INTERNATIONAL STANDARD

ISO 20078-3

Second edition
2021-11

Road vehicles — Extended vehicle (ExVe) web services —

Part 3: Security

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

Partie 3: Sécurité

Reference number
ISO 20078-3:2021(E)

© ISO 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2021 – All rights reserved

Contents

Page

Foreword ... **iv**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 General ... **2**
4.1 Processes ... 2
4.2 Conditions ... 2

5 Basic communication flow ... **3**
5.1 Offering party authorization domain ... 3
5.1.1 General ... 3
5.1.2 Authentication ... 3
5.1.3 Authorization ... 4
5.1.4 Resource access ... 6
5.1.5 Separation of duties ... 7
5.1.6 Implementation related considerations ... 9
5.2 Accessing party authorization domain ... 11
5.2.1 General ... 11
5.2.2 Authorization ... 11
5.2.3 Pushing resources ... 12

Annex A (informative) **Reference implementation using OAuth 2.0 and OpenID Connect 1.0** ... **13**

Annex B (informative) **Reference implementation for push** ... **21**

Bibliography ... **24**

© ISO 2021 – All rights reserved

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 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.

© ISO 2021 – All rights reserved

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

© ISO 2021 – All rights reserved

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.

© ISO 2021 – All rights reserved