International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2723

(11/2013)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Security

Support for OAuth in next generation networks

Recommendation ITU-T Y.2723

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	**Y.2700–Y.2799**
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2723

Support for OAuth in next generation networks

Summary

Recommendation ITU-T Y.2723 specifies the mechanisms and procedures for employing "The OAuth 2.0 Authorization Framework (OAuth)", defined by the Internet Engineering Task Force, for the scenarios where the role of the OAuth authorization server is performed by a next generation network (NGN) provider.

The companion document, Recommendation ITU-T Y.2724, "Framework for supporting OAuth and OpenID in next generation networks", provides the context, architectural considerations and high-level framework for employing OAuth in NGNs.

This Recommendation specifies the requirements pertinent to the restriction of OAuth option selections, as well as additional requirements that make the use of OAuth consistent with NGN security and identity management requirements.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2723	2013-11-15	13

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Recommendation ITU-T Y.2723 provides a framework for the support and use of OAuth and OpenID in next generation networks (NGNs). This Recommendation builds upon Recommendation ITU-T Y.2724 to define specific methods for supporting OAuth.

NOTE – This Recommendation does not make any changes or modifications to the OAuth protocol. It focuses only on the support and use of OAuth by NGNs.

Recommendation ITU-T Y.2723

Support for OAuth in next generation networks

1 Scope

This Recommendation describes the mechanisms and procedures for the support of OAuth 2.0 authorization protocol (OAuth) in next generation networks (NGNs). The mechanisms and procedures described in this Recommendation can be used to support application services in a multi-service, multi-provider environment. This Recommendation assumes that the OAuth authorization service is provided by the NGN.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1.*

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

[ITU-T Y.2721] Recommendation ITU-T Y.2721 (2010), *NGN identity management requirements and use cases.*

[ITU-T Y.2724] Recommendation ITU-T Y.2724 (2013), *Framework for supporting OAuth and OpenID in next generation networks.*

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access token [IETF RFC 6749]: Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client. The string is usually opaque to the client. Tokens represent specific scopes and durations of access, granted by the resource owner, and enforced by the resource server and authorization server.

3.1.2 (entity) authentication [b-ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

3.1.3 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 authorization grant [IETF RFC 6749]: An authorization grant is a credential representing the resource owner's authorization (to access its protected resources) used by the client to obtain an access token.

3.1.5 authorization server [IETF RFC 6749]: The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.

3.1.6 client [IETF RFC 6749]: An application making protected resource requests on behalf of the resource owner and with its authorization. The term "client" does not imply any particular implementation characteristics (e.g., whether the application executes on a server, a desktop or other devices).

3.1.7 confidential clients [IETF RFC 6749]: These are clients capable of maintaining the confidentiality of their credentials (e.g., client implemented on a secure server with restricted access to the client credentials), or capable of secure client authentication using other means.

3.1.8 public clients [IETF RFC 6749]: These are clients incapable of maintaining the confidentiality of their credentials (e.g., clients executing on the device used by the resource owner, such as an installed native application or a web browser-based application), and incapable of secure client authentication via any other means.

3.1.9 resource owner [IETF RFC 6749]: An entity capable of granting access to a protected resource. When the resource owner is a person, they are referred to as an end-user.

3.1.10 resource server [IETF RFC 6749]: The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IdM	Identity Management
NGN	Next Generation Network
OAuth	OAuth 2.0 Authorization Protocol
SAML	Security Assertion Markup Language
URI	Uniform Resource Identifier

5 Conventions

None.

6 Support for OAuth in NGN

This clause describes the main aspects of supporting OAuth in NGN.

6.1 Selection of OAuth client types based on NGN security requirements

[IETF RFC 6749] defines two OAuth client types: confidential and public clients.

Public clients do not meet the authentication requirements for NGN third party application providers [ITU-T Y.2702], because public clients cannot be authenticated by the NGN provider [ITU-T Y.2724]. This Recommendation recommends that the NGN supports only confidential clients. The clients must meet the following requirements:

1. The NGN OAuth client must be able to be authenticated at specific assurance levels [ITU-T Y.2702], [ITU-T X.1254].
2. The NGN OAuth client must be registered with the authorization server as specified in section 2 of [IETF RFC 6749].

OAuth 2.0 [IETF RFC 6749] defines the following client profiles: web application, user-agent-based application, and native application. The web application is a profile of a private client, while the last two are profiles of the public clients. This Recommendation describes NGN support only for the client of the web application profile.

6.2 Selection of the authorization grant types

[IETF RFC 6749] defines the following types of authorization grants: authorization code, implicit, resource owner password credentials, and client credentials. Additionally, IETF are currently working on defining an extension, which specifies the SAML 2.0 assertion grant type for OAuth 2.0.

[IETF RFC 6749] explains that "when issuing an access token during the implicit grant flow, the authorization server does not authenticate the client. In some cases, the client identity can be verified via the redirection URI used to deliver the access token to the client. The access token may be exposed to the resource owner or other applications with access to the resource owner's user-agent".

Thus, the OAuth flows that use the implicit grant type do not result in authentication that meets the requirements for authentication of the NGN third party application provider [ITU-T Y.2702].

This Recommendation focuses on describing NGN support of the confidential client of the web application profile with the use of the following authorization grants:

- authorization code
- resource owner password credentials
- client credentials
- SAML 2.0 assertion.

6.3 Recommendations on the OAuth options for NGN-supported clients

[IETF RFC 6749] flows are optimized for several client profiles of the two types of clients. The RFC specifies the options for selecting the authorization grant types, parameters and security requirements.

This clause provides recommendations for supporting confidential clients of the web application profile. This clause also focuses on those requirements and optional parameters whose selection is essential for *OAuth* support in NGNs.

6.3.1 Client registration

Section 2.2 of [IETF RFC 6749] recommends the registration of the clients' redirection URIs with an authorization server, because the clients with the registered URIs enable higher security.

This Recommendation requires that NGN-supported clients register their redirection URIs with the authorization server.

6.3.2 Confidentiality of the messages to the client redirection endpoint

Section 3.1.2.1 of [IETF RFC 6749], makes the following recommendation: "the redirection endpoint SHOULD require the use of TLS as described in section 1.6 when the requested response type is "code" or "token", or when the redirection request will result in the transmission of sensitive credentials over an open network". This Recommendation requires that TLS be used for the transmission of any sensitive information.

6.3.3 Client authentication

The clients defined by the web application profile are confidential clients. Therefore, the client's authentication to an authorization server is required.

6.3.4 Authorization procedures

This Recommendation covers confidential clients of the web application profile that use the authorization procedures of the following authorization grant types:

- authorization code
- resource owner password credential
- client credentials
- SAML extension.

6.3.4.1 Authorization code

The authorization procedure for confidential clients with the use of the authorization code is specified in section 4.1 of [IETF RFC 6749]. This Recommendation requires the inclusion of the *redirect_uri* parameter in authorization requests.

The following requirements apply to the authorization server's interaction with the clients of the web application profile using an authorization code. The authorization server MUST:

- authenticate the client that issued the authorization request;
- ensure that the value of the *redirect_uri* parameter in the client's authorization request matches the registered value for the client;
- issue the authorization code only to authenticated and authorized clients;
- before issuing an access token, ensure that the authorization code is valid.

6.3.4.2 Resource owner password credentials

The authorization procedure that uses this grant type is optimized for the clients that have established trust with the resource owner. A client uses the resource owner's password credentials to get an access token from the authorization server. The procedure specified in section 4.3 of [IETF RFC 6749] satisfies the NGN security requirements.

NOTE – [IETF RFC 6749] permits the use of this procedure by public clients. This Recommendation considers only confidential clients, which are required to authenticate to the authorization server.

In accordance with [IETF RFC 6749] the authorization server, when interacting with a client that uses the grant type resource owner password credentials, MUST:

- authenticate the client;
- validate the resource owner password credentials presented by the client;
- issue an access token if the client has authenticated to the authorization server and presented the valid resource owner credentials.

6.4 Authentication of a resource owner

The OAuth specification [IETF RFC 6749] does not specify resource owner's (e.g., end-user) authentication by the authorization server. In the NGN environment, a mechanism for authentication of a resource owner must meet the requirements of [ITU-T Y.2702].

6.5 Security considerations

The section "Security Considerations" for the specification of OAuth 2.0 [IETF RFC 6749] provides security guidelines for all OAuth 2.0 client profiles – web application, user-agent-based application and native application. This Recommendation recommends the support of web application clients in NGN. Consequently, only the security considerations of [IETF RFC 6749] that are related to the web application clients apply here. In addition, [b-IETF RFC 6819] provides a comprehensive OAuth security model and background for the protocol design. The material of [b-IETF RFC 6819] that is relevant to the web application clients should be considered for the implementations that support OAuth in NGN.

The solutions should also comply with the NGN and IdM security requirements specified in [ITU-T Y.2701], [ITU-T Y.2720], [ITU-T Y.2721].

Bibliography

[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/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013