International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2725

(07/2014)

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

Next Generation Networks – Security

Support of OpenID in next generation networks

Recommendation ITU-T Y.2725

International Telecommunication Union

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.2725

Support of OpenID in next generation networks

Summary

Recommendation ITU-T Y.2725 specifies mechanisms and procedures for supporting and using OpenID for the scenarios where the role of OpenID provider is performed by the NGN provider.

Recommendation ITU-T Y.2724 provides a framework for NGN support and the use of OAuth and OpenID. Recommendation ITU-T Y.2725 builds upon Recommendation ITU-T Y.2722 and Recommendation ITU-T Y.2724 to define specific mechanisms for supporting OpenID.

NOTE – Recommendation ITU-T Y.2725 does not make any changes or modifications to the OpenID protocol. It focuses only on the support and use of OpenID by NGN.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2725	2014-07-18	13	11.1002/1000/12079

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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

Recommendation ITU-T Y.2725

Support of OpenID in next generation networks

1 Scope

This Recommendation describes mechanisms and procedures for support of OpenID in NGN. The mechanisms and procedures described in this Recommendation can be used to support application services in a multi-service provider environment. This Recommendation assumes that the NGN provider is the OpenID provider.

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 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*.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

3.1.3 authorization grant [b-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.

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

3.1.5 client [b-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).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FE Functional Entity

FRA Functional Requirements and Architecture

IdM Identity Management

IdP Identity Provider

IETF Internet Engineering Task Force

IP Internet Protocol

OAuth OAuth 2.0 Authorization Protocol

OP OpenID Provider

SAML Security Assertion Markup Language

URI Uniform Resource Identifier

WS Web Server

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Support for OpenID in NGN

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

6.1 Reference model

According to the specification of OpenID [b-OpenID v.2], the OpenID IdP server participates throughout the authentication workflow. Refer to [ITU-T Y.2724] for a general overview of OAuth and OpenID framework.

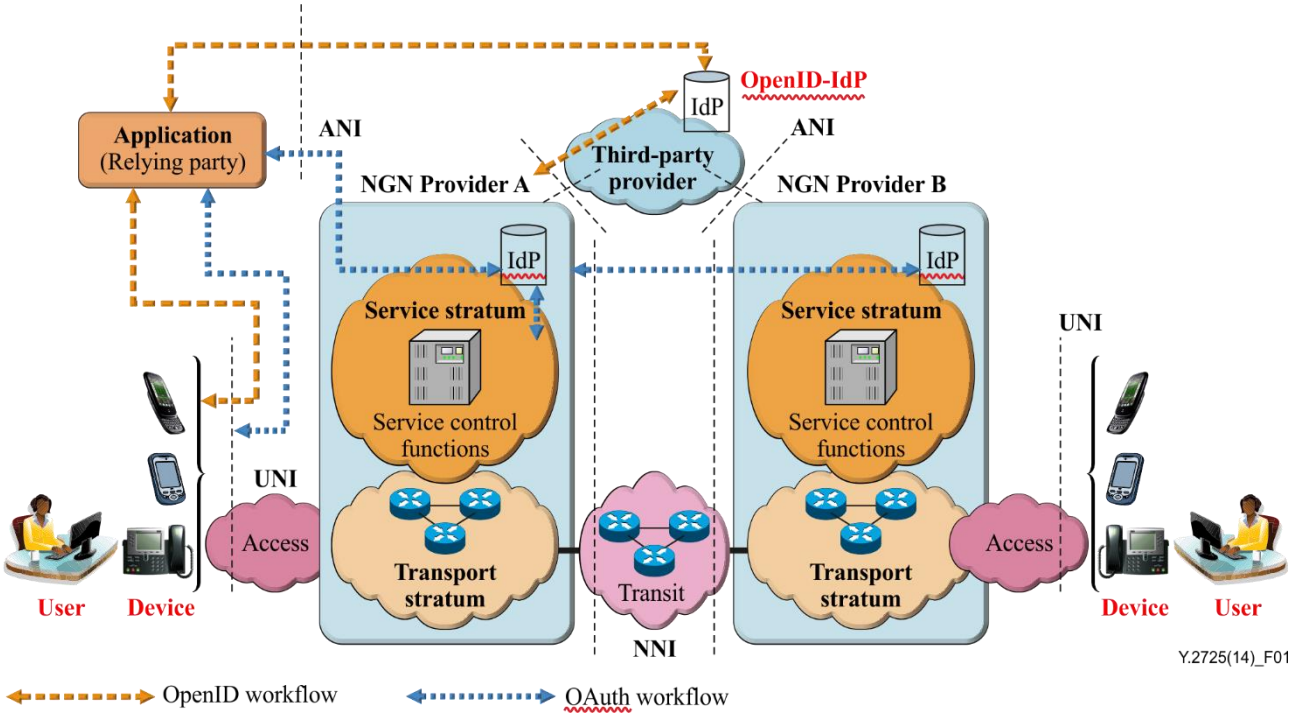

Figure 1 – The OpenID and the OAuth flows for NGN

6.2 Protocol message formats in the context of NGN

[b-OpenID v.2] defines two protocol message format types:

- Key-Value form encoding,
- HTTP encoding.

Section 4.1.1 of [b-OpenID v.2] explains that "Key-Value form encoding is used for signature calculation and for direct responses to relying parties".

For HTTP encoding, section 4.1.2 of [b-OpenID v.2], explains that "this model applies to messages from the user-agent to both the relying party and the OP, as well as messages from the relying party to the OP".

The NGN-supported entities are required to meet the requirements when sending a protocol message.

6.3 Communication types

[b-OpenID v.2] defines two communication types:

- direct communication,
- indirect communication.

Section 5.1 of [b-OpenID v.2] explains that direct communication is initiated by a relying party to an OP endpoint URL. It is used for establishing associations and verifying authentication assertions.

Section 5.2 of [b-OpenID v.2] explains that in indirect communication, messages are passed through the user-agent. This can be initiated by either the relying party or the OP. Indirect communication is used for authentication requests and authentication responses.

The NGN-supported entities are required to meet these requirements when initiating the communication context.

6.4 Generating signatures

OpenID authentication supports two signature algorithms:

- HMAC-SHA1 – 160 bit key length
- HMAC-SHA256 – 256 bit key length

This clause provides recommendations for the use of HMAC-SHA256. The procedure to generate a message signature specified in section 6.1 of [b-OpenID v.2] satisfies the NGN security requirements.

6.5 Procedures of OpenID authentication in NGN

6.5.1 Authentication requests

Section 13 of [b-OpenID v.2] recommends that "relying parties are recommended to use the Yadis protocol to publish their valid return_to URLs. The relying party can optionally publish this information at any URL, and are recommended to publish it under the realm so that providers can verify return_to URLs".

This Recommendation requires that relying parties are recommended to use Yadis protocol to publish their valid return message_to URLs in NGN.

The authentication requests are specified in section 9 of [b-OpenID v.2].

The following requirements apply to the relying party's interaction with an end user. The relying party is required to:

- Initiate OpenID authentication
- Normalize a user-supplied identifier
- Discover the necessary information for initiating requests

6.5.1.1 Initiating OpenID authentication

Section 7.1 of [b-OpenID v.2] makes the following recommendation: "To initiate OpenID authentication, the relying party is recommended to present the end user with a form that has a field for entering a user-supplied identifier".

The form field's "name" attribute is recommended to have the value "openid_identifier", so that user-agents can automatically determine that this is an OpenID form. Browser extensions or other software that support OpenID authentication may not detect a relying party's support if this attribute is not set appropriately.

This Recommendation requires the inclusion of the "openid_identifier" field in the form that the relying party entity presented in NGN.

6.5.1.2 Normalizing a user-supplied identifier

[b-OpenID v.2] defines three types of identifiers: "http" or "https" URI, (commonly referred to as a "URL" within this document), or an XRI [OASIS XRI SYNTAX 2.0].

The end user's input is required to be normalized into an identifier, the procedure specified in section 7.2 of [b-OpenID v.2] satisfies the NGN normalization requirements.

6.5.1.3 Discovery of the necessary information for initiating requests

[b-OpenID v.2] explains that discovery is the "process where the relying party uses the identifier to look up (discover) the necessary information for initiating requests".

OpenID authentication has three paths through which to do discovery, as specified in section 7.3 of [b-OpenID v.2].

[b-OpenID v.2] defines two discovery methods:

- XRDS-based discovery
- HTML-based discovery

If XRI [b-OASIS XRI SYNTAX 2.0] or Yadis discovery is used, the result will be an XRDS document. This is an XML document with entries for services that are related to the identifier, as specified in section 7.3.2.1 of [b-OpenID v.2].

HTML-based discovery is required to be supported by relying parties. HTML-based discovery is only usable for discovery of claimed identifiers. OP identifiers are required to be XRI [b-OASIS XRI SYNTAX 2.0] or URLs that support XRDS discovery. To use HTML-based discovery, it is required that an HTML document be available at the URL of the claimed identifier, as specified in section 7.3.3 of [b-OpenID v.2].

This Recommendation requires that the relying party is required to meet the requirements when performing the discovery and that the identifier is recommended to accord XRI or URL format.

6.5.2 Authentication responses

Section 10 of [b-OpenID v.2] recommends that when an authentication request comes from the User-Agent via indirect communication, the OP is recommended to determine that an authorized end user wishes to complete the authentication. If an authorized end user wishes to complete the authentication, the OP is recommended to send a positive assertion to the Relying Party.

This Recommendation requires the inclusion of the "return_to" parameter in authorization requests.

NOTE – Methods of identifying authorized end users and obtaining approval to return an OpenID authentication assertion are beyond the scope of this specification.

6.5.2.1 Positive assertions

Positive assertions are indirect responses, for information on the response parameters, see section 10.1 of [b-OpenID v.2].

In accordance with [b-OpenID v.2], the OP, when in indirect communication with a relying party via a user-agent, is required to:

- Verify that the return_to URL matches one of the relying party endpoints
- Determine that an authorized end user wishes to complete the authentication
- Generate response nonce
- Sign a positive response
- Send the positive assertion to the relying party via user-agent.

6.5.2.2 Negative assertions

If the OP is unable to identify the end user or the end user does not or cannot approve the authentication request, the OP is recommended to send a negative assertion to the relying party as an indirect response. See also section 10.2 of [b-OpenIDv.2].

When receiving a negative assertion in response to a "checkid_immediate" mode request, relying parties are recommended to construct a new authentication request using "checkid_setup" mode.

6.5.2.2.1 Negative assertions in response to immediate requests

If the request was an immediate request, there is no chance for the end user to interact with pages on the OP to provide identifying credentials or approval of a request. A negative assertion of an immediate request takes the form specified in section 10.2.1 of [b-OpenID v.2].

6.5.2.2.2 Negative assertions in response to non-immediate requests

Since the OP may display pages to the end user and request credentials from the end user, a negative response to a request that is not immediate is definitive. It takes the form specified in section 10.2.2 of [b-OpenID v.2].

If a relying party receives the "cancel" response, authentication was unsuccessful and the relying party is required to treat the end user as non-authenticated.

6.5.3 Verifying assertions

In accordance with [b-OpenID v.2], the relying party, when receiving a positive assertion, is required to:

- Verify the return URL
- Verify discovered information
- Check the nonce
- Verify signatures

If an assertion is verified and the assertion contained a claimed identifier, the user is now authenticated with that identifier.

6.6 Security considerations

Section 15 (Security Considerations) of the OpenID 2.0 specification [b-OpenID v.2] provides security guidelines for preventing attacks, user-agents, user interface, HTTP and HTTPS URL identifiers and protocol variants. This Recommendation recommends support of all the security considerations in NGN.

Solutions should also comply with the NGN and IdM security requirements specified in [ITU-T Y.2701], [ITU-T Y.2720] and [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-OpenIDv.2] OpenID Authentication 2.0.
http://openid.net/specs/openid-authentication-2_0.html

[b-Yadis] Yadis Protocol.
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

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, 2015