INTERNATIONAL STANDARD

ISO 20078-1

First edition
2019-02

Road vehicles — Extended vehicle (ExVe) web services —

Part 1: Content

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

Partie 1: Contenu

Reference number
ISO 20078-1:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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*.

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

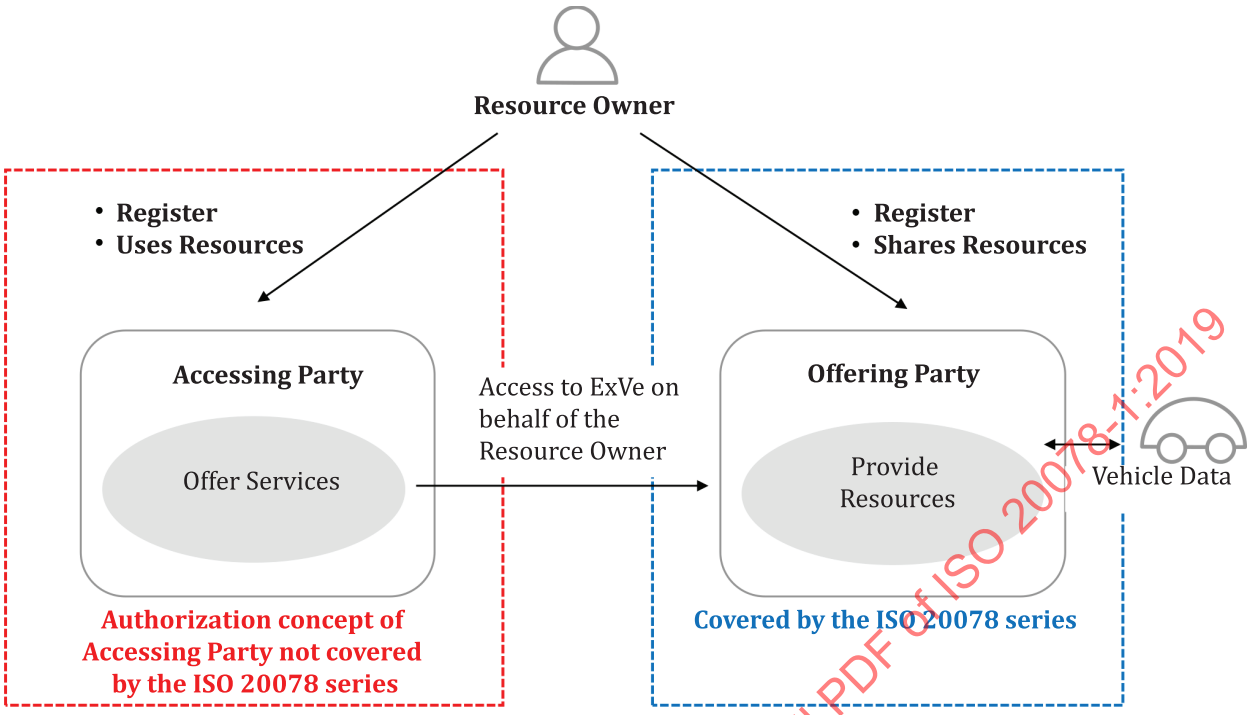
General

This document was developed to address the needs of different parties to access data, aggregated information and functionality (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 (see ISO 20078-3).

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

This solution is supported by the fact that Vehicle Manufacturers (VM) by design and in factory more and more include telematics support for their vehicles, making vehicle data, information and functionality 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 previously 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.



— Registration and verification of service consumer
— Registration with Offering Party and configuration of required resources
— Obtain authorization and consume resources
— Offer own services (not only ExVe based)
— Requires appropriate authorization concept

— Registration of Resource Owner
— Verification of ownership
— Requesting and validation of Resource Owner's consent
— Implementation of authorization concept as defined by ISO 20078-3
— Definition and provision of Resources

Figure 1 — Vision of the ISO 20078 series to standardize IT over the telematics backend

The authorization concept described by ISO 20078-3 covers only the authorization domain of the Offering Party; not the authorization domain of the Accessing Party. If an OAuth-compatible framework (see ISO 20078-3) is used to provide authorization by the Offering Party, three roles are technically mandatory:

— An Identity Provider; validates the identity of the Resource Owner;

— An Authorization Provider; manages the consents (grants) of the Resource Owner;

— A Resource Provider; shares Resources, depending on the consent of the Resource Owner.

The Access to Resources (data, aggregated information, and functions) cannot be authorized without validation of the Resource ownership and validation of the given consent of the Resource Owner. For registration, identity validation, and management of the Resource Owner an Identity Provider is used.

The Offering Party controls the Access to different Resources (URIs; see ISO 20078-2 Access) dependent on the availability of the Resource Owner's consent and owner's verification status. As such, the role of the Authorization Provider is required.

The Resource Provider exposes the actual Resources (via URIs; see ISO 20078-2) and enforces the Authorization Policy defined by the Authorization Provider.

The Accessing Party as a consumer of the Resources obtains Authorization from the Authorization Provider in order to access URIs (see ISO 20078-2). This requires:

— The registration of an Accessing Party as an ExVe client of the Offering Party;

— Configuration of required Resources (URIs) and may be providing intended purpose of use;

— Requesting Access to pre-configured Resource Groups and/or Containers.

The Accessing Party offers its own independent services based on the shared Resources (data, aggregated information, and functions). These Accessing Party services may depend on additional Resources and not only — per se — the Extended Vehicle Resources.

The Authorization domains of Accessing and Offering Parties are different, and the Accessing Party requires its own appropriate authorization concept (e.g. an additional Accessing Party Authorization Provider, if the OAuth 2.0 framework is also applied technically at the Accessing Party). Such Accessing Party authorization concepts are not in scope of ISO 20078-3 and held open.

Overview of the ISO 20078 series

This document states the minimum requirements, recommendations, permissions and external constrains for ensuring interoperable web services from an Accessing Party's perspective. The document:

— states requirements on the structure and format of Resources;

— 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.

The above-mentioned requirements and guidelines areas are addressed in the ISO 20078 series.

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 need to be described in the specific application or use case; e.g. see ISO 20080 Remote Diagnostics Support.

To elaborate more, this document 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 XML and JSON.

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 20078-2].

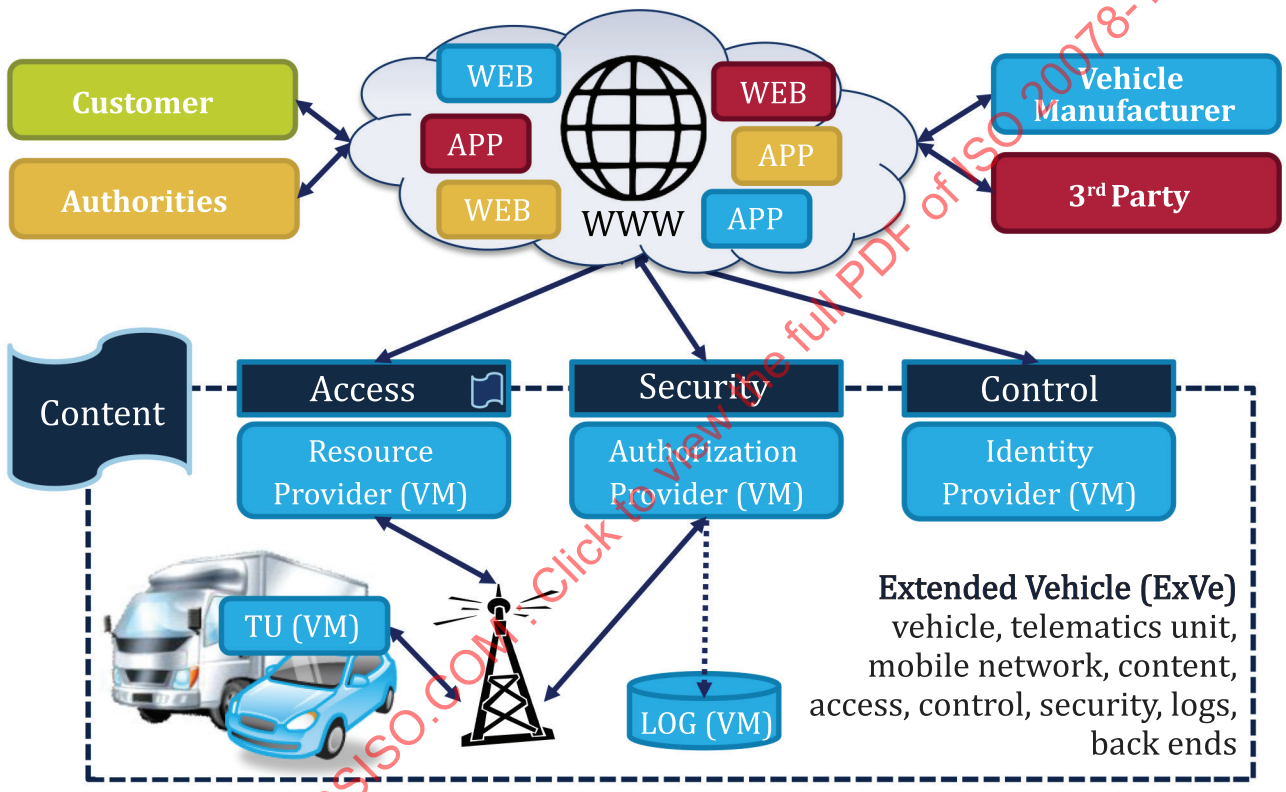
ISO 20078-3 standardizes the security model of the web service, including different roles and entities involved in an Authorization Policy. Three roles are defined: Identity Provider, Authorization Provider and Resource Provider at the Offering Party. Additional roles are the Accessing Party and the 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 20078-3].

ISO /TR 20078-4 summarizes this document, ISO 20078-2, and ISO 20078-3 by *logical processes* for the displaying the interaction of all defined roles and entities[1]. The processes define the needs for a registration, authentication, and authorization of an Accessing Party. For granting, denying and

revoking Access to Resources, processes involving the Resource Owner are defined. The Resource Owner is generally in charge of those processes, which may depend on certain use case. However, these processes allow for a full self-determination of the Resource Owner on sharing Resources to Accessing Parties.

The ISO 20078 series defines in general a framework based on the communication and authorization protocols listed in from 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.

In this document, entities are defined as the fundamental objects that represent, for example — vehicles, ECUs, drivers and fleets, and servers at an IT backend. Roles are defined as a grouping of entities and have relationships that allow for an interaction; e.g. The "Offering Party" (IT 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 & WEB — application & web services

Stakeholders — customer, authorities, VM, 3rd party

Figure 2 — Schematic presentation of the vision of the ISO 20078 series

ExVe web services are comprised of road vehicles combined with the telematics backend system of the Vehicle Manufacturer (the "Offering Party"), mainly acting as a Resource provider. This enables for a 3rd party, as well as the Vehicle Manufacturer, mainly acting as a service/application provider (the "Accessing Party") to access offered Resources via the internet; see Figure 2.

The concept of Containers is also introduced which allows an Accessing Party to specify what Resources it wants to access. Containers are a recommended solution where (data) privacy by design applies.

Logging (LOG of Figure 2) 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 (in addition to XML and Key-Value listing) is recommended for representation of Resources (URIs).

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
	Key-Value
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

1 Scope

This document defines the different concepts, entities and roles involved in implementing and delivering ExVe web services. In addition, it also gives an overview of the necessary activities that should be executed by the different roles involved and a logical order for those activities.

This document defines the concept of identifiers (direct and correlated), different Resource categories (e.g. personal, vehicle related, pseudonymized and anonymized Resources) and different approaches on how to bundle sharable Resources (e.g. Resource Group or Container).

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 20078-2, *Road vehicles — Extended vehicle (ExVe) web services — Part 2: Access*

ISO 20078-3:—[1)], *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 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 http://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.

1) Under preparation. Stage at the time of publication: ISO/FDIS 20078-3:2019.

3.1.3
Offering Party
OP
entity who provides web services access to Resources

3.1.4
Resource Owner
RO
responsible party for the Resource(s)

Note 1 to entry: The Resource Owner is responsible for granting, denying, and revoking Access to Resource(s).

Note 2 to entry: The responsible Resource Owner is determined by the concrete Resource.

3.1.5
3rd party
person or body which is not the Vehicle Manufacture or the Resource Owner

Note 1 to entry: Formally defined as the “Service Owner”/the “Service Provider”.

3.1.6
Accessing Party
AP
entity which accesses Resources via web services

Note 1 to entry: Other than the Offering Party or the Resource Owner.

Note 2 to entry: Implements technically and independently an Identity, Authorization, and a Resource Provider/Service Provider that are not in scope of this document.

Note 3 to entry: The Resource Provider and Service Provider might 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 users, through the use of credentials

Note 1 to entry: Offering Party 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 that protects and provides Resources.

3.1.9
Authorization Provider
entity at the Offering Party that manages the access rights to Resources and Resource Owner 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 in general for some Use Cases.

3.2 Technical concepts and terms

3.2.1
Resource
data, aggregated information or functionalities of the Connected Vehicle

Note 1 to entry: Resources can be

— Resources (by a RID),

— Resource Owner information (by a Resource Owner ID),

— Resource and Resource Owner related information,

— anonymous Resources,

— pseudonymized Resources,

— vehicle related Resources, or

— personalized Resources,

at the Offering Party.

3.2.2
Resource Group
logical set of Resources

3.2.3
Superset
set of all unique Resources

3.2.4
Container
logical group of Resources defined for a single Accessing Party purpose

3.2.5
Resource Owner Profile
information regarding the Resource Owner

EXAMPLE Name, address, contact information, and RID.

3.2.6
Access
delegated right to an Accessing Party to access a Resource Owner's Resources

3.2.7
Authorization Policy
set of rules that define Access control to protected Resources

3.2.8
Token
sequence of characters representing a verified identity and/or Access

Note 1 to entry: The issuer of the token is responsible for the interpretation and the integrity of the token; e. g. the Authorization Provider of the Offering Party 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, Accessing Party and/or Offering Party.

3.2.9
Fleet
group of Connected Vehicles associated to a specific Resource Owner

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[2] 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 [2]. 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 at the Offering Party

3.3.4
ContainerID
CID
ID that identifies a unique Container at the Offering Party

3.3.5
AccessingPartyID
APID
ID that identifies a unique Accessing Party at the Offering Party

3.3.6
AccessID
AID
ID that represents a unique Access of the Accessing Party at the Offering Party

3.3.7
CorrelationID
CoID
ID agreed between the Offering Party and the Accessing Party to support pseudonymization of the RIDs or the Resource Owner IDs

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

3.4 Credentials

3.4.1
ResourceOwnerCredentials
ROC
credentials shared from a party to the Resource Owner

3.4.2
ResourceOwnerCredentialsOP
ROCOP
credentials shared from the Offering Party to the Resource Owner

3.4.3
ResourceOwnerCredentialsAP
ROCAP
credentials shared from the Accessing Party to the Resource Owner

3.4.4
AccessingPartyCredentials
APC
credentials shared from the Offering Party to the Accessing Party

4 Abbreviated terms

AID	Access ID
AP	Accessing Party
APC	Accessing Party Credentials
API	Application Programming Interface
APID	Accessing Party ID
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	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	Resource ID

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 external constraints are formalized as follows:

REQ_NUM	Text of the requirement, recommendation, permission or external constraint

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

— REQ the acronym stands for requirement, recommendation, permission, or the external constrain,

— 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 external constraint can be introduced beforehand by an explanatory text. The ISO convention about verbs (shall be, should be, maybe, or can be) denotes the type.

6 Relationship of defined Entities

6.1 Overview of Entities

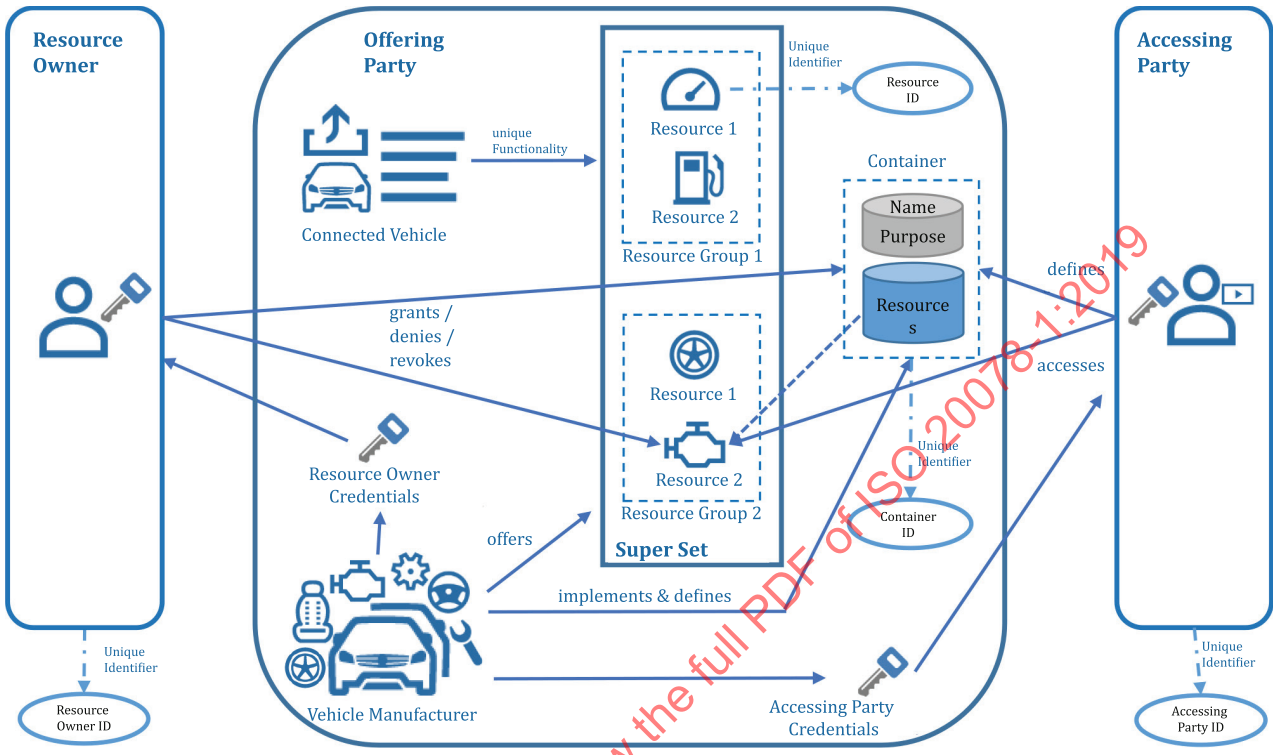


Figure 3 — Overview of defined entities and their overall roles

Figure 3 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

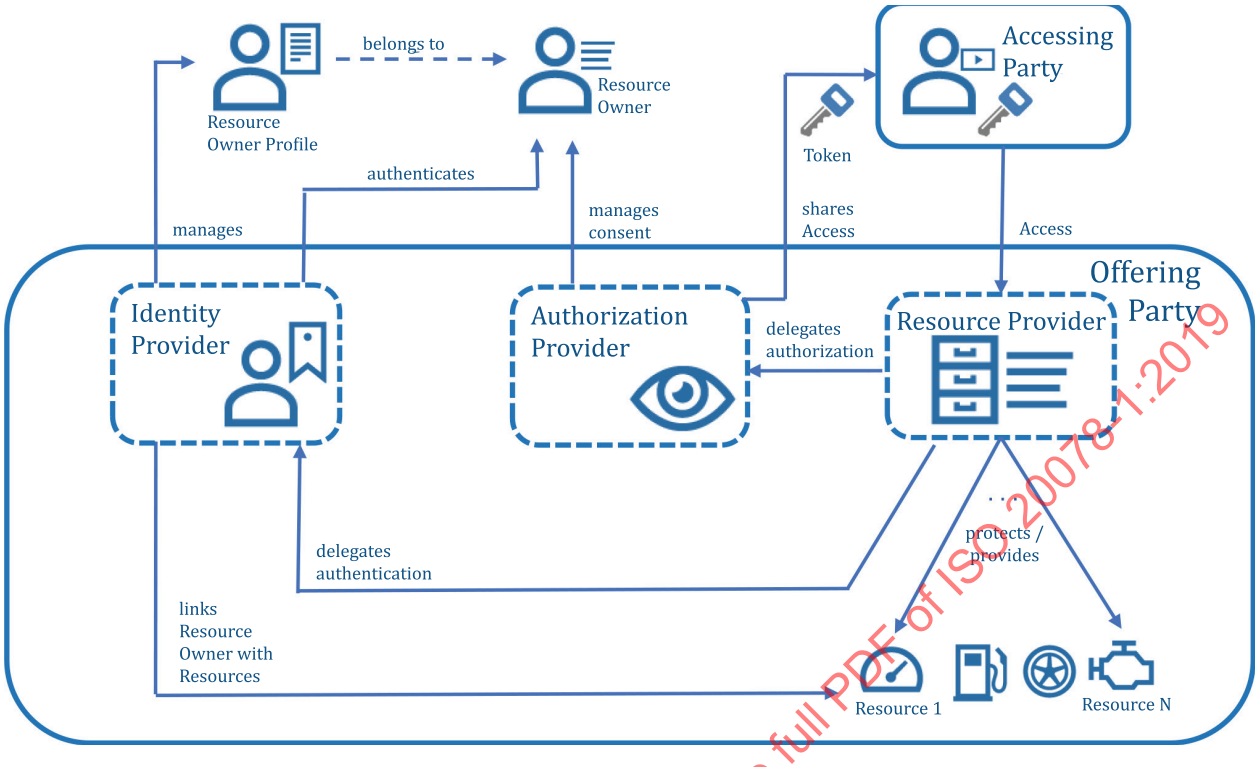


Figure 4 — Roles and their relationship to entities

Figure 4 describes roles and their relationship to entities required for granting an Accessing Party Access to a Resource Owner's Resources.

NOTE 1 Each role could 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_01_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_02_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[2]. Such identifiers allow for an indirect identification between the Accessing 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 kinds of Resources are mainly used for ensuring mobility, for increasing traffic flow, or for enhanced road safety. For 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:—, Annex A, with consent of the Offering Party (acting as the Resource Owner).

8.3 Pseudonymized Resources

Pseudonymized Resources are Resources, shared with direct identifiers or pseudonyms. These kind of Resources are mainly shared to make cross brand services available.

EXAMPLE Remote field studies of component suppliers, like gearboxes.

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:—, A.3.1 or A.3.2, as 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:—, 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 (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.

EXAMPLE 2 By a vehicle identification number (VIN) or a pseudonymized ID.

REQ_08_04_02	Access on technical (vehicle) Resources may be performed by the simplified flow of ISO 20078-3:—, 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 needs 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 an UUID that refers to the RID or the VIN number of the road vehicle.

REQ_08_05_03	Access on personalized Resources shall require consent of the Resource Owner at the Offering Party.

NOTE See reference implementation in ISO 20078-3:—, 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 adding a purpose of data processing; see 9.2, 9.3, and 9.4.

REQ_09_01_03	The Offering Party decides how they want to display the available Resources 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 grouping 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.

REQ_09_03_05	A Resource should be defined in a minimal way.

NOTE 3 For example a Resource can be the identifier, the value, and the timestamp of generation.

NOTE 4 Principles of data normalization can support data minimization.

More complex Resources are also reduced to the minimum consistent set of information and do not include other secondary information. For example, a diagnostic trouble code Resource of a Connected Vehicle does not include the position Resource of the Connected Vehicle.

9.4 Containers

9.4.1 Container

A Container is a selection of Resources (see 9.3). The Accessing 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 in a web portal provided by the Offering Party. Due to the explicit granting of Access to Resources grouped by the Containers, such Containers can only be created or deleted, not updated.

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 picked 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[2] can be used.

REQ_09_04_05	Containers may be defined by the Accessing 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.