FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/FDIS
20078-1**

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 1:
Content and definitions

Reference number
ISO/FDIS 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 compared to the previous edition 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.

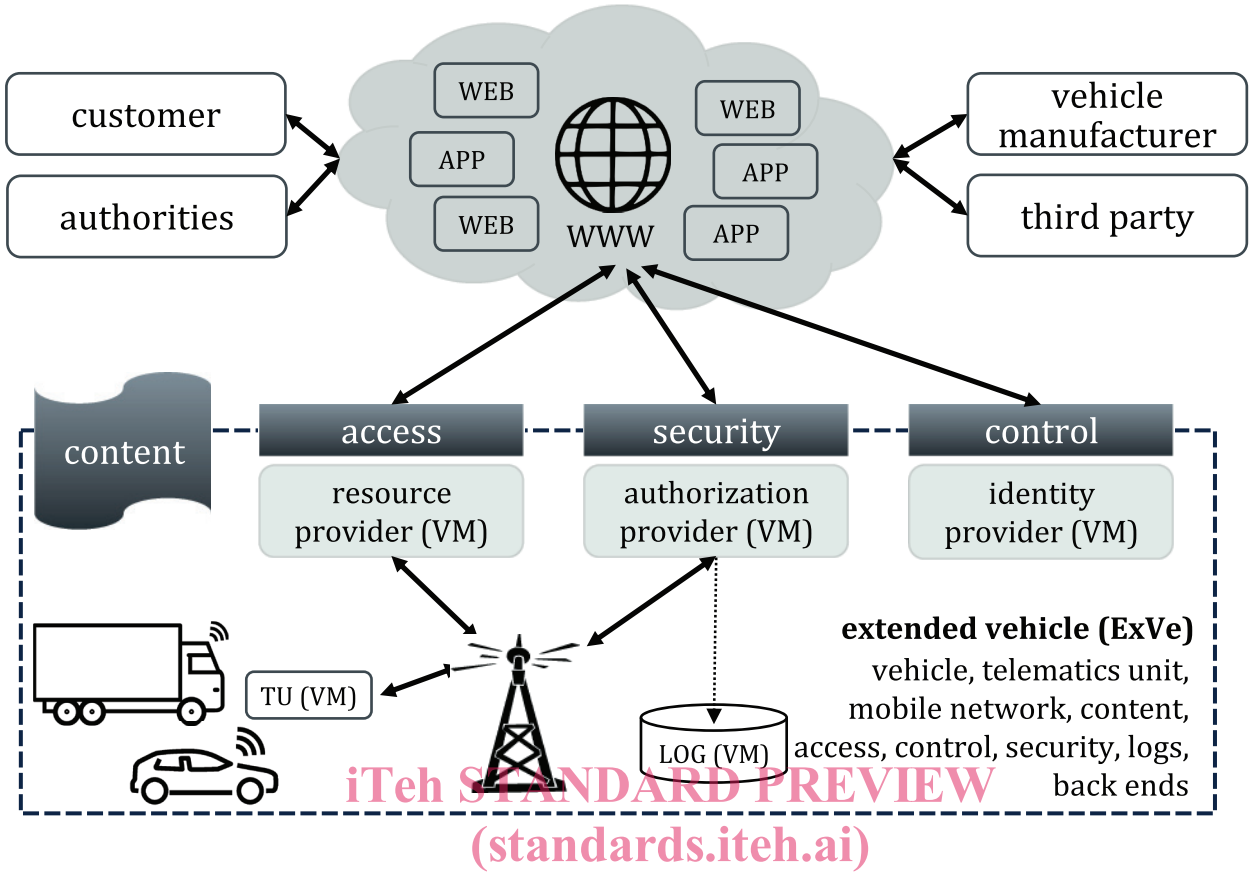
This document, ISO 20078-1, defines all entities and roles that are used over in the ISO 20078 series. It standardizes how an offering party defines resources. Depending on resource category, the offering party uses different kind of identifiers. Such resources can be exposed directly or through containers.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

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)