INTERNATIONAL STANDARD

ISO 20078-1

Second edition
2021-11

Road vehicles — Extended vehicle (ExVe) web services —

Part 1: Content and definitions

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

Partie 1: Contenu et définitions

Reference number
ISO 20078-1:2021(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

Page

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 20078-1:2019), which has been technically revised.

The main changes are as follows:

— revised Clause 3 "Terms and definitions";

— removed the subclause “Key Value List” including related requirements, as it was not used in the ISO 20078 series;

— added new definitions for request/reply (3.2.10), push (3.2.12) and subscription profile (3.2.13);

— revised the subclause 9.4 "Containers".

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.

Introduction

This document was developed to address the needs of different parties to access data, aggregated information and functionalities (resources) from connected vehicles in a standardized, safe and secure way. A framework is defined for interoperable web services used by several parties via the internet by adapting current and widely used IT approaches based on OAuth 2.0 and OpenID Connect 1.0 (see ISO 20078-3).

As personal data protection rights are becoming stronger in several countries, this document also defines and recommends common methods to handle data protection and data privacy issues when accessing personalized vehicle data, information or functionalities via web services.

The ISO 20078 series is supported by the fact that vehicle manufacturers (VM) include telematics support for their vehicles, making vehicle data, information and functionalities available at their VM backend system. Thus, instead of installing additional third-party telematics equipment in the vehicle to achieve intended service goals, the already existing infrastructure can be (re)used via interoperable web services. Such web services allow a third party to (re)use the infrastructure in same manners as the VM uses it.

NOTE Web service interfaces have been available and have been offered by VMs previous to this document but lack of standardization over the VMs, especially on authentication and authorization, led to the fact that third parties accommodate and design for several different VM implementations.

The ISO 20078 series is applicable for any application or service that intends to use web services.

The ISO 20078 series does not cover requirements for specific applications, resource definitions or XML/JSON schemas. These are described in the specific application or use case; e.g. see ISO 20080 remote diagnostics support.

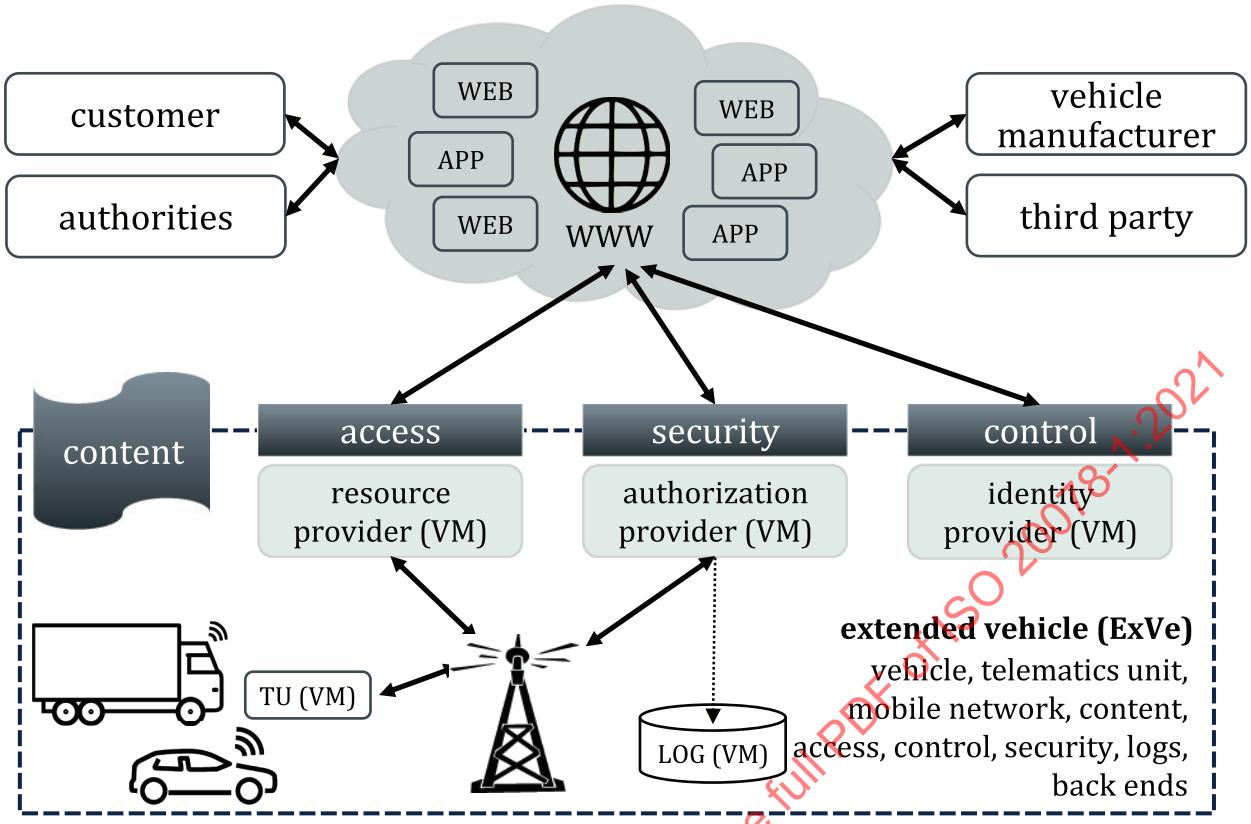
This document, ISO 20078-1, defines all entities and roles that are used over in the ISO 20078 series. It standardizes how an offering party defines resources. Depending on resource category, the offering party uses different kind of identifiers. Such resources can be exposed directly or through containers. It also describes different ways of representing resources in web services, such as JSON and XML.

ISO 20078-2 defines the usage of a common communication protocol that enables access to resources (URIs), thereby standardizing how an accessing party can access resources via web services of an offering party, using Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS); i.e. HTTP secure (HTTPS). The Representational State Transfer (REST) is selected for using a common way to represent data, aggregated information, and functions (resources).

ISO 20078-3 standardizes the security model of the web services, including different roles and entities involved in an authorization policy. Three roles are defined: identity provider, authorization provider and resource provider at the offering party. Additional roles are the accessing party and the resource owner. The resource owner is in charge of its resources. The role model is defined as a reference implementation of OAuth 2.0 and OpenID Connect 1.0 compatible frameworks.

ISO/TR 20078-4 summarizes this document, ISO 20078-2, and ISO 20078-3 by logical processes for displaying the interaction of all defined roles and entities[4]. The processes of registration, authentication, and authorization of an accessing party are determined by the requirements set by previous parts. The processes described include registration between the entities, granting, denying, ignoring and revoking access as well as container management possibilities.

In this document, entities are defined as the fundamental objects that represent, for example, vehicles, ECUs, drivers and fleets, and servers at an ExVe backend. Roles are defined as a grouping of entities and have relationships that allow for an interaction; e.g. the “offering party” (ExVe backend) offers resources (ECU data) to an “accessing party” (service implementer).



ISO 20078-1 Content
ISO 20078-2 Access
ISO 20078-3 Security
ISO/TR 20078-4 Control

TU — vehicle integrated telematics unit
LOG — records access, events, failures, and intrusions
APP and WEB — application and web services
Stakeholders — customer, authorities, VM, third party

Figure 1 — Schematic presentation of the vision of the ISO 20078 series

ExVe web services are comprised of road vehicles combined with the ExVe backend system of the vehicle manufacturer (the "offering party"), mainly acting as a resource provider. This enables for both a third party and a vehicle manufacturer, mainly acting as a service/application provider (the "accessing party") to access offered resources via the internet; see Figure 1.

The concept of containers is also introduced which allows resource grouping for a single accessing party purpose. Containers are a recommended solution where (data) privacy by design applies.

Logging (LOG of Figure 1) is an important part of any IT solution. It is, however, not considered within the scope of the ISO 20078 series due to potentially strong dependencies on certain IT backend infrastructures.

JSON (recommended) or XML are used for representation of resources (URIs).

The ISO 20078 series defines in general a framework based on the communication and authorization protocols listed in Table 1. Those technologies can be used for implementation of individual web services to share resources and, therefore, allow for any service or application implementation on the accessing party domain.

Table 1 — List of used information technologies

Transport protocol	HTTP 1.1 (or later version) over TLS 1.2 (or later version)
Service design	RESTful
Data format	JSON (recommended)
	XML
Authorization	An OAuth 2.0 (or later version) compatible framework
End user authentication	An OpenID Connect 1.0 (or later version) compatible framework

Road vehicles — Extended vehicle (ExVe) web services —

Part 1:
Content and definitions

1 Scope

This document states the minimum requirements, recommendations, permissions and possibilities for ensuring interoperable web services from an accessing party's perspective. The document:

— states requirements on the structure and format of resources;

— defines the concept of resource identifiers (direct and correlated);

— provides different resource categories (e.g. anonymous, pseudonymized, technical, and personal resources);

— provides different approaches on how to bundle shareable resources (e.g. resource group or container);

— contains guidelines on how to define the unique resources of an individual application;

— defines the entities and roles, necessary for granting an accessing party access to resource owner's resources;

— states requirements on how an accessing party accesses resources, including requirements on how to use the defined and referenced technologies, see Table 1.

See Annex A for additional information about roles and responsibilities covered by ISO 20078 series.

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 20078-3, *Road vehicles — Extended vehicle (ExVe) web services — Part 3: Security*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology 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 Roles and entities

3.1.1
vehicle manufacturer
VM
company manufacturing road vehicles

3.1.2
connected vehicle
road vehicle that is enabled for communication over a wide area network (WAN)

Note 1 to entry: A WAN can, for example, be defined as a nationwide mobile phone network with a corresponding backend (server) architecture.

3.1.3
offering party
OP
entity who provides web services *access* (3.2.6) to *resources* (3.2.1)

3.1.4
resource owner
RO
responsible party for the *resource(s)* (3.2.1)

Note 1 to entry: The resource owner is responsible for granting, denying, and revoking *access* (3.2.6) to resource(s).

Note 2 to entry: The responsible resource owner is determined by the concrete resource.

3.1.5
third party
person or body who is not the *vehicle manufacturer* (3.1.1) or the *resource owner* (3.1.4)

3.1.6
accessing party
AP
entity which accesses *resources* (3.2.1) via web services

Note 1 to entry: It is an entity other than the *offering party* (3.1.3) or the *resource owner* (3.1.4).

Note 2 to entry: Implements technically and independently an identity, authorization, and a *resource provider* (3.1.8)/*service provider* (3.1.10) that are not within the scope of this document.

Note 3 to entry: The resource provider and service provider can be split into two separate roles at the AP: resource provider and service provider strongly depend on the individually developed service.

3.1.7
identity provider
entity responsible for authentication (identification) of *resource owners* (3.1.4), through the use of credentials

Note 1 to entry: *Offering party* (3.1.3) confirms the identity of the authenticated resource owner.

Note 2 to entry: There is an identity provider technically mandatory at the offering party, but that identity provider may reference services exposed by an intermediate body when confirming the identity of a resource owner in general for some use cases.

3.1.8
resource provider
entity at the *offering party* (3.1.3) that protects and provides *resources* (3.2.1)

3.1.9
authorization provider
entity at the *offering party* (3.1.3) that manages the *access* (3.2.6) rights to *resources* (3.2.1) and *resource owner* (3.1.4) information

Note 1 to entry: There is an authorization provider technically mandatory at the offering party, but that authorization provider may reference services exposed by an intermediate body when enforcing the *authorization policy* (3.2.7) in general for some use cases.

3.1.10
service provider
vehicle manufacturer (3.1.1) or a *third party* (3.1.5), providing a service to the vehicle owner based on the *access* (3.2.6) to vehicle data and functionalities

3.2 Technical concepts and terms

3.2.1
resource
data, aggregated information or functionalities of the *connected vehicle* (3.1.2)

Note 1 to entry: resources can be:

— resources (by a RID),

— references to resources,

— resource-related notifications,

— *resource owner* (3.1.4) information (by a ResourceOwnerID),

— resource and resource owner related information,

— anonymous resources,

— pseudonymized resources,

— vehicle related resources, or

— personal resources,

at the *offering party* (3.1.3).

3.2.2
resource group
logical set of *resources* (3.2.1)

3.2.3
superset
set of all unique *resources* (3.2.1)

3.2.4
container
logical group of *resources* (3.2.1) defined for a single *accessing party* (3.1.6) purpose

3.2.5
resource owner profile
information regarding the *resource owner* (3.1.4)

EXAMPLE Name, address, contact information, and RID.

3.2.6
access
delegated right to an *accessing party* (3.1.6) to access a *resource owner's* (3.1.4) *resources* (3.2.1)

3.2.7
authorization policy
set of rules that define access control to protected *resources* (3.2.1)

3.2.8
token
sequence of characters representing a verified identity and/or *access* (3.2.6)

Note 1 to entry: The issuer of the token is responsible for the interpretation and the integrity of the token; for example, the *authorization provider* (3.1.9) of the *offering party* (3.1.3) or in a second example an intermediate body for the authorization provider of the offering party.

Note 2 to entry: The token is used for securely transmitting verifiable identity and/or authorization information between involved parties like *resource owner* (3.1.4), *accessing party* (3.1.6) and/or offering party.

3.2.9
fleet
group of *connected vehicles* (3.1.2) associated to a specific *resource owner* (3.1.4)

3.2.10
request/reply
communication method, where the *accessing party* (3.1.6) requests *resource(s)* (3.2.1) and the *offering party* (3.1.3) replies

3.2.11
subscription
accessing party (3.1.6) requests the *offering party* (3.1.3) to *push* (3.2.12) *resources* (3.2.1) when certain conditions are fulfilled

Note 1 to entry: A condition can be a vehicle event, such as a DTC becoming active, or based on a time interval.

3.2.12
push
method used by the *offering party* (3.1.3) to send *resource(s)* (3.2.1) to the *accessing party* (3.1.6) according to the *subscription* (3.2.11)

Note 1 to entry: Instead of sending the resource, a reference to the resource can be sent, i.e. a notification. The accessing party can use the reference to request the resource(s).

3.2.13
subscription profile
URI locations and authorization information making it possible to *push* (3.2.12) *resources* (3.2.1) to the *accessing party* (3.1.6)

3.2.14
access token
AT
credentials used to access protected resources, issued by the *identity provider* (3.1.7) or *authorization provider* (3.1.9) and consumed by the *resource provider* (3.1.8)

Note 1 to entry: An access token represents an authorization that is issued to the client and limited by scope and has a defined expiration time in unix time format (seconds).

Note 2 to entry: An access token may be a digitally signed JWT.

3.2.15
refresh token
RT
credential (string) issued to the client by the *identity provider* (3.1.7) or the *authorization provider* (3.1.9) and used to obtain a new *access token* (3.2.14) when the currently used AT expires, or to obtain additional ATs depending on the intended scope of use

3.2.16
bearer token
token (3.2.8) which can be used to get *access* (3.2.6) to *resource(s)* (3.2.1)

Note 1 to entry: Usage of bearer tokens is defined in RFC 6750[10].

3.3 Identifiers

3.3.1
identifier
ID
number or a string that is unique within a defined context

Note 1 to entry: A UUID[7] can be used as an ID.

3.3.2
universally unique identifier
UUID
128-bit value generated in accordance with ISO/IEC 9834-8 and providing unique values between systems and over time

Note 1 to entry: See Reference [7]. Often represented as a string in hex format, e.g. f81d4fae-7dec-11d0-a765–00a0c91e6bf6.

3.3.3
ResourceID
RID
ID that identifies a unique *resource* (3.2.1) at the *offering party* (3.1.3)

3.3.4
ContainerID
CID
ID that identifies a unique *container* (3.2.4) at the *offering party* (3.1.3)

3.3.5
AccessingPartyID
APID
ID that identifies a unique *accessing party* (3.1.6) at the *offering party* (3.1.3)

3.3.6
CorrelationID
CoID
ID agreed between the *offering party* (3.1.3) and the *accessing party* (3.1.6) to support pseudonymization of the RIDs or the *resourceOwnerIDs* (3.3.8)

Note 1 to entry: The definition includes two pseudonymization examples.

3.3.7
SubscriptionID
ID uniquely identifying a *subscription* (3.2.11) at an *offering party* (3.1.3)

3.3.8
ResourceOwnerID
ID that identifies a unique *resource owner* (3.1.4)

3.3.9
VehicleID
ID that identifies uniquely a vehicle (e.g. VIN)

Note 1 to entry: VIN is defined in ISO 3779.

3.4 Credentials

3.4.1
ResourceOwnerCredentials
ROC
credentials shared from a party to the *resource owner* (3.1.4)

3.4.2
ResourceOwnerCredentialsOP
ROCOP
credentials shared from the *offering party* (3.1.3) to the *resource owner* (3.1.4)

3.4.3
ResourceOwnerCredentialsAP
ROCAP
credentials shared from the *accessing party* (3.1.6) to the *resource owner* (3.1.4)

3.4.4
AccessingPartyCredentials
APC
credentials shared from the *offering party* (3.1.3) to the *accessing party* (3.1.6)

4 Abbreviated terms

AP	Accessing Party
APC	Accessing Party Credentials
API	Application Programming Interface
APID	Accessing Party ID
AT	Access Token
ROC	Resource Owner Credentials
CID	Container ID
CoID	Correlation ID
ExVe	Extended Vehicle
GSM	Global System for Mobile Communication
HATEOAS	Hypermedia As The Engine Of Application State
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
JSON	JavaScript Object Notation
JWS	JSON Web Signature (signed JWT)
JWT	JSON Web Token
OAuth	Open standard for authorization

OBD	On-Board Diagnostics
OIDC	OpenID Connect
OP	Offering Party
OSI	Open System Interconnection
REST	Representational State Transfer
RID	ResourceID
ROC	Credentials of a Resource Owner
ROCAP	ROC of the Accessing Party
ROCOP	ROC of the Offering Party
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
VIN	Vehicle Identification Number
VM	Vehicle Manufacturer
XML	Extensible Mark-up Language

5 Convention

In this document, requirements, recommendations, permissions and possibilities are formalized as follows:

REQ_NUM	Text of the requirement, recommendation, permission or possibility

NUM: reference of the requirement, recommendation, permission or possibility in which:

— REQ the acronym stands for requirement, recommendation, permission, or the possibility,

— NUM is a reference split in 00_00_00 and 99_99_99 denoting section by increasing each number between 01 and 99. NUM manifests like: XX_YY_ZZ.

EXAMPLE REQ_04_01_01 and REQ_04_02_01 are different denoting different sections and REQ_04_01_01 and REQ_04_01_02 are different denoting different counting.

A requirement, recommendation, permission, or possibility can be introduced beforehand by an explanatory text. The ISO convention about verbs (shall, should, may, or can) denotes the type.

6 Relationship of defined entities

6.1 Overview of entities

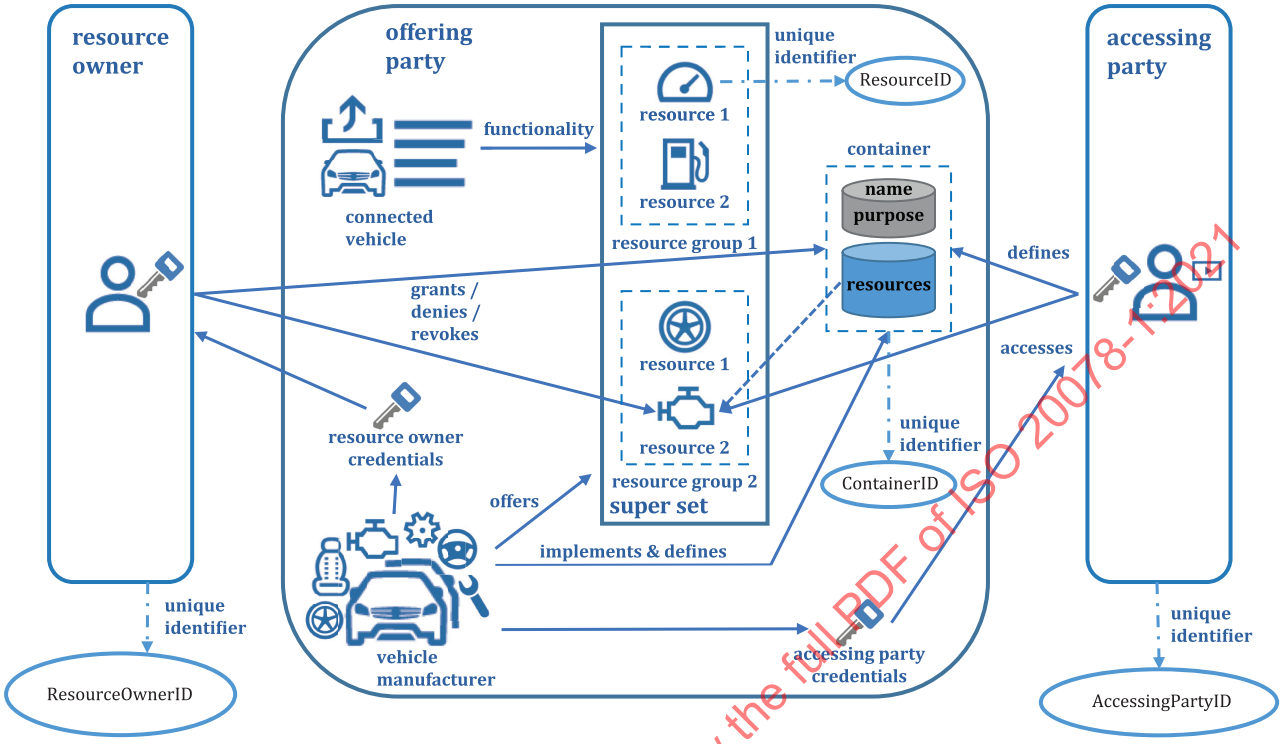


Figure 2 — Overview of defined entities and their overall roles

Figure 2 identifies the relationship of defined entities and their overall roles in providing and granting an access to resources.

6.2 Roles and relationships of entities

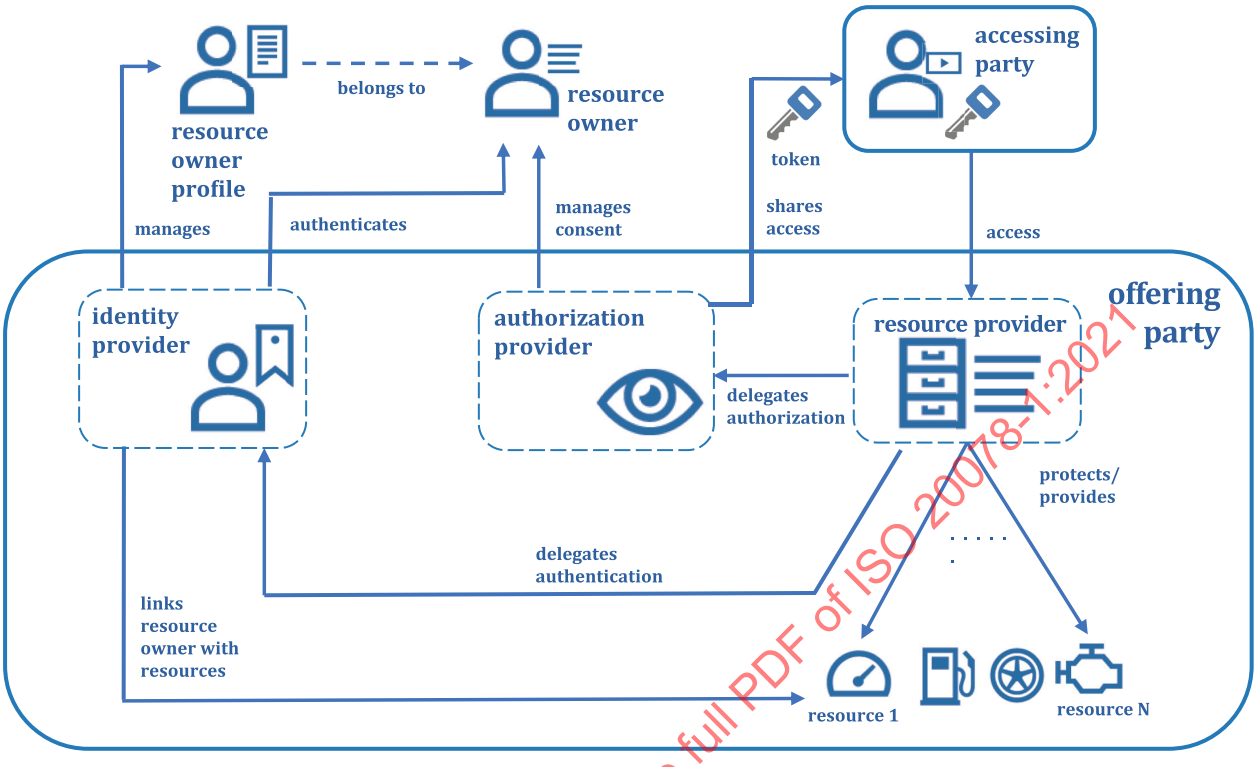


Figure 3 — Roles and their relationship to entities

Figure 3 describes roles and their relationship to entities required for granting an accessing party access to a resource owner's resources.

NOTE 1 Each role can be implemented by the VM or other parties (e.g. IT web developers, contractor agencies, or third-party software developers).

NOTE 2 When the implementation is performed by other parties, the VM can remain responsible for data, data management, and data processing, subject to different national data protection legislations.

7 Identifiers

7.1 General

Identifiers are used to uniquely identify a specific resource or a party and are typically allocated by the offering party. Some identifiers are publicly known, whereas some are only shared between two parties.

7.2 Direct identifiers

REQ_07_02_01	A direct identifier shall uniquely identify a resource at the offering party.

NOTE 1 A direct identifier can be the VIN of a road vehicle or the ResourceID of a resource.

NOTE 2 A direct identifier is typically used by many accessing parties and can thereby be seen as public.

EXAMPLE WDB1240211B783045, a vehicle identification number (VIN); see ISO 3779.

7.3 Correlation identifiers

REQ_07_03_01	A correlation identifier (CorrelationID) shall identify a resource (URI) or a container at the offering party and the translation to a direct identifier shall only be known by the concerned parties.

NOTE Dependent on how a correlation identifier is used, it can give a higher level of (data) privacy by design.

EXAMPLE 848d8c29-c2e6–4a88–8069–8e4e37454814, a universally unique identifier (UUID) of version 4[7]. Such identifiers allow for an indirect identification between the accessing party and the offering party.

8 Resource categories

8.1 General

Resources associated with ExVe can be categorized into four different types.

8.2 Anonymous resources

Anonymous resources are resources, which can be shared publicly without disclosing any identity. These kind of resources are mainly used for ensuring mobility, for increasing traffic flow, or for enhanced road safety.

EXAMPLE Traffic sign recognition or local hazard warnings, etc.

REQ_08_02_01	Access to anonymous resources shall not be matched against a specific resource of the offering party.

REQ_08_02_02	Access to anonymous resources may be performed by the simplified flow of ISO 20078-3:2021, Annex A, with consent of the offering party (acting as the resource owner).

8.3 Pseudonymized resources

Pseudonymized resources are resources, shared with pseudonyms, e.g. the CorrelationID. These kind of resources are mainly shared to make multi-brand services available.

EXAMPLE Remote field studies of, for example, gearboxes from component suppliers.

REQ_08_03_01	Access to pseudonymized resources shall only be matched against a specific resource at the offering party.

Such access ensures that a specific resource can be only matched at the presentation layer of the web service by the offering party. At the accessing party a pseudonymized resource is similar to an anonymous resource; see 8.2.

The main difference between anonymized and pseudonymized resources is that latter resources from the same source cannot be correlated at the accessing party.

The main advantage of pseudonymized resources is that in case of a data breach at the accessing party the real identities of resources, e.g. VIN or chassis, are not disclosed.

REQ_08_03_02	Access to pseudonymized resources shall not be matched against a specific resource at the accessing party.

NOTE See ISO 20078-3:2021, A.3.1 or A.3.2, as a recommendation.

REQ_08_03_03	Access to pseudonymized resources shall require consent of the resource owner at the offering party and may follow the reference implementation of ISO 20078-3:2021, Annex A.

A revoked consent or a denied consent for the same resources and the same parties shall be established separately by a new consent-based flow in accordance with ISO 20078-3, if the access to the pseudonymized resource was initially based on a consent-based flow.

REQ_08_03_04	In case of consent-based access on pseudonymized resources and a revocation or a denial of the resource owner, the consent-based flow of ISO 20078-3 may be newly initiated; this implies that consent-based flow shall be independent of any causality.

8.4 Technical (vehicle) resources

Technical or technical vehicle resources are non-personal resources which are considered as non-personal data of the resource owner.

EXAMPLE 1 Number of axles, vehicle colour, number of seats, etc.

The vehicle manufacturer is considered as resource owner for technical resources. Therefore, in some cases the VM can be the offering party as well as the resource owner for the same technical resource.

REQ_08_04_01	Access on technical (vehicle) resources shall be matched against a specific resource at the offering party.

Such access ensures that a specific resource can be matched by the offering party, e.g. by vehicle identification number (VIN) or pseudonymized ID.

REQ_08_04_02	Access on technical (vehicle) resources may be performed by the simplified flow of ISO 20078-3:2021, Annex A, with consent of the offering party (as resource owner).

8.5 Personal resources

Personal resources are those resources which are considered as personal data of the resource owner. Those include the resources associated with the resource owner.

EXAMPLE 1 VIN, RID, address, etc.

To maintain resource integrity and security, the offering party may share this kind of resources as pseudonymized resources (see 8.3), by generating a CorrelationID for each resource, and sharing this CorrelationID with the accessing party. Otherwise, the access to personal resources can be done using direct IDs. Both shall have the consent of the resource owner to guarantee (data) privacy by design.

REQ_08_05_01	Access to personal resources shall be verified at the offering party.

REQ_08_05_02	A CorrelationID may be generated for a personal resource at the offering party and shared with the accessing party.

EXAMPLE 2 A random number or a UUID that refers to the RID or the VIN number of the road vehicle.

REQ_08_05_03	Access on personal resources shall require consent of the resource owner at the offering party.

NOTE See reference implementation in ISO 20078-3:2021, 4.3.

REQ_08_05_04	In case of revocation (or denial) of the consent of the resource owner, the CorrelationID shall be immediately withdrawn. This implies that no access of accessing party is possible until consent is given by a new consent flow.

A revoked or denied consent by the resource owner cannot be re-established other than by a new consent-based flow (ISO 20078-3).

9 Resources

9.1 Superset of resources

REQ_09_01_01	The offering party shall define the superset consisting of its available resources.

NOTE 1 The actual availability of a resource can depend on vehicle model, vehicle generation, vehicle model year, and the optional equipment or — in general — the (activated) vehicle services, etc.

REQ_09_01_02	The offering party shall provide one of two optional concepts: resources or containers.

NOTE 2 Containers and resource groups are technically identical; see Clause 10 representation.

NOTE 3 Containers group resources and define a purpose of data processing; see 9.2, 9.3, and 9.4.

REQ_09_01_03	The offering party decides how available resources shall be displayed towards accessing parties. This could be done using resources, resource groups or containers.

9.2 Resource groups

REQ_09_02_01	Resource groups may be defined as sub sets of the superset by the offering party.

A resource group can be any possible grouping of resources and is defined by the offering party. It could be, for example, a group of functionally related resources.

REQ_09_02_02	Resources may be shared across multiple resource groups.

9.3 Resource

A resource is named and extended by any other information.

EXAMPLE 1 The resource is extended by a brief description to allow more transparency to the resource owner while granting.

REQ_09_03_01	A resource shall consist of data, aggregated information or functionality associated to a connected vehicle.

NOTE 1 A resource can be extended; e.g. by a unique brief description.

REQ_09_03_02	Data shall be defined by the offering party.

REQ_09_03_03	Aggregated information shall be defined by the offering party and shall consist of data structures and/or processed data.

NOTE 2 An aggregated information can be self-descriptive.

REQ_09_03_04	Functionality shall be defined by the offering party and shall consist of a well-defined interaction with the connected vehicle.

EXAMPLE 2 Parameterizing a resource or changing the state of a resource, can be triggered by selecting or sending a parameter by the accessing party.

9.4 Containers

9.4.1 Container

A container is a selection of resources (see 9.3). The accessing party or the offering party define a container. A container has a name, a list of resources, and the purpose of resource processing, making it possible for the resource owner to understand the implication of the given consent.

Containers are typically configured by the accessing party by means of a container management API or in a web portal provided by the offering party. Due to the explicit granting of access to resources grouped by the containers, the purpose of the container can only be specified at container creation.

EXAMPLE 1 The creation of a container may be achieved by a web-based portal where the accessing party logs in with its own credentials and individually selects resources of the superset offered by the offering party, adds a name and a purpose of resource processing.

REQ_09_04_01	The offering party may offer the possibility to use containers to accessing parties.

REQ_09_04_02	A container shall consist of a set of resources that are selected from the superset and may be from different resource groups.

NOTE 1 The use of the concept “containers” can help to comply with some regional legal requirements due to its (data) privacy by design.

REQ_09_04_03	The container shall have an ID (ContainerID), a name and a purpose.

NOTE 2 The container could have additional items, e.g. a brief use case description.

REQ_09_04_04	The ContainerID shall uniquely identify a container at the offering party.

NOTE 3 For the ContainerID a UUID[7] can be used.

REQ_09_04_05	Containers may be defined by the accessing party or the offering party.

NOTE 4 The accessing party can use a web portal operated by the offering party or can use an individually defined process operated by the offering party to define a container.

NOTE 5 The offering party can also predefine containers for foreseeable use cases that can be used by accessing parties.

REQ_09_04_06	The offering party can reject the creation or delete a container if the included resources and purpose of data processing do not match.

NOTE 6 The purpose of data processing is normally publicized by the service conditions of the accessing party, due to several national data protection laws.

REQ_09_04_07	The accessing party shall have access to individual resources (URIs; end points) of a container.

NOTE 7 It is not necessary to get all resources of a container with every access. For convenience the offering party can provide a container end point (URI) where a combined data set can be retrieved.

EXAMPLE 2 The resource owner has granted access for resources defined by a container that consists of resource A and resource B; the accessing party can access the resources A and B (separate URIs). The offering party can additionally offer a container end point to retrieve the combined data set A + B (one URI).

REQ_09_04_08	Vehicles can be connected to a container by the accessing party also before access is granted. This shall be seen as a request for access from the accessing party to the resource owner.

NOTE 8 Connecting a vehicle to a container allows the offering party to identify the resource owner and verify if the access is granted.

NOTE 9 One container can have many vehicles connected to it.

9.4.2 Management of containers

Management of containers addresses the necessary processes for listing, creation and deletion of containers.

REQ_09_04_09	The technical realization of the processes for creation and deletion of a container shall be held open to the offering party.

REQ_09_04_10	It shall not be possible to update the purpose of the container or its resource list.

NOTE 1 Updating the purpose or resource list would revoke the explicit resource owner consent for the original container.

Figure 4 — Relationship of accessing party or offering party, containers and resources

Figure 4 visualizes the relationship of the accessing party or the offering party to containers and to resources. Additionally, the cardinality for each relationship is shown: one accessing party or one offering party may have multiple containers and multiple containers may have multiple resources.

REQ_09_04_11	The offering party may limit the number of allowed containers.

NOTE 2 The offering party manages the number of containers according to the capability of its design.