الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2724

(2013/11)

السلسلة Y: البُنية التحتية العالمية للمعلومات
وملامح بروتوكول الإنترنت وشبكات الجيل التالي
شبكات الجيل التالي – الأمـــن

إطار لدعم التخويل المفتوح (OAuth) وتعرف الهوية المفتوح (OpenID) في شبكات الجيل التالي

التوصيـــة ITU-T Y.2724

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
نوعية 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
نوعية الخدمة والأداء	Y.2199-Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249-Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2299-Y.2250
الترقيم والتسمية والعنونة	Y.2399-Y.2300
إدارة الشبكة	Y.2499-Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599-Y.2500
الشبكات الذكية الشمولية	Y.2699-Y.2600
الأمـــن	**Y.2799-Y.2700**
التنقلية المعممة	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.2724

إطار لدعم التخويل المفتوح (OAuth) وتعرف الهوية المفتوح (OpenID) في شبكات الجيل التالي

ملخص

تصف التوصية ITU-T Y.2724 إطاراً لدعم استخدام بروتوكول التخويل المفتوح (OAuth) وبرتوكول تعرف الهوية المفتوح (OpenID) الصادرين عن فريق مهام هندسة الإنترنت في سياق شبكات الجيل التالي (NGN). وجرى تعريف البروتوكولين للاستعمال العام في شبكة الإنترنت العالمية.

والمتطلبات المعززة لإدارة الأمن والهوية في شبكات الجيل التالي تتطلب تقييداً متأنياً للبروتوكولين أعلاه. وتشرح هذه التوصية تطبيق هذين البروتوكولين على شبكات الجيل التالي وتقدم مبادئ توجيهية رفيعة المستوى بشأن استعمالهما.

وهناك توصية أخرى من نفس العائلة، التوصية ITU-T Y.2723، "دعم التخويل المفتوح (OAuth) في شبكات الجيل التالي"، تقدم مجموعة مفصلة من مواصفات شبكات الجيل التالي.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	المعرف الوحيد*
1.0	ITU-T Y.2724	2013-11-15	13	11.1002/1000/11914

* للوصول إلى التوصية يرجى إدخال العنوان URL التالي: http://handle.itu.int/ في حقل العنوان في متصفح الويب الخاص بك ثم إدخال المعرف الوحيد 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، تعد 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، كان الاتحاد قد تلقّى 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/.

© ITU 2014

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

1 مجال التطبيق 1

2 المراجع 1

3 التعاريف 1

1.3 المصطلحات المعرَّفة في وثائق أخرى 1

2.3 مصطلحات معرَّفة في هذه التوصية 2

4 المختصرات 2

5 إصطلاحات 3

6 إطار دعم التخويل المفتوح OAuth وتعرّف الهوية المفتوح OpenID في شبكات الجيل التالي 3

1.6 النموذج المرجعي 4

2.6 تدفقات بروتوكولي OAuth وOpenID 4

التذييل I – حالات استخدام منتقاة 9

1.I حالة استخدام: مخدم على شبكة الإنترنت 9

2.I حالة الاستخدام: بيانات اعتماد العميل 10

3.I حالة الاستخدام: التأكيد 11

بيبليوغرافيا 12

إطار لدعم التخويل المفتوح (OAuth) وتعرف الهوية المفتوح (OpenID) في شبكات الجيل التالي

1 مجال التطبيق

تصف هذه التوصية إطاراً لدعم واستخدام التخويل المفتوح (OAuth) وتعرف الهوية المفتوح (OpenID) في شبكات الجيل التالي (NGN). ويشمل مجال تطبيق هذه التوصية ما يلي:

- إطار وظيفي لدعم واستخدام التخويل المفتوح (OAuth) وتعرف الهوية المفتوح (OpenID) في شبكات الجيل التالي
- متطلبات دعم التخويل المفتوح (OAuth) وتعرف الهوية المفتوح (OpenID) في شبكات الجيل التالي
- حالات استخدام التخويل المفتوح (OAuth) وتعرف الهوية المفتوح (OpenID) (موثقة في التذييل I).

ملاحظـــة – يتعين على المنفذين والمشغلين للتكنولوجيا الموصوفة أن يلتزموا بجميع القوانين واللوائح والسياسات الوطنية والإقليمية السارية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. 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. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T Y.2012] التوصية ITU-T Y.2012 (2010)، *المتطلبات الوظيفية والمعمارية في شبكات الجيل التالي*.

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

[ITU-T Y.2722] التوصية ITU-T Y.2722 (2011)، *آليات إدارة الهوية في شبكات الجيل التالي*.

[IETF RFC 6749] المعيار IETF RFC 6749 (2012)، *إطار التخويل OAuth 2.0* .<http://tools.ietf.org/html/rfc6749>.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 تأشيرة النفاذ [IETF RFC 6749]: تأشيرات النفاذ هي بيانات اعتماد تُستخدم للنفاذ إلى موارد محمية. وتأشيرة النفاذ هي سلسلة تمثل التخويل الصادر إلى العميل. وهذه السلسلة مبهمة عادة بالنسبة إلى العميل. وتمثل التأشيرات نطاقات وفترات محددة من النفاذ الممنوح من مالك المورد، ويُعمل بها لدى مخدم المورد ومخدم التخويل.

2.1.3 الاستيقان (من كيان) [b-ITU-T X.1252]: عملية تحقيق قدر كافٍ من الثقة في الربط بين الكيان والهوية المقدمة.

ملاحظـــة – يؤخذ استخدام مصطلح استيقان في سياق إدارة الهوية (IdM) على أنه يعني الاستيقان من كيان.

3.1.3 التخويل [b-ITU-T X. 800]: منح حقوق النفاذ، التي تشمل السماح بالنفاذ بناءً على حقوق النفاذ.

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

5.1.3 **العميل** [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 مخدّم أو على سطح المكتب، أو في أجهزة أخرى).

6.1.3 **الكيان** [b-ITU-T X.1252]: أي شيء له وجود قائم بذاته ومميز يمكن تعريفه في سياق ما.

ملاحظـــة – يمكن أن يكون الكيان شخصاً طبيعياً أو حيواناً أو شخصاً اعتبارياً أو منظمة، أو شيئاً فاعلاً أو منفعلاً، أو تطبيقاً برمجياً، أو خدمة وما إلى ذلك، أو مجموعة مما تقدم. وفي سياق الاتصالات، تشمل أمثلة الكيانات نقاط نفاذ ومشتركين وعناصر شبكة وشبكات وتطبيقات برمجيات وخدمات وأجهزة وسطوح بينية، وما إلى ذلك.

7.1.3 **معرّف الهوية** [b-ITU-T X.1252]: نعت واحد أو أكثر يستخدم لتحديد هوية كيان ضمن سياق ما.

ملاحظـــة – في سياق شبكات الجيل التالي على النحو المعرَّف في [التوصية b-ITU-T Y.2091]، معرف الهوية هو مجموعة أرقام وسمات ورموز أو أي شكل آخر من أشكال البيانات المُستخدمة لتحديد هوية المشترك (المشتركين)، أو المستخدم (المستخدمين)، أو عنصر (عناصر) شبكة أو وظيفة (وظائف) أو كيان (كيانات) الشبكة التي توفر الخدمات/التطبيقات، أو سواها من الكيانات (كالكائنات المادية أو المنطقية).

8.1.3 **مقدم الهوية (IdP)** [b-ITU-T X.1252]: انظر مقدم خدمة الهوية (IdSP).

9.1.3 **مقدم خدمة الهوية (IdSP)** [b-ITU-T X.1252]: كيان يقوم بالتحقق من معلومات هويات الكيانات الأخرى مع الحفاظ عليها وإدارتها ويمكن أن يستحدثها ويخصصها.

10.1.3 **تأشيرة التجديد** [IETF RFC 6749]: يصدر مخدّم التخويل تأشيرات التجديد للعميل. وتُستخدم هذه التأشيرات للحصول على تأشيرة نفاذ جديدة عندما تصبح تأشيرة النفاذ الحالية غير صالحة أو تنقضي مدتها، أو للحصول على تأشيرات نفاذ إضافية لها النطاق نفسه أو نطاقٌ أضيق (يمكن أن تكون مدة صلاحية تأشيرات النفاذ أقصر وبعدد أقل من الأذونات من التي أذن بها مالك المورد). وإصدار تأشيرة التجديد هو شأن اختياري يعود لتقدير مخدّم التخويل. وإذا أصدر مخدّم التخويل تأشيرة تجديد، تكون من ضمن إصدار تأشيرة نفاذ.

11.1.3 **مالك المورد** [IETF RFC 6749]: كيان قادر على منح حق النفاذ إلى مورد محمي. وعندما يكون مالك المورد شخصاً، يشار إليه باسم المستخدم النهائي.

12.1.3 **مخدم المورد** [IETF RFC 6749]: المخدم المستضيف للموارد المحمية، القادر على قبول الطلبات على الموارد المحمية والاستجابة لها باستخدام تأشيرات النفاذ.

2.3 مصطلحات معرَّفة في هذه التوصية

لا توجد.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

AKA اتفاق الاستيقان والمفتاح (*Authentication and Key Agreement*)

ANI السطح البيني من التطبيق إلى الشبكة (*Application-to-Network Interface*)

FE كيان وظيفي (*Functional Entity*)

GBA معمارية الإنهاض التنوعية (*Generic Bootstrapping Architecture*)

IdM إدارة الهوية (*Identity Management*)

IdP مقدم الهوية (*Identity Provider*)

IdSP مقدم خدمة الهوية (*Identity Service Provider*)

IMPI هوية خاصة للوسائط المتعددة القائمة على بروتوكول الإنترنت (*IP Multimedia Private Identity*)

IMSI الهوية الدولية للمشترك المتنقل (*International Mobile Subscriber Identity*)

NGN شبكات الجيل التالي (*Next Generation Network*)

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

SNI السطح البيني لشبكة الخدمة (*Service Network Interface*)

UNI السطح البيني لشبكة المستخدم (*User Network Interface*)

5 اصطلاحات

في هذه التوصية:

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

وكلمة "يُوصَى" 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.

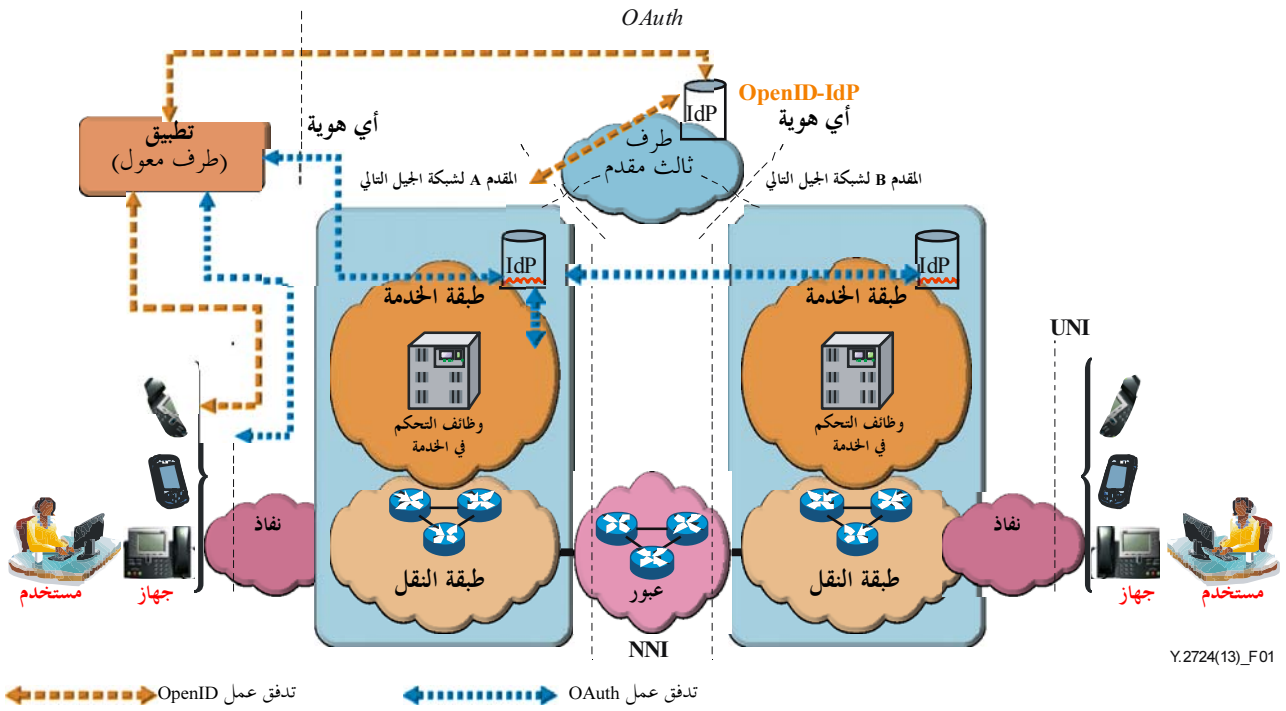
وكلمات"يمكن اختيارياً"، أو "يجوز"، أو "من الجائز"، أو "ربما" تدل على مطلب خياري مسموح به دون أن ينطوي على أي توصية به. ولا ترمي هذه المصطلحات إلى إلزام التطبيق بتوفير الجهة البائعة لهذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مقدم الخدمة خيارياً. بل إن الجهة البائعة يمكنها إدراج هذا الخيار وزعم مطابقة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

وفي متن هذه التوصية وملحقاتها، تظهر في بعض الأحيان كلمات *يتعين*، *ويتعين ألا*، *وينبغي*، *ويمكن*. وفي هذه الحالة يكون تأويلها، على التوالي، على *"يجب"*، أو *"يلزم"*، أو *"مطلوب"*، و*"يجب ألا"*، أو *"يلزم ألا"*، أو *"يحظر"*، و*"يوصي"*، و*"ربما"*، أو*"يجوز"*، أو *"من الجائز"*. ويأوّل انتفاء القصد المعياري عند ظهور مثل هذه العبارات أو الكلمات الرئيسية في تذييل أو في مادة موسومة صراحةً على أنها *إعلامية*.

6 إطار دعم التخويل المفتوح OAuth وتعرّف الهوية المفتوح OpenID في شبكات الجيل التالي

كما هو موضح في التوصية [ITU-T Y.2720]، تتكون شبكة الجيل التالي من عناصر وظيفية متعددة تستخدم معرفات هويات الكيانات لأداء وظائفها من أجل دعم خدمة الاستيقان المفتوح وتسهيلها للمقدمين الآخرين. ويمكن دعم هذا الترتيب باستخدام بروتوكولي OpenID وOAuth على النحو المبين في الشكل 1. ويصوَّر في الشكل 1 استخدام بروتوكولي OpenID وOAuth في شبكات الجيل التالي.

وحسب المواصفة OpenID [b-OpenID v.2]، يشارك مخدّم مقدم الهوية الخاص بتعرّف الهوية المفتوح (OpenID IdP) في كامل تدفق عمل الاستيقان، ويسمح التخويل OAuth للطرف المعوِّل بإرسال رسالة الاستيقان مباشرة إلى مقدم الهوية في شبكة الجيل التالي (NGN-IdP) من خلال البروتوكول OAuth.

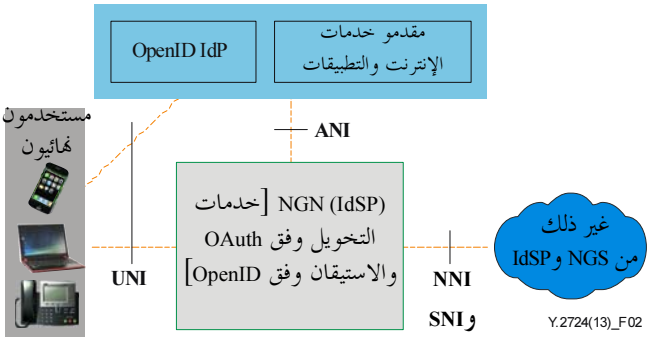


الشكل 1 – تدفقات العمليتين OAuth وOpenID في شبكات الجيل التالي

1.6 النموذج المرجعي

يقدم الشكل 1 نظرة عامة على إطاري العمليتين OAuth وOpenID.

يصور الشكل 2 نموذجاً مرجعياً لشبكات الجيل التالي لتقديم خدمات تخويل وفق بروتوكول OAuth واستيقان وفق بروتوكول OpenID. ويمكن لمقدمي شبكات الجيل التالي أن يقدموا خدمات مقدم خدمة الهوية وأن يتشاركوا مع مقدمي المحتوى والتطبيق و/أو غيرهم من مقدمي الخدمات.



الشكل 2 – النموذج المرجعي

2.6 تدفقات بروتوكولي OAuth وOpenID

توفر هذه الفقرة الوصف العام لتدفقات الرسالة وفق بروتوكولي OAuth وOpenID في شبكات الجيل التالي.

1.2.6 الكيانات المشتركة في تدفق المعلومات

تحدد هذه الفقرة الكيانات (بما في ذلك الكيانات الوظيفية المذكورة في التوصية [ITU-T Y.2012]) التي تشارك في تدفق المعلومات وفق بروتوكولي OAuth وOpenID.

2.2.6 الكيانات المشترَكة في تدفقات بروتوكولي OAuth وOpenID

الكيانات المشترَكة في تدفقات بروتوكولي OAuth وOpenID هي كما يلي:

- وظيفة المستخدم النهائي المزوَد بقدرة عميل في شبكة الإنترنت (متصفح مثلاً)؛
- A-2: كيان وظيفي لبوابة التطبيق (APL-GW-FE) [ITU-T Y.2012]. ينبغي لهذا الكيان الوظيفي أن يكون قادراً على دعم بروتوكولي OAuth و/أو OpenID.

وتعرِّف التوصية [ITU-T Y.2012] "الكيان الوظيفي لبوابة التطبيق على أنه كيان العمل البيني لمختلف وظائف شبكات الجيل التالي وجميع مخدمات التطبيق الخارجية ومفعلات الخدمة". وهذا يجعل من الكيان A-2 خياراً منطقياً لتقديم الدعم لبروتوكولي OAuth وOpenID. وبالإضافة إلى ذلك، نظراً لارتباطه مع الكيان الوظيفي للبيانات الوصفية لمستخدم الخدمة (S-5) (SUP-FE) [ITU-T Y.2012]، يمكن للكيان A-2 أن يدعم الاستيقان القائم على اتفاق الاستيقان والمفتاح (AKA)، بما في ذلك المعمارية العامة للاكتفاء الذاتي (GBA) في أجهزة المستخدم. ويرد في التقرير التقني [b-3GPP TS 33.220] توصيف أسلوب للاستيقان في بروتوكول OpenID على أساس معمارية الاكتفاء الذاتي. ويرد في الفقرة 8.2.6 من التوصية [ITU-T Y.2722] توصيف أسلوب آخر للاستيقان في بروتوكول OpenID على أساس اتفاق الاستيقان والمفتاح. وإذا ما نُفذ مخدم التخويل الخاص ببروتوكول OAuth ومقدم الهوية الخاص ببروتوكول OpenID [ITU-T Y.2722] كلاهما على الكيان A-2، يمكنهما استخدام الاستيقان القائم على اتفاق الاستيقان والمفتاح من خلال التفاعل مع الكيان S-5.

3.2.6 الكيانات الخاصة بتدفق OAuth

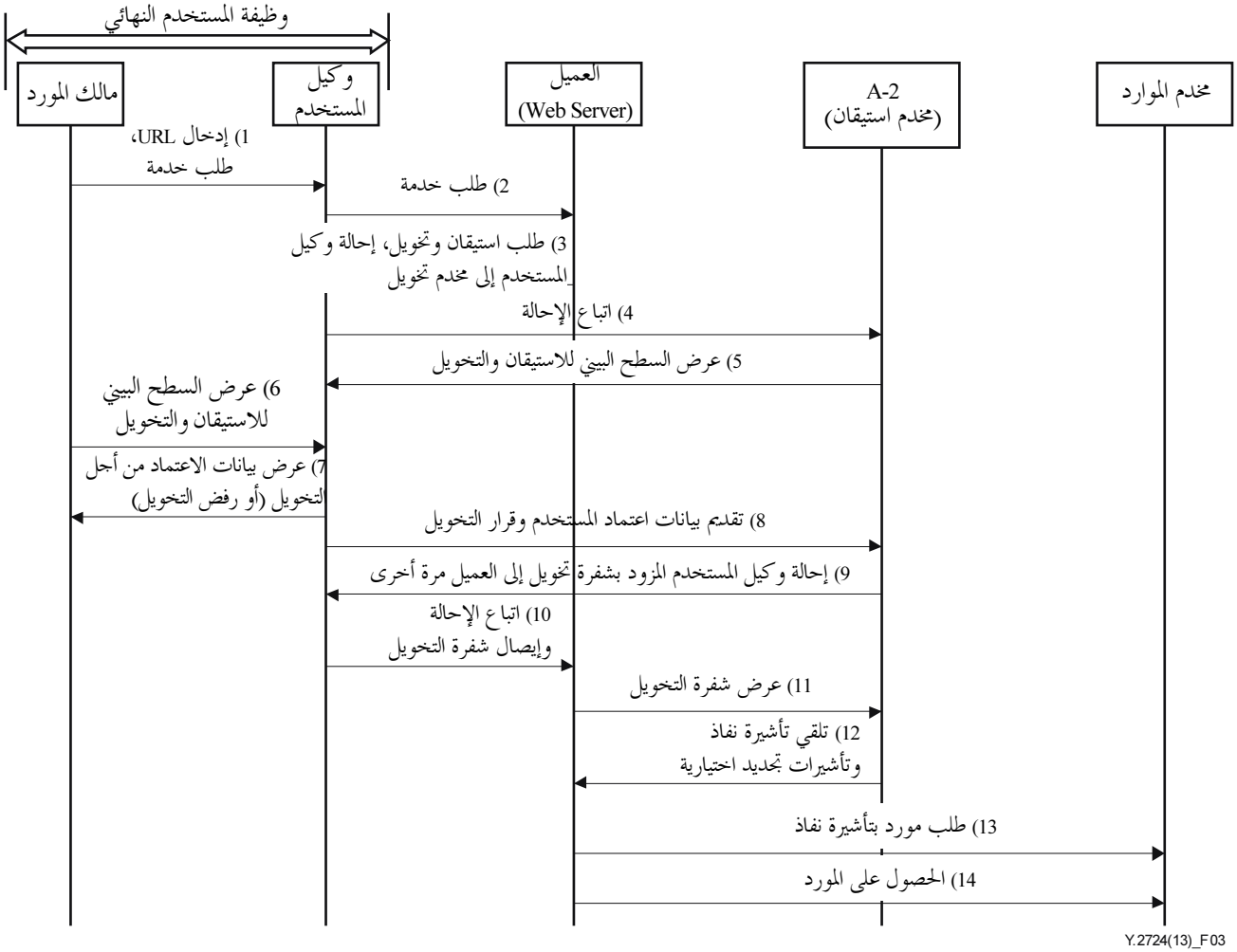
إن الكيانات الخاصة بتدفق OAuth هي التالية:

- مخدم تطبيق على الإنترنت يؤدي خدمة لمستخدم هو عميل OAuth. وقد يعمل العميل على أحد كيانات OAuth ولكنه غير ملزم بذلك.
- مخدم تخويل منفَّذ كجزء من الكيان الوظيفي لبوابة التطبيق (A-2).

  ويقوم مخدم تخويل أولاً بالاستيقان من المستخدم ثم يخول تلبية طلب العميل. وإذا نجح الإجراءان، يؤدي التبادل وفق بروتوكول OAuth إلى إصدار مخدم التخويل لتأشيرة نفاذ إلى المستخدم. ولدعم الاستيقان القائم على اتفاق الاستيقان والمفتاح، يتعين أن يكون مخدم التخويل قادراً على التفاعل مع الكيان S-5.
- مخدم الموارد

  يلبي مخدم الموارد طلب العميل عندما يكون مصحوباً بتأشيرة نفاذ صالحة. ويرد توصيف نوعين من الإجراءات للحصول على حق النفاذ إلى الموارد باستخدام تأشيرات النفاذ. تأشيرات الحالات في [b-IETF RFC 6750] ويعمل فريق مهام هندسة الإنترنت حالياً من أجل مواصفة للتأشيرات MAC. وفي الكيان الوظيفي لبوابة التطبيق (A-2) يمكن أن يقع مخدم الموارد أو لا يقع في نفس الموضع مع مخدم التخويل.

ويصوَّر في الشكل 3 أدناه المستوى العالي لتدفقات معلومات OAuth في حالة استخدام مخدم على شبكة الإنترنت (يرد وصفها في التذييل I) مع وصف تحته.



الشكل 3 – تدفق معلومات OAuth في حالة استخدام مخدم على شبكة الإنترنت

1) يوجه المستخدم وكيل المستخدم (على سبيل المثال، المتصفح) لطلب خدمة من العميل.

2) يقدم وكيل المستخدم الطلب إلى العميل.

3) يعد العميل رداً ويحيل وكيل المستخدم إلى مخدم التخويل للاستيقان من المستخدم وتخويل طلب العميل.

4) يتّبع وكيل المستخدم الإحالة.

5) يستجيب مخدم التخويل بتزويد وكيل المستخدم بالسطح البيني للاستيقان والتخويل.

6) يعرض وكيل المستخدم للمستخدم (مالك المورد) السطح البيني للاستيقان والتخويل.

7) يقدم المستخدم بيانات اعتماد الاستيقان ويشير إلى قرار التخويل عبر وكيل المستخدم.

8) يرسل وكيل المستخدم البيانات التي قدمها المستخدم إلى مخدم التخويل.

9) بعد الاستيقان من المستخدم والتأكد من أن المستخدم قد خول تلبية طلب العميل، يحيل مخدم التخويل وكيل المستخدم إلى العميل مرة أخرى. ويتضمن الرد شفرة التخويل.

10) ويوافي وكيلُ المستخدم العميلَ بشفرة التخويل عملاً بالإحالة.

11) يرسل العميل شفرة التخويل إلى مخدم التخويل.

12) ويستجيب مخدم التخويل بتأشيرة نفاذ مع تأشيرات تجديد اختيارية.

13) يرسل العميل طلباً إلى مخدم الموارد ويقدم تأشيرة النفاذ.

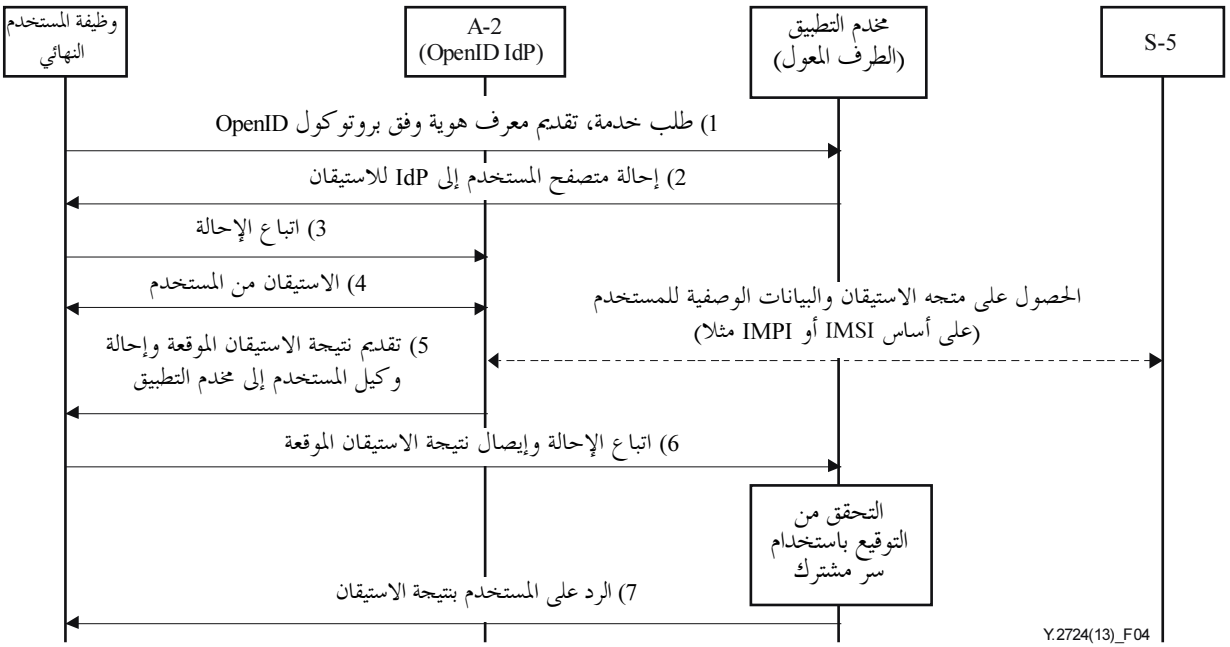
14) يقدم مخدم الموارد المورد المطلوب.

4.2.6 الكيانات الخاصة بتدفق OpenID

إن الكيانات الخاصة بتدفق OpenID هي التالية:

- مخدم تطبيق يعول على الاستيقان الذي يقوم به مخدّم مقدم الهوية الخاص ببروتوكول OpenID (OpenID IdP).
- مقدم الهوية الخاص ببروتوكول OpenID كجزء من الكيان A-2. ولدعم الاستيقان القائم على اتفاق الاستيقان والمفتاح (AKA)، يجب أن يكون هذا الكيان قادراً على التفاعل مع الكيان S-5.
- الكيان S-5 المشارك في الاستيقان وفق بروتوكول OpenID إذا قامت شبكة الجيل التالي بالاستيقان من وظيفة المستخدم النهائي على أساس اتفاق الاستيقان والمفتاح على النحو الموصَّف في التوصية [ITU-T Y.2722].

ويصوَّر في الشكل 4 تدفق معلومات بروتوكول OpenID ويرد وصفه تحته. ويصف النص والشكل إجراء OpenID للحالة التي ينشئ فيها مقدم الهوية ومخدم التطبيق سراً مشتركاً فيما بينهما. ويُستخدم السر لتوقيع رسالة تحمل نتيجة استيقان من مقدم الهوية ليتحقق منها مخدم التطبيق.



الشكل 4 – تدفق معلومات بروتوكول OpenID

1) يرسل متصفح المستخدم إلى مخدم التطبيق طلباً للحصول على الخدمة، ويحتوي الطلب على معرف هوية المستخدم وفق بروتوكول OpenID.

2) استناداً إلى معرف الهوية وفق بروتوكول OpenID، يكتشف مخدم التطبيق مقدم الهوية للمستخدم وفق بروتوكول OpenID. ثم يحيل مخدم التطبيق متصفحَ المستخدم للاستيقان لدى مقدم الهوية وفق بروتوكول OpenID (OpenID IdP).

3) يتبع المتصفح طلب الإحالة.

4) يستيقن مقدم الهوية وفق بروتوكول OpenID من المستخدم من خلال تبادل المعلومات عن طريق متصفح المستخدم.

5) وإذا ما قام مقدم الهوية وفق بروتوكول OpenID بالاستيقان على أساس اتفاق الاستيقان والمفتاح (AKA) (على النحو الموضح في التوصية [ITU-T Y.2722] مثلاً)، فإنه يحتاج للتفاعل مع الكيان S-5. ويشار إلى هذه التفاعلات بواسطة سهم متقطع.

6) يحيل مقدم الهوية وفق بروتوكول OpenID متصفح المستخدم تارة أخرى إلى مخدم التطبيق مع استجابة تحتوي على رسالة موقعة تحمل نتيجة الاستيقان.

7) يتبع المتصفح طلب الإحالة ويوافي مخدم التطبيق بالرسالة الموقعة.

8) وبعد التحقق من صحة التوقيع والتحقق من نتيجة الاستيقان، يبلِّغ مخدم التطبيق المستخدمَ ما إذا كان الاستيقان ناجحاً. ويرد توصيف إجراءات التوقيع والاستيقان في [b-OpenID v.2].

التذييل I

حالات استخدام منتقاة

(لا يشكل هذا التذييل جزءاً من هذه التوصية)

1.I حالة استخدام: مخدم على شبكة الإنترنت

الوصف

تدخل أليس إلى تطبيق قيد التشغيل على مخدم على شبكة الإنترنت عبر الرابط www.X-printphotos.example وتكلفه بطباعة صورها المخزنة في المخدم في الرابط www.X-storephotos.example. ولدى أليس اشتراك مع مقدم خدمة شبكة الجيل التالي الذي يشغل مخدم التخويل OAuth في الرابط www.X-carrier.example. فيتلقى التطبيق في الرابط www.X-printphotos.example تخويل أليس للنفاذ إلى صورها دون أن يطلع على بيانات اعتماد الاستيقان منها عبر الرابط www.x-storephotos.example أو www.X-carrier.example.

الشروط المسبقة

- سجلت أليس في الرابط www.X-carrier.example لتمكين الاستيقان.
- أنشأ التطبيق في الرابط www.X-printphotos.example بيانات اعتماد الاستيقان مع مخدم تخويل OAuth في الرابط www.X-printphotos.example.
- يستطيع التطبيق في الرابط www.X-storephotos.example أن يتحقق من صحة تأشيرة النفاذ الصادرة عن مخدم التخويل في الرابط www.X-carrier.example.

الشروط اللاحقة

يؤدي نجاح الإجراء إلى تلقي التطبيق في الرابط www.X-printphotos.example شفرة تخويل من الرابط www.X-carrier.example. وترتبط هذه الشفرة بالتطبيق في الرابط www.X-printphotos.example وبمحدد موقع الموارد الموحد (URL) لنداء الرد الذي يورده التطبيق. ويستخدم التطبيق في الرابط www.X-storephotos.example شفرة التخويل للحصول على تأشيرة نفاذ من الرابط www.X-carrier.example. ويصدر التطبيق في الرابط www.X-storephotos.example تأشيرة نفاذ بعد الاستيقان من التطبيق في الرابط www.X-printphotos.example والتحقق من صحة تأشيرة التخويل التي قدمت. ويستخدم التطبيق في الرابط www.X-printphotos.example تأشيرة النفاذ للحصول على حق النفاذ إلى صور أليس في الرابط www.X-storephotos.example.

ملاحظـــة – عند انتهاء صلاحية تأشيرة النفاذ، تحتاج الخدمة في الرابط www.X-printphotos.example إلى تكرار إجراء البروتوكول OAuth للحصول على تخويل أليس بالنفاذ إلى صورها في الرابط www.X-storephotos.example. وبدلاً من ذلك، إذا منحت أليس التطبيق حقاً بالنفاذ طويل الأمد إلى مواردها في الرابط www.X-storephotos.example، يمكن لمخدم التخويل في الرابط www.X-storephotos.example أن يصدر تأشيرات تطول مدة صلاحيتها. وتمكن مقايضة هذه التأشيرات بتأشيرات قصيرة الأمد تلزم للنفاذ إلى الرابط www.X-storephotos.example.

المتطلبات

- يجب أن يكون المخدم في الرابط www.X-printphotos.example، الذي يستضيف عميل OAuth، قادراً على إصدار طلبات إحالة وفق بروتوكول HTTP إلى وكيل المستخدمة أليس – وهو المتصفح.
- يجب أن يكون مخدم التخويل في الرابط www.X-carrier.example قادراً على الاستيقان من أليس. وأسلوب الاستيقان لا يقع في مجال تطبيق بروتوكول OAuth.

- يجب على التطبيق في الرابط www.X-carrier.example أن يحصل على تخويل أليس من أجل النفاذ إلى صورها في الرابط www.X-printphotos.example.
- يمكن للتطبيق في الرابط www.X-carrier.example أن يحدد لأليس نطاق النفاذ الذي طلبه الرابط www.X-printphotos.example عندما التمس تخويل أليس.
- يجب أن يكون مخدم التخويل في الرابط www.X-carrier.example قادراً على الاستيقان من التطبيق في الرابط www.X-printphotos.example والتحقق من صحة شفرة التخويل قبل إصدار تأشيرة نفاذ. ويجب على التطبيق في الرابط www.X-printphotos.example أن يوفر محدد موقع الموارد الموحد (URL) الخاص بنداء الرد إلى مخدم التخويل في الرابط www.X-carrier.example (**ملاحظة**: ينبغي أن يكون محدد موقع الموارد الموحد (URL) مسجلاً مسبقاً لدى الرابط www.X-carrier.example).
- مطلوب من مخدم التخويل في الرابط www.X-carrier.example أن يحتفظ بسجل يقرن شفرة التخويل بالتطبيق في الرابط www.X-printphotos.example ومحدد موقع الموارد الموحد (URL) الخاص بنداء الرد المقدم من التطبيق.
- وتأشيرات النفاذ هي تأشيرات تعود لحاملها (فهي لا ترتبط بتطبيق معين، مثل www.X-printphotos.example) وينبغي أن يكون عمرها قصيراً.
- يجب على مخدم التخويل في الرابط www.X-carrier.example أن يبطل شفرة التخويل بعد أول استخدام لها.
- يجب ألا تُتطلب مشاركة أليس اليدوية في إجراء التخويل وفق بروتوكول OAuth (من قبيل إدخال URL أو كلمة مرور). (والاستيقان من أليس لدى الرابط www.X-carrier.example يقع خارج مجال تطبيق OAuth).

2.I حالة الاستخدام: بيانات اعتماد العميل

الوصف

تعد الشركة Good-X-Pay كشوف مرتبات الشركة Good-X-Work. ومن أجل القيام بذلك، يحصل التطبيق في الرابط www.Good-X-Pay.example على حق النفاذ المستيقَن منه إلى بيانات حضور الموظفين المخزنة في الرابط www.Good-X-Work.example. ويجرى الاستيقان بواسطة مخدم التخويل، الذي يشكل جزءاً من شبكات الجيل التالي بمحدد موقع الموارد الموحد (URL) في الرابط www.X-carrier.example.

الشروط المسبقة

- أنشأ التطبيق في الرابط www.Good-X-Pay.example، من خلال تسجيل، معرف هوية وسراً مشتركاً مع مخدم التخويل في الرابط www.X-carrier.example.
- حُدد نطاق نفاذ التطبيق في الرابط www.Good-X-Pay.example إلى البيانات المخزنة في الرابط www.Good-X-Work.example.

الشروط اللاحقة

يؤدي نجاح الإجراء إلى تلقي التطبيق في الرابط www.Good-X-Pay.example تأشيرة نفاذ بعد الاستيقان لدى مخدم التخويل في الرابط www.X-carrier.example. ثم يستخدم التطبيق في الرابط www.good-x-pay.example تأشيرة النفاذ للنفاذ إلى بيانات الحضور في الرابط www.Good-X-Work.example.

المتطلبات

- يُتطلب استيقان التطبيق في الرابط www.Good-X-Pay.example لدى مخدم التخويل في الرابط www.X-carrier.example.

- يجب أن يستند أسلوب الاستيقان إلى معرف الهوية والسر المشترك، المقدمان من التطبيق قيد التشغيل في الرابط www.Good-X-Pay.example إلى مخدم التخويل في الرابط www.X-carrier.example طي الطلب الأولي وفق بروتوكول HTTP.
- ولأن الإجراء يؤدي إلى النفاذ إلى بيانات حساسة للشركة Good-X-Work، يتعين أن تقيم هذه الشركة علاقة ثقة مع شركة Good-X-Pay ومخدم التخويل في الرابط www.X-carrier.example.

3.I حالة الاستخدام: التأكيد

الوصف

تعد الشركة Good-X-Pay كشوف مرتبات الشركة Good-X-Work. ومن أجل القيام بذلك، يحصل التطبيق في الرابط www.Good-X-Pay.example على حق النفاذ المستيقَن منه إلى بيانات حضور الموظفين المخزنة في الرابط www.Good-X-Work.example. ويمنح المخدم في هذا الرابط حق النفاذ للتطبيق في الرابط www.Good-X-Pay.example بعد تلقي تأشيرة نفاذ صادرة عن مخدم التخويل في الرابط www.X-carrier.example. ويستيقن مخدم التخويل هذا من التطبيق في الرابط www.Good-X-Pay.example من خلال التحقق من التأكيد المقدم من الرابط www.Good-X-Pay.example.

وتصف حالة الاستخدام هذه حلاً بديلاً من ذلك الموصوف بحالة استخدام بيانات اعتماد العميل.

الشروط المسبقة

- حصل التطبيق في الرابط www.Good-X-Pay.example على تأكيد الاستيقان من طرف موثوق لدى مخدم التخويل في الرابط www.X-carrier.example.
- حُدد نطاق نفاذ التطبيق في الرابط www.Good-X-Pay.example إلى البيانات المخزنة في الرابط www.Good-X-Work.example.
- أقام مخدم التخويل في الرابط www.X-carrier.example علاقة ثقة مع الطرف المؤكد، وهو قادر على التحقق من صحة تأكيداته.

الشروط اللاحقة

يؤدي نجاح الإجراء إلى تلقي التطبيق في الرابط www.Good-X-Pay.example تأشيرة نفاذ بعد الاستيقان لدى مخدم التخويل في الرابط www.X-carrier.example بتقديم تأكيد (كتأكيد بلغة SAML مثلاً). ثم يستخدم تأشيرة النفاذ للحصول على حق النفاذ إلى بيانات حضور الموظفين.

المتطلبات

- يلزم استيقان التطبيق في الرابط www.Good-X-Pay.example لدى مخدم التخويل في الرابط www.X-carrier.example.
- يجب أن يكون مخدم التخويل في الرابط www.X-carrier.example قادراً على التحقق من صحة التأكيدات الصادرة عن الطرف المؤكِد والتي يقدمها التطبيق قيد التشغيل في الرابط www.Good-X-Pay.example.
- ويتعين على شركة Good-X-Work أن تقيم علاقة ثقة مع شركة Good-X-Pay ومخدم التخويل في الرابط www.X-carrier.example.

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-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks.*

[b-IETF RFC 6750] IETF RFC 6750, *The OAuth 2.0 Authorization Framework: Bearer Token Usage.*

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

[b-3GPP TS 33.220] 3GPP TS 33.220 (2013) *Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture, Release 12.*

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، 2014