الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2723

(2013/11)

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

شبكات الجيل التالي – الأمن

دعم بروتوكول OAuth في شبكات الجيل التالي

التوصيـــة ITU-T Y.2723

الاتحاد الدولي للاتصالات ITU

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
التشغيل والإدارة 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
التشغيل والإدارة 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 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
شبكات أسلوب الرزم	Y.2699-Y.2600
الأمن	**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.2723

دعم بروتوكول OAuth في شبكات الجيل التالي

ملخص

توصِّف التوصية ITU-T Y.2723 آليات وإجراءات لاستخدام "إطار التخويل OAuth 2.0 (OAuth)" الذي حدده فريق مهام هندسة الإنترنت، لسيناريوهات يؤدي فيها مقدم شبكات الجيل التالي (NGN) دور مخدم تخويل OAuth.

وتوفر الوثيقة المرافقة، التوصية ITU-T Y.2724، "إطار دعم بروتوكولي OAuth وOpenID في شبكات الجيل التالي"، السياق والاعتبارات ذات الصلة بالمعمارية، وإطاراً رفيع المستوى لاستخدام OAuth في شبكات الجيل التالي.

وتحدد هذه التوصية المتطلبات ذات الصلة بتقييد اختيارات الخيار OAuth وكذلك المتطلبات الإضافية التي تجعل من استخدام OAuth متسقاً مع متطلبات أمن شبكات الجيل التالي وإدارة الهوية.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T Y.2723	2013.11.15	13

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 لأي طرف.

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/.

جدول المحتويات

الصفحة

مقدمة

توفر التوصية ITU-T Y.2723 إطاراً لدعم واستخدام بروتوكولي OAuth وOpenID في شبكات الجيل التالي (NGN). وتبنى هذه التوصية على التوصية ITU-T Y.2724 لتعرّف أساليب محددة لدعم OAuth.

ملاحظـــة – لا تُدخل هذه التوصية أي تغييرات أو تعديلات على بروتوكول OAuth؛ بل تكتفي بالتركيز على دعم واستخدام بروتوكول OAuth في شبكات الجيل التالي.

التوصيـــة ITU-T Y.2723

دعم بروتوكول OAuth في شبكات الجيل التالي

1 مجال التطبيق

تصف هذه التوصية آليات وإجراءات لدعم الإصدار 2 من بروتوكول التخويل (OAuth) في شبكات الجيل التالي. ويمكن استخدام الآليات والإجراءات الموضحة في هذه التوصية لدعم خدمات التطبيقات في بيئة تتعدد فيها الخدمات ومقدمي الخدمات. وتفترض هذه التوصية أن شبكة الجيل التالي هي التي تقدم خدمة تخويل OAuth.

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 X.1254] التوصية ITU-T X.1254 (2012)، *إطار ضمان الاستيقان من كيان*.

[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 بروتوكولي OpenID وOAuth في شبكات الجيل التالي*.

[IETF RFC 6749] طلب التعليقات IETF RFC 6749 (2012)، *إطار تخويل OAuth 2.0*. <http://datatracker.ietf.org/doc/rfc6749/>.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل 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 تستعمل لتحقيق قدر كاف من الثقة في الربط بين الكيان والهوية المقدمة.

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

4.1.3 **منح التخويل** [IETF RFC 6749]: منح التخويل هو بيان اعتماد يمثل تخويل مالك المورد (بالنفاذ إلى موارده المحمية) ويستخدمه العميل للحصول على تأشيرة نفاذ.

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

6.1.3 **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).

7.1.3 **العملاء السريون** [IETF RFC 6749]: عملاء قادرون على إبقاء بيانات اعتمادهم طي الكتمان (على سبيل المثال عميل منفَّذ على مخدِّم آمن بنفاذ مقيد إلى بيانات اعتماد العميل)، أو مستفيدون من الاستيقان الآمن من العميل باستخدام وسيلة أخرى.

8.1.3 **العملاء المعلنون** [IETF RFC 6749]: عملاء غير قادرين على إبقاء بيانات اعتمادهم طي الكتمان (على سبيل المثال، عميل ينفِّذ على جهاز مالك المورد من قبيل تطبيق محلي مثبت في الجهاز، أو تطبيق قائم على وكيل المستخدم)، أو غير مستفيدين من الاستيقان الآمن من العميل باستخدام أي وسيلة أخرى.

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

10.1.3 **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 والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

IdM إدارة الهوية *(Identity Management)*

NGN شبكة الجيل التالي *(Next Generation Network)*

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

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

URI معرف الموارد الموحد *(Uniform Resource Identifier)*

5 الاصطلاحات

لا توجد.

6 دعم بروتوكول OAuth في شبكات الجيل التالي

تصف هذه الفقرة الجوانب الرئيسية لدعم بروتوكول OAuth في شبكات الجيل التالي.

1.6 اختيار أنماط عميل OAuth بناءً على متطلبات الأمن في شبكات الجيل التالي

يُعرِّف طلب التعليقات [IETF RFC 6749] نمطين من عملاء OAuth: العملاء السريون والمعلنون.

ولا يفي العملاء المعلنون بمتطلبات الاستيقان لأطراف ثالثة تقدم التطبيقات في شبكات الجيل التالي [ITU-T Y.2702]، وذلك لأن مقدم شبكة الجيل التالي لا يمكنه الاستيقان من العملاء المعلنين. وتوصي التوصية [ITU-T Y.2724] بأن تدعم شبكات الجيل التالي العملاء السريين فقط. ويجب على العملاء تلبية المتطلبات التالية:

1 يجب أن يتسنى الاستيقان من عميل OAuth بمستويات محددة من الضمان [ITU-T Y.2702] و[ITU-T X.1254].

2 يجب أن يسجَّل عميل OAuth في شبكات الجيل التالي لدى مخدم التخويل على النحو المحدد في الفقرة 2 من طلب التعليقات [IETF RFC 6749].

ويُعرّف بروتوكول OAuth 2.0 [IETF RFC 6749] البيانات الوصفية التالية للعميل: تطبيق على شبكة الإنترنت، وتطبيق قائم على وكيل المستخدم، وتطبيق محلي. والتطبيق على شبكة الإنترنت هو البيانات الوصفية لعميل خاص، أما التطبيقان الآخران فهما البيانات الوصفية لعملاء معلنين. وتكتفي هذه التوصية بوصف دعم شبكات الجيل التالي لعميل البيانات الوصفية للتطبيق على شبكة الإنترنت.

2.6 اختيار أنماط منح التخويل

يُعرِّف طلب التعليقات [IETF RFC 6749] الأنماط التالية من منح التخويل: شفرة التخويل، والمنح الضمني، وبيانات اعتماد كلمة مرور مالك المورد، وبيانات اعتماد العميل. وبالإضافة إلى ذلك، يعمل فريق مهام هندسة الإنترنت حالياً على تحديد توسعة توصِّف نمط منح التأكيد بلغة SAML 2.0 في بروتوكول OAuth 2.0.

ويوضح طلب التعليقات [IETF RFC 6749] أن مخدِّم التخويل لا يستيقن من العميل عند إصدار تأشيرة نفاذ أثناء تدفق منح ضمني. وفي بعض الحالات، يمكن التحقق من هوية العميل عن طريق إعادة توجيه معرف الموارد الموحد (URI) الذي استُخدم في نقل تأشيرة النفاذ إلى العميل. ويجوز كشف تأشيرة النفاذ لمالك المورد أو للتطبيقات الأخرى التي يمكنها النفاذ إلى وكيل المستخدم لدى مالك المورد.

وهكذا، فإن تدفقات OAuth التي تستخدم نمط المنح الضمني لا تؤدي إلى استيقان يفي بمتطلبات الاستيقان لطرف ثالث يقدم التطبيقات في شبكات الجيل التالي [ITU-T Y.2702].

وتركز هذه التوصية على وصف دعم شبكات الجيل التالي للعميل السري للبيانات الوصفية لتطبيق على شبكة الإنترنت باستخدام منح التخويل التالية:

- شفرة التخويل
- بيانات اعتماد كلمة مرور مالك المورد
- بيانات اعتماد العميل
- تأكيد SAML 2.0.

3.6 التوصيات بشأن خيارات بروتوكول OAuth للعملاء الذين تدعمهم شبكات الجيل التالي

أُعدت تدفقات طلب التعليقات [IETF RFC 6749] على النحو الأمثل لعدة بيانات وصفية لعملاء من نمطين. فيحدد طلب التعليقات هذا خيارات لاختيار أنماط منح التخويل، والمعلمات، والمتطلبات الأمنية.

وتقدم هذه الفقرة توصيات لدعم العملاء السريين للبيانات الوصفية لتطبيق على شبكة الإنترنت. وتركز أيضاً على تلك المتطلبات والمعلمات الاختيارية التي يعد اختيارها ضرورياً لدعم بروتوكول *OAuth* في شبكات الجيل التالي.

1.3.6 تسجيل عميل

توصي الفقرة 2.2 من طلب التعليقات [IETF RFC 6749] بتسجيل إعادة توجيه معرف الموارد الموحد (URI) الخاص بالعملاء لدى مخدِّم تخويل، لأن العملاء ذوي معرفات URI المسجلة يتيحون درجة أعلى من الأمن.

وتتطلب هذه التوصية أن يسجل العملاء الذين تدعمهم شبكات الجيل التالي إعادة توجيه معرف الموارد الموحد (URI) الخاص بهم لدى مخدِّم التخويل.

2.3.6 سرية الرسائل إلى النقطة الطرفية لإعادة توجيه العميل

توصي الفقرة 1.2.1.3 من طلب التعليقات [IETF RFC 6749] بما يلي: **ينبغي** للنقطة الطرفية لإعادة توجيه أن تتطلب استخدام أمن طبقة النقل (TLS) على النحو الموضح في الفقرة 6.1 عندما يكون نوع الرد المطلوب "شفرة" أو "تأشيرة"، أو متى كان طلب إعادة التوجيه سيؤدي إلى إرسال بيانات اعتماد حساسة عبر شبكة مفتوحة. وتتطلب هذه التوصية استخدام أمن طبقة النقل لإرسال أي معلومات حساسة.

3.3.6 الاستيقان من العميل

إن العملاء المعرفين بالبيانات الوصفية لتطبيق على شبكة الإنترنت هم عملاء سريون. لذلك يُتطلب أن يستيقن مخدِّم تخويل من العميل.

4.3.6 إجراءات التخويل

تشمل هذه التوصية العملاء السريين للبيانات الوصفية لتطبيق على شبكة الإنترنت ممن يستخدمون إجراءات تخويل من أنماط التخويل التالية:

- شفرة التخويل
- بيانات اعتماد كلمة مرور مالك المورد
- بيانات اعتماد العميل
- ملحق اسم الملف SAML.

1.4.3.6 شفرة التخويل

تحدد الفقرة 1.4 من طلب التعليقات [IETF RFC 6749] إجراء التخويل للعملاء السريين باستخدام شفرة التخويل. وتتطلب هذا التوصية إدراج المعلمة *redirect_uri* في طلبات التخويل.

وتسري المتطلبات التالية على تفاعل مخدم التخويل مع عملاء للبيانات الوصفية لتطبيق على شبكة الإنترنت يستخدمون شفرة التخويل. **ويجب** على مخدِّم التخويل أن يقوم بما يلي:

- الاستيقان من العميل الذي أصدر طلب تخويل؛
- التأكد من أن قيمة المعلمة *redirect_uri* في طلب تخويل العميل تطابق القيمة المسجلة للعميل؛
- إصدار شفرة تخويل للعملاء المخولين والمستيقن منهم حصراً؛
- التأكد من صلاحية شفرة التخويل قبل إصدار تأشيرة نفاذ.

2.4.3.6 بيانات اعتماد كلمة مرور مالك المورد

إن إجراء التخويل الذي يستخدم هذا النمط من المنح أُعد على النحو الأمثل للعملاء الذين رسخوا الثقة مع مالك المورد. فيستخدم العميل بيانات اعتماد كلمة مرور مالك المورد للحصول على تأشيرة نفاذ من مخدم التخويل. والإجراء المحدد في الفقرة 3.4 من طلب التعليقات [IETF RFC 6749] يلبي المتطلبات الأمنية لشبكات الجيل التالي.

ملاحظـــة – يسمح طلب التعليقات [IETF RFC 6749] أن يستخدم العملاء المعلنون هذا الإجراء. ولا تنظر هذه التوصية إلا في العملاء السريين الملزمين بتمكين مخدِّم التخويل من الاستيقان منهم.

ووفقاً لطلب التعليقات [IETF RFC 6749]، عند التفاعل مع عميل يستخدم نمط المنح المتمثل في بيانات اعتماد كلمة مرور مالك المورد، يجب على مخدِّم التخويل أن يقوم بما يلي:

- الاستيقان من العميل؛
- التحقق من صحة بيانات اعتماد كلمة مرور مالك المورد التي قدمها العميل؛
- إصدار شفرة تخويل للعميل إذا استيقن مخدِّم التخويل منه، وقدم بيانات اعتماد صالحة كمالك مورد.

4.6 الاستيقان من مالك المورد

إن مواصفة OAuth في طلب التعليقات [IETF RFC 6749] لا توصِّف استيقان مخدِّم التخويل من مالك المورد (المستخدم النهائي مثلاً). وفي بيئة شبكات الجيل التالي يجب أن تفي آلية الاستيقان من مالك المورد بمتطلبات التوصية [ITU-T Y.2702].

5.6 اعتبارات الأمن

يُقدم قسم "اعتبارات الأمن" في المواصفة OAuth 2.0 (طلب التعليقات [IETF RFC 6749]) تقدم مبادئ توجيهية بشأن الأمن لجميع البيانات الوصفية لبروتوكول OAuth 2.0، وهي: تطبيق على شبكة الإنترنت، وتطبيق قائم على وكيل المستخدم، وتطبيق محلي. وتوصي هذه التوصية بدعم عملاء التطبيقات على شبكة الإنترنت في شبكات الجيل التالي. ومن ثم، لا تسري هنا إلا الاعتبارات الأمنية الواردة في طلب التعليقات [IETF RFC 6749] فيما يتعلق بعملاء التطبيقات على شبكة الإنترنت. وبالإضافة إلى ذلك، يقدم طلب التعليقات [b-IETF RFC 6819] نموذجاً شاملاً لأمن OAuth ومعلومات أساسية لتصميم البروتوكول. وينبغي النظر في المواد الواردة في طلب التعليقات [b-IETF RFC 6819] ذات الصلة بعملاء التطبيقات على شبكة الإنترنت من أجل التطبيقات التي تدعم بروتوكول OAuth في شبكات الجيل التالي.

وينبغي للحلول أيضاً أن تلتزم بالمتطلبات الأمنية لشبكات الجيل التالي المحددة 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-IETF RFC 6819] IETF RFC 6819, *OAuth 2.0 Threat Model and Security Considerations.*
http://datatracker.ietf.org/doc/rfc6819/

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