الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2725
(2014/07)

السلسلة Y: البنية التحتية العالمية للمعلومات
وملامح بروتوكول الإنترنت وشبكات الجيل التالي
شبكات الجيل التالي – الأمن

دعم تعرف الهوية المفتوح في شبكات الجيل التالي (NGN)

التوصيـــة ITU-T Y.2725

الاتحاد الدولي للاتصالات

توصيات السلسلة Y الصادرة عن قطاع تقييس الاتصالات

البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

البنية التحتية العالمية للمعلومات	
اعتبارات عامة	Y.199-Y.100
الخدمات والتطبيقات، والبرمجيات الوسيطة	Y.299-Y.200
الجوانب الخاصة بالشبكات	Y.399-Y.300
السطوح البينية والبروتوكولات	Y.499-Y.400
الترقيم والعنونة والتسمية	Y.599-Y.500
الإدارة والتشغيل والصيانة	Y.699-Y.600
الأمن	Y.799-Y.700
مستويات الأداء	Y.899-Y.800
جوانب متعلقة ببروتوكول الإنترنت	
اعتبارات عامة	Y.1099-Y.1000
الخدمات والتطبيقات	Y.1199-Y.1100
المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد	Y.1299-Y.1200
النقل	Y.1399-Y.1300
التشغيل البيني	Y.1499-Y.1400
جودة الخدمة وأداء الشبكة	Y.1599-Y.1500
التشوير	Y.1699-Y.1600
الإدارة والتشغيل والصيانة	Y.1799-Y.1700
الترسيم	Y.1899-Y.1800
تلفزيون بروتوكول الإنترنت عبر شبكات الجيل التالي	Y.1999-Y.1900
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099-Y.2000
جودة الخدمة والأداء	Y.2199-Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249-Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات في شبكات الجيل التالي	Y.2299-Y.2250
تحسينات على شبكات الجيل التالي	Y.2399-Y.2300
إدارة الشبكة	Y.2499-Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599-Y.2500
الشبكات القائمة على الرزم	Y.2699-Y.2600
الأمن	**Y.2799-Y.2700**
التنقلية العامة	Y.2899-Y.2800
البيئة المفتوحة عالية الجودة	Y.2999-Y.2900
شبكات المستقبل	Y.3499-Y.3000
الحوسبة السحابية	Y.3999-Y.3500

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـــة ITU-T Y.2725

دعم تعرف الهوية المفتوح في شبكات الجيل التالي (NGN)

ملخص

توصف التوصية ITU-T Y.2725 آليات وإجراءات لدعم واستعمال تعرف الهوية المفتوح "OpenID" من أجل السيناريوهات التي يقوم فيها مورد شبكات الجيل التالي بدور مورد معرف الهوية المفتوح.

وتقدم التوصية ITU-T Y.2724 إطاراً لدعم شبكات الجيل التالي واستعمالها للاستيقان المفتوح (OAuth) وتعرف الهوية المفتوح (OpenID). وتعتمد التوصية ITU-T Y.2725 على التوصيتين ITU-T Y.2722 وITU-T Y.2724 لتعريف آليات محددة لدعم تعرف الهوية المفتوح.

ملاحظـــة – لا تدخل التوصية ITU-T Y.2725 أي تغييرات أو تعديلات على بروتوكول تعرف الهوية المفتوح، حيث تركز على دعم واستعمال شبكات الجيل التالي لتعرف الهوية المفتوح.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T Y.2725	2014-07-18	13	11.1002/1000/12079

* للنفاذ إلى التوصية، يرجى طباعة العنوان الإلكتروني التالي: http://handle.itu.int/ في حقل العنوان بمتصفح الويب الخاص بك، متبوعاً بمعرف الهوية الفريد للتوصية. على سبيل المثال، http://handle.itu.int/11.1002/1000/11830-en.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

المحتـــويات

الصفحة

التوصيـــة ITU-T Y.2725

دعم تعرف الهوية المفتوح في شبكات الجيل التالي (NGN)

1 مجال التطبيق

تصف هذه التوصية آليات وإجراءات لدعم تعرف الهوية المفتوح في شبكات الجيل التالي. والآليات والإجراءات الموصوفة في هذه التوصية يمكن أن تستعمل من أجل دعم خدمات التطبيق في بيئة تضم موردي خدمات متعددين. وتفترض هذه التوصية أن مورد الشبكات NGN هو نفسه مورد تعرف الهوية المفتوح. والإحالة داخل هذه التوصية إلى وثيقة ما، لا يضفي على هذه الوثيقة صفة توصية.

2 المراجع

يشتمل ما يلي من توصيات قطاع تقييس الاتصالات والمراجع الأخرى على أحكام تشكل، من خلال الإشارة إليها في هذا النص، أحكاماً في هذه التوصية. وكانت الطبعات المشار إليها صالحة وقت نشر هذه التوصية. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات سارية الصلاحية.

[ITU-T Y.2701] التوصية ITU-T Y.2701 (2007)، *متطلبات الأمن لشبكة الجيل التالي – الإصدار 1.*

[ITU-T Y.2702] التوصية ITU-T Y.2702 (2008)، *متطلبات الاستيقان والتخويل في شبكات الجيل التالي الإصدار 1.*

[ITU-T Y.2720] التوصية ITU-T Y.2720 (2009)، *إطار إدارة الهوية في شبكات الجيل التالي.*

[ITU-T Y.2721] التوصية ITU-T Y.2721 (2010)، *متطلبات إدارة الهوية في شبكات الجيل التالي وحالات استخدامها.*

[ITU-T Y.2724] التوصية ITU-T Y.2724 (2013)، *إطار لدعم واستخدام بروتوكولي OAuth وOpenID في شبكات الجيل التالي.*

المعيار [OASIS XRI SYNTAX] *الإصدار 2.0 من قواعد تركيب معرف هوية الموارد الموسع (XRI).*

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في وثائق أخرى:

1.1.3 الاستيقان (من كيان) [b-ITU-T X.1252]: عملية تستعمل لتحقيق قدر كاف من الثقة في الربط بين الكيان والهوية المقدمة.

2.1.3 التخويل [b-ITU-T X.800]: منح الحقوق، الذي يتضمن منح النفاذ استناداً إلى حقوق النفاذ.

3.1.3 منح التخويل [b-IETF RFC 6749]: منح التخويل هو بيان اعتماد يمثل تخويل مالك المورد (بالنفاذ إلى موارده المحمية) ويستخدمه العميل للحصول على تأشيره نفاذ.

4.1.3 مخدم التخويل [b-IETF RFC 6749]: مخدم يصدر تأشيرات النفاذ إلى العميل بعد نجاح استيقان مالك المورد والحصول على تخويل.

5.1.3 العميل [b-IETF RFC 6749]: تطبيق يتقدم بطلبات على مورد محمي نيابة عن مالك المورد وبتخويل منه. ومصطلح "العميل" لا يعبر عن أي خصائص تنفيذ معينة (على سبيل المثال، ما إذا كان التطبيق ينفذ في مخدم أو على سطح المكتب، أو في أجهزة أخرى).

2.3 مصطلحات معرّفة في هذه التوصية

لا توجد.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

FE كيان وظيفي *(Functional Entity)*

FRA المتطلبات الوظيفية والمعمارية *(Functional Requirements and Architecture)*

IdM إدارة الهوية *(Identity Management)*

IdP مورّد الهوية *(Identity Provider)*

IETF فريق مهام هندسة الإنترنت *(Internet Engineering Task Force)*

IP بروتوكول الإنترنت *(Internet Protocol)*

OAuth بروتوكول التخويل OAuth 2.0 *(OAuth 2.0 Authorization Protocol)*

OP مورد خدمة تعرف الهوية المفتوح *(OpenID Provider)*

SAML لغة ترميز تأكيد الأمن *(Security Assertion Markup Language)*

URI معرف الموارد الموحد *(Uniform Resource Identifier)*

WS مخدم ويب *(Web Server)*

5 اصطلاحات

الكلمات الرئيسية "**يجب**"، أو "**يلزم**"، أو "**مطلوب**" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

وكلمة "**يوصَى**" تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا حاجة تدعو لتوفر هذا المتطلب لزعم المطابقة.

وكلمة "**يحظر**" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

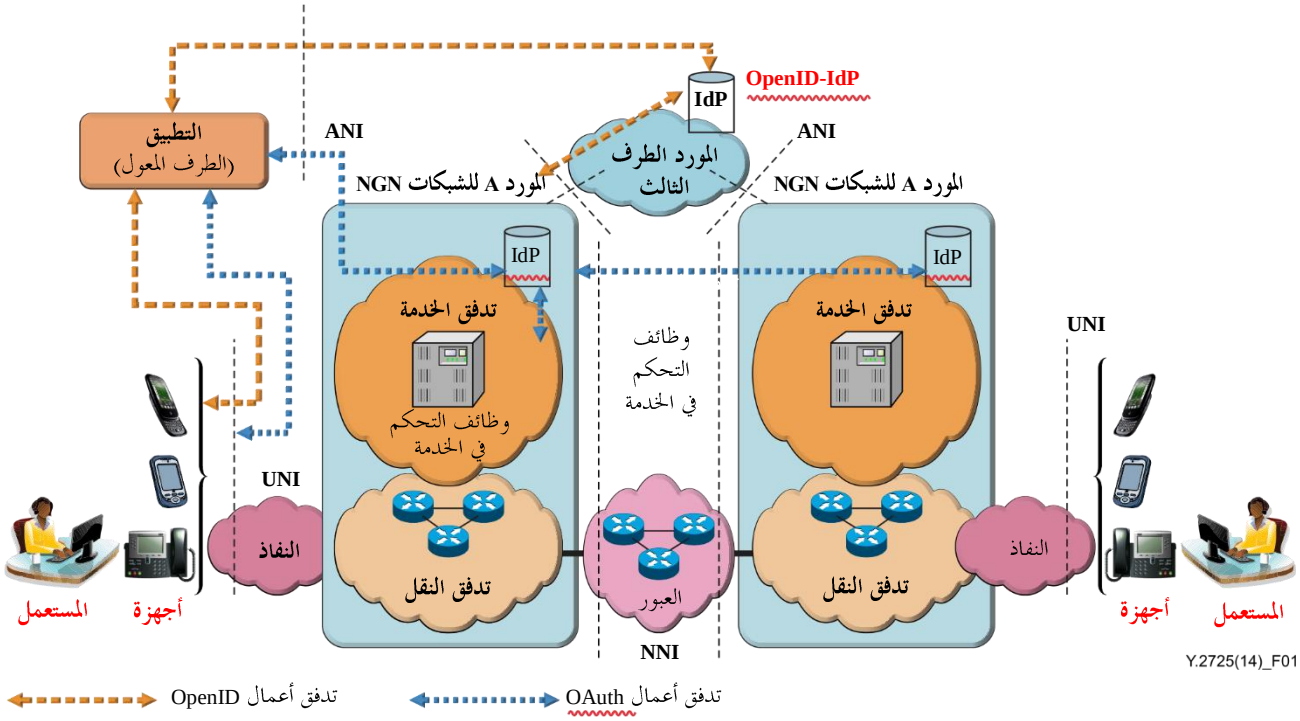
وكلمات "**يمكن اختيارياً**"، أو "**يجوز**" أو "**من الجائز**"، أو "**ربما**" تدل على مطلب خياري مسموح به دون أن ينطوي على أي توصية به. ولا ترمي هذه المصطلحات إلى إلزام التطبيق بتوفير الجهة البائعة لهذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مقدم الخدمة خيارياً. بل إن الجهة البائعة يمكنها إدراج هذا الخيار وزعم مطابقة المواصفة في نفس الوقت.

6 دعم تعرف الهوية المفتوح (OpenID) في شبكات الجيل التالي

تشرح هذه الفقرة الجوانب الرئيسية لدعم تعرف الهوية المفتوح (OpenID) في شبكات الجيل التالي.

1.6 النموذج المرجعي

طبقاً لمواصفة تعرف الهوية المفتوح [b-OpenID v.2]، يشارك مخدم مورد الهوية لتعرف الهوية المفتوح في كامل تدفق أعمال الاستيقان. يرجى الرجوع إلى التوصية [ITU-T Y.2724] للاطلاع على مجمل عام لإطار الاستيقان وتعرف الهوية المفتوحين ((OAuth) و(OpenID)).



الشكل 1 – تدفقات أعمال OpenID وOAuth في شبكات الجيل التالي

2.6 أنساق رسائل البروتوكول في سياق شبكات الجيل التالي

يعرف الإصدار [b-OpenID v.2] نمطين من أنماط أنساق رسائل البروتوكول:

- تشفير شكل قيمة المفتاح،
- وتشفير HTTP.

ويشرح القسم 1.1.4 من هذا الإصدار أن "تشفير شكل قيمة المفتاح يستعمل في حساب التوقيع وفي الردود المباشرة على الأطراف المعولة".

وبالنسبة للتشفير HTTP، يشرح القسم 2.1.4 من هذا الإصدار أن "هذا النموذج ينطبق على الرسائل الصادرة عن وسيط المستعمل إلى كل من الطرف المعول والمورِّد OP، فضلاً عن الرسائل الصادرة عن الطرف المعول إلى المورِّد OP".

من الضروري وجود كيانات مدعومة لشبكات الجيل التالي للوفاء بالمتطلبات اللازمة عند إرسال أي من رسائل البروتوكول.

3.6 أنماط الاتصالات

يعرف الإصدار [b-OpenID v.2] نمطين من أنماط الاتصالات:

- الاتصالات المباشرة،
- الاتصالات غير المباشرة.

ويشرح القسم 1.5 من هذا الإصدار أن الاتصالات المباشرة يستهلها أي من الأطراف المعولة إلى موقع URL لنقطة طرفية OP. وتستعمل هذه الاتصالات من أجل إقامة روابط وللتحقق من إثباتات الاستيقان.

ويشرح القسم 2.5 من الإصدار نفسه أنه في الاتصالات غير المباشرة، تمر الرسائل عبر وسيط للمستعمل. وتستهل هذه الاتصالات إما بواسطة الطرف المعول أو المورِّد OP. وتستعمل الاتصالات غير المباشرة لطلبات وردود الاستيقان.

والكيانات المدعومة بشبكات الجيل التالي ضرورية للوفاء بهذه المتطلبات عند استهلال سياق الاتصالات.

4.6 توليد التوقيعات

استيقان تعرف الهوية المفتوح يدعم خوارزميتين للتوقيع:

- HMAC-SHA1 – طول المفتاح 160 بتة
- HMAC-SHA256 – طول المفتاح 256 بتة

ويقدم هذا القسم توصيات من أجل استعمال الخوارزمية HMAC-SHA256. وإجراء توليد توقيع على رسالة الوارد توصيفه في القسم 1.6 من الإصدار [OpenID v.2]، يستوفي متطلبات أمن الشبكات الجيل التالي.

5.6 إجراءات استيقان تعرف الهوية المفتوح في شبكات الجيل التالي

1.5.6 طلبات الاستيقان

يوصي القسم 13 من الإصدار [b-OpenID v.2] بأنه "يوصى بأن تستعمل الأطراف المعولة البروتوكول Yadis لنشر عودتهم السارية إلى المواقع URL. وبوسع الطرف المعول أن ينشر اختيارياً هذه المعلومات على أي من المواقع URL ويوصى بأن ينشرها في إطار يسمح للموردين بالتحقق من العودة إلى المواقع URL".

وتستوجب هذه التوصية أن توصي الأطراف المعولة باستعمال البروتوكول Yadis لنشر رسائل العودة السارية الخاصة بها إلى المواقع URL في شبكات الجيل التالي.

ويرد توصيف طلبات الاستيقان في القسم 9 من الإصدار [b-OpenID v.2].

وتطبق المتطلبات التالية على معاملة الطرف المعول مع أي من المستعملين النهائيين. ويتعين على الطرف المعول:

- أن يستهل استيقاناً OpenID
- أن يعاير معرف هوية مقدم من المستعمل
- أن يكتشف المعلومات الضرورية لاستهلال الطلبات

1.1.5.6 استهلال استيقان OpenID

يوصي القسم 1.7 من الإصدار [b-OpenID v.2] بالتالي: "لاستهلال استيقان OpenID، يوصي الطرف المعول بتزويد المستعمل النهائي باستمارة تتضمن حقلاً لإدخال معرف هوية مقدم من المستعمل".

ويوصي بأن يكون لنعت حقل الاسم "name" بالاستمارة القيمة "openid_identifier"، بحيث يتسنى لوسطاء المستعملين أن يحددوا أوتوماتياً أن هذه استمارة OpenID. وقد لا تكتشف توسيعات المتصفحات أو غيرها من البرمجيات التي تدعم الاستيقان OpenID دعم طرف معول ما إذا لم يضبط هذا النعت بالشكل المناسب.

وتستوجب هذه التوصية إدراج حقل "openid_identifier" في الاستمارة التي يعرضها كيان الطرف المعول في شبكات الجيل التالي.

2.1.5.6 معايرة معرف هوية مقدم من المستعمل

يعرف الإصدار [b-OpenID v.2] ثلاثة أنواع من معرفات الهوية: معرف هوية URI من النمط "http" أو "https" (يشار إليه عادةً بموقع "URL" في هذه الوثيقة) أو معرف XRI [b-OASIS XRI SYNTAX 2.0].

وتتعين معايرة دخل المستعمل النهائي إلى معرف هوية، ويستوفي الإجراء الموصف في القسم 2.7 من الإصدار [b-OpenID v.2] متطلبات المعايرة الخاصة بشبكات الجيل التالي.

3.1.5.6 اكتشاف المعلومات اللازمة لاستهلال الطلبات

يشرح الإصدار [b-OpenID v.2] أن الاكتشاف "عملية يستخدم فيها الطرف المعول معرف الهوية للبحث عن ("اكتشاف") المعلومات اللازمة لاستهلال الطلبات".

وللاستيقان OpenID ثلاثة مسيرات يقوم خلالها بعملية الاكتشاف، يرد وصفها في القسم 3.7 من نفس الإصدار.

ويحدد هذا الإصدار طريقتين للاكتشاف:

- اكتشاف قائم على XRDS
- اكتشاف قائم على HTML

فعند استعمال اكتشاف XRI [b-OASIS XRI SYNTAX 2.0] أو Yadis، تكون النتائج وثيقة XRDS. وهذه الوثيقة تعتبر وثيقة XML بمدخلات للخدمات تتعلق بمعرف الهوية، كما هو محدد في القسم 1.2.3.7 من هذا الإصدار.

ويجب أن يدعم الطرف المعول الاكتشاف القائم على HTML. ولا يستخدم هذا الاكتشاف إلا في اكتشاف معرفات هوية مزعومة. ويجب أن تكون معرفات الهوية XRI OP [b-OASIS XRI SYNTAX 2.0] أو مواقع URL تدعم الاكتشاف XRDS. ولاستخدام الاكتشاف القائم على HTML، يجب توفر وثيقة HTML عند الموقع URL لمعرف الهوية المزعوم، كما هو موصف في القسم 3.3.7 من الإصدار [b-OpenID v.2].

وتستوجب هذه التوصية ضرورة استيفاء الطرف المعول لهذه المتطلبات عند إجراء الاكتشاف ويوصى بأن يتفق معرف الهوية مع النسق XRI أو النسق URL.

2.5.6 ردود الاستيقان

يوصي القسم 10 من الإصدار [b-OpenID v.2] بأنه عندما يصل طلب استيقان من وسيط المستعمل عبر اتصالات غير مباشرةً، فإن المورد OP يوصى بأن يحدد أن هناك مستعمل نهائي مخول يرغب في استكمال الاستيقان، فإذا كان هناك مستعمل نهائي مخول يرغب في استكمال الاستيقان، يوصي المورد OP بأن يرسل تأكيد إيجابي إلى الطرف المعول.

وتستوجب هذه التوصية إدراج "عودة إلى" المعلمة ضمن طلبات التخويل.

ملاحظـــة – طرائق تحديد المستعملين النهائيين المخولين والحصول على الموافقة على إعادة تأكيد استيقان OpenID خارج مجال تطبيق هذه المواصفة.

1.2.5.6 التأكيدات الإيجابية

التأكيدات الإيجابية عبارة عن ردود غير مباشرة لمعلومات عن معلمات الردود، انظر القسم 1.10 من الإصدار [b-OpenID v.2].

وطبقاً لهذا الإصدار، فإن المورد OP، عند إقامته لاتصالات غير مباشرة مع طرف معول عبر وسيط لمستعمل، يجب عليه:

- التحقق من أن العودة إلى الموقع URL تتفق مع أي من النقاط الطرفية للطرف المعول
- تحديد أن هناك مستعملاً نهائياً مخولاً يرغب في استكمال الاستيقان
- توليد رسالة رد
- توقيع رد إيجابي
- إرسال التأكيد الإيجابي إلى الطرف المعول عبر وسيط المستعمل.

2.2.5.6 التأكيدات السلبية

إذا تعذر على المورد OP تعريف المستعمل النهائي أو إذا لم يقم المستعمل النهائي بقبول طلب الاستيقان أو تعذر عليه ذلك، يوصي المورد OP بإرسال تأكيد سلبي إلى الطرف المعول كرد غير مباشر، انظر كذلك في القسم 2.10 من الإصدار [b-OpenID v.2].

عند تلقي تأكيد سلبي رداً على طلب الأسلوب "checkid_immediate"، توصى الأطراف المعولة بإعداد طلب استيقان جديد باستخدام الأسلوب "checkid_setup".

1.2.2.5.6 التأكيدات السلبية عند الرد على طلبات فورية

إذا كان الطلب طلباً فورياً، فلن تكون هناك فرصة أمام المستعمل النهائي للتعامل مع صفحات المورد OP لتوفير إثباتات التعريف أو لقبول الطلب. ويأخذ التأكيد السلبي على الطلبات الفورية الشكل الموصف في القسم 1.2.10 من الإصدار [b-OpenID v.2].

2.2.2.5.6 التأكيدات السلبية عند الرد على طلبات غير فورية

حيث إنه يمكن للمورد OP أن يعرض على المستعمل النهائي صفحات ويطلب منه إثباتات، فإن الرد السلبي على أي طلب غير فوري يكون نهائياً. ويأخذ هذا الرد الشكل الموصف في القسم 2.2.10 من الإصدار [b-OpenID v.2].

وإذا تلقى الطرف المعول الرد "إلغاء"، فهذا يعني أن الاستيقان لم ينجح ويجب على الطرف المعول التعامل مع المستعمل النهائي بوصفه غير مستيقن منه.

3.5.6 التحقق من التأكيدات

طبقاً للإصدار [b-OpenID v.2]، يتعين على الطرف المعول أن يقوم، عند تلقي تأكيد إيجابي، بما يلي:

- التحقق من موقع URL للعودة
- التحقق من المعلومات المكتشفة
- فحص الرسالة
- التحقق من التوقيعات

إذا ما تم التحقق من التأكيد وكان يتضمن معرف هوية مزعوماً، يكون المستعمل في هذه الحالة مستيقناً بمعرف الهوية هذا.

6.6 الاعتبارات الأمنية

يقدم القسم 15 (الاعتبارات الأمنية) من المواصفة OpenID 2.0 [b-OpenID v.2] توجيهات أمنية لتفادي الهجمات ووسطاء المستعملين والسطوح البينية للمستعملين ومعرفات المواقع URL من النمطين HTTP وHTTPS وتغايرات البروتوكول. وتوصي هذه التوصية بدعم جميع الاعتبارات الأمنية في شبكات الجيل التالي.

وينبغي للحلول أن تمتثل كذلك للمتطلبات الأمنية لشبكات الجيل التالي ولإدارة الهوية الموصفة في التوصيات [ITU-T Y.2701] و[ITU-T Y.2720] و[ITU-T Y.2721].

بيبليوغرافيا

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-OpenIDv.2] OpenID Authentication 2.0.
http://openid.net/specs/openid-authentication-2_0.html

[b-Yadis] Yadis Protocol.
http://infogrid.org/trac/wiki/Yadis

[b-IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework*.
http://tools.ietf.org/html/rfc6749

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن
السلسلة Y	**البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي**
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2015