Union internationale des télécommunications

# UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

# Y.2723

(11/2013)

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

Réseaux de prochaine génération – Sécurité

## Prise en charge d'OAuth dans les réseaux de prochaine génération

Recommandation UIT-T Y.2723

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 |
| | 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.2723

## Prise en charge d'OAuth dans les réseaux de prochaine génération


### Résumé

La Recommandation UIT-T Y.2723 spécifie les mécanismes et procédures applicables à l'utilisation du cadre d'autorisation OAuth 2.0 (OAuth), défini par l'Internet Engineering Task Force, dans les scénarios dans lesquels le rôle du serveur d'autorisation OAuth est rempli par un fournisseur de réseau de prochaine génération (NGN).

Le document associé, à savoir la Recommandation UIT-T Y.2724 (Cadre pour la prise en charge d'OAuth et d'OpenID dans les réseaux de prochaine génération) traite du contexte, de considérations relatives à l'architecture et du cadre de haut niveau pour l'utilisation d'OAuth dans les réseaux NGN.

La Recommandation UIT-T Y.2723 spécifie les exigences relatives à la restriction du choix des options OAuth, ainsi que les exigences supplémentaires permettant de faire en sorte que l'utilisation d'OAuth respecte les exigences relatives à la sécurité et à la gestion d'identité dans les réseaux NGN.



### Historique

| Edition | Recommandation | Approbation | Commission d'études | ID unique* |
|---|---|---|---|---|
| 1.0 | ITU-T Y.2723 | 2013-11-15 | 13 | 11.1002/1000/11913-en |


* 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

## Introduction

La Recommandation UIT-T Y.2723 définit un cadre pour la prise en charge et l'utilisation d'OAuth et d'OpenID dans les réseaux de prochaine génération (NGN). Elle s'appuie sur la Recommandation UIT-T Y.2724 pour définir des méthodes particulières pour la prise en charge d'OAuth.

NOTE – Dans la présente Recommandation, aucune modification n'est apportée au protocole OAuth; on s'intéresse uniquement à la prise en charge et à l'utilisation d'OAuth dans les réseaux NGN.

# Recommandation UIT-T Y.2723

## Prise en charge d'OAuth dans les réseaux de prochaine génération

### 1 Domaine d'application

La présente Recommandation décrit les mécanismes et procédures permettant de prendre en charge le protocole d'autorisation OAuth 2.0 (OAuth) dans les réseaux de prochaine génération (NGN). Ces mécanismes et procédures peuvent être utilisés pour prendre en charge des services d'application dans un environnement multiservice et multifournisseur. Dans la présente Recommandation, on suppose que le service d'autorisation OAuth est assuré par les réseaux NGN.

### 2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1254] Recommandation UIT-T X.1254 (2012), *Cadre de garantie d'authentification des entités*.

[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 version 1*.

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

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

[UIT-T Y.2724] Recommandation UIT-T Y.2724 (2013), *Cadre pour la prise en charge d'OAuth et d'OpenID dans les réseaux de prochaine génération*.

[IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework*. <http://datatracker.ietf.org/doc/rfc6749/>

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 jeton d'accès** [IETF RFC 6749]: justificatif utilisé pour accéder à une ressource protégée. Un jeton d'accès est une chaîne représentant une autorisation délivrée au client. Cette chaîne est généralement opaque pour le client. Les jetons représentent des types et durées d'accès spécifiques, accordés par le propriétaire de ressources et appliqués par le serveur de ressources et le serveur d'autorisation.

**3.1.2 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.

**3.1.3 autorisation** [b-UIT-T X.800]: attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

**3.1.4 justificatif d'autorisation** [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.

**3.1.5 serveur d'autorisation** [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.

**3.1.6 client** [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).

**3.1.7 clients confidentiels** [IETF RFC 6749]: clients pouvant maintenir la confidentialité de leurs justificatifs (par ex. un client mis en œuvre sur un serveur sécurisé avec un accès restreint aux justificatifs du client), ou pouvant être authentifiés de manière sécurisée par d'autres moyens.

**3.1.8 clients publics** [IETF RFC 6749]: clients ne pouvant pas maintenir la confidentialité de leurs justificatifs (par ex. des clients mis en œuvre sur le dispositif utilisé par le propriétaire de ressources, tels qu'une application native installée ou une application basée sur un navigateur web), et ne pouvant pas être authentifiés de manière sécurisée par quelque autre moyen que ce soit.

**3.1.9 propriétaire de ressources** [IETF RFC 6749]: entité capable d'octroyer l'accès à une ressource protégée. Lorsque le propriétaire de ressources est une personne, il est appelé utilisateur final.

**3.1.10 serveur de ressources** [IETF RFC 6749]: serveur hébergeant les ressources protégées, capable d'accepter les demandes de ressource protégée utilisant des jetons d'accès et de répondre à ces demandes.

### 3.2 Termes définis dans la présente Recommandation

Aucun.

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes ci-après:

IdM gestion d'identité (*identity management*)

NGN réseau de prochaine génération (*next generation network*)

OAuth protocole d'autorisation OAuth 2.0

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

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

## 5 Conventions

Aucune.

## 6 Prise en charge d'OAuth dans les réseaux NGN

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

### 6.1 Choix des types de client OAuth en fonction des exigences de sécurité des réseaux NGN

Le document [IETF RFC 6749] définit deux types de client OAuth, à savoir les clients confidentiels et les clients publics.

Les clients publics ne respectent pas les exigences d'authentification pour les fournisseurs d'application tiers NGN [UIT-T Y.2702], car ils ne peuvent pas être authentifiés par le fournisseur NGN [UIT-T Y.2724]. La présente Recommandation recommande que les réseaux NGN ne prennent en charge que les clients confidentiels. Les clients doivent respecter les exigences suivantes:

1) Le client OAuth NGN doit pouvoir être authentifié avec certains niveaux de garantie [UIT-T Y.2702], [UIT-T X.1254].

2) Le client OAuth NGN doit être enregistré auprès du serveur d'autorisation, comme spécifié au paragraphe 2 du document [IETF RFC 6749].

Le document [IETF RFC 6749] (OAuth 2.0) définit les profils de client suivants: application web, application basée sur un agent d'utilisateur et application native. L'application web est un profil de client privé, tandis que les deux autres sont des profils de client public. La présente Recommandation décrit la prise en charge dans les réseaux NGN uniquement du client du profil d'application web.

### 6.2 Choix des types de justificatif d'autorisation

Le document [IETF RFC 6749] définit les types suivants de justificatifs d'autorisation: code d'autorisation, implicite, information de mot de passe du propriétaire de ressources et justificatif client. En outre, l'IETF travaille actuellement à la définition d'une extension, qui spécifie le type de justificatif d'autorisation assertion SAML 2.0 pour OAuth 2.0.

Dans le document [IETF RFC 6749], il est expliqué que, "lors de la délivrance d'un jeton d'accès pendant la procédure fondée sur un justificatif d'autorisation implicite, le serveur d'autorisation n'authentifie pas le client. Dans certains cas, l'identité du client peut être vérifiée via l'URI de redirection utilisé pour délivrer le jeton d'accès au client. Le jeton d'accès peut être présenté au propriétaire de ressources ou à d'autres applications ayant accès à l'agent d'utilisateur du propriétaire de ressources."

Ainsi, pour les procédures OAuth qui utilisent le type de justificatif d'autorisation implicite, les exigences d'authentification pour le fournisseur d'application tiers NGN [UIT-T Y.2702] ne sont pas respectées.

La présente Recommandation décrit uniquement la prise en charge dans les réseaux NGN du client confidentiel du profil d'application web avec l'utilisation des justificatifs d'autorisation suivants:

- code d'autorisation;
- information de mot de passe du propriétaire de ressources;
- justificatif client;
- assertion SAML 2.0.

### 6.3 Recommandations sur les options OAuth pour les clients pris en charge dans les réseaux NGN

Les procédures [IETF RFC 6749] sont optimisées pour plusieurs profils de client pour les deux types de clients. Le document RFC spécifie les options permettant de choisir les types de justificatif d'autorisation, les paramètres et les exigences de sécurité.

Le présent paragraphe donne des recommandations pour la prise en charge des clients confidentiels du profil d'application web. Il porte aussi sur les exigences et les paramètres optionnels dont le choix est essentiel pour la prise en charge d'*OAuth* dans les réseaux NGN.

### 6.3.1 Enregistrement du client

Au paragraphe 2.2 du document [IETF RFC 6749], il est recommandé que les URI de redirection des clients soient enregistrés auprès d'un serveur d'autorisation, car les clients dont les URI sont enregistrés offrent une meilleure sécurité.

La présente Recommandation impose aux clients pris en charge dans les réseaux NGN d'enregistrer leurs URI de redirection auprès du serveur d'autorisation.

### 6.3.2 Confidentialité des messages destinés au point d'extrémité de redirection du client

Au paragraphe 3.1.2.1 du document [IETF RFC 6749], il est recommandé ce qui suit: "le point d'extrémité de redirection DEVRAIT exiger l'utilisation de TLS comme décrit au paragraphe 1.6 lorsque le type de réponse demandée est "code" ou "jeton", ou lorsque la demande de redirection implique la transmission de justificatifs sensibles sur un réseau ouvert". La présente Recommandation impose l'utilisation de TLS pour la transmission de n'importe quelle information sensible.

### 6.3.3 Authentification du client

Les clients définis par le profil d'application web étant des clients confidentiels, leur authentification auprès d'un serveur d'autorisation est obligatoire.

### 6.3.4 Procédures d'autorisation

Dans la présente Recommandation, on s'intéresse aux clients confidentiels du profil d'application web qui utilisent les procédures d'autorisation avec les types de justificatif d'autorisation suivants:

- code d'autorisation;
- information de mot de passe du propriétaire de ressources;
- justificatif client;
- extension SAML.

#### 6.3.4.1 Code d'autorisation

La procédure d'autorisation des clients confidentiels utilisant un code d'autorisation est spécifiée au paragraphe 4.1 du document [IETF RFC 6749]. La présente Recommandation impose de faire figurer le paramètre *redirect_uri* dans les demandes d'autorisation.

Les exigences suivantes s'appliquent à l'interaction entre le serveur d'autorisation et les clients du profil d'application web utilisant un code d'autorisation. Le serveur d'autorisation DOIT:

- authentifier le client qui a soumis la demande d'autorisation;
- vérifier que la valeur du paramètre *redirect_uri* figurant dans la demande d'autorisation du client correspond à la valeur enregistrée pour le client;
- ne délivrer un code d'autorisation qu'aux clients authentifiés et autorisés;
- avant de délivrer un jeton d'accès, vérifier que le code d'autorisation est valable.

#### 6.3.4.2 Information de mot de passe du propriétaire de ressources

La procédure d'autorisation qui utilise ce type de justificatif d'autorisation est optimisée pour les clients dont la fiabilité a été établie auprès du propriétaire de ressources. Un client utilise l'information de mot de passe du propriétaire de ressources pour obtenir un jeton d'accès auprès du serveur d'autorisation. La procédure spécifiée au paragraphe 4.3 du document [IETF RFC 6749] satisfait aux exigences de sécurité dans les réseaux NGN.

NOTE – Le document [IETF RFC 6749] permet l'utilisation de cette procédure par les clients publics. Dans la présente Recommandation, seuls sont pris en compte les clients confidentiels, dont l'authentification auprès du serveur d'autorisation est obligatoire.

Conformément au document [IETF RFC 6749], lorsque le serveur d'autorisation interagit avec un client qui utilise comme type de justificatif d'autorisation l'information de mot de passe du propriétaire de ressources, il DOIT:

- authentifier le client;
- valider l'information de mot de passe du propriétaire de ressources présentée par le client;
- délivrer un jeton d'accès si le client a été authentifié et a présenté une information de mot de passe du propriétaire de ressources valable.

### 6.4 Authentification du propriétaire de ressources

La spécification d'OAuth [IETF RFC 6749] ne spécifie pas l'authentification du propriétaire de ressources (par ex. un utilisateur final) par le serveur d'autorisation. Dans l'environnement des réseaux NGN, un mécanisme d'authentification du propriétaire de ressources doit respecter les exigences de la Recommandation [UIT-T Y.2702].

### 6.5 Considérations relatives à la sécurité

Dans la spécification d'OAuth 2.0 [IETF RFC 6749], le paragraphe sur les considérations relatives à la sécurité contient des lignes directrices en matière de sécurité pour tous les profils de client OAuth 2.0 – application web, application basée sur un agent d'utilisateur et application native. La présente Recommandation recommande la prise en charge des clients d'application web dans les réseaux NGN. Par conséquent, seuls les aspects de sécurité du document [IETF RFC 6749] qui se rapportent aux clients d'application web s'appliquent ici. En outre, le document [b-IETF RFC 6819] fournit un modèle de sécurité OAuth complet et des informations générales relatives à la conception du protocole. Pour les mises en œuvre qui prennent en charge OAuth dans les réseaux NGN, il convient de tenir compte des dispositions du document [b-IETF RFC 6819] qui s'appliquent aux clients d'application web.

Les solutions devraient aussi respecter les exigences relatives à la sécurité et à la gestion d'identité dans les réseaux NGN, spécifiées dans [UIT-T Y.2701], [UIT-T Y.2720], [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-IETF RFC 6819] IETF RFC 6819, *OAuth 2.0 Threat Model and Security Considerations*. http://datatracker.ietf.org/doc/rfc6819/

## 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, 2014