
**Road vehicles — Extended vehicle
(ExVe) web services —**

**Part 4:
Control**

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

Partie 4: Contrôle

iTech Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/TR 20078-4:2019

<https://standards.iteh.ai/catalog/standards/iso/4c3d8efb-4ff3-4b8d-9afd-2a3702fbabdc/iso-tr-20078-4-2019>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/TR 20078-4:2019

<https://standards.iteh.ai/catalog/standards/iso/4c3d8efb-4ff3-4b8d-9afd-2a3702fbabdc/iso-tr-20078-4-2019>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

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
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviations	1
4 Roles	1
4.1 Resource owner	1
4.1.1 Resources	1
4.1.2 Containers	2
4.2 Accessing Party	3
4.3 Offering Party	4
5 Processes	4
5.1 Registration	4
5.1.1 Accept registration of a requesting Party	4
5.1.2 Reject Registration of a requesting Party	4
5.1.3 Accept Resource Owner Registration	5
5.1.4 Reject Resource Owner Registration	5
5.2 Resources	6
5.2.1 Grant Access to Resources	6
5.2.2 Reject Access to Resources	7
5.2.3 Ignore Access Request to Resources	8
5.2.4 Revoke Access to Resources	8
5.3 Containers	9
5.3.1 Creation of a Container	9
5.3.2 Deletion of a Container	9
5.3.3 Grant Access to Resources grouped by a Containers	10
5.3.4 Reject Access to Containers	11
5.3.5 Ignore Access Request to Containers	12
5.3.6 Revoke Access to Containers	12
5.4 Resource Access	13
5.4.1 Access	13
5.4.2 No Access	13
Annex A (informative) Registration of the service/application owner at the Accessing Party	15
Bibliography	16

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.

Road vehicles — Extended vehicle (ExVe) web services —

Part 4: Control

1 Scope

This document describes the processes of an Offering Party's implementation to provide (ISO 20078-2) Access controlled (ISO 20078-3) Resources (ISO 20078-1) to Accessing Parties. The processes are summarized as: Registration of different stakeholder as well as granting, denying and revoking of Access to Resources. Those processes are held as examples of combining ISO 20078-1, ISO 20078-2 and ISO 20078-3 and can vary depending on the actual implementation of the Offering Party.

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' — Part 1: Content*

3 Terms, definitions and abbreviations

For the purposes of this document, the terms, definitions and abbreviations given in ISO 20078-1 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/>

4 Roles

4.1 Resource owner

4.1.1 Resources

The Resource Owner is in control of the access to its Resources. To control access, the Resource Owner uses the processes: granting, denying, ignoring and revoking.

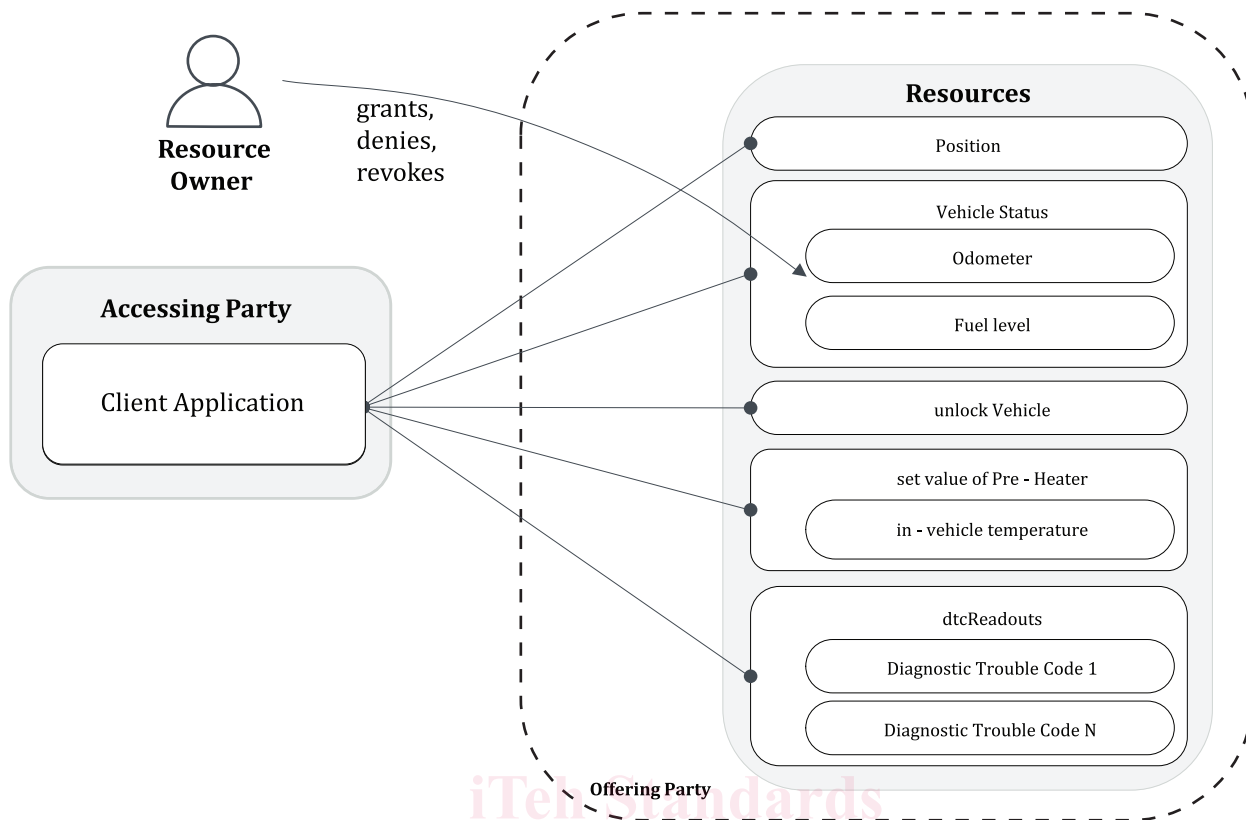


Figure 1 — The Resource Owner grants, denies or revokes access to Resources

[Figure 1](#) illustrates an example of how a Resource Owner controls access to Resources offered to the accessing Party by the offering Party. The Resource Owner can grant, deny or revoke access (ISO 20078-3) to its Resources at any time.

- **Granting:** The Resource Owner reviews the resources presented by the Offering Party and decides to **grant** access to the Accessing Party.
- **Denying:** The Resource Owner reviews the Resources presented by the Offering Party and decides to **deny** access to the Accessing Party.
- **Ignoring:** The Resource Owner does not grant or deny access to the Accessing Party. The request stays pending for a pre-defined time, after which it will be denied.
- **Revoking:** The Resource Owner revokes an already granted access to an Accessing Party.

NOTE The Accessing Party is a third-party service provider or the VM when acting as a service provider both acting for after sales services after the ExVe has been sold or leased.

4.1.2 Containers

The Resource Owner is in control of the Access (ISO 20078-3) to their Resources (ISO 20078-1) grouped by a Container. The Resource Owner uses the processes: registration, granting, denying, ignoring, revoking to grant, deny or revoke Access Resources.

The content of a Container is defined by the Accessing Party or the Offering Party. The Offering Party offers the Container with the granted Resources if available.

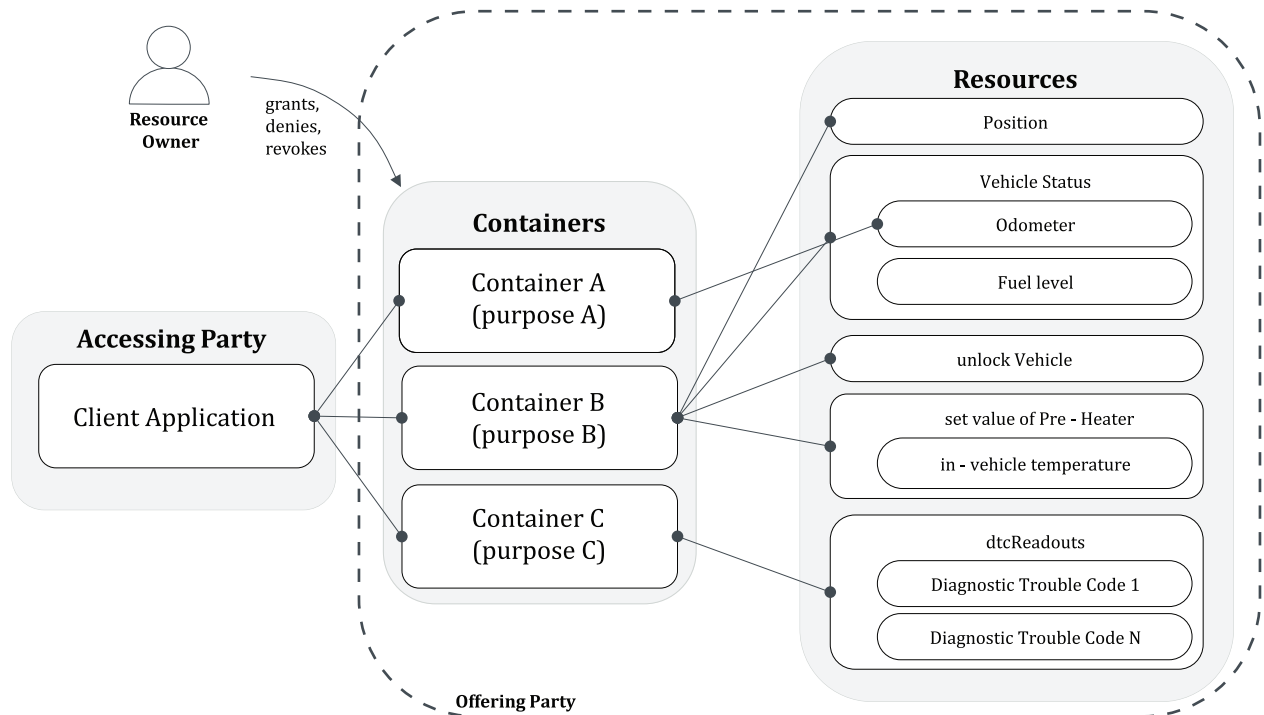


Figure 2 — The Resource Owner grants, denies or revokes Access to Containers

Figure 2 displays an example for one Accessing Party. The Accessing Party or the Offering Party defines Containers, each identified by a unique “CID”, to Access Resources of the Offering Party. The Resource Owner can individually grant, deny or revoke — at any time — Access (ISO 20078-3) to Resources of defined Containers (ISO 20078-1). Such decisions made by the Resource Owner are collectively called the *request permission processes*. Possible states or outcomes of these processes are:

- *Granted*: A certain Container is defined by the Accessing or the Offering Party. The Resource Owner grants Access to the Container for the Accessing Party. Through this grant process the Resource Owner verifies that both the Resources, and the purpose of data processing of the Container are presented by the Offering Party; see Figure 15 and/or Figures 16 and 17.
- *Denied*: A certain Container is defined by the Accessing or the Offering Party. The Resource Owner denies the Access to the Container for the Accessing Party. Because of this action, the Resource Owner does not approve the Access to the Resources and/or the purpose of data processing of the Container that are presented by the Offering Party; see Figure 18.
- *Pending/Ignored*: A certain Container is defined by the Accessing or the Offering Party and selected for a grant request. After starting the request, the Resource Owner does not continue to either grant or to deny. The request stays pending as long as it is ignored by the Resource Owner. If a pre-defined time passes, and the request has been ignored, it is denied by the Offering Party; see Figure 19.
- *Revoked*: A certain Container is defined by the Accessing Party or the Offering Party and was granted by the Resource Owner. After a certain time, the Resource Owner revokes the Access to Resources of the Container for the Accessing Party. This immediately denies any further Access to Resources for the Accessing Party; see Figure 20.

4.2 Accessing Party

The Accessing Party uses the issued credentials to authenticate itself when requesting Access tokens from the Offering Party. To retrieve an Access token and Access the Resource Owner’s Resources, an explicit grant from the Resource Owner is required.

Afterwards the Accessing Party registers its own digital customers on its digital services/applications and/or on its resource providing services; see Annex A.1 as an example.

These digital customers consume the digital services/applications that are developed, offered and maintained by the Accessing Party. These services are available for use for as long as Access to Resources of the Offering Party is granted by the Resource Owner.

4.3 Offering Party

The Offering Party makes Resources available via web-services for Access by an Accessing Party. The Offering Party provides Access to Resources based on the consent of the Resource Owner either on a single resource or Resources grouped by a Container. Additionally, the Offering Party manages the processes defined in (Clause 5).

5 Processes

5.1 Registration

5.1.1 Accept registration of a requesting Party

A requesting Party (not yet an Accessing Party) sends a registration request with the mandatory registration information (identification) to the Offering Party.

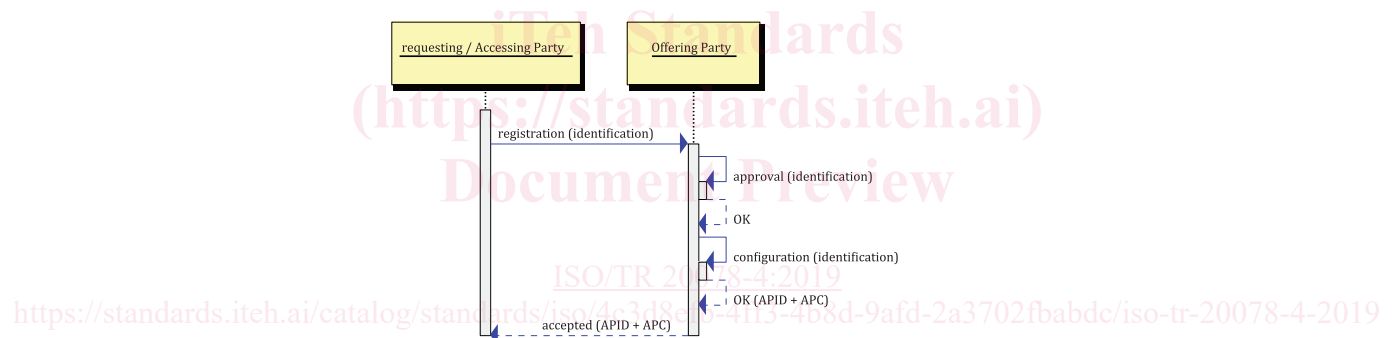


Figure 3 — Registration request of a requesting Party accepted by the Offering Party

The approval of the registration is in responsibility of the Offering Party. If the registration is approved, the Offering Party provides information on how to Access web-services and (if available) web portals, e.g. web service documentation, URIs and necessary credentials.

After successful registration, the requesting Party receives the role of an Accessing Party and may (for example) create Containers.

The registration process (Figure 3) can be online, offline or a combination of both.

NOTE Accessing Party ID (APID) and Accessing Party Credentials (APC) are issued; see ISO 20078-1.

5.1.2 Reject Registration of a requesting Party

A requesting party sends a registration request with the mandatory registration information to the Offering Party.

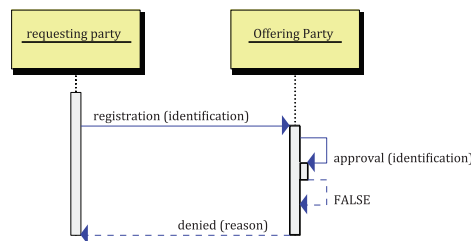


Figure 4 — Registration of a requesting party is rejected by the Offering Party

The Offering Party verifies the request. Invalid requests are rejected, e.g. if the identity cannot be verified, or information is missing (see [Figure 4](#)). If technically possible, the requesting party is informed of the reason.

If circumstances change and any registrations become invalid, the Offering Party cancels such registrations.

5.1.3 Accept Resource Owner Registration

A Resource Owner sends a registration request including the mandatory information (identification) to the Offering Party.

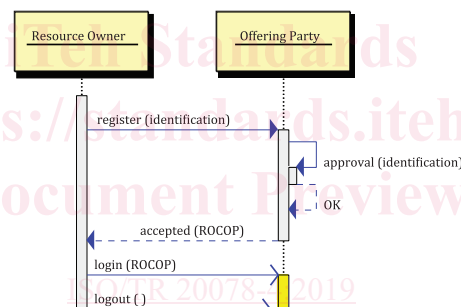


Figure 5 — Accepting registration of the Resource Owner at the Offering Party

The Offering Party verifies the request. If the request can be approved, the Offering Party provides information to allow the Resource Owner to manage Access to its Resources, e.g. credentials (ROCOP, see 20078-1), instructions and URIs to portals.

The registration process ([Figure 5](#)) can be online, offline or a combination of both.

NOTE The Resource Owner can register independently at the Accessing Party; see [Annex A](#).

5.1.4 Reject Resource Owner Registration

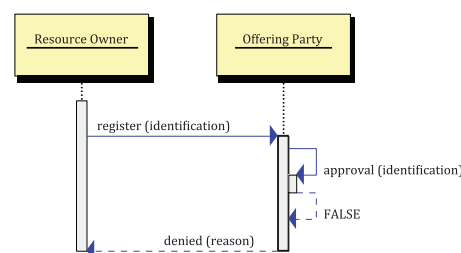


Figure 6 — Rejecting registration of the Resource Owner at the Offering Party

A Resource Owner sends a registration request including the mandatory registration information (identification) to the Offering Party.

If possible, the Resource Owner is informed about the reason (for example, it was not possible to verify the identity, or general information is missing).

If circumstances change and any registrations become invalid, the Offering Party cancels such registrations (see [Figure 6](#)).

5.2 Resources

5.2.1 Grant Access to Resources

After registering and selecting Resources, the Accessing Party can initiate the granting process, by requesting consent *directly* from the Resource Owner to retrieve Access (ISO 20078-3) to Resources at the Offering Party.

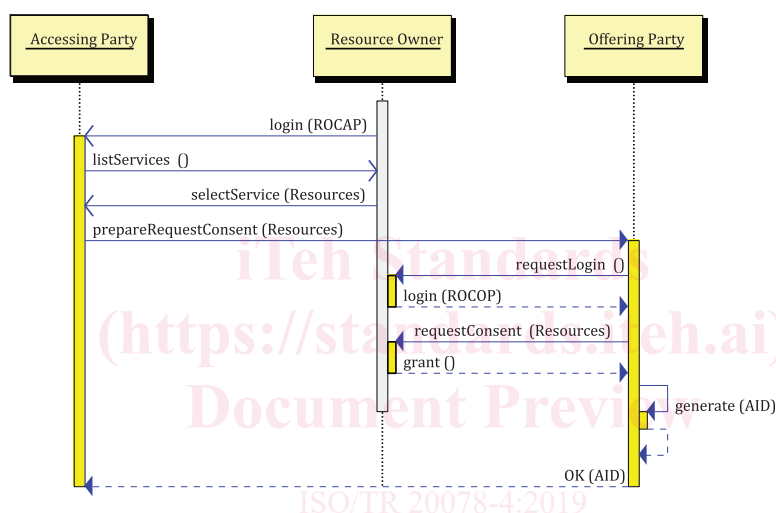


Figure 7 — Granting Access to Resources

[Figure 7](#) shows the process for granting Access to Resources by the Resource Owner at the Offering Party. The Resource Owner starts at the Accessing Party and is redirected to the Offering Party. On both sides, the Resource Owner authenticates by separate credentials. For the Resource Owner side, those credentials are the ROCAP, and for the Offering Party those credentials are the ROCOP (see; ISO 20078-1). After authentication with the Offering Party, the Resource Owner checks the Resources to be granted (ISO 20078-3). When granting Access, the Offering Party can generate an AccessID, which will be transferred securely to the Accessing Party.

The AccessID should be stored at the Accessing Party and at the Offering Party.

The process of [Figure 7](#) can be simplified to an implicit grant.