Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2725

(07/2014)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

Réseaux de prochaine génération – Sécurité

Prise en charge du protocole OpenID dans les réseaux de prochaine génération

Recommandation UIT-T Y.2725

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Améliorations concernant les réseaux de prochaine génération	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	**Y.2700–Y.2799**
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.2725

Prise en charge du protocole OpenID dans les réseaux de prochaine génération

Résumé

La Recommandation UIT-T Y.2725 spécifie les mécanismes et procédures applicables à la prise en charge et à l'utilisation du protocole OpenID dans les scénarios dans lesquels le rôle du fournisseur OpenID est rempli par le fournisseur NGN.

La Recommandation UIT-T Y.2724 définit un cadre pour la prise en charge et l'utilisation des protocoles OAuth et OpenID dans les réseaux NGN. La Recommandation UIT-T Y.2725 s'appuie sur les Recommandations UIT-T Y.2722 et UIT-T Y.2724 pour définir des mécanismes particuliers pour la prise en charge du protocole OpenID.

NOTE – Dans la Recommandation UIT-T Y.2725, aucune modification n'est apportée au protocole OpenID; on s'intéresse uniquement à la prise en charge et à l'utilisation du protocole OpenID dans les réseaux NGN.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.2725	2014-07-18	13	11.1002/1000/12079

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T Y.2725

Prise en charge du protocole OpenID dans les réseaux de prochaine génération

1 Domaine d'application

La présente Recommandation décrit les mécanismes et procédures permettant de prendre en charge OpenID dans les réseaux NGN. Ces mécanismes et procédures peuvent être utilisés pour prendre en charge des services d'application dans un environnement avec plusieurs fournisseurs de services. Dans la présente Recommandation, on suppose que le fournisseur NGN est le fournisseur OpenID.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T Y.2701] Recommandation UIT-T Y.2701 (2007), *Prescriptions de sécurité des réseaux de prochaine génération de version 1*.

[UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation pour les réseaux de prochaine génération de version 1*.

[UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité dans les réseaux NGN*.

[UIT-T Y.2721] Recommandation UIT-T Y.2721 (2010), *Spécifications et cas d'utilisation de la gestion d'identité dans les réseaux NGN*.

[UIT-T Y.2724] Recommandation UIT-T Y.2724 (2013), *Cadre pour la prise en charge des protocoles OAuth et OpenID dans les réseaux de prochaine génération*.

[OASIS XRI SYNTAX] *Extensible Resource Identifier (XRI) Syntax V2.0*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 authentification (d'entité) [b-UIT-T X.1252]: processus utilisé pour obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

3.1.2 autorisation [b-UIT-T X.800]: octroi de droits et octroi d'accès sur la base de ces droits.

3.1.3 justificatif d'autorisation [b-IETF RFC 6749]: justificatif représentant l'autorisation du propriétaire de ressources (pour accéder à ses ressources protégées) et utilisé par le client pour obtenir un jeton d'accès.

3.1.4 serveur d'autorisation [b-IETF RFC 6749]: serveur délivrant des jetons d'accès au client une fois menées à bien l'authentification du propriétaire de ressources et l'obtention de l'autorisation.

3.1.5 client [b-IETF RFC 6749]: application soumettant des demandes de ressource protégée pour le compte du propriétaire de ressources et avec son autorisation. Le terme "client" n'implique aucune caractéristique particulière pour la mise en œuvre (par ex. l'application peut être exécutée aussi bien sur un serveur que sur un ordinateur de bureau ou sur d'autres dispositifs).

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

FE entité fonctionnelle *(functional entity)*

FRA exigences fonctionnelles et architecture *(functional requirements and architecture)*

IdM gestion d'identité (*identity management*)

IdP fournisseur d'identité (*identity provider*)

IETF Internet Engineering Task Force

IP protocole Internet *(Internet protocol)*

OAuth protocole d'autorisation OAuth 2.0

OP fournisseur OpenID *(OpenID provider)*

SAML langage de balisage d'assertion de sécurité (*security assertion markup language*)

URI identificateur uniforme de ressource (*uniform resource identifier*)

WS serveur web *(web server)*

5 Conventions

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**il est interdit**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "**peut, à titre d'option**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en oeuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

6 Prise en charge du protocole OpenID dans les réseaux NGN

Le présent paragraphe décrit les principaux aspects de la prise en charge d'OpenID dans les réseaux NGN.

6.1 Modèle de référence

Conformément à la spécification du protocole OpenID [b-OpenID v.2], le serveur IdP OpenID participe à tous les flux d'authentification. Voir [UIT-T Y.2724], qui donne une vue d'ensemble du cadre applicable aux protocoles OAuth et OpenID.

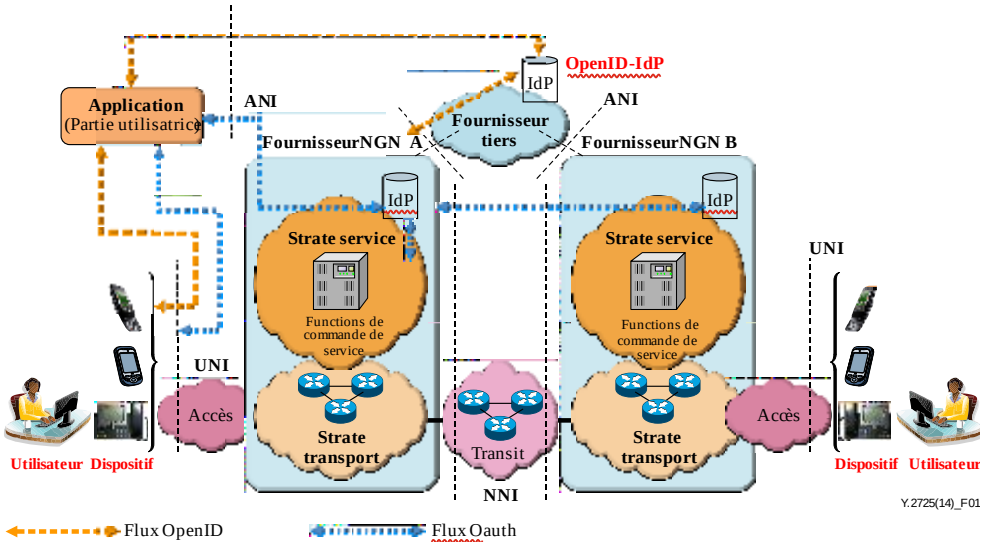

Figure 1 – Flux OpenID et OAuth pour les réseaux NGN

6.2 Format des messages de protocole dans le contexte des NGN

[b-OpenID v.2] définit deux types de format pour les messages de protocole:

- le codage sous forme de clé-valeur,
- le codage HTTP.

Dans le § 4.1.1 de [b-OpenID v.2], il est indiqué que le codage sous la forme clé-valeur est utilisé pour le calcul de la signature et les réponses directes envoyées aux parties utilisatrices.

S'agissant du codage HTTP, le § 4.1.2 de [b-OpenID v.2] indique que ce modèle s'applique aux messages adressés par l'agent utilisateur à la partie utilisatrice et au fournisseur OpenID, ainsi qu'aux messages adressés par la partie utilisatrice au fournisseur OpenID.

Il est obligatoire que les entités prises en charge dans les réseaux NGN respectent les exigences lorsqu'elles envoient un message de protocole.

6.3 Types de communication

[b-OpenID v.2] définit deux types de communication:

- la communication directe,
- la communication indirecte.

Il est précisé dans le § 5.1 de [b-OpenID v.2] que la communication directe est lancée par une partie utilisatrice vers l'URL d'un point d'extrémité du fournisseur OpenID. Elle sert à établir des associations et à vérifier les assertions d'authentification.

Il est indiqué dans le § 5.2 de [b-OpenID v.2] que dans le cas de la communication indirecte, les messages sont transmis par l'intermédiaire de l'agent utilisateur. La communication indirecte peut être lancée par la partie utilisatrice ou par le fournisseur OpenID. Elle est utilisée pour les demandes et les réponses d'authentification.

Il est obligatoire que les entités prises en charge dans les réseaux NGN respectent ces exigences lorsqu'elles ouvrent le contexte de communication.

6.4 Création de signatures

L'authentification OpenID prend en charge deux algorithmes de signature:

- HMAC-SHA1 – clé d'une longueur de 160 bits
- HMAC-SHA256 – clé d'une longueur de 256 bits

Le présent paragraphe contient des recommandations concernant l'utilisation de l'algorithme HMAC-SHA256. La procédure de création d'une signature de message définie au § 6.1 de [b-OpenID v.2] est conforme aux exigences de sécurité pour les réseaux NGN.

6.5 Procédures d'authentification OpenID dans les réseaux NGN

6.5.1 Demandes d'authentification

Aux termes du § 13 de [b-OpenID v.2], il est recommandé que les parties utilisatrices utilisent le protocole Yadis pour publier leurs URL return_to valides. Les parties utilisatrices peuvent, à titre d'option, publier cette information à une URL quelconque et il est recommandé qu'elles publient cette information sous l'ensemble d'URL correspondantes afin que les fournisseurs puissent vérifier les URL return_to.

Conformément à la présente Recommandation, il est recommandé que les parties utilisatrices utilisent le protocole Yadis pour publier leurs URL return message_to valides dans les réseaux NGN.

Les demandes d'authentification sont spécifiées dans le § 9 de [b-OpenID v.2].

Les exigences ci-après s'appliquent à l'interaction entre la partie utilisatrice et un utilisateur final. La partie utilisatrice doit:

- lancer l'authentification OpenID;
- normaliser un identificateur fourni par l'utilisateur;
- découvrir l'information nécessaire pour lancer des demandes.

6.5.1.1 Lancement de l'authentification OpenID

Le paragraphe 7.1 de [b-OpenID v.2] contient la recommandation suivante: Pour lancer l'authentification OpenID, il est recommandé que la partie utilisatrice présente à l'utilisateur final un formulaire qui contient un champ permettant d'entrer un identificateur fourni par l'utilisateur.

Il est recommandé que l'attribut "name" du champ du formulaire ait la valeur "openid_identifier" afin que les agents utilisateurs puissent automatiquement établir qu'il s'agit d'un formulaire OpenID. Il se peut que les extensions de navigateur ou d'autres logiciels prenant en charge l'authentification OpenID ne détectent pas la prise en charge d'une partie utilisatrice si cet attribut n'a pas la valeur appropriée.

Conformément à la présente Recommandation, il est obligatoire que le champ "openid_identifier" figure dans le formulaire que la partie utilisatrice a présenté dans le réseau NGN.

6.5.1.2 Normalisation d'un identificateur fourni par l'utilisateur

[b-OpenID v.2] définit trois types d'identificateurs: un identificateur URI "http" ou "https" (désigné par l'acronyme "URL" dans le présent document), ou un identificateur XRI [OASIS XRI SYNTAX 2.0].

Il est obligatoire que l'élément fourni par l'utilisateur final soit normalisé sous la forme d'un identificateur. La procédure spécifiée dans le § 7.2 de [b-OpenID v.2] est conforme aux exigences de normalisation des réseaux NGN.

6.5.1.3 Découverte de l'information nécessaire pour lancer des demandes

Dans [b-OpenID v.2], il est expliqué que la découverte est le processus dans le cadre duquel la partie utilisatrice utilise l'identificateur pour rechercher (découvrir) l'information nécessaire pour lancer des demandes.

L'authentification OpenID prévoit trois possibilités pour la découverte, comme indiqué dans le § 7.3 de [b-OpenID v.2].

[b-OpenID v.2] définit deux méthodes de découverte:

- la découverte fondée sur XRDS,
- la découverte fondée sur HTML.

Si la découverte XRI [b-OASIS XRI SYNTAX 2.0] ou Yadis est utilisée, le résultat sera un document XRDS, qui est un document XML avec des entrées pour des services qui sont liés à l'identificateur, comme spécifié dans le § 7.3.2.1 de [b-OpenID v.2].

Il est obligatoire que la découverte fondée sur HTML soit prise en charge par les parties utilisatrices. Elle ne peut être utilisée que pour la découverte d'identificateurs déclarés. Il est obligatoire que les identificateurs de fournisseur OpenID soient des identificateurs XRI [b-OASIS XRI SYNTAX 2.0] ou des URL qui prennent en charge la découverte XRDS. Pour que la découverte fondée sur HTML puisse être utilisée, il est obligatoire qu'un document HTML soit disponible à l'URL de l'identificateur déclaré, comme spécifié au § 7.3.3 de [b-OpenID v.2].

Conformément à la présente Recommandation, il est obligatoire que la partie utilisatrice respecte les exigences lorsqu'elle effectue la découverte et il est recommandé que l'identificateur soit conforme au format XRI ou URL.

6.5.2 Réponses d'authentification

Aux termes du § 10 de [b-OpenID v.2], lorsqu'une demande d'authentification émane de l'agent utilisateur via une communication indirecte, il est recommandé que le fournisseur OpenID établisse qu'un utilisateur final autorisé souhaite mener à bien l'authentification. Si un utilisateur final autorisé souhaite mener à bien l'authentification, il est recommandé que le fournisseur OpenID envoie une assertion positive à la partie utilisatrice.

Conformément à la présente Recommandation, il est obligatoire que les demandes d'autorisation comportent le paramètre "return_to".

NOTE – Les méthodes permettant d'identifier les utilisateurs finals autorisés et d'obtenir l'approbation pour renvoyer une assertion d'authentification OpenID ne relèvent pas de la présente spécification.

6.5.2.1 Assertions positives

Les assertions positives sont des réponses indirectes contenant des informations sur les paramètres de réponse. Voir le § 10.1 de [b-OpenID v.2].

Conformément à [b-OpenID v.2], il est obligatoire que le fournisseur OpenID, dans le cadre d'une communication indirecte avec une partie utilisatrice via un agent utilisateur:

- vérifie que l'URL return_to correspond à l'un des points d'extrémité de partie utilisatrice;
- établisse qu'un utilisateur final autorisé souhaite mener à bien l'authentification;
- génère un mot de circonstance pour la réponse;
- signe une réponse positive;
- envoie l'assertion positive à la partie utilisatrice via l'agent utilisateur.

6.5.2.2 Assertions négatives

Si le fournisseur OpenID n'est pas en mesure d'identifier l'utilisateur final ou si l'utilisateur final n'approuve pas ou ne peut pas approuver la demande d'authentification, il est recommandé que le fournisseur OpenID envoie une assertion négative à la partie utilisatrice sous la forme d'une réponse indirecte. Voir également le § 10.2 de [b-OpenID v.2].

Lorsque les parties utilisatrices reçoivent une assertion négative en réponse à une demande en mode "checkid_immediate", il est recommandé qu'elles génèrent une nouvelle demande d'authentification en utilisant le mode "checkid_setup".

6.5.2.2.1 Assertions négatives en réponse à des demandes de type immédiat

Si la demande était de type immédiat, l'utilisateur final est dans l'impossibilité d'interagir par l'intermédiaire de pages affichées par le fournisseur OpenID pour fournir des justificatifs d'identité ou donner son approbation à une demande. Une assertion négative en réponse à une demande de type immédiat prend la forme spécifiée au § 10.2.1 de [b-OpenID v.2].

6.5.2.2.2 Assertions négatives en réponse à des demandes de type non immédiat

Dans la mesure où le fournisseur OpenID peut afficher des pages accessibles à l'utilisateur final et demander à celui-ci des justificatifs, une réponse négative à une demande qui n'est pas de type immédiat est définitive. Elle prend la forme spécifiée au § 10.2.2 de [b-OpenID v.2].

Si une partie utilisatrice reçoit la réponse "cancel", l'authentification a échoué et il est obligatoire que la partie utilisatrice considère l'utilisateur final comme non authentifié.

6.5.3 Vérification des assertions

Conformément à [b-OpenID v.2], il est obligatoire que la partie utilisatrice, lorsqu'elle reçoit une assertion positive:

- vérifie l'URL de retour;
- vérifie l'information découverte;
- vérifie le mot de circonstance;
- vérifie les signatures.

Une fois qu'une assertion qui contenait un identificateur déclaré a été vérifiée, l'utilisateur est authentifié avec cet identificateur.

6.6 Considérations relatives à la sécurité

Le chapitre 15 (Considérations relatives à la sécurité) de la spécification du protocole OpenID [b-OpenID v.2] donne des lignes directrices en matière de sécurité concernant la prévention des attaques, les agents utilisateurs, l'interface d'utilisateur, les identificateurs d'URL HTTP et HTTPS et les variantes des protocoles. La présente Recommandation préconise la prise en charge de toutes les considérations relatives à la sécurité dans les réseaux NGN.

Les solutions devraient en outre être conformes aux exigences de sécurité applicables aux réseaux NGN et à la gestion IdM définies dans [UIT-T Y.2701], [UIT-T Y.2720] et [UIT-T Y.2721].

Bibliographie

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*

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

[b-Yadis] Protocole Yadis
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

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	**Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2015