FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/FDIS 20078-3

ISO/TC **22**/SC **31**

Secretariat: DIN

Voting begins on:
2021-08-23

Voting terminates on:
2021-10-18

Road vehicles — Extended vehicle (ExVe) web services —

Part 3: Security

Véhicules routiers — Web services du véhicule étendu (ExVe) —

Partie 3: Sécurité

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/FDIS 20078-3:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*.

This second edition cancels and replaces the first edition (ISO 20078-3:2019), which has been technically revised.

The main changes compared to the previous edition are as follows:

— defined authorization domains for the offering party and the accessing party;

— added new requirements and description related to push method to make the offering party authorized to push resources to the accessing party;

— added Annex B containing description of reference implementation for push.

A list of all parts in the ISO 20078 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Road vehicles — Extended vehicle (ExVe) web services —

Part 3:
Security

1 Scope

This document defines how to authenticate users and accessing parties on a web-services interface. It also defines how a resource owner can delegate access to its resources to an accessing party. Within this context, this document also defines the necessary roles and required separation of duties between these in order to fulfil requirements stated on security, data privacy and data protection.

All conditions and dependencies of the roles are defined towards a reference implementation using OAuth 2.0[1] compatible framework and OpenID Connect 1.0[2] compatible framework.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 20078-1, *Road vehicles — Extended vehicle (ExVe) web services — Content and definitions*

3 Terms and definitions

For the purposes of this document, the convention, terms and definitions given in ISO 20078-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
identity token
ID token
digitally signed JWT and contains *claims* (3.3) about the authenticated resource owner

3.2
authorization code
intermediate result of a successful resource-owner authorization process and that is used by authorized clients to obtain access tokens and optionally refresh tokens

3.3
claim
asserted information about a certain entity

EXAMPLE ROID, resource owner's first name, last name, address, connected vehicle's capability and/or other attributes.

3.4
token issuer
entity that generates and provides *identity tokens* (3.1), access tokens, and refresh tokens

3.5
authorization domain
domain of activity where an entity controls the authorization

Note 1 to entry: The offering party controls the authorization in the offering-party authorization domain and the accessing party controls the authorization in the accessing-party authorization domain.

Note 2 to entry: Due to the description of push communication in 5.2 there exists two different authorization providers. One at the side of the accessing party and one at the side of the offering party.

4 General

4.1 Processes

The following processes are specific to each offering party. The definition of these processes is not part of this document but shall be in place in order to apply this specification.

REQ_04_01_01	The process to register a resource owner at the identity provider shall be the responsibility of the offering party.

REQ_04_01_02	The process to register an accessing party at the authorization provider shall be the responsibility of the offering party.

REQ_04_01_03	The process to confirm the technical eligibility of connected vehicles and provision of their associated ExVe resources shall be the responsibility of the offering party.

REQ_04_01_04	The process to verify a resource owner's current and valid ownership of the concerned resource shall be the responsibility of the offering party.

REQ_04_01_05	The process to register the offering party in the accessing party authorization domain shall be the responsibility of the accessing party. This is only needed if resources shall be pushed.

4.2 Conditions

REQ_04_02_05	The offering party shall be able to restrict or deny the accessing party and/or the resource owner access to the offering party's web services and portals.

NOTE 1 This can be done, for example, to fulfil security and legislation requirements.

REQ_04_02_06	If the offering party revokes a granted registration of an accessing party, the offering party may delete all containers created by the accessing party, if containers are used.

NOTE 2 Revocation of the registration can be due to access violation or other misuse of the web services.

REQ_04_02_07	The accessing party shall be able to restrict or deny the offering party's ability to push resources.

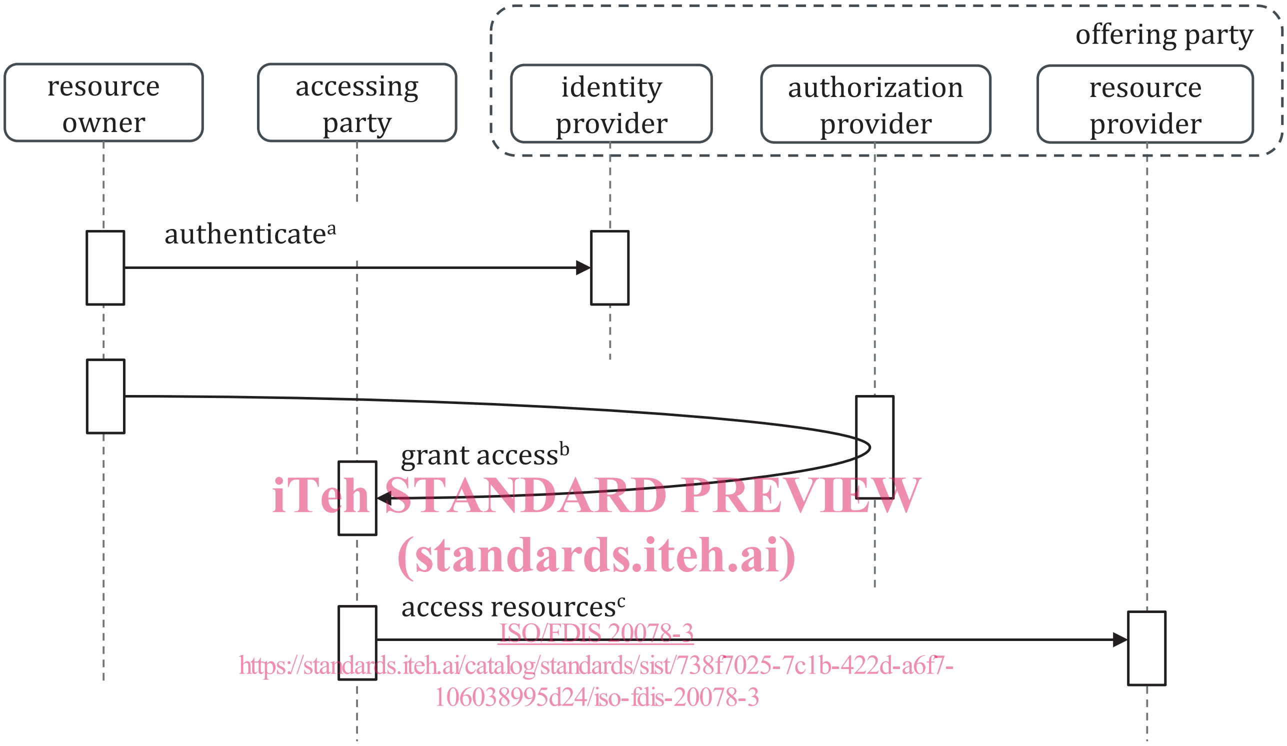
NOTE 3 This can be done, for example, to fulfil security and legislation requirements.

5 Basic communication flow

5.1 Offering party authorization domain

5.1.1 General

This document separates the activities necessary for authentication, authorization and resource access into three distinct communication flows with separate duties (see Figure 1).



[a] Step 1: the resource owner is authenticated by the identity provider.

[b] Step 2: the resource owner is granting access to the accessing party. The granting is handled by the authorization provider.

[c] Step 3: the accessing party is accessing resources from the resource provider.

Figure 1 — The roles and the three distinct communication flows

5.1.2 Authentication

The identity provider is responsible for authenticating the resource owner and managing the resource owner profile, based on the resource owner registration. The resource owner credentials are revealed only to the identity provider, and the identity provider confirms a successful authentication to concerned parties. If the resource owner has given consent, the accessing party will be authorized to access the resource owner's profile (Figure 2).

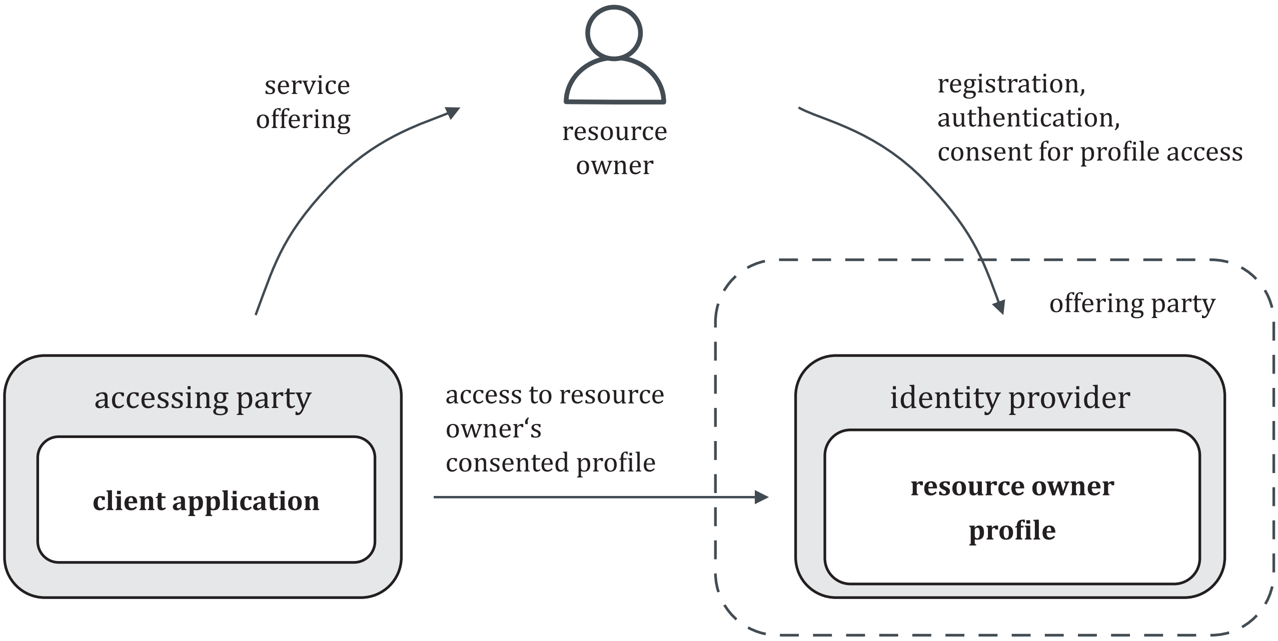


Figure 2 — Resource owner authentication and access to resource owner’s profile

REQ_05_01_01	The identity provider shall offer a suitable authentication method and shall perform the authentication process. After a successful authentication, the identity provider shall confirm the identity of the authenticated resource owner.

REQ_05_01_02	The resource owner’s credentials shall only need to be known by the resource owner and be possible to be verified by the identity provider.

REQ_05_01_03	The resource owner’s registration and authentication (at the identity provider), shall be separated from the authorization process to grant access to resources (via the authorization provider).

REQ_05_01_04	If the identity provider is able to expose the resource owner’s profile to the accessing party, it is only the resource owner that shall be able to grant or deny access.

5.1.3 Authorization

The client application as a component of the accessing party requires access to resources on behalf of the resource owner. At the authorization step, the accessing party requests authorization to access the resources provided by the resource provider (offering party). The required authorization is requested at the authorization provider, providing the intended scope. By the consent of the resource owner, the authorization provider returns a limited authorization to the client application of the accessing party. Using the obtained authorization, the client application can access resources. authorization to access resources is done in the same way regardless, if the resources are fetched by the accessing party using request/reply or pushed by the offering party (see Figure 3). See ISO 20078-2 for details regarding request/reply and push.

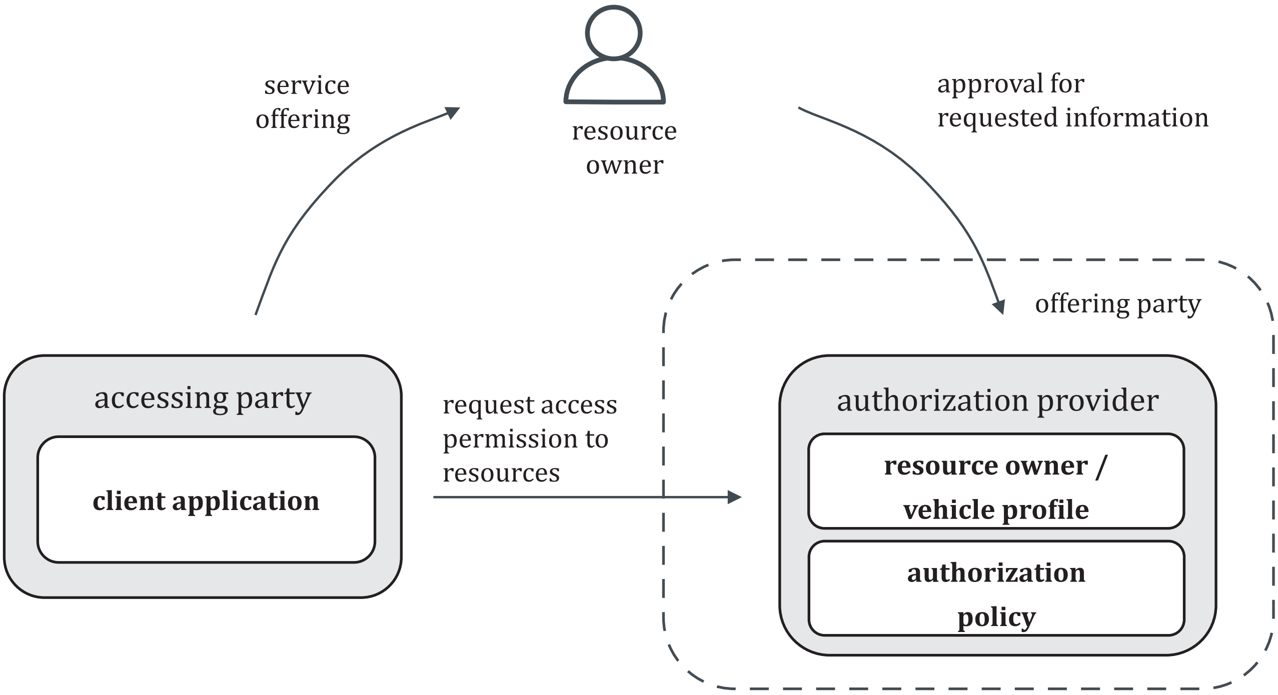


Figure 3 — Requesting access to resources

REQ_05_01_05	Before accessing the resource, the accessing party shall request access at the authorization provider providing the intended scope.

REQ_05_01_06	The authorization provider shall be responsible for the management of the authorization policy and shall manage all granted accesses.

NOTE 1 The authorization policy, for example, defines the permissions of the accessing party, primarily the conditions to be met for granted access to resources.

REQ_05_01_07	The authorization provider shall trust the confirmation of successful authentication as provided by the identity provider.

REQ_05_01_08	The authorization policy shall be defined by the offering party concerning the authorization process.

REQ_05_01_09	The authorization provider shall be able to verify the relationship between resource owners and their resources.

REQ_05_01_10	Only the resource owner shall be able to grant access to a resource.

NOTE 2 The access is granted to an accessing party at the offering party.

REQ_05_01_11	Granting access to resources shall be done either directly or via containers. The offering party decides if one or both of the granting methods shall be provided to the accessing parties.

REQ_05_01_12	The resource owner shall be able to revoke a granted access to a resource at any time.

REQ_05_01_13	If containers are used, the resource owner shall be able to revoke a granted access to a containers at any time.

REQ_05_01_14	The authorization provider shall ask the resource owner for the approval before providing the authorization to the accessing party resulting in a granted access.

REQ_05_01_15	Upon request the offering party shall present a resource owner's granted accesses to the resource owner.

REQ_05_01_16	The resource owner shall be able to deny an access request to a resource, or if containers are used, to a container at any time.

REQ_05_01_17	If the ownership of a resource or the relationship between the resource owner and the resource ends, access to the corresponding resources, and if containers are used, also to containers, shall be revoked.

REQ_05_01_18	If containers are used and if a container is deleted, all access granted to that container shall be revoked.

5.1.4 Resource access

Using the access, the accessing party can access the resources, hosted by the resource provider (see Figure 4).

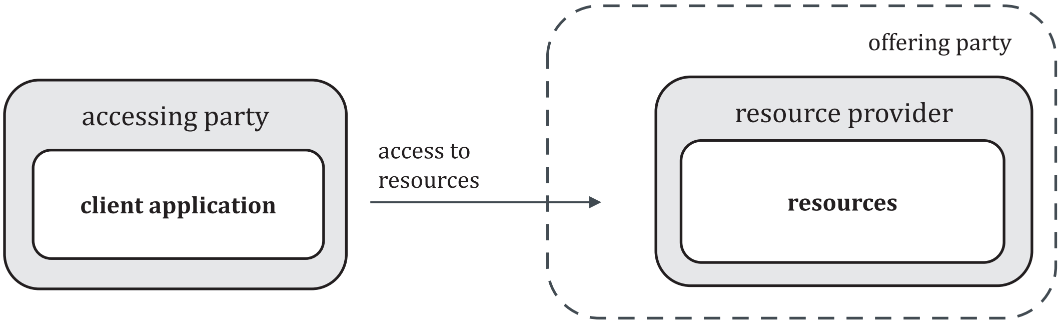


Figure 4 — Access to resources via the resource provider

REQ_05_01_19	The resource provider shall perform access control to the resources according to the authorization policy.

5.1.5 Separation of duties

Separation of duties concerns the separation of tasks and responsibilities between entities involved in the authentication, authorization and access to resources.

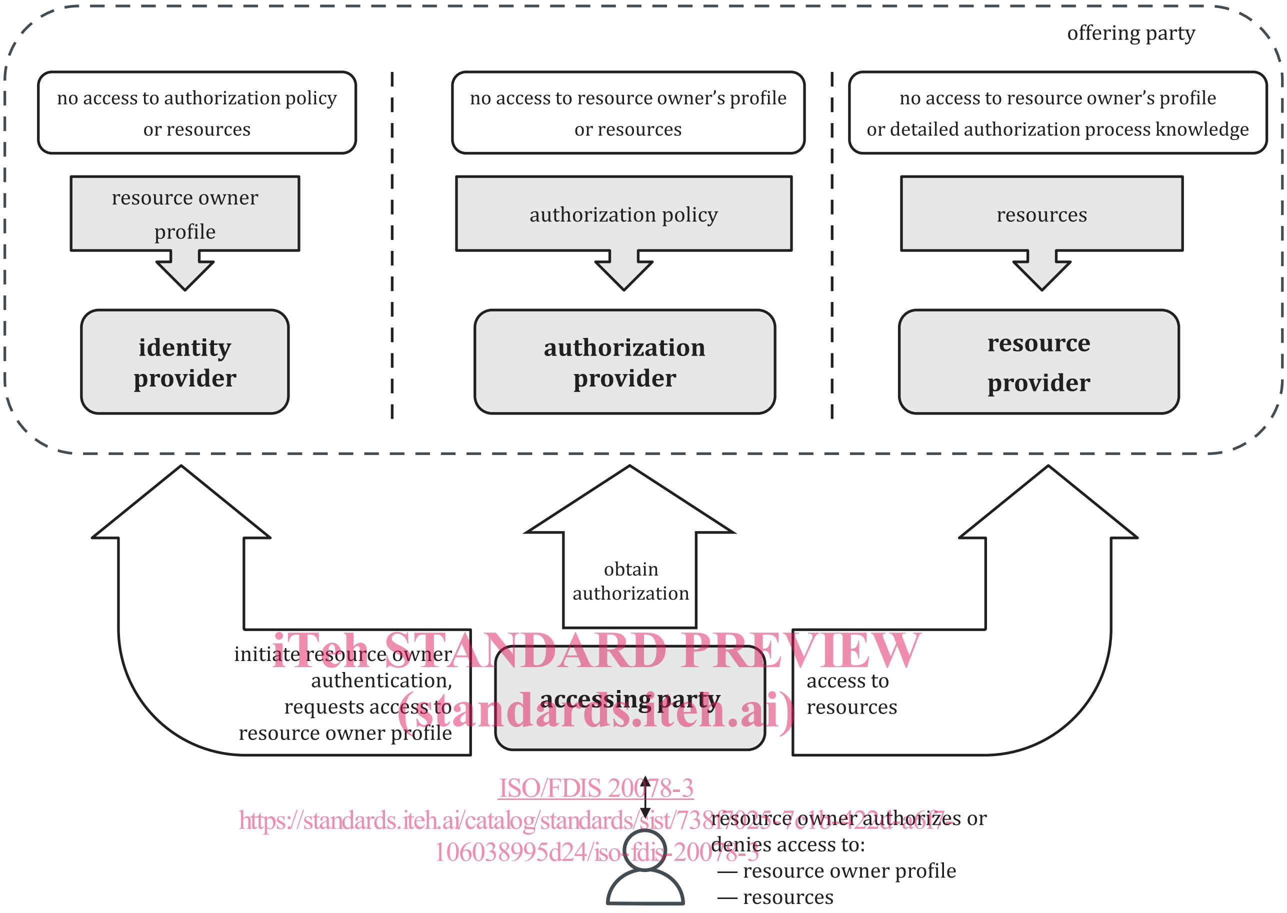

offering party
no access to authorization policy or resources
no access to resource owner’s profile or resources
no access to resource owner’s profile or detailed authorization process knowledge
resource owner profile
authorization policy
resources
identity provider
authorization provider
resource provider
obtain authorization
initiate resource owner authentication, requests access to resource owner profile
accessing party
access to resources
resource owner authorizes or denies access to:
— resource owner profile
— resources

Figure 5 — Separation of duties between involved roles

Figure 5 describes the separation of duties between involved roles, where the offering party has the three roles: identity provider, authorization provider, and resource provider.

REQ_05_01_20	The identity provider shall not be dependent on the authorization policy.

REQ_05_01_21	The identity provider shall not influence the authorization policy.

REQ_05_01_22	The identity provider shall not access the resources.

REQ_05_01_23	The authorization provider shall not access the resource owner profile.

REQ_05_01_24	The authorization provider shall only use the unique ResourceOwnerID to identify the resource owner.

NOTE 1 The ResourceOwnerID is generated and communicated by the trusted identity provider.

REQ_05_01_25	The authorization provider shall not have access to resources provided by the resource provider.

REQ_05_01_26	The resource provider shall not access the resource owner profile.

REQ_05_01_27	The resource provider shall not know details about the authorization process.

REQ_05_01_28	The resource provider trusts the authorization provider and shall verify whether the provided authorization matches the access control rules defined for the requested resources.

REQ_05_01_29	The resource owner shall not need to share credentials with the accessing party to enable the accessing party to access the resources.

REQ_05_01_30	The accessing party shall only access the resources with the consent of the resource owner.

NOTE 2 The requirements stated above do not impose requirements on specific architecture, design or organizational structure.

Figure 6 shows the major logical components of the involved roles and the associated entities.