إطار التوثيق الإلكتروني في قطر

المجلس الأعلى للاتصالات وتكنولوجيا المعلومات "ictQATAR"

مرجع الوثيقة: CS 1212

تاريخ النشر: يونيو 2013

جدول المحتويات

التعريفات

جهة حكومية	أية جهة حكومية أو شبه حكومية، أو جهة مشمولة ضمن نطاق الوثيقة.
مزودو الخدمة (SP)	يقصد بمزود الخدمة مزود خدمات الاتصال بشبكة الإنترنت للمستخدمين. ويعتمد مزودو الخدمة على AOs لتوثيق المستخدمين قبل تزويدهم بالخدمة. كما يشار إلى مزودي الخدمة باسم "Relying Parties".
المستخدمون	المستخدمون هم الأطراف المشتركون في خدمات الاتصال بشبكة الإنترنت مثل المواطنين والمقيمين وكيانات الأعمال. حيث أن المستخدمين هم من يبدأ خدمة/ عملية الاتصال بشبكة الإنترنت، فإنهم يعرفون أيضاً باسم *"الطالب"* أثناء عملية التوثيق لأن المستخدم يقدم طلباً بشأن هويته.
تسجيل المستخدم	يعرف تسجيل المستخدم بالعمليات التي يشتمل عليها الإنشاء الأولي لهوية الكترونية لمستخدم ما. ويشمل ذلك عمليات *دليل الهوية (EOI)* أو عمليات *دليل العلاقة (EOR)*.
إصدار وإدارة الرمز	الرمز عبارة عن شيء يمتلكه الطالب ويتحكم فيه، ويستخدم لتوثيق هوية الطالب. ويقدم الرمز إلى المستخدم لعمليات التوثيق اللاحقة على شبكة الإنترنت. ولا يعتبر الرمز ثابتاً، وتعتبر الجهة المصدرة هي المسؤولة عن ضمان صلاحية الرمز طوال دورة حياته، وكذلك عن أية إجراءات تحديد لاحقة مطلوبة في حالة حدوث خلل وظيفي.
إدراج المستخدم	يشير إدراج المستخدم إلى عملية ربط اعتماد توثيق الكتروني بمثال معروف لمستخدم ضمن سياق أحد موارد تكنولوجيا المعلومات (مثل شبكة أو موقع الكتروني أو نظام طلبات) بهدف إتاحة وصول المستخدم.
التحقق من الاعتماد	يقصد بالتحقق من الاعتماد التحقق من أي رمز مدرج، وهو ما يتم قبل السماح بالعملية. ويشمل ذلك إصدار مؤشر هوية إيجابي، يُعرف باسم "التأكيد", إلى

	مزود الخدمة الذي قام بطلب العملية. ويستخدم مصطلح "الاعتماد" في هذا السياق مقابل كلمة الرمز: فالرمز كان سيتم إدراجه وربطه بمعرف قبل الحاجة للتحقق. وتعد المصادقة ضمنية هنا، وهو ما يشير إلى التأكد من حالة الاعتماد وقت التحقق.

1- التكليف القانوني

نص المرسوم بقانون رقم 36 لسنة 2004 على إنشاء المجلس الأعلى للاتصالات وتكنولوجيا المعلومات (ictQATAR)، وعينه كصانع سياسات ومنظم قطاع **الاتصالات و تكنولوجيا المعلومات**.

وبصفة خاصة، تنص المادة رقم 3 من المرسوم بقانون رقم 36 لسنة 2004 بإنشاء المجلس الأعلى للاتصالات وتكنولوجيا المعلومات على أن هدف المجلس يتمثل في تنظيم قطاعي الاتصالات و تكنولوجيا المعلومات ، وإنشاء مجتمع معلوماتي متقدم عن طريق إعداد بيئة مناسبة من البنية الأساسية ومجتمع قادر على استخدام مختلف أشكال الاتصالات و تكنولوجيا المعلومات.

بالإضافة إلى ذلك، تقر المادة رقم 4 من المرسوم بقانون رقم 36 لسنة 2004 بأن المجلس الأعلى هو أعلى سلطة مختصة في شؤون الاتصالات و تكنولوجيا المعلومات ؛ كما تنص على أن للمجلس صلاحية إنشاء البيئة القانونية والتنظيمية، وتنسيق المبادرات الوطنية المتعلقة بقطاعي الاتصالات و تكنولوجيا المعلومات وأهداف دولة قطر المتعلقة بذلك.

2- مقدمة

التوثيق الإلكتروني عبارة عن عملية تحديد درجة الثقة التي يمكن أن تُمنح للتأكيدات بأن مستخدم ما هو من يزعم أنه هو، أو أن هوية ما هي ما تعلن أنها هي. وتشمل التأكيدات الهوية والدور والتفويض والقيمة.
ويعنى إطار التوثيق الإلكتروني في قطر (QeAF) في المقام الأول بتأكيدات التوثيق الإلكتروني. وتتم العمليات الإلكترونية من خلال عدد من القنوات التي تشمل:

- ✓ شبكة الإنترنت
- ✓ الهاتف (الرد الصوتي التفاعلي IVR)
- ✓ رسائل الفاكس

وكنماذج التوثيق الأخرى، يعتمد التوثيق الإلكتروني على واحد أو أكثر مما يلي:

- ✓ شيء ما يعرفه المستخدم (مثل كلمة مرور، أسئلة وإجابات سرية)، أو
- ✓ شيء ما يمتلكه المستخدم (مثل رمز سري)، أو
- ✓ شيء ما ضمن خصائص المستخدم (مثل المواصفات الشخصية)

ويجب أن يحقق الأسلوب المختار التوازن بين متطلبات سهولة الاستخدام (سهولة الاستخدام من جانب المستخدم النهائي وعامل التكلفة) ومستوى مقبول من المخاطر.

وتتطلب التطبيقات ونظم المعلومات الحيوية نماذج توثيق أكثر قوة قادرة على مطابقة الهوية الرقمية للمستخدم بدقة، وذلك مقارنة بالتطبيقات منخفضة المخاطر.

3- النطاق والتطبيق

3-1 النطاق

ينطبق نطاق إطار التوثيق الإلكتروني في قطر على ما يلي:

- ✓ جميع الجهات الحكومية وشبه الحكومية
- ✓ جميع أجهزة القطاعات الحيوية
- ✓ منشآت الأعمال الخاصة المؤسسة أو التي تعمل في قطر.

ويجب أن تستخدم كل جهة هذا الإطار لتقييم وسائل التوثيق الإلكتروني القائمة لديها. كما يمكنها أيضاً أن تستخدم هذا الإطار كدليل عند وضع ضوابط جديدة للتوثيق الإلكتروني.

3-2 الحاجة لإطار التوثيق الإلكتروني

ومع التقدم الذي يتحقق في مجال التكنولوجيا وزيادة توفر الخدمات الإلكترونية على شبكة الإنترنت، يظهر المواطنون والمقيمون في قطر تفضيلاً واضحاً لتنفيذ معاملاتهم على شبكة الإنترنت. كما تدرك كيانات الأعمال أيضاً فوائد توسيع أفق انتشارها إلى ما وراء الوسائل التقليدية للعمليات.

ويهدف توفير الخدمات الإلكترونية على شبكة الإنترنت إلى تبسيط التفاعل والعمليات للمواطنين والمقيمين وكيانات الأعمال للتفاعل مع الحكومة من منازلهم ومكاتبهم بما يضمن لهم الراحة.

ومع ذلك، فإن هذه الراحة ترتبط بمخاطر التأكد من الهوية الإلكترونية للشخص أو المنشأة لتقديم توكيد معلوماتي للعملية المعنية.

ويرمي إطار التوثيق الإلكتروني في قطر إلى ضمان إقرار أسلوب استراتيجي من جانب الجهات المشاركة لتوكيد التحقق من الهوية الإلكترونية. ويدعم الإطار أسلوباً يعتمد على المخاطر، محققاً التوازن بين أهداف الأعمال والمخاطر.

3-3 الأدوار والمسؤوليات

إن مفتاح الوصول إلى حل ناجح للتوثيق الإلكتروني لا يتمثل في التكنولوجيا، بل في العمليات والإجراءات المساندة، ودعم الإدارة، والإدارة الفاعلة للإشكاليات الثقافية التي تنشأ عن التغيير.

أدوار ومسؤوليات أجهزة الدولة:

- ✓ دراسة حاجات وتطلعات الأفراد والشركات
- ✓ نشر التوعية بين المستخدمين
- ✓ توفير خدمات آمنة وموثوقة
- ✓ الالتزام بالسياسات والقواعد واللوائح الضرورية.
- ✓ معالجة البيانات الشخصية وفقاً لأخلاقيات العمل والقوانين ذات الصلة.

أدوار ومسؤوليات المستخدم:

- ✓ تقديم إثبات دقيق للهوية أو دليل على معلومات العلاقة.
- ✓ ضمان أمن الاعتمادات الصادرة.
- ✓ استخدام الاعتماد في الغرض المصدر له فحسب ووفقاً للإرشادات الصادرة.

4- أحكام أو مواد أو مقترحات السياسة

4-1 إطار التوثيق الإلكتروني

يقدم إطار التوثيق الإلكتروني في قطر إرشاداً بشأن النماذج المختلفة للتوثيق، ومختلف أنواع رموز التوثيق المتاحة ونقاط قوتها وضعفها، كما أنه يعرف المخاطر ذات الصلة في الحد من التهديدات المتعلقة بالهوية.

ويدعم هذا الإطار الخطوات المتكررة التالية كجزء من العملية العامة لإدارة المخاطر في أجهزة الدولة. وسوف يقدم ذلك إرشاداً بشأن اختيار نظام توثيق مناسب مزود بمستويات التوكيد المرغوبة اللازمة للوصول إلى المعلومات التي يتيح الوصول إليها.

4-2 تحديد متطلبات الأعمال

هذه هي الخطوة الأولى، كما أنها تعد جزءً من تعريف المتطلبات/ مرحلة التجميع.

فيما يلي بعض المتطلبات الرئيسية للأعمال والتي ستحكم اختيار حل التوثيق الإلكتروني:

1- تصنيف المعلومات: ما هي الخدمات/ المعلومات التي يتم الوصول إليها؟

2- مجتمع المستخدم: حدد المستخدم المستهدف (هل هو فرد أم فرد يتصرف نيابةً عن جهة؟) ومستوى المهارات التي يمتلكها المستخدم.

3- ما هي قنوات التسليم الإلكتروني المتاحة/ التي سيتم استخدامها؟
4- مخاوف/ آثار الخصوصية؟ هذا من ناحية المعلومات الشخصية التي يتم إتاحة الوصول إليها وكذلك استخدام الرموز الشخصية (البيانات الشخصية) في آلية التوثيق.
5- الالتزامات القانونية والتنظيمية.
6- أية متطلبات أخرى مثل اكتمال البيانات وسريتها وعدم إنكارها.

وتلتزم أجهزة الدولة بإجراء تحليل مخاطر يشمل مجموعة متنوعة من السيناريوهات المحتملة لتحديد التهديدات الممكنة المرتبطة بالعملية. فقد تنشأ التهديدات المحتملة من أعطال فنية أو من أطراف أخرى خبيثة أو لتعطل العمليات أو لخطأ بشري، على سبيل المثال لا الحصر.

ويوضح الجدول التالي مستوى إرشادي للتأكيدات التي يمكن استخدامها لتصنيف مختلف عمليات الأعمال.

غياب التأكيد	الحد الأدنى من التأكيد	تأكيد منخفض	تأكيد متوسط	تأكيد مرتفع
المستوى 0	المستوى 1	المستوى 2	المستوى 3	المستوى 4
لا يشترط الثقة في تأكيد الهوية.	يشترط توفر الحد الأدنى من الثقة في تأكيد الهوية.	يشترط مستوى منخفض من الثقة في تأكيد الهوية.	يشترط مستوى متوسط من الثقة في تأكيد الهوية.	يشترط مستوى مرتفع من الثقة في تأكيد الهوية.
البيانات المتاحة بشكل عام	المعلومات العامة	البيانات الشخصية	عمليات مالية/ حكومية	معلومات حساسة/ بيانات سرية على مستوى الدولة

جدول 1: مستويات التوكيد

وتشمل العوامل الرئيسية التي ستشكل متطلبات مستوى التوكيد على سبيل المثال البيانات أو المعلومات التي يجري معالجتها/ التعامل عليها، ومستوى الثقة أو الأمانة اللازم للتنفيذ.

3-4 تحديد شرط مستويات التوكيد

يمثل مستوى التوكيد الحد الأدنى من قوة التوثيق (الثقة) التي تتيحها عملية التوثيق (تماشياً مع متطلبات الأعمال والقيمة الممكنة للمعلومة أو العملية) للتخفيف من الأثر المحتمل في حالة تمكن مهاجم من الاستيلاء على وصول مستخدم شرعي.

ولتحديد مستويات التوكيد المطلوبة، تحتاج أجهزة الدولة إلى دراسة قوة المكونات التي تشكل حل التوثيق جنباً إلى جنب مع التهديدات المرتبطة بها وإدارة المخاطر بشكل عام للتخفيف من تلك المخاطر أو تقليلها إلى مستوياتها الدنيا.

ويعتبر مستوى التوكيد المطلوب وظيفة لما يلي:

1- قوة آلية التوثيق

2- قوة تسجيل هوية الجهة

ويساعد الجدول التالي في حساب مستوى التوكيد المطلوب.

قوة تسجيل هوية الجهة (1-4)	مرتفعة	الحد الأدنى (1)	منخفضة (2)	متوسطة (3)	**مرتفعة (4)**
	متوسطة	الحد الأدنى (1)	منخفضة (2)	متوسطة (3)	متوسطة (3)
	منخفضة	الحد الأدنى (1)	منخفضة (2)	منخفضة (2)	منخفضة (2)
	الحد الأدنى	الحد الأدنى (1)	الحد الأدنى (1)	الحد الأدنى (1)	الحد الأدنى (1)
		الحد الأدنى	منخفضة	متوسطة	مرتفعة
		قوة آلية التوثيق (1-4)			

جدول 2: مستوى التوكيد، وظيفة عملية تسجيل الهوية وآلية التوثيق

4-4 تحديد آلية التوثيق الإلكتروني ونظام إدارة الاعتماد

تعتمد قوة أو مستوى توكيد أي حل خاص من حلول التوثيق الإلكتروني على ما يلي:

1- قوة عملية التسجيل

2- قوة آلية التوثيق الإلكتروني التي تعتمد بدورها على:

أ- قوة رمز الاعتماد

ب-قوة استخدام إدارة الاعتماد

ويعرف رمز التوثيق أو الاعتماد بأنه شيء ملموس يخضع لتحكم المستخدم أو المشترك ويشمل واحد أو أكثر من الخصائص التالية:

- شيء ما يعرفه المستخدم/ المشترك
- شيء ما يمتلكه المستخدم/ المشترك
- أحد صفات المستخدم/ المشترك

كما تعرف هذه الخصائص أيضاً بمصطلح *العوامل*.

وتشمل عملية الإدارة العملية التي ينطوي عليها إنشاء الاعتماد/ الرمز وتوزيعه على المشترك/ المستخدم، وتنشيطه واستخدامه ضمن بروتوكول توثيق أوسع نطاقاً يؤسس بين المشترك وموثق هوية المستخدم.

وتعتمد القوة الفعالة لآلية التوثيق على القوة الفعالة لرمز الاعتماد وعمليات الإدارة التي تبنى حوله. ويجب أخذ العوامل التالية في الاعتبار عند اختيار رمز الاعتماد وأثناء بناء عملية الإدارة حوله.

رموز الاعتماد

1- أمثلة الرموز:

أ- عامل وحيد مثل كلمات المرور أو رمز بيانات شخصية أو بطاقة دخول... الخ

ب- عدة عوامل (مزيج من رمزين أو أكثر) مثل البطاقات الذكية المحمية برقم سري شخصي (PIN) وبطاقة دخول مع رمز بيانات شخصية...الخ

2- قوة رمز بعينه بالنسبة لمستوى التوكيد المطلوب.

3- سهولة استخدام الاعتماد بالنسبة لمجموعة العملاء المعنية.

4- قابلية الحل للترقية.

5- الاعتمادات القائمة التي يمكن أن تستخدم

6- القدرة على تلبية المتطلبات الإضافية مثل عدم الإنكار.

عملية الإدارة

1. من الممكن أن يؤثر سلوك حامل الاعتماد بشكل سيء على قوة التوكيد المقدم من الاعتماد نفسه وكذلك على عملية الإدارة. يجب إجراء فحص نافي للجهالة لضمان أخذ تلك التهديدات في الحسبان عند اتخاذ أية قرارات تتعلق باختيار آلية التوثيق.
2. تقديم التدريب والتوعية الكافية للمستخدمين النهائيين للتخفيف من مخاطر الاستخدام الاحتيالي.

فيما يلي جدول يوضح قوة آلية التوثيق.

قوة الاعتماد (1–4)	مرتفعة	منخفضة (2)	متوسطة (3)	**مرتفعة (4)**	**مرتفعة (4)**
	متوسطة	منخفضة (2)	متوسطة (3)	متوسطة (3)	**مرتفعة (4)**
	منخفضة	منخفضة (2)	منخفضة (2)	متوسطة (3)	متوسطة (3)
	الحد الأدنى	الحد الأدنى (1)	منخفضة (2)	منخفضة (2)	منخفضة (2)
		الحد الأدنى	منخفضة	متوسطة	مرتفعة
	قوة إدارة الاعتماد(1–4)				

جدول 3: قوة آليات التوثيق

5-4 تحديد شرط التسجيل

يتضمن التسجيل التحقق من أن هوية المشترك أو غيرها من الخصائص تصل إلى مستوى توكيد مفهوم* قبل إنشاء اعتماد توثيق إلكتروني.

وثمة عدد من العوامل التي تؤثر على متطلبات التسجيل. منها ما يلي:

1. طبيعة التوكيد المطلوب توثيقه
2. مستوى التوكيد المطلوب
3. ما إذا كان المستخدم قد صدر له اعتماد من قبل جهاز آخر من أجهزة الدولة. في هذه الحالة يجب أن تؤخذ عوامل إضافية في الاعتبار مثل:
   - أ- عملية التسجيل المستخدمة من قبل ذلك الجهاز
   - ب- عملية إدارة دورة حياة الاعتماد التي يستخدمها ذلك الجهاز.
4. السياسات والتشريعات التي تؤثر على العملية ككل.

ويعتمد أسلوب التسجيل على طبيعة التوكيد المطلوب توثيقه. ومنها ما يلي:

1- تسجيل أفراد (بأنفسهم)
2- تسجيل أفراد كممثلين لشركات
فيما يلي أكثر الأساليب شيوعاً:

إثبات الهوية(EoI) : يتطلب إثبات الهوية عرض الأفراد لوثائق سبق اعتمادها والتحقق منها وذلك من أجل التحقق من ادعائهم هوية ما. وتشمل تلك الوثائق شهادات ميلاد صادرة من جهات قانونية، أو وثائق جنسية أو جوازات سفر أو طرق تحقق مادية من قبل الجهات القانونية..الخ

*** يشير مستوى التوكيد هنا إلى الثقة التي تقدمها عملية التسجيل.**

إثبات العلاقة (EoR): يشار إلى إثبات العلاقة باسم آخر "عميل معروف"، ويتطلب هذا الإثبات قيام الافراد بإثبات وجود علاقة قائمة بينهم وبين جهاز الحكومة المعني. وبصفة عامة، فإن نشأة العلاقة الأصلية ستكون قد اشتملت على عملية إثبات الهوية. وقد يشمل إثبات العلاقة تقديم مستندات مثل تصاريح إقامة أو رخص قيادة...الخ

6-4 مراجعة حل التوثيق

بمجرد موافقة الجهة على مستوى التوكيد المطلوب، وتحديدها للمكونات الضرورية لتحقيق مستوى التوكيد المطلوب، يتعين تحديد وإقرار حل فني مناسب.

ولا تقع الاعتبارات المتعلقة باختيار التكنولوجيا ضمن نطاق هذه الوثيقة. ومع ذلك، فإن التكنولوجيا تعد عاملاً مهماً في الحل، ويجب إجراء فحص نافي للجهالة للتأكد من اختيار التصميم/ الطراز الصحيح (كحل مستقل مثلاً، أو حل تسجيل دخول أحادي (موحد) أو حلاً مركزياً للتوثيق الإلكتروني) والتكنولوجيا المناسبة لإكمال حل التوثيق الإلكتروني.

كما يجب إجراء إعادة المصادقة النهائية بعد تنفيذ الحل للتأكد من أن النظام يحقق مستوى التوكيد المطلوب ويلبي المتطلبات الأمنية اللازمة.

ويقوم الجهاز المعني من أجهزة الدولة بإعادة تقييم الحل على فترات دورية للتأكد من استمرار تلبيته لمتطلبات توثيق الهوية على نحو ملائم نتيجة لتغيرات التكنولوجيا أو التغيرات التي تطرأ على عمليات أو أهداف الأعمال.

5- التوصيات

يجب أن تعمل خدمات إدارة الهوية على ما يلي:

- ✓ إصدار رموز مطابقة الهوية بناءً على معيار سليم للتحقق من كينونة الفرد.
- ✓ أن تقاوم بقوة عمليات انتحال الهوية والتلاعب والتزوير وأي استغلال.

ويمكن الالتزام بهذه التوصيات بسهولة باستخدام نظام موحد للهوية.

الملاحق

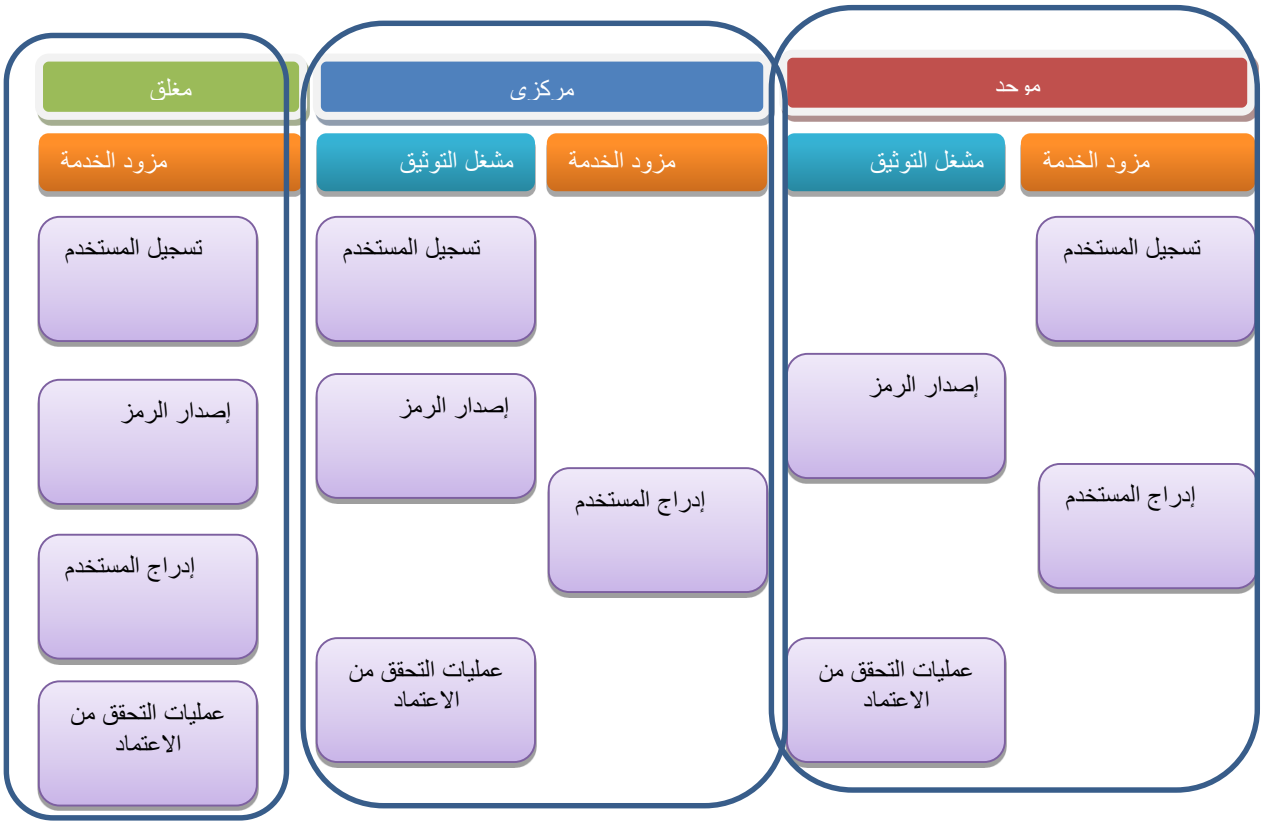
الملحق (أ) نموذج التوثيق الإلكتروني

يحتوي نظام التوثيق الإلكتروني على المكونات التالية ويدعم هذه الوظائف.

- ✓ مشغلو التوثيق (AO)
- ✓ مزودو الخدمة (SP)
- ✓ المستخدمون
- ✓ تسجيل المستخدم
- ✓ إصدار وإدارة الرمز
- ✓ إدراج المستخدم
- ✓ التحقق من الاعتماد

ويمكن تصنيف هيكل نظام التوثيق بصفة عامة إلى النماذج الثلاثة التالية:

1. مغلق Siloed
2. مركزي
3. موحد (نظام تسجيل أحادي)



جدول 4: نماذج التوثيق الإلكتروني

النموذج المغلق Siloed

يمثل هذا النموذج آليات التوثيق الحالية المستخدمة في شريحة الأجهزة الكبرى في الدولة في قطر.ويتم تقديم كافة الوظائف المركبة من قبل مزود الخدمة. ويتعاقد كل جهاز من أجهزة الدولة مع مزود الخدمة بشكل مستقل بغرض شراء وإنشاء آليات توثيق داخلية خاصة. وقد نتج عن ذلك امتلاك الفرد الواحد (المستخدم) عدة رموز توثيق في صورة رمز لكل جهاز يتعامل معه الفرد.

وحيث أن هذا النموذج يلغي الحاجة لمشغلو التوثيق، فإنه يؤدي في النهاية إلى عملية مبسطة لإنجاز المعاملة، بالإضافة إلى سرعة إنجاز المعاملات. ومع ذلك، فإن الحاجة لبنية تحتية داخلية سوف تتطلب إنفاق رأس مال أولي كبير، هذا بالإضافة إلى تكاليف الصيانة المستمرة، وهو ما قد يثبت أنه عائق أمام إتاحة الدخول للجميع، باستثناء المؤسسات الكبيرة جداً. ولا يستفيد هذا النموذج من اقتصادات الحجم التي يمكن تبادلها مع الشركاء والنظراء.

النموذج المركزي

يستهدف هذا النموذج المستخدم الذي يسجل مع مشغل توثيق لتقديم معرف موحد ورمز. بعد ذلك يتم إدراج بيانات اعتماد المستخدم (المعرف والرمز الموحد) لدى كل مزود خدمة. وعندما يطلب المستخدم خدمة، يقدم المستخدم بيانات اعتماده إلى مزود الخدمة؛ ويتم بعد ذلك إعادة توجيهها إلى مشغل التوثيق للتحقق منها.

وحيث أن خدمات التوثيق مسندة إلى جهة خارجية، لا يحتاج مزودو الخدمة إلى تحمل التكاليف المتعلقة بصيانة الأنظمة الداخلية لديهم. وتقل التكاليف التي يتحملها كل من مزود الخدمة والفرد بسبب المشاركة في البنية التحتية.

كما يتاح للفرد أيضاً أن يختار عامل وطريقة التوثيق. وتشمل المخاوف المتعلقة بهذا النموذج احتمالية ظهور نقطة عطل مفردة، وزيادة وقت العملية، وقضايا تتعلق بالخصوصية وتنشأ عن تسجيل معرف موحد لدى جميع مزودي الخدمة.

النموذج الموحد (نظام التسجيل الأحادي)

يختلف النموذج الموحد عن النموذج المركزي من ناحية عدم اشتراط وجود معرف موحد. وتقتصر مسؤولية مشغل التوثيق على إصدار الرمز فحسب. ويقوم المستخدم بإدراج الرمز المصدر لدى مزود الخدمة؛ ويتم ربط الرمز وخصائصه بالمعرف الخاص بالمستخدم لدى مزود الخدمة، وينتج الاعتماد عن ذلك. وفي كل مرة يطلب فيها المستخدم خدمة، يقوم المستخدم بعرض بيانات اعتماده إلى مزود الخدمة. ويقوم مزود الخدمة بدوره بطلب تحقق منفصل من الرمز المرفق من مشغل التوثيق. ويتم نقل التحقق الإيجابي إلى مزود الخدمة من مشغل التوثيق في صورة تأكيد.

وتخدم هذه الآلية كأساس **لنظام التسجيل الأحادي (SSO)** الذي ينعكس في صورة راحة أكثر للمستخدم حيث لا يتطلب الأمر سوى عملية توثيق واحدة للوصول إلى عدة مزودي خدمة، وذلك على أساس افتراض أن جميع مزودي

الخدمة المعنيين لهم علاقة بنفس مشغل التوثيق. ويقدم النموذج الموحد درجة إضافية من الخصوصية للمستهلك. فليس هناك معرف موحد كما هو الحال في النموذج المركزي، مما ينتج عنه انخفاض مخاطر ربط المحتوى من مزودي خدمة مختلفين بنفس المستخدم. ومن المتوقع أن يكون الوقت الأولي للعملية أطول نتيجة للتعقيد الكبير لتشغيل نظام التسجيل الأحادي؛ ولكن الأداء والتوكيد سيحظى بتعزيز أفضل بصورة عامة.

الملحق (ب): الأنواع المختلفة لرمز التوثيق الإلكتروني

الرمز عبارة عن شيء يمتلكه الطالب (المستخدم)ويتحكم فيه، ويستخدم لتوثيق هوية الطالب.ويقدم الرمز إلى الطالب (المستخدم) بغرض التوثيق الإلكتروني.

فيما يلي بعض الرموز التي يمكن استخدامها للتوثيق الإلكتروني. ولكل رمز منها نقاط قوة ونقاط ضعف. بالإضافة إلى ذلك، فإن الرمز قابل للعطل أو التلف أو التلاعب سواءً عن قصد أو بدون قصد.

ويتعين على الجهاز/ الجهة التي تصدر الرمز أن تأخذ الخطوات اللازمة لضمان صلاحية الرمز طوال دورة حياته.

الرمز السري المشترك

الرمز المشترك عبارة عن مجموعة رموز (حروف وأرقام ورموز خاصة مستخدمة في تراكيب مختلفة) أو مجموعة رسائل وإجابات محددة سلفاً (معلومات مشتركة) يتفق عليها بين الطالب (المستخدم) والمصدر. ويعبر عن أي تعديل طفيف في المعلومات المشتركة *بالمعلومات المشتركة الخاصة بالسياق* والتي تعتمد على المعلومات المتعلقة بالعلاقة بين الطرف موثق الهوية والطالب (المستخدم)

وتشمل هذه الأنواع من الرموز كلمات المرور ورقم الهوية الشخصية (PIN) والرسائل والإجابات المشتركة.

رمز البحث

رمز البحث عبارة عن شكل من أشكال كلمات المرور التي تستخدم لمرة واحدة لإتمام عمليات. ويتألف رمز البحث من قائمة أو قاعدة بيانات من *الرموز المشتركة* يقدمها المدقق للطالب (المستخدم). ويقدم الطالب (المستخدم) رمزاً غير مستخدم من هذه القائمة أو قاعدة البيانات بناءً على طلب المدقق.

وبصفة عامة، تستخدم رموز البحث كدرجة ثانية من التوثيق (*عامل مزدوج*) بعد التوثيق التقليدي الذي يعتمد على كلمة المرور الواحدة. ويشمل هذا النوع من الرموز دفاتر الرموز وبطاقات توثيق العمليات (TAN).

الرمز خارج النطاق

الرمز خارج النطاق عبارة عن سر يرسل من المدقق إلى المستخدم عن طريق *وسيلة اتصال ثانوية محددة مسبقاً*؛ ويقوم المستخدم بعد ذلك بتقديم ذلك السر في القناة الرئيسية للتوثيق. ويشمل هذا الاتصال خارج النطاق القنوات الصوتية الهاتفية والاتصالات الهاتفية التفاعلية (IVR) والرسائل النصية القصيرة على الهواتف النقالة، ورسائل البريد الإلكتروني...الخ. كما تشمل أشكال الاتصال خارج النطاق رد النداء على مصدر مسجل مسبقاً مثل عنوان بروتوكول الإنترنت (IP) أو أرقام الهواتف...الخ.

رمز كلمة المرور لمرة واحدة لكل حالة

رمز كلمة المرور التي تستخدم لمرة واحدة عبارة عن كلمة مرور تصلح لجلسة دخول أو لعملية واحدة فقط. ومن الصعب على الإنسان أن يتذكر كلمات المرور التي تستخدم لمرة واحدة، وبالتالي تتطلب هذه الرموز تكنولوجيا إضافية حتى تعمل. إن جهاز كلمة المرور لمرة واحدة عبارة عن جهاز يعرض كلمة مرور تستخدم لمرة واحدة وتحسب داخل الجهاز على أساس سر مشترك مع مصدر الاعتماد. وقد تتطلب أجهزة كلمات المرور التي تستخدم لمرة واحدة تقديم رقم تعريف شخصي (PIN) لتنشيط الجهاز لإنشاء كلمة مرور تستخدم لمرة واحدة، على الرغم من أن ذلك قد لا يكون ضرورياً في كل مرة.

الرمز المشفر

الرمز المشفر عبارة عن رمز متصل ومشفر متماثل أو غير متماثل يخزن في أجهزة أو برامج أو ينشأ فيها.
على سبيل المثال، يستخدم رمز مشفر لتشفير اعتراض صادر من المدقق ويقدم الرد. ويقوم المدقق بدوره بتشفير الرد، وإذا كان يتفق مع الاعتراض الذي أصدره في الأصل، فإنه يقوم بتفعيل توثيق الطالب (المستخدم) حيث أن المستخدم وحده هو الذي سيكون لديه الرمز الصحيح لتشفير الاعتراض في المقام الأول.

رمز البيانات الشخصية

رمز البيانات الشخصية عبارة عن سمة فسيولوجية أو سلوكية مميزة تقدم للتحقق بالرجوع إلى قاعدة بيانات لتلك السمات، ويتم إدارة وصيانة قاعدة البيانات تلك من قبل المدقق.
ومثال ذلك فحص شبكية العين أو قزحية العين أو بصمة الإصبع أو الصوت...الخ

الرمز الهجين

الرمز الهجين ليس رمزاً في حد ذاته، ولكنه يشير إلى استخدام رمزين أو أكثر معاً لرفع مستوى قوة عملية التوثيق.
ويشار إلى هذا النوع من الرموز أيضاً باسم *التوثيق متعدد العوامل*.
ومثال ذلك استخدام سر مشترك (كلمة مرور) أو رمز بيانات شخصية لفتح بطاقة ذكية تحتوي على الرمز المشفر الخاص بالمستخدم.

الملحق (ج) إدارة المخاطر

قد يحتوي النظام الخاص بأي جهاز من أجهزة الدولة على عدة فئات أو أنواع من العمليات، كما قد يمتد ذلك النظام إلى العديد من أجهزة الدولة؛ وقد تتطلب كافة تلك الأجهزة اعتبارات أمنية مختلفة ضمن التقييم العام للمخاطر.

وسوف يساعد برنامج رسمي لإدارة المخاطر على تحديد المخاطر المرتبطة بإدارة التوثيق الإلكتروني والحد منها. وقد تشمل هذه المخاطر ما يلي:

1. توثيق الهوية: هل بيانات الاعتماد الإلكتروني المقدمة ترجع إلى الشخص الذي يدعي أنه هو ذلك الشخص أو تحدد هويته؟
2. سلامة البيانات: هل تم تعديل المعلومات أثناء نقلها أو معالجتها؟
3. السرية: هل يمكن لجهاز الدولة ضمان استمرار سرية المعلومات أثناء تخزينها أو نقلها؟
4. عدم الإنكار: هل يمكن لجهاز الدولة أن يثبت أن هوية ما قد قدمت أو اعتمدت أو أشرت على المعلومات المستلمة؟

يجب أن تجري أجهزة الدولة تحليلاً شاملاً لكافة التهديدات الممكنة والتي تشمل عوامل مثل الأعطال العامة والسلوك البشري. وقد تصنف المخاطر العامة بأنها "منخفضة" بناءً على احتمالية تحقق التهديد، إلا أنه ينصح إضافة كافة سيناريوهات التهديد المحتملة أثناء مرحلة التحليل.

ويعد الخطر الناشئ من خطأ توثيق وظيفة عاملين هما:

1. التأثير المحتمل
2. احتمالية التأثير

وتشمل الفئات الممكنة للتأثير ما يلي:

1. ضياع سمعة جهاز الدولة أو التأثير عليها
2. أثر مالي
3. تأثير على برامج جهاز الدولة أو المصالح العامة
4. الإعلان عن معلومات حساسة دون موافقة
5. السلامة الشخصية
6. مخالفات مدنية أو جنائية/ تأثير قانوني

الخطوة التالية هي تحديد الأثر المحتمل لأخطاء التوثيق

الفئة	مستويات الشدة				
	غير مؤثر	أثر ضعيف	أثر متوسط	أثر كبير	أثر حاد
ضياع أو تضرر سمعة جهاز الدولة/ وقوع إزعاج لأي طرف	لا يوجد تأثير/ لا يوجد إزعاج	لا يوجد تأثير/ يوجد إزعاج بسيط	أثر ضعيف: ضرر قصير المدى/ إزعاج طفيف	ضرر محدود طويل المدى/ إزعاج مؤثر	إزعاج حاد أو خطير طويل المدى، إرباك لكافة أو بعض الأطراف المعنية
أثر مالي	لا توجد خسائر	خسارة بسيطة أقل من 2% من الموازنة الشهرية للجهاز	خسارة طفيفة ما بين 2% إلى أقل من 5% من الموازنة الشهرية للجهاز	خسارة متوسطة ما بين 5% إلى أقل من 10% من الموازنة الشهرية للجهاز	خسارة كبيرة تزيد عن 10% من الموازنة الشهرية للجهاز
ضرر لبرامج جهاز الدولة أو المصالح العامة	لا يوجد تهديد	لا يوجد تهديد	تعطل نشاط الجهاز أو الخدمة التي يقدمها على نحو طفيف. تأثير الخدمات على المستخدمين الداخليين، وبطريقة بسيطة على العملاء الخارجيين للجهاز.	تعطل نشاط الجهاز أو الخدمة التي يقدمها على نحو متوسط. تأثير الخدمات على العملاء الخارجيين لجهاز بطريقة رئيسية.	تعطل نشاط الجهاز أو الخدمة التي يقدمها على نحو حاد. تأثير الخدمات على الأجهزة الأخرى للدولة وخدماتها
الإعلان عن معلومات حساسة دون	لا يوجد تأثير	سيكون له تأثير بسيط	تأثير قابل للقياس، إخلال باللوائح أو	الإفصاح عن المعلومات سيكون له أثر	سيكون له نتائج خطيرة على الشخص أو

موافقة			بالالتزام بالحفاظ على السرية	كبير.	الجهاز أو النشاط.
السلامة الشخصية	لا يوجد مخاطر	لا يوجد مخاطر	خطر طفيف بحدوث إصابة لا تتطلب علاجاً طبياً	خطر متوسط بوقوع إصابة طفيفة أو خطر محدود بوقوع إصابة تتطلب علاجاً طبياً	خطر مرتفع بوقوع إصابة خطيرة أو وفاة
مخالفات مدنية أو جنائية/ تأثير قانوني	لن تساعد في الكشف عن نشاط غير قانوني أو تعوق الكشف عنه.	لن تساعد في الكشف عن نشاط غير قانوني أو تعوق الكشف عنه.	تضر بالتحقيق أو تسهل ارتكاب مخالفات سوف تخضع لجهود تنفيذ.	تعوق التحقيق أو تسهل ارتكاب جرائم خطرة.	تمنع إجراء التحقيق أو تسمح بصورة مباشرة بارتكاب جريمة خطيرة.

جدول 5: تقييم التأثير

كما أنه من الضروري أن نخطط لاحتمالية وقوع هذه التأثيرات من أجل تحديد مستوى التوكيد الذي سيتم تطبيقه.
ويوضح الجدول التالي تخطيط مرجعي للتأثيرات مقابل الاحتمالية:

الاحتمالية	النتائج/ التأثيرات				
	غير مؤثر	أثر ضعيف	أثر متوسط	أثر كبير	أثر حاد
شبه مؤكد	لا شيء	أثر منخفض	أثر متوسط	أثر كبير	أثر كبير
محتمل	لا شيء	أثر منخفض	أثر متوسط	أثر كبير	أثر كبير
ممكن	لا شيء	أثر بسيط	أثر منخفض	أثر متوسط	أثر كبير
غير محتمل	لا شيء	أثر بسيط	أثر منخفض	أثر متوسط	أثر متوسط
نادر	لا شيء	أثر بسيط	أثر منخفض	أثر متوسط	أثر متوسط

جدول 6: التأثير مقابل الاحتمالية (مستويات التوكيد المرجعية)

وعند تحليل المخاطر المحتملة، يجب على جهاز الدولة أن يأخذ في الاعتبار كافة النتائج المحتملة المباشرة وغير المباشرة لأي خلل في التوثيق، بما في ذلك إمكانية حدوث أكثر من خلل أو التأثير على عدة أشخاص.
ويشمل تعريف التأثير المحتمل مسميات مثل "خطير" أو "طفيف"، ويعتمد معنى "طفيف" على السياق. ويجب على أجهزة الدولة أن تأخذ في الاعتبار السياق وطبيعة الأشخاص أو الكيانات المتأثرة لتقرر الحجم النسبي لتلك التأثيرات.

إدارة المخاطر

يجب تلخيص تقييمات المخاطر من حيث فئات التأثير المحتمل (جدول رقم 5).

- ✓ حدد مستوى شدة التأثير لفئة التأثير المعنية بناءً على التحليل الذي تقوم به.
- ✓ حدد احتمالية تحقق التأثير أو التهديد.
- ✓ الوظيفة ستحدد لك مستوى المخاطر (جدول رقم 6).
- ✓ اختر الحد الأدنى لمستوى المخاطر الذي سيشمل كافة فئات التأثيرات أو التهديدات.
- ✓ يؤدي مستوى المخاطر الذي يتم اختياره إلى تحديد مستوى التوكيد.

المخاطر	مستوى التوكيد
لا يوجد	المستوى 0
بسيطة	المستوى 1
منخفضة	المستوى 2
متوسطة	المستوى 3
مرتفعة	المستوى 4

الجدول (7): تخطيط مستوى المخاطر تبعاً لمستوى التوكيد

وقد يكون حل التوثيق الإلكتروني الذي يتمتع بمستوى مرتفع من التوكيد إحدى طرق الحد من التهديدات، إلا أن أجهزة الدولة يجب أن تأخذ الأساليب البديلة لإدارة المخاطر بعين الاعتبار أيضاً. وقد يكون ذلك في شكل تعزيز الأمن في التطبيق، والحد تبادل المعلومات أو الكشف عنها، وتقييد بعض مجتمعات المستخدمين "المعرضة للخطر"...الخ.

كما يجب أن تكرر أجهزة الدولة تحليل المخاطر لضمان استيفاء الاستراتيجيات الحالية لأمن المعلومات لمتطلباتها، وضمان فعالية الضوابط والوظائف المنفذة حسب المطلوب.

ويتعين القيام بهذه الإجراءات على فترات دورية لإدارة المشهد المتغير للتهديدات، وكذلك كلما تغيرت متطلبات الأعمال.

الملحق (د): الإطار القانوني

يقدم إطار التوثيق الإلكتروني في قطر لأجهزة الدولة نظرة عامة على المبادئ والعوامل التي يجب دراستها عند تصميم حل التوثيق الإلكتروني. كما تحتاج أجهزة الدولة عند تطبيق هذه الوثيقة إلى دراسة العديد من السياسات والتوجيهات والتشريعات الوطنية التي قد يكون لها تأثير على مثل ذلك الحل.

فيما يلي بعض أبرز تلك السياسات والتوجيهات والتشريعات الوطنية:

1- سياسة تأمين المعلومات الحكومية
2- سياسة تسجيل وتوثيق الخدمات الإلكترونية الحكومية الصادرة بموجب قرار مجلس الوزراء رقم 18 لسنة 2010 بشأن تنفيذ سياسات الحكومة الإلكترونية.
3- قانون التجارة الإلكترونية والتوقيع الرقمي.
4- مقترح قانون حماية خصوصية البيانات الشخصية.
5- مقترح قانون حماية البنية التحتية المعلوماتية الهامة.

الملحق (هـ): حالة للمطابقة الهوية الموحدة

أصبح بإمكان الأفراد والشركات اليوم التواصل والوصول إلى موارد هامة بسهولة أكثر من ذي قبل. فشبكة الإنترنت تتيح للمستخدمين الاتصال المباشر بالبضائع والخدمات والمعلومات، في الوقت الذي تتيح فيه للشركات التواصل مع عملائها وموظفيها وشركائها في التجارة.

وتعد الهوية الرقمية عنصراً هاماً في نمو البيانات الحساسة والعلاقات السرية على شبكة الإنترنت. ويقوم جميع المستخدمين بإنشاء هويات رقمية عندما يجوبون الفضاء الإلكتروني. وفي الوقت نفسه، تقوم كل شركة بإنشاء هويات من تزويد الأفراد بوصول آمن للموارد والخدمات على شبكة الإنترنت. وبدون الهويات الرقمية، لا توجد طريقة لمنح بعض المستخدمين الوصول إلى بعض الموارد. وقد تشمل تلك الموارد كشف حساب بنكي أو وضع شحن طلبية أو دليل عناوين بريد إلكتروني لزملاء عمل أو شبكة داخلية لشركة، إلى غير ذلك مما لا يمكن حصره.

والقاعدة هي وجود هويات متعددة. فالأفراد يستخدمون أسماء مستخدمين وكلمات مرور مختلفة وغيرها من الخصائص المعرفة في مختلف السياقات على شبكة الإنترنت نظراً للقيود العملية أو للرغبة في إخفاء هوياتهم. فقد يكون لنفس الشخص عدة اتصالات بعدة جهات. كما قد يكون عميل شركة كيوتل مستخدماً لخدمات وزارة الداخلية وحساب لدى المؤسسة العامة القطرية للكهرباء والماء. وحتى داخل نفس الشركة، غالباً ما تظهر البيانات المرتبطة بنفس الشخص في عدة قواعد بيانات مختلفة، سواءً كان ذلك بحكم التصميم أو بشكل عرضي.

إن انتشار الهويات الرقمية يخلق تحديات كبيرة. فالمستخدمون يعانون مشكلة تذكر أسماء المستخدمين وكلمات المرور العديدة. كما تجد جهات تكنولوجيا المعلومات صعوبة متزايدة في إدارة قواعد بيانات الهوية الكبيرة، حتى مع وجود الجدران النارية للشركات. وتزداد المشكلة سوءً عندما تنتشر الهويات خارج نطاق حدود الجهة المعنية، كما هو الحال عندما يتم تزويد الشركاء بإمكانية الوصول إلى موارد شركة ما؛ مما يسمح للمستخدمين بالوصول إلى الخدمات الإلكترونية لشركة ما بقواعد بيانات متعددة نظراً لعمليات الاستحواذ والإرث. وعندما يأخذ المستخدمون أو الشركة طرقاً مختصرة، تكون النتيجة هي ارتفاع تكاليف الإدارة وزيادة المخاطر الأمنية.

لماذا الهوية الموحدة؟

الاتحاد عبارة عن طريقة موحدة تتيح لأجهزة الدولة تقديم الخدمات مباشرة للمستخدمين الموثوقين الذين لا تديرهم تلك الجهات بشكل مباشرة. ويتم منح الوصول لهويات من نطاق شركة ما (أو مزود هوية) إلى خدمات شركة أخرى (أو مزود خدمة).

وفي عملية الاتحاد، تلعب الجهات أحد دورين أو كلاهما: دور مزود الهوية أو دور مزود الخدمة.

ومزود الهوية هو الجهة الموثوقة والمسؤولة عن توثيق أي مستخدم نهائي وتأكيد هوية لذلك المستخدم بطريقة موثوقة لشركاء موثوقين. كما أن مزود الهوية مسؤول عن إنشاء الحساب وصيانته وإدارة كلمة المرور وإدارة الحساب بشكل عام. ويمكن أن يتم ذلك بآليات وأدوات أمنية قائمة مقبولة داخلياً. وإذا أخذنا رخصة القيادة كمثال، تكون الحكومة هي مزود الهوية المسؤول عن المصادقة على الهوية الحقيقية للمواطن.

ويُعرف الشركاء الذين يقدمون الخدمات أو يشتركون في الموارد ولكنهم لا يعملون كمزودي هوية باسم مزودي الخدمة. ويعتمد مزود الخدمة على مزود الهوية لتأكيد المعلومات الخاصة بالمستخدم، ثم يترك مزود الخدمة لإدارة مراقبة الوصول والانتشار بناءً على مجموعات الخصائص الموثوقة هذه.

فوائد الاتحاد

يضع الاتحاد آلية تعتمد على المعايير الموحدة لكل من مشاركة وإدارة معلومات الهوية مع تحركها بين النطاقات الأمنية والقانونية والخاصة بالجهات.

ويتيح الاتحاد وسائل منخفضة التكلفة لإنشاء نطاق مشترك للدخول الأحادي وكذلك معلومات موحدة بين مختلف الأجهزة. هو ما يعرف باسم نظام تسجيل الدخول الأحادي.

كما يتيح الاتحاد للأجهزة الأمنية إدارة عدة نطاقات أمنية بآلية بسيطة تتسم بالفعالية لربط الهويات المتكررة وإتاحة تسجيل الدخول الأحادي بين النطاقات الأمنية.

الخلاصة

في حين أن حلول إدارة الهوية المتوفرة اليوم قادرة على المساعدة في رفع مستوى الأمن وتقليل أوجه القصور المرتبطة بإدارة المستخدمين الداخليين والوصول إلى المعلومات الداخلية، إلا أن زيادة المستخدمين الذين يطلبون الوصول خارجة عن سيطرة أي جهاز واحد بعينه. وتتيح الهوية الموحدة لأجهزة الدولة أسلوباً منفتح المعايير لإتاحة الوصول المتزايد للمعلومات عبر الحدود الفاصلة.

ملاحظات

بناءً على قرار مجلس الوزراء رقم 18 لسنة 2010 بشأن تنفيذ سياسات الحكومة الإلكترونية، أصدر المجلس الأعلى للاتصالات وتكنولوجيا المعلومات سياسة تسجيل وتوثيق الخدمات الإلكترونية الحكومية والتي تنص على توثيق كافة الخدمات الإلكترونية الحكومية سواءً كانت مستضافة ومدمجة (خدمات مدمجة) أو مجرد خدمات يمكن الوصول إليها (بشكل عابر) من خلال بوابة "حكومي" من خلال خدمات إدارة الهوية التي تقدمها بوابة حكومي.