International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2724

(11/2013)

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

Next Generation Networks – Security

Framework for supporting OAuth and OpenID in next generation networks

Recommendation ITU-T Y.2724

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.2724

Framework for supporting OAuth and OpenID in next generation networks

Summary

Recommendation ITU-T Y.2724 describes a framework for the support and use of the IETF open authorization protocol (OAuth) and the OpenID protocol in the context of next generation networks (NGNs). Both protocols have been defined for general use on the worldwide web.

The heightened security and identity management requirements of NGNs require careful restriction of the above protocols. This Recommendation explains the applicability of these protocols to NGNs and provides high-level guidelines for their use.

The companion Recommendation ITU-T Y.2723, "Support for OAuth in next generation networks" provides a detailed set of NGN profiles.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2724	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

Recommendation ITU-T Y.2724

Framework for supporting OAuth and OpenID in next generation networks

1 Scope

This Recommendation describes a framework for the support and use of OAuth and OpenID by next generation networks (NGNs). The scope of this Recommendation includes:

- functional framework for NGN support of OAuth and OpenID
- requirements for NGN support of OAuth and OpenID
- OAuth and OpenID use cases (documented in Appendix I).

NOTE – Implementers and operators of the described technology shall comply with all applicable national and regional laws, regulations and policies.

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.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

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

[ITU-T Y.2722] Recommendation ITU-T Y.2722 (2011), *NGN identity management mechanisms.*

[IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework.* <http://tools.ietf.org/html/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.

NOTE – Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication.

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

3.1.5 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).

3.1.6 entity [b-ITU-T X.1252]: Something that has a separate and distinct existence and that can be identified in context.

NOTE – An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.

3.1.7 identifier [b-ITU-T X.1252]: One or more attributes used to identify an entity within a context.

NOTE – In the context of NGN as defined in [b-ITU-T Y.2091], an identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects).

3.1.8 identity provider (IdP) [b-ITU-T X.1252]: See identity service provider (IdSP)

3.1.9 identity service provider (IdSP) [b-ITU-T X.1252]: An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

3.1.10 refresh token [IETF RFC 6749]: Refresh tokens are issued to the client by the authorization server and are used to obtain a new access token when the current access token becomes invalid or expires, or to obtain additional access tokens with identical or narrower scope (access tokens may have a shorter lifetime and fewer permissions than authorized by the resource owner). Issuing a refresh token is optional at the discretion of the authorization server. If the authorization server issues a refresh token, it is included when issuing an access token.

3.1.11 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.

3.1.12 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:

AKA Authentication and Key Agreement

ANI Application-to-Network Interface

FE Functional Entity

GBA Generic Bootstrapping Architecture

IdM Identity Management

IdP Identity Provider

IdSP Identity Service Provider

IMPI IP Multimedia Private Identity

IMSI International Mobile Subscriber Identity

NGN Next Generation Network

SAML Security Assertion Markup Language

SNI Service Network Interface

UNI User Network Interface

5 Conventions

In this Recommendation:

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.

In the body of this Recommendation and its annexes, the words shall, shall not, should and may sometimes appear, in which case they are to be interpreted respectively as, is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Framework for supporting OAuth and OpenID in NGN

As described in [ITU-T Y.2720], the NGN network consists of multiple functional elements that use identifiers of entities to perform their functions in order to support and facilitate open authentication services to other providers. Such arrangements could be supported using OpenID and OAuth as shown in Figure 1. The use of OpenID and OAuth in NGNs is depicted in Figure 1.

According to the OpenID specification [b-OpenID v.2], the OpenID IdP server participates in the whole authentication workflow, and the OAuth allows the relying party to send the authentication message directly to the NGN-IdP through the OAuth protocol.

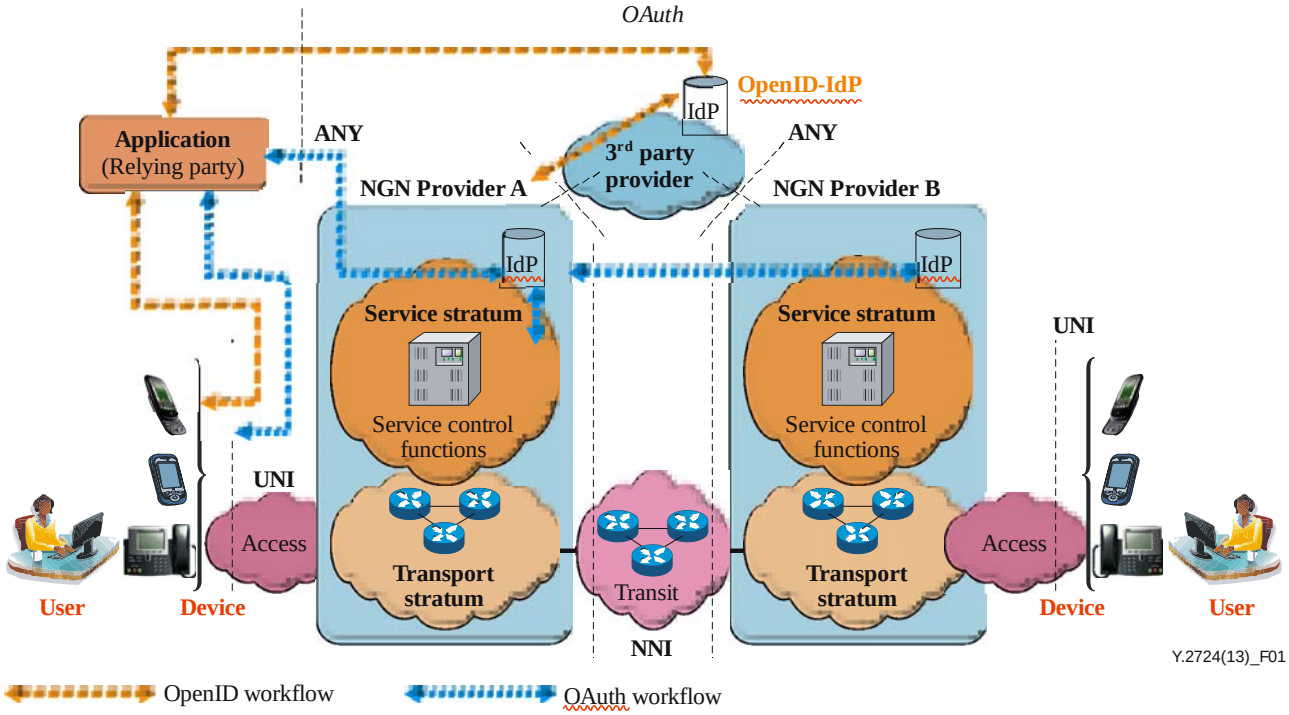

Figure 1 – The OpenID and OAuth flows for NGN

6.1 Reference model

Figure 1 provides a general overview of OAuth and OpenID frameworks.

Figure 2 depicts a reference model for NGN to provide OAuth authorization and OpenID authentication services. NGN providers may use OpenID and OAuth to offer IdSP services and partner with content and application providers and/or other service providers.

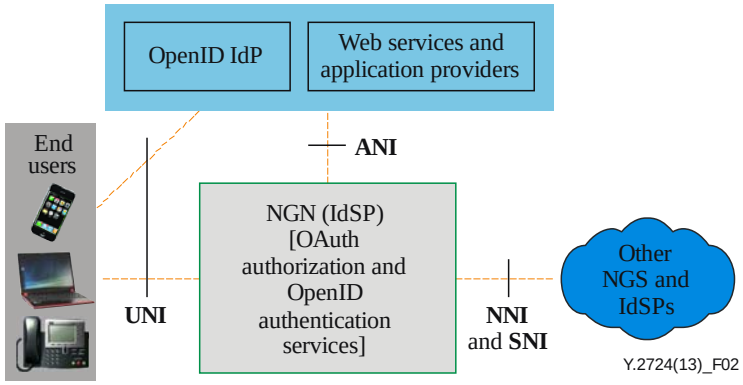

Figure 2 – Reference model

6.2 OAuth and OpenID flows

This clause provides the general description of the message flows for OAuth and OpenID in NGN.

6.2.1 Entities involved in information flows

This clause identifies the entities (including the functional entities of [ITU-T Y.2012]) that participate in the OAuth and OpenID information flows.

6.2.2 Entities that are common to the OAuth and OpenID flows

The entities involved in both the OAuth and OpenID flows are as follows:

- end-user function with the capability of a web client (e.g., browser);
- A-2: application gateway functional entity (APL-GW-FE) [ITU-T Y.2012]. This functional entity should be capable of supporting OAuth and/or OpenID protocols.

As defined in [ITU-T Y.2012], the "APL-GW-FE is the interworking entity between various functions of NGN and all external application servers and service enablers". That makes A-2 a logical choice for providing support for OpenID and OAuth. Additionally, because of its connection with S-5 – service user profile functional entity (SUP-FE) [ITU-T Y.2012], A-2 is capable of supporting AKA-based authentication, including generic bootstrapping architecture (GBA), of the user devices. A method of OpenID authentication based on GBA is specified in [b-3GPP TS 33.220]. Another method for OpenID authentication based on AKA, similar to GBA in some aspects, is described in clause 6.2.8 of [ITU-T Y.2722]. If the OAuth authorization server and OpenID IdP [ITU-T Y.2722] are both implemented on A-2, they can use AKA-based authentication, through the interaction with S-5.

6.2.3 Entities that are specific to the OAuth flow

The OAuth-specific entities are the following:

- A web application server that performs a service for a user – an OAuth client. A client may, but not have to, run on an NGN entity.
- An authorization server implemented as part of A-2.

  An authorization server first performs user authentication and then performs authorization of the client request. If both procedures succeed, the OAuth exchange results in the issuing of an access token to the client by the authorization server. In order to support AKA-based authentication, the authorization server shall be able to interact with S-5.
- Resource server

  The resource server serves the client's request when it is accompanied by a valid access token. Two types of procedures for getting access to a resource with the use of access tokens are specified; bearer tokens are specified in [b-IETF RFC 6750] and IETF is currently working on the specification for MAC tokens. The resource server may or may not be collocated with the authorization server in A-2.

The high level of OAuth information flows for a web-server use case (described in Appendix I) are depicted by Figure 3 below, with a description underneath.

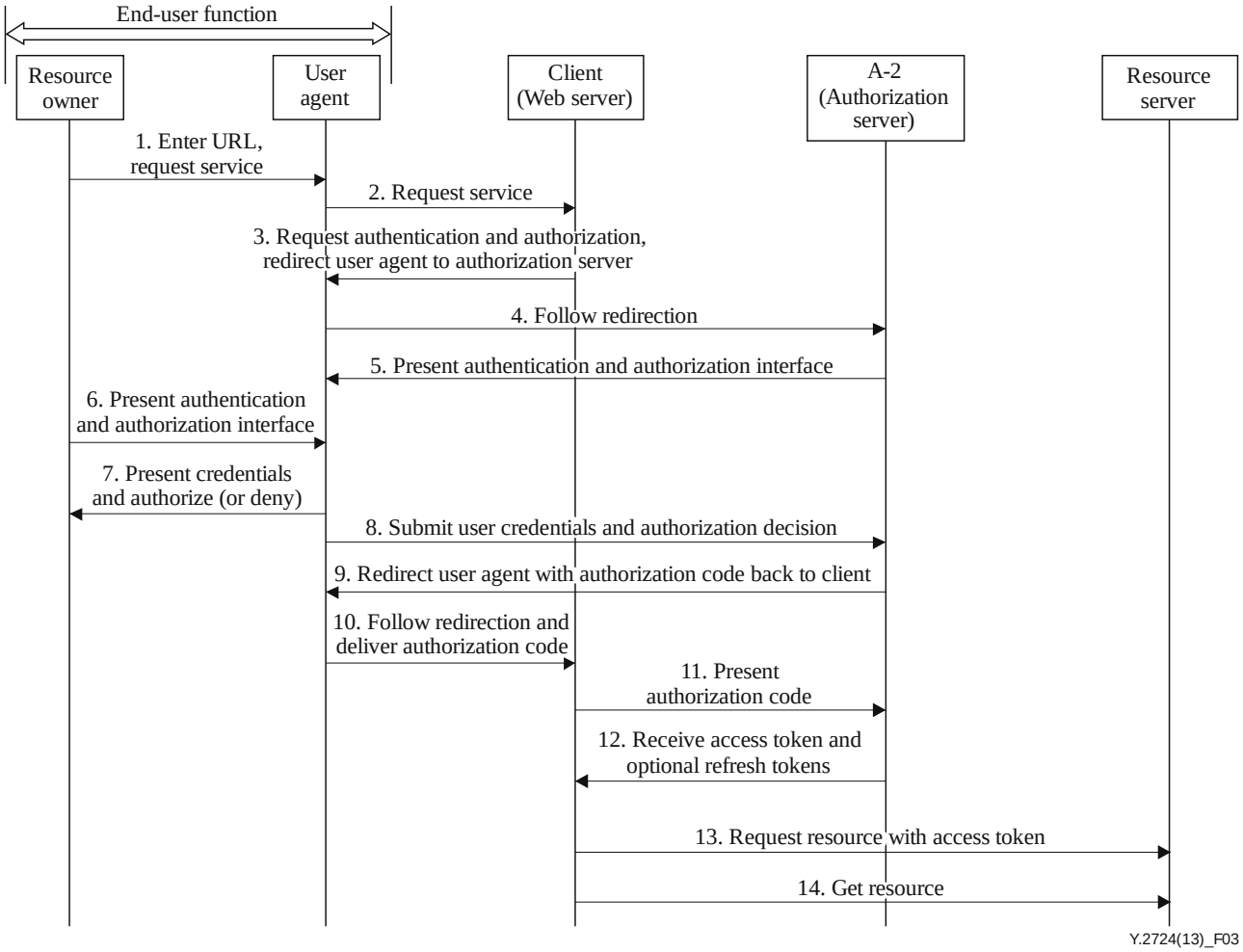

Figure 3 – OAuth flow for a web-server use case

1. The user directs the user agent (e.g., browser) to request a service from the client.
2. The user agent submits a request to the client.
3. The client forms a response and redirects the user agent to the authorization server for user authentication and authorization of the client's request.
4. The user agent follows the redirection.
5. The authorization server responds by providing the authentication and authorization interface to the user agent.
6. The user agent displays the authentication and authorization interface to the user (resource owner).
7. The user provides authentication credentials and indicates the authorization decision through the user agent.
8. The user agent sends the user-provided data to the authorization server.
9. The authorization server, after authenticating the user and ensuring that the user has authorized the client's request, redirects the user agent back to the client. The response includes the authorization code.
10. The user agent, following the redirection, delivers the authorization code to the client.
11. The client sends the authorization code to the authorization server.
12. The authorization server responds with an access token with the optional refresh tokens.

13. The client sends a request to the resource server and presents an access token.

14. The resource server provides the requested resource.

6.2.4 Entities that are specific to the OpenID flow

The OpenID-specific entities are the following:

- An application server that relies on authentication performed by the OpenID IdP.
- An OpenID IdP implemented as a part of A-2. In order to support AKA-based authentication, this entity shall be able to interact with S-5.
- An S-5 which is involved in OpenID authentication if the NGN performs the AKA-based authentication of the end-user function as specified in [ITU-T Y.2722].

The OpenID information flows are depicted by Figure 4 and described underneath. The text and figure describe the OpenID procedure for the case when the IdP and the application server have established a shared secret. The secret is used for signing a message with the authentication result by the IdP and for verifying it by the application server.

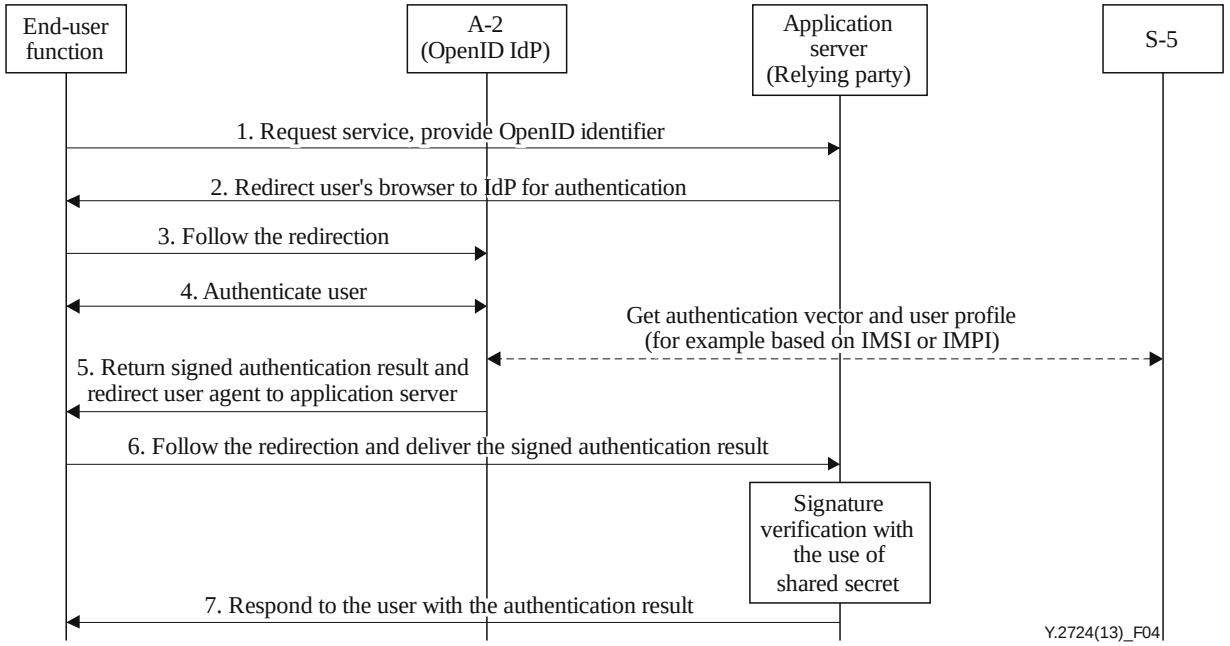

Figure 4 – OpenID flow

1. The user's browser sends a request for a service to an application server; the request contains the user OpenID identifier.
2. Based on the OpenID identifier, the application server discovers the user's OpenID IdP. Then the application server redirects the user browser for authentication to the OpenID IdP.
3. The browser follows the redirection request.
4. The OpenID IdP authenticates the user by exchanging information via the user browser.
5. If the OpenID IdP performs an AKA-based authentication (e.g., as described in [ITU-T Y.2722]), it needs to interact with S-5. Such interactions are denoted by a dashed arrow.
6. The OpenID IdP redirects the user browser back to the application server with a response containing a signed message with the authentication result.
7. The browser follows the redirection request and delivers the signed message to the application server.

8. The application server, after validating the signature and checking the authentication result, notifies the user whether the authentication was successful. The signing and validation procedures are specified in [b-OpenID v.2].

Appendix I

Selected use cases

(This appendix does not form an integral part of this Recommendation.)

I.1 Use case: web server

Description

Alice accesses an application running on a web server at www.X-printphotos.example and instructs it to print her photographs that are stored on a server www.X-storephotos.example. Alice has a subscription with her NGN service provider that runs an OAuth authorization server at www.X-carrier.example. The application at www.X-printphotos.example receives Alice's authorization for accessing her photographs without learning her authentication credentials with www.X-storephotos.example or www.X-carrier.example.

Pre-conditions

- Alice has registered with www.X-carrier.example to enable authentication.
- The application at www.X-printphotos.example has established the authentication credentials with the OAuth authorization server at www.X-carrier.example.
- The application at www.X-storephotos.example is capable of validating the access token issued by the authorization server at www.X-carrier.example.

Post-conditions

A successful procedure results in the application www.X-printphotos.example receiving an authorization code from www.X-carrier.example. The code is bound to the application at www.X-printphotos.example and to the callback URL supplied by the application. The application at www.X-printphotos.example uses the authorization code for obtaining an access token from www.X-carrier.example. The application at www.X-carrier.example issues an access token after authenticating the application at www.X-printphotos.example and validating the authorization code that it has submitted. The application at www.X-printphotos.example uses the access token for getting access to Alice's photographs at www.X-storephotos.example.

NOTE – When an access token expires, the service at www.X-printphotos.example needs to repeat the OAuth procedure for getting Alice's authorization to access her photographs at www.X-storephotos.example. Alternatively, if Alice wants to grant the application a long-lasting access to her resources at www.X-storephotos.example, the authorization server at www.X-carrier.example may issue the long-living tokens. Those tokens can be exchanged for short-living access tokens required to access www.X-storephotos.example.

Requirements

- The server www.X-printphotos.example, which hosts an OAuth client, must be capable of issuing the HTTP redirect requests to Alice's user agent – a browser.
- The authorization server at www.X-carrier.example must be able to authenticate Alice. The authentication method is not in the OAuth's scope.
- The application at www.X-carrier.example must obtain Alice's authorization for the access to her photos by www.X-printphotos.example.
- Application at www.X-carrier.example may identify to Alice the scope of access that www.X-printphotos.example has requested when asking for Alice's authorization.

- The authorization server at www.X-carrier.example must be able to authenticate the application at www.X-printphotos.example and validate the authorization code before issuing an access token. The application at www.X-printphotos.example must provide a callback URL to the authorization server at www.X-carrier.example (NOTE – URL should be pre-registered with www.X-carrier.example).
- The authorization server at www.X-carrier.example is required to maintain a record that associates the authorization code with the application at www.X-printphotos.example and the callback URL provided by the application.
- The access tokens are the bearer's tokens (they are not associated with a specific application, such as www.X-printphotos.example) and should have a short lifespan.
- The authorization server at www.X-carrier.example must invalidate the authorization code after its first use.
- Alice's manual involvement in the OAuth authorization procedure (e.g., entering a URL or a password) should not be required. (Alice's authentication to www.X-carrier.example is not in the OAuth's scope).

I.2 Use case: client credentials

Description

The company Good-X-Pay prepares the employee payrolls for the company Good-X-Work. In order to do this, the application at www.Good-X-Pay.example gets authenticated access to the employees' attendance data stored at www.Good-X-Work.example. Authentication is performed by the authorization server, which is a part of an NGN with the URL www.X-carrier.example.

Pre-conditions

- The application at www.Good-X-Pay.example has established through registration an identifier and a shared secret with the authorization server at www.X-carrier.example.
- The scope of the access by the application at www.Good-X-Pay.example to the data stored at www.Good-X-Work.example has been defined.

Post-conditions

A successful procedure results in the application at www.Good-X-Pay.example receiving an access token after authenticating to the authorization server at www.X-carrier.example. The application at www.Good-X-Pay.example then uses the access token to get access to the attendance data at www.Good-X-Work.example.

Requirements

- Authentication of the application at www.Good-X-Pay.example to the authorization server at www.X-carrier.example is required.
- The authentication method must be based on an identifier and a shared secret, which the application running at www.Good-X-Pay.example submits to the authorization server at www.X-carrier.example in the initial HTTP request.
- Because the procedure results in access to Good-X-Work's sensitive data, Good-X-Work shall establish trust with Good-X-Pay and the authorization server at www.X-carrier.example.

I.3 Use case: assertion

Description

Company Good-X-Pay prepares the employee payrolls for the company Good-X-Work. In order to do that, the application at www.Good-X-Pay.example gets authenticated access to the employees' attendance data stored at www.Good-X-Work.example. The server www.Good-X-Work.example grants access to the application at www.Good-X-Pay.example upon receiving an access token issued by the authorization server www.X-carrier.example.The authorization server www.X-carrier.example authenticates the application at www.Good-X-Pay.example through validating an assertion that www.Good-X-Pay.example has presented.

This use case describes an alternative solution to the one described by the use case "client credentials".

Pre-conditions

- The application at www.Good-X-Pay.example has obtained an authentication assertion from a party that is trusted by the authorization server www.X-carrier.example.
- The scope of the access by the application at www.Good-X-Pay.example to the data stored at www.Good-X-Work.example has been defined.
- The authorization server www.X-carrier.example has established a trust relationship with the asserting party and is capable of validating its assertions.

Post-conditions

A successful procedure results in the application at www.Good-X-Pay.example receiving an access token after authenticating to the authorization server at www.X-carrier.example by presenting an assertion (e.g., SAML assertion). It gets access to the employees' attendance data using the access token

Requirements

- Authentication of the application at www.Good-X-Pay.example to the authorization server www.X-carrier.example is required.
- The authorization server www.X-carrier.example must be capable of validating assertions issued by the asserting party and presented by the application running at www.Good-X-Pay.example.
- Good-X-Work shall establish trust with Good-X-Pay and the authorization server www.X-carrier.example.

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-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks.*

[b-IETF RFC 6750] IETF RFC 6750, *The OAuth 2.0 Authorization Framework: Bearer Token Usage*.

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

[b-3GPP TS 33.220] 3GPP TS 33.220 (2013) *Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture, Release 12*.

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