة مؤلف من عدة مكونات (ممر خدمات، سجل الخدمات، خدمة المعلومات الحكومية، خدمة إدارة الإتصال بقواعد البيانات، الأوركيسترا، خدمة النسخ المتزامن، خدمة إدارة ومراقبة ممر الخدمات، خدمة ضمان الأمان)، ثم قاموا باسقاط المقترح النظري على بئية تطبيقية باستخدام بيئة جافا، بشكل عام الدراسة مهنية وتتميز بالوضوح إلا أن اعتماد ممر الخدمات فيها على واجهة التطبيقات البرمجية يعني أن وظائف ممر الخدمات ستتعرض لتحديثات دورية وأخطاء ناجمة عنها وهذه التحديثات ستنعكس على المزود والمستفيد مما يعني مزيد من الأعباء [13].

(4) الحكومة الإلكترونية في الدول العربية خارطة طريق من 6 مراحل استعرض "الخوري" واقع الحكومات الالكترونية في المنطقة العربية، وقدم خارطة طريق تحدد الأولويات التي يجب مراعاتها مكونة من ست مراحل (أتمتة الأعمال المكتبية، تقديم الخدمات العامة من خلال نظام النافذة الواحدة، إنشاء الهوية الرقمية، تطوير الخدمات الإلكترونية المتكاملة، تحقيق التخاطب البيني محلياً بين الأنظمة الحكومية باعتماد SOA، تحقيق التخاطب البيني دولياً باعتماد e-GIF، أقتصرت الدراسة على تحليل واقع الحكومة الالكترونية بالدول العربية وتقديم الأفكار والإرشادات لتحفيز مبادرات هذه الدول [14].

(5) إطار عمل أمني –عقدة لعقدة – للخدمات الموجهة ناقش "شاشوات وآخرون" متطلبات أمن الخدمات الموجهة في حالة اتصال عقد لعقدة وأوصوا باستخدام بروتوكول SSL والتخزين المؤقت، لم يتم التطرق للحالات الأكثر تشعباً، حيث لا يلبي

بروتوكول SSL المتطلبات الأمنية معتبرين أن الخدمات التي تسلك مسارات متعددة تعاني من مخاطر أمنية ولابد من استخدام أدوات أمنية لهذا الغرض [15].

(6) هيكلية مرجعية لأمن الخدمات الموجهة– الأمن كخدمة اقتراح "ميمون وأخرون" نشر الخدمات الأمنية على نطاق محدد لتشترك باستخدمها نقاط الخدمات التي تقع في نطاق واحد، يطلق على هذا الاسلوب منهجية الأمان كخدمة (SAAS) ، يتألف الكائن (SAAS) من مخزن السياسات ومخزن الـ PKI بالاضافة لخدمات المصادقة، التفويض، عدم النكران، تسجيل الدخول والمراقبة الأمنية، وتعتمد هذه الخدمات على بعضها البعض، اعتماد المقترح على خدمة أمن مركزية قد تتسبب بحالة فشل "عنق الزجاجة"، كما أن الكائن لايتمتع بالاستقلالية بسبب اعتماده على خدمات ويب مرتبطة بالمزودين لحالات المصادقة الخارجية، بالاضافة لاعتماده على نمط واحد من أنماط التشفير PKI هي نقطة ضعف اضافية كون أن الأنظمة الموزعة تعتمد معايير تشفير متنوعة [16].

2-4-مراجعة للحكومة الالكترونية السورية

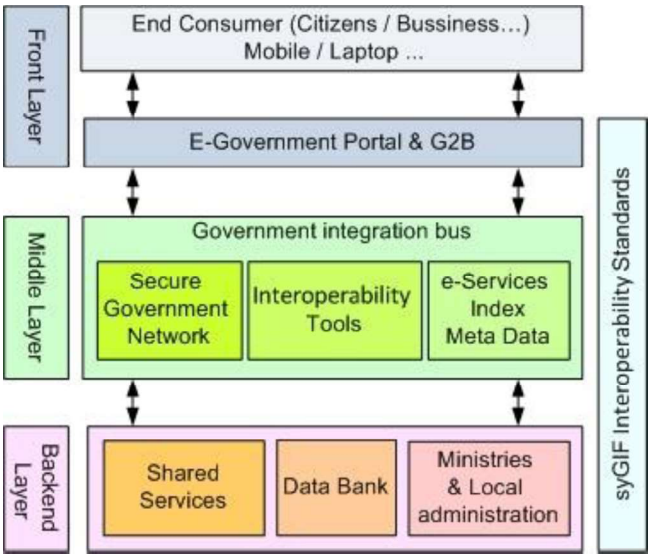
إنطلقت مبادرة الحكومة الالكترونية السورية سنة 2009 وحددت ثلاث مراحل للحكومة الالكترونية (مرحلة نشر المعلومات، مرحلة التفاعل بخصوص القواعد الناظمة، مرحلة إنجاز المعاملات الكترونياً)، ونشرت عدة وثائق ترسم فيها ملامح الحكومة الالكترونية:

(1) وثيقة الأسس والمبادىء أفترضت ان التخاطب بين الجهات الحكومية يجب أن يكون على مستوى الخدمة بتبادل رسائل xml مستقلة وبطريقة غير مترامنة، ويتولى إدارة هذه الرسائل وسيط يتمع بإمكانية الإضافة التدريجية للخدمات، وإمكانية تجميع عدة خدمات لتركيب خدمة جديدة [17].

(2) وثيقة التوجهات أشارت لضرورة تقديم الخدمات الحكومية بشكل متجانس مع دعم التنفيذ اللامركزي لتخفف العبىء على الوزارات [18].

(3) وثيقة البرامج أوصت بالابتعاد عن نهج المشاريع العملاقة وبناء المشاريع بطريقة تزايدية خطوات صغيرة قابلة للتحقيق لبناء نجاح تراكمي وثقة متزايدة [19].

(4) وثيقة التخاطب البيني قدمت هيكلية مقترحة للحكومة الالكترونية السورية مكونة من ثلاث طبقات، الطبقة الأمامية والطبقة الوسطى والطبقة الخلفية بالإضافة لمعايير التخاطب البيني (SyGIF) والذي يتضمن معايير تقنية ومعايير دلالية ومعايير توصيف البيانات –الطبقة الخلفية تتكون من بنك البيانات والخدمات المشتركة. الطبقة الوسطى تتكون من شبكة آمنة، دليل الخدمات، أدوات التخاطب، والطبقة الأمامية عبارة البوابة الالكترونية المسؤولة عن تزويد الخدمات [20].



الشكل رقم (1): هيكلية الحكومة الالكترونية السورية 2009

تم إنشاء بوابة الكترونية تتضمن ارتباطات إلى الخدمات الحكومية المزودة الكترونياً، بالإضافة الى معلومات عن حوالي 2552 معاملة تبين شروط الاستفادة من الخدمات [21].

3-النتائج والمناقشة

استعرضنا مفهوم منهجية الخدمات الموجهة باعتباره استراتيجية لترابط واندماج العمليات الموزعة، وتبين لنا أن من أهم القرارات المتعلقة بممر الخدمات الإحترافي هو اختيار نموذج التقنية التي سيعتمدها (واجهة تطبيقات برمجية أم بروتوكول) وخلصنا إلى نتيجة أن استخدام البروتوكول (SOAP) مع خدمات الويب هو الخيار الأفضل، تم التطرق لمجموعة من الإرشادات منها: ضرورة استخدام بروكول SSL لضمان أمن إستداعاء الخدمات، وضرورة توحيد أسلوب تسجيل واستكشاف وتنفيذ الخدمات، بالإضافة لضرورة معيرة أسلوب تسجيل الأحداث كون أن هذا الأمر يتقاطع مع كل التطبيقات مما يتطلب أن يتمتع مكون التدقيق بمرونة كافية لاستيعاب المستجدات وأن يكون قابل لإعادة الاستخدام مع أكثر من تطبيق، وفيما يخص البوابة باعتبارها نقطة الوصول للخدمات، فيجب أن توفر الخصوصية والتخصيص للمستفيد استنادًا إلى السماحيات، استعرضنا مجموعة من المعيار ذات الصلة، كمعيار أمن خدمات الويب WS-Security الذي قدم توليفة من المعايير المعتمدة والمتخصصة بالأمن والتشفير واستخدمها في أمن خدمات الويب بشكل حيادي دون أن يتدخل بطريقة عملها، فهو معيار يستخدم أفضل الممارسات المتوفرة في أمن المعلومات بالإضافة لسهولة إستخدام وظائفه (بالأمن والتشفير)، المعيار WSDL وهو المعيار الأساسي لإستدعاء خدمات الويب ولا يمكن الاستغناء عنه أو تجاهله وله دور مهم في ممر الخدمات، أما المعيار UDDI لم يلق نجاحاً منذ اطلاق نسخته الأولى، ثم جاء قرار مايكروسوفت التي أوقفت استخدامه كأحد مكونات نظام التشغيل وألحقته بمنتج تجاري Biztalk الأمر الذي يضطرنا لإستبعاد هذا المعيار لتجنب التكلفة المالية، وللحفاظ على توافقية مكونات إطار العمل، المعيار VPN تبدو مواصفاته الأمنية مناسبة لإستخدامه كشبكة حكومية خاصة لتشكل البنية التحتية لممر الخدمات الإحترافي.

بناءاً على ما تقدم نقدم حلاً مقترحاً يعزز توصيات وتوجهات مبادرة الحكومة الالكترونية السورية لعام 2009، لتحقيق العمل المشترك بين القطاعات الحكومية.

4-إطار العمل المقترح

4-1 المخطط المفاهيمي لإطار العمل

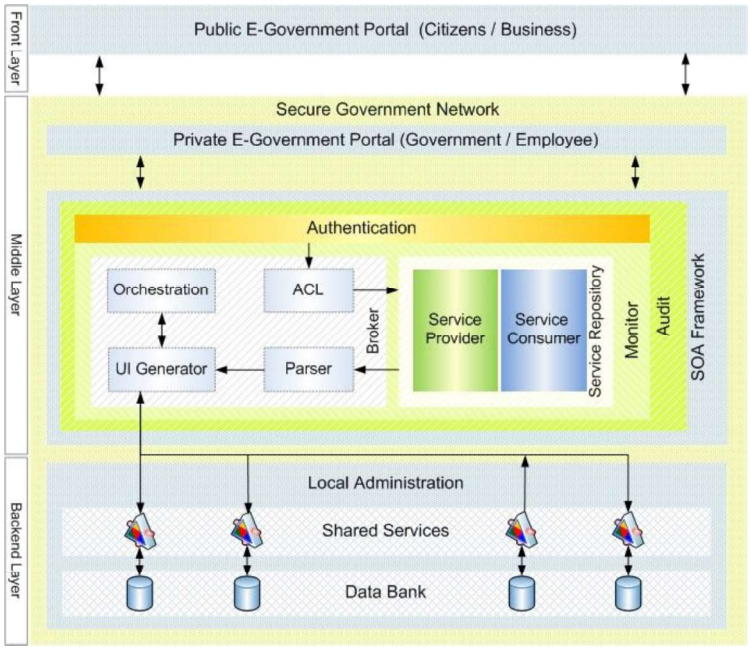
أجرى الحل المقترح إعادة ترتيب لمكونات الهيكلية المقترحة للحكومة الالكترونية السورية، الشكل (1) وأضاف لها إطار العمل المقترح لتصبح كما هو موضح بالشكل (2) مكونة من ثلاث طبقات (طبقة أمامية عبارة عن بوابة عامة، طبقة وسطى مكونة من بوابة حكومية خاصة مع إطار العمل المقترح، وطبقة خلفية هي بنك البيانات والخدمات المشتركة) تعمل الطبقتين الوسطى والخلفية فوق شبكة حكومية آمنة، ويشكل إطار العمل مع الشبكة الحكومية ممر خدمات إحترافي آمن، يتولى مهمة تكامل وإندماج الخدمات الالكترونية للجهات الحكومية فقط في هذه المرحلة.

يتكون إطار عمل الحكومة الالكترونية المقترح من خمس مكونات أساسية:

1- خزان الخدمات Service Repository ويسجل فيه عقود تزويد الخدمة Service Provider وعقود الاستفادة من الخدمة Service Consumer والإجرائيات الخاصة بالخدمات المركبة Orchestration ، بالاضافة لواجهة بحث مجردة لإستكشاف الخدمات وتنفيذها، 2- المصادقة Authentection أو التحقق من هوية المستخدم ويعتمدهذا المكون على عناصر WS-Security لإنشاء اعتماد للمستخدم ومنحه إذونات الوصول للمصادر المسموحة في المكون ACL، 3- التدقيق Audit: يتولى هذا الكائن تسجيل الأحداث المرسلة إليه من كائن المصادقة وكائن المراقبة، لتستخدم في حالات الاستقصاء عن الخروقات أو حالات الفشل، 4- المراقبة Monitor : يستلم هذا الكائن رسائل من كافة العمليات التي تجري

ضمن إطار العمل، فإن تضمنت الرسالة معلومات ذات أهمية يقوم بارسالها لسجل التدقيق، كما يراقب طلبات الخدمة ونتائج تنفيذ الخدمة المطلوبة وحالات الفشل ويراقب حالة العقد المتصلة أو غير المتصلة.

5- الوسيط ويتكون من أربع مكونات: 5-1- قائمة التحكم بالوصول Access Control List (ACL) تتضمن سياسة الوصول لمصادر إطار العمل وسسياسة الوصول للخدمات المزودة، حسب شروط عقد الخدمة، 5-2- العراب WSDL Parser لا يتطلب تسجيل الخدمة في مخزن الخدمات أي تفاصيل تقنية سوى مسار خدمة الويب وعند طلب الخدمة يتولى العراب قراءة ملف WSDL من مساره، للحصول على وظائف خدمة الويب ونوع البيانات المطلوبة بشكل ديناميكي ويرسلها لمولد الواجهات، 5-3- مولد الواجهات UI Generator يقوم بتوليد نموذج لإدخال برمترات الخدمة مع وظائف التحقق من نوع البيانات حسب التوصيف المستلم من العراب، 5-4- الأوركسترا Orchestration تتولى مهمة إنشاء خدمة مُركبة من عدة خدمات جزئية، تقوم بتحديد الخدمات الجزئية المطلوبة وتسلسل تنفيذها وطريقة ربط برامتراتها، حسب رغبة المستفيد، ترسل هذه البيانات لمولد الوجهات لينشيء واجهة جديدة للخدمة المُركبة، وتسجل هذه الخدمة ضمن تفضيلات المستفيد ليستخدمها عند الحاجة.

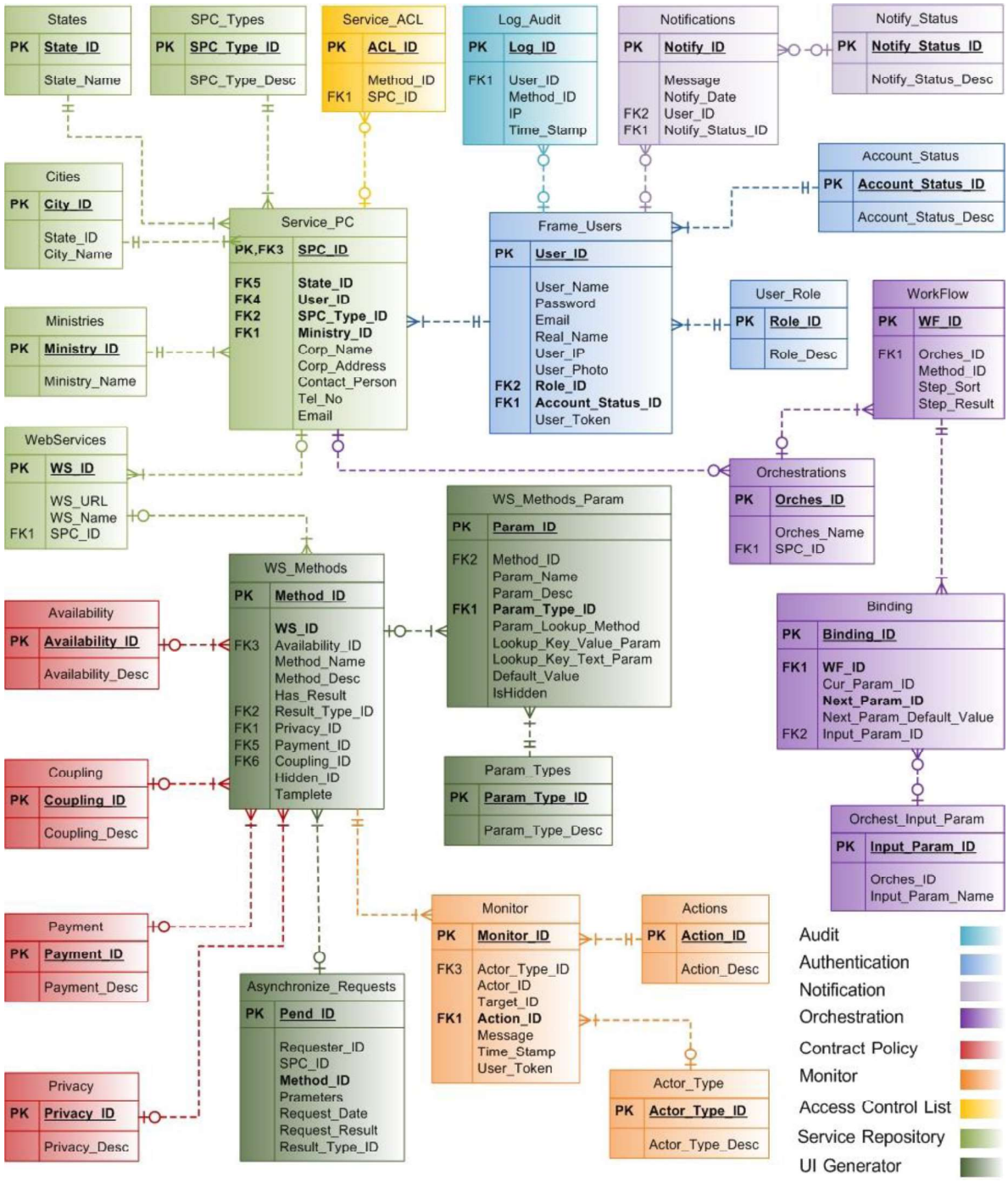


الشكل رقم (2): هيكلية الحكومة الالكترونية مع إطار العمل

2-4 مخطط الكينونات لإطار العمل

يستخدم إطار العمل لإنجاز وظائفه الرئيسية كينونات علائقية موضحة بالشكل (3):

(1)	مزود/مستهلك	Service_PC	(2)	مولد	WS_Methods, WS_Methods_Param
(3)	سجل الخدمات	WebServices	(4)	عقد الخدمة	Coupling,Privacy,Payment, Availability
(5)	المصادقة	Frame_Users	(6)	الأوركسترا	Orchestration, Orchest_Input_Param, Workflow, Binding
(7)	التحكم بالوصول	Service_ACL	(8)	خدمات غير	Asynchronize_Requests
(9)	التدقيق	Log_Audit	(10)	المراقبة	Monitor, Notifications



الشكل رقم (3): كينونات إطار العمل

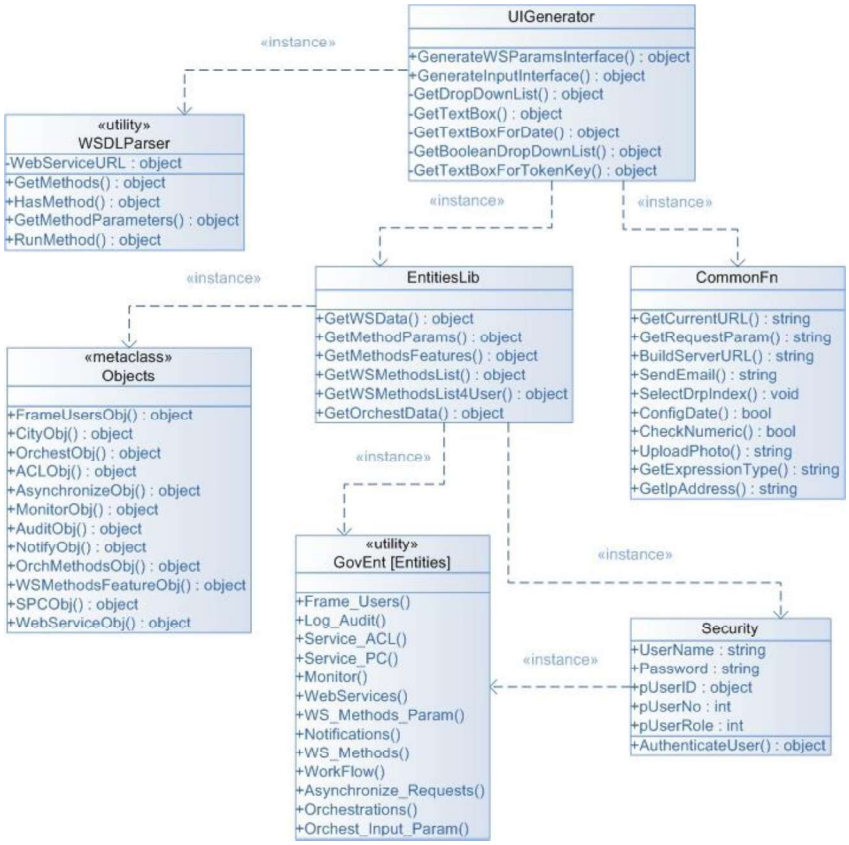
3-4 مخطط الصفوف لإطار العمل

تشترك مكونات إطار العمل بسبعة صفوف أساسية لتنفيذ الوظائف والمهام موضحة بالشكل (4):

(1) GovEnt يتضمن الوظائف الرئيسية لإدارة الكينونات (LINQ to SQL).

(2) EntitiesLib يتولى مهمة تنفيذ عمليات قواعد البيانات القياسية.

(3) Objects مجموعة من الصفوف الوصفية يستخدمها EntitiesLib كخزان لنقل البيانات ما بين مكونات إطار العمل.
(4) Security يتولى مهمة التحقق من هوية المستخدم وتسجيل جلسة دخول خاصة به.
(5) CommonFn يستخدم لتنفيذ بعض الوظائف العمومية غير المرتبطة بالكينونات.
(6) WSDLParser كائن مجرد يتولى مهمة قراءة ملف توصيف خدمة الويب WSDL.
(7) UIGenerator يتولى بناء واجهة استهلاك الخدمة بالاعتماد على البيانات الوصفية المسجلة ويمرر مدخلات المستهلك إلى WSDLParser لتنفيذها، ومن ثم يستلم النتيجة ويظهرها للمستهلك.
ويتموضع كائن المراقبة في مفاصل عمليات إطار العمل لمراقبة وتسجيل النتائج والأخطاء.



الشكل رقم (4): مخطط الصفوف

4-4 بيئة تشغيل إطار العمل

يتم تشغيل إطار العمل على مخدم ويندوز، مُنصّب عليه قواعد بيانات SQL Server الاصدار 2005 وما بعد، وخدمات معلومات الانترنت (Internet Information Services) IIS، مع حزمة Dot Net Framework 4.0.

يُوضع مخدم إطار العمل على الشبكة الحكومية الآمنة ويُمنح عنوان محدد، حتى يتمكن المشتركون المرخص لهم، الوصول إليه والبدء باستثمار إطار العمل الحكومي.

لضمان استمرارية العمل يفضل أن يكون هناك نسخة ثانية من إطار العمل مع نسخة احتياطية متزامنة من قاعدة البيانات، في حال تعطلت النسخة الأولى يمكن التحول مباشرة إلى النسخة الاحتياطية.

4-5 اختبار إطار العمل

بهدف اختبار إطار العمل تم إنشاء أربع قواعد بيانات لمحاكاة أربعة من السجلات الحكومية هي: (CivilianRecord للسجل المدني، CommerceRecord للسجل التجاري، CriminalRecord للسجل الجنائي، RealStateRecord للسجل العقاري) وحشرت ضمن هذه القواعد، بيانات معبرة عن طبيعة كل سجل، فتم حشر بيانات نصية وأخرى رقمية (صورة شخصية) مرمزة بالصيغة Base64، وتم تطوير خدمات ويب لكل من هذه السجلات لاسترداد المعلومات المستعلم عنها من خلال الرقم الوطني، الخدمات المطورة تسترد بيانات السجل المستهدف بصيغة نصية، تم اختبار إطار العمل ضمن ثلاث بيئات مختلفة:

1-جهاز محلي: احتضن كل من قواعد البيانات وإطار العمل وشغل خدمات الويب على عناوين مختلفة.

2-شبكة محلية: تضمنت أربع خوادم ويب موزعة على عناوين شبكة IP مختلفة كل منها عليه قاعدة بيانات وخدمة ويب خاصة بأحد السجل الحكومية الأربعة، ومخدم خامس مخصص لتشغيل إطار العمل.

3-شبكة الانترنت: تم نشر قواعد البيانات وإطار العمل وخدمات الويب على عناوين انترنت فرعية مختلفة كما يلي:

- ✓ إطار عمل الحكومة الالكترونية: http://egov.hama.gov.sy
- ✓ خدمة السجل التجاري: http://comrec.hama.gov.sy
- ✓ خدمة السجل الجنائي: http://interrec.hama.gov.sy
- ✓ خدمة السجل العقاري: http://realrec.hama.gov.sy
- ✓ خدمة السجل المدني: http://civilrec.hama.gov.sy

بالمجمل كانت نتائج الاختبار ناجحة ومتقاربة دون أية فوارق، سوى سرعة الأداء التي تعتمد على سرعة الاتصال.

4-6 النتائج العملية

الهدف الرئيسي للبحث هو وضع استراتيجية استثمار لمنهجية الخدمات الموجهة، ضمن إطار تفعيل مبادرة الحكومة الالكترونية السورية، والمخرج النهائي للبحث هو تطبيق تنفيذي لهذه الاستراتيجية.

في هذه الفقرة نستعرض ثلاث وظائف أساسية من وظائف إطار العمل المنفذ حسب الدراسة السابقة:

(1) تسجيل مزود/مستهلك:

للبدء باستثمار خدمات إطار العمل، لا بد من تسجيل اشتراك وفق النموذج الموضح بالشكل (5)

الشكل رقم (5): نموذج تسجيل مزود/مستهلك

بعد تسجيل الطلب، يتم اشعار مدير إطار العمل بالمشترك الجديد للتحقق من صحة البيانات، ويرسل بريد الكتروني لمقدم الطلب لتفعيل حسابه.

(2) تسجيل خدمة:

هذه الوظيفة متاحة لمزود الخدمة، وهي عملية بسيطة لا تحتاج لمعلومات تقنية أكثر من عنوان خدمة الويب على مخدم المزود Web Service URL، يدخل مزود الخدمة عنوان خدمة الويب، وبعد أن يتحقق إطار العمل من صحة العنوان، يقوم مزود الخدمة بإضافة الوظائف Methods كخدمات الكترونية مستهلكة، ويحدد شروط استهلاكها كما هو موضح بالشكل (6):

الشكل رقم (6): نموذج تسجيل خدمة الكترونية

(3) استهلاك الخدمة:

يدخل المستهلك محددات البحث، فيحصل على لائحة بالخدمات المتوفرة على إطار العمل كما في الشكل (7):

الشكل رقم (7): مخزن الخدمات الالكترونية

لإستهلاك الخدمة يختار وظيفة "تشغيل"، فيظهر له نموذج استهلاك الخدمة ويطالبه بإدخال البرامترات كما في الشكل (8):

الشكل رقم (8): نموذج إدخال برامترات استهلاك خدمة

بعد إدخال البرامترات المطلوبة "الرقم الوطني" يحصل المستهلك على خرج الخدمة مع إمكانية الطباعة، وبنفس الوقت يقوم كائن المراقبة بتوثيق عملية الاستهلاك من خلال رقم فريد UserToken وختم زمني TimeStamp لكل عملية، تسجل بأسفل خرج استهلاك الخدمة كما في الشكل (9):

الشكل رقم (9): خرج استهلاك خدمة (بيان قيد مدني)

يوفر إطار العمل أساليب مختلفة لاستهلاك الخدمة، وأكثر من طريقة لحماية الخدمة، يمكن اختيار المناسب منها حسبما تقتضيه الضرورة، وإذا أخذنا بعين الاعتبار الرقم الفريد المتولد مع الختم الزمني لكل عملية استهلاك، بالإضافة لضرورة حصوله على تفويض لاستهلاك الخدمات المحمية، نحصل على مقاربة لأسلوب عمل التوقيع الرقمي، أما الخدمات المحمية بكلمة مرور فهي تؤمن اسلوب حماية موزعة لا تشكل ضغط على إطار العمل أو تتسبب بحالات اختناق "عنق الزجاجة"، وتعتمد على التدابير الأمنية التي يحددها مزودة الخدمة مما يعزز ثقة المزود بسلامة وأمن استهلاك خدمته.

5-الاستناجات والتوصيات

(1) منهجية الخدمات الموجهة (SOA) ليست منتجاً يمكن استثماره، وإنما هي استثمار لاستراتيجية عمل، وهذا ما سعى البحث أن يوضحه ويطبقه من خلال مخرج نهائي يحقق معايير هذه المنهجية.

(2) لا يمكن لفريق عمل واحد مهما كان حجمه وامكانياته، أن يتحمل عبء إدارة كل الخدمات الالكترونية الحكومية، لذلك لم يغب البحث عن بعض الأهداف الأساسية المتعلقة بمقومات الواقع الاقتصادي والبشري، في ضرورة إيجاد حل رشيق سهل الاستخدام وبتكاليف مادية منخفضة ولا يشكل عبءً على الكادر الإداري للحكومة الالكترونية، فاعتمد منهجية الخدمات الموجهة بهدف توزيع العمل على كل مؤسسات الدولة، مما يسهم بتخفيف الأعباء وتسريع وتيرة العمل، ولم يشترط وجود بنية تحتية ذات مواصفات غير اعتيادية، اذ يمكنه العمل على الشبكة الحكومية الآمنة أو الشبكة الافتراضية الخاصة أو شبكة الانترنت، وللتخفيف من التكاليف المالية اتجه لتبني البروتوكولات القياسية وتجنب استخدام المنتجات التجارية.

(3) موضوع البحث هو "إطار عمل حكومة الكترونية"، وهو ليس موضوعاً بسيطاً يمكن لبحث واحد أن يلبي كل متطلباته، وبالرغم من أن إطار العمل المنجز قد حقق معظم ميزات الاقتران الفضفاض، إلا أنه ما من شك أن بعض من النقاط ما زالت مفتوحة، وهي محفز لانطلاق بحوث جديدة، لذلك يوصي البحث بما يلي:

أ-الخدمات المركبة هي أتمته لتنفيذ خدمات الكترونية متعددة ضمن شروط وحالات تفرع مختلفة، حرص البحث ألا يغفل عن هذا الجانب المهم، فقدم ضمن إطار العمل نموذج أساسي للخدمات المركبة، يقوم بتنفيذ متسلسل لعدة خدمات، حالات الاستخدام الأكثر تشعباً بحاجة لبحث مستقل لتغطيته هذا الجانب.

ب-اعتمد البحث على خدمات الويب web service (asmx) في استهلاك الخدمات، ولكن من المعلوم أن هناك حزمة أخرى للخدمات الموزعة هي Windows Communication Foundation (wcf) لذلك نوصي بفتح بحث جديد لإستهلاك هذا النوع من الخدمات.

ج-قدم البحث أساليب أمنية لحماية الخدمات وأرفق استهلاك الخدمة باجراءات توثيقية، لإعطائها صبغة قانونية، ولكن الأنسب أن يتم استخدام التوقيع الرقمي لهذا الهدف، وهذه نقطة بحث إضافية يوصى بها.

6-المراجع

[1] UN, D. o. (2014). United Nations E-Government Survey 2014. New York: United Nations.

[2] UN. (2018). United Nations E-Government Survey 2018. New York: United Nations.

[3] Josuttis, N. M. (August 2007). SOA in Practice The Art of Distributed System Design First Edition. O'Reilly Media, Inc.

[4] Fedict, e-gov Architecture, Blueprint. Retrieved from https://dt.bosa.be/sites/default/files/downloads/egov_architecture_architecture_blueprint_en.pdf

[5] OASIS. (2012, May 18). Web Services Security: SOAP Message Security Version 1.1.1. Retrieved from http://docs.oasis-open.org: http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SOAPMessageSecurity-v1.1.1.html

[6] W3C. (2007, June 26). Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language. Retrieved from W3C Recommendation: https://www.w3.org/TR/wsdl20/

[7] Karsten Januszewski, M. (2001, 10 3). *Web Service Description and Discovery Using UDDI, Part I*. Retrieved from MSDN: https://msdn.microsoft.com/en-us/library/aa480517.aspx

[8] IBM, M. O. (2005, FEBRUARY 3). UDDI v3.0 Ratified as OASIS Standard. Retrieved from oasis-open.org: https://www.oasis-open.org/news/pr/uddi-v3-0-ratified-as-oasis-standard

[9] Microsoft. (2018, May 31). Removal of UDDI Services. Retrieved from Microsoft Dev Center: https://docs.microsoft.com/en-us/windows/desktop/win7appqual/removal-of-uddi-services-from-server-os

[10] K. Karuna Jyothi, D. B. (2018, 10 08). Study on Virtual Private Network (VPN), VPN's Protocols And Security. IJSRCSEIT , 919-932.

[11] Regalado Reyes Jr, M. S. (2017). Interoperability Framework for Government EServices. Pacific Asia Conference on Information Systems (PACIS). Langkawi: Association for Information Systems AIS Electronic Library (AISeL).

[12] Zuhoor Al-Khanjari, N. A.-H. (2014). Developing A Service Oriented E-Government Architecture Towards Achieving E-Government Interoperability. International Journal of Software Engineering and Its Applications , 29-42.

[13] Suhail Madoukh, R. B. (2014). A SOA-Based e-Government Data Integration. International Arab Journal of e-Technology , 138-145.

[14] Al-Khouri, D. A. (2013). e-Government in Arab Countries: A 6-Staged Roadmap to Develop the Public Sector. Journal of Management and Strategy , 1-28.

[15] Anurag Shashwat, D. K. (2017). An End to End Security Framework for Service. International Conference on Infocom Technologies and Unmanned Systems (pp. 476-480). Dubai, UAE: IEEE.

[16] Memon M., H. M. (2009). Security as a Service - A Reference Architecture for SOA Security. SciTePress , 79-89.

[17] MOCT. (2009, October). eGov Strategy. Retrieved from moct.gov.sy: http://www.moct.gov.sy/sites/default/files/uploadss/eGov_Strategy_-_v2_04-Vol1_0.pdf

[18] MOCT. (2009, October). eGov Strategy Orientation. Retrieved from moct.gov.sy: http://moct.gov.sy/sites/default/files/uploadss/eGov_Strategy_-_v2_04-Vol2%20En.pdf

[19] MOCT. (2009, October). eGov Strategy Programs. Retrieved from moct.gov.sy: http://www.moct.gov.sy/moct.gov.sy/sites/default/files/uploadss/eGov_Strategy_-_v2_04-Vol3_0.pdf

[20] MOCT. (2009, October). SyGIF. Retrieved from moct.gov.sy: http://moct.gov.sy/sites/default/files/uploadss/SyGIF%20Arabic.pdf

[21] Portal, S. E.-G. (2012). E-Gov. Retrieved from http://www.egov.sy: http://portal.egov.sy