TECHNICAL REPORT

ISO/TR 20078-4

Second edition
2021-10

Road vehicles — Extended vehicle (ExVe) web services —

Part 4: Control

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

Partie 4: Contrôle

Reference number
ISO/TR 20078-4:2021(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 ... **iv**

1 Scope ... **1**

2 Normative references ... **1**

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

4 Roles ... **1**
4.1 Resource owner ... 1
4.1.1 Resources ... 1
4.1.2 Containers ... 2
4.2 Accessing party ... 4
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 ... 5
5.1.3 Accept resource owner registration ... 5
5.1.4 Reject resource owner registration ... 6
5.2 Resources ... 6
5.2.1 Grant access to resources ... 6
5.2.2 Reject access to resources ... 8
5.2.3 Ignore access request to resources ... 9
5.2.4 Revoke access to resources ... 10
5.3 Containers ... 10
5.3.1 Creation of a container ... 10
5.3.2 Deletion of a container ... 11
5.3.3 Grant access to resources grouped by a container ... 12
5.3.4 Reject access to containers ... 14
5.3.5 Ignore access request to containers ... 15
5.3.6 Revoke access to containers ... 15
5.4 Resource access ... 16
5.4.1 Access ... 16
5.4.2 No access ... 16
5.4.3 Push of resources ... 17

Annex A (informative) **Registration of the service/application owner at the accessing party** ... **19**

Bibliography ... **21**

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/TR 20078-4:2019), which has been technically revised.

The main changes are as follows:

— revised the clause containers;

— added new subclause describing push of resources (5.4.3).

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 and definitions*

3 Terms and definitions

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

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.

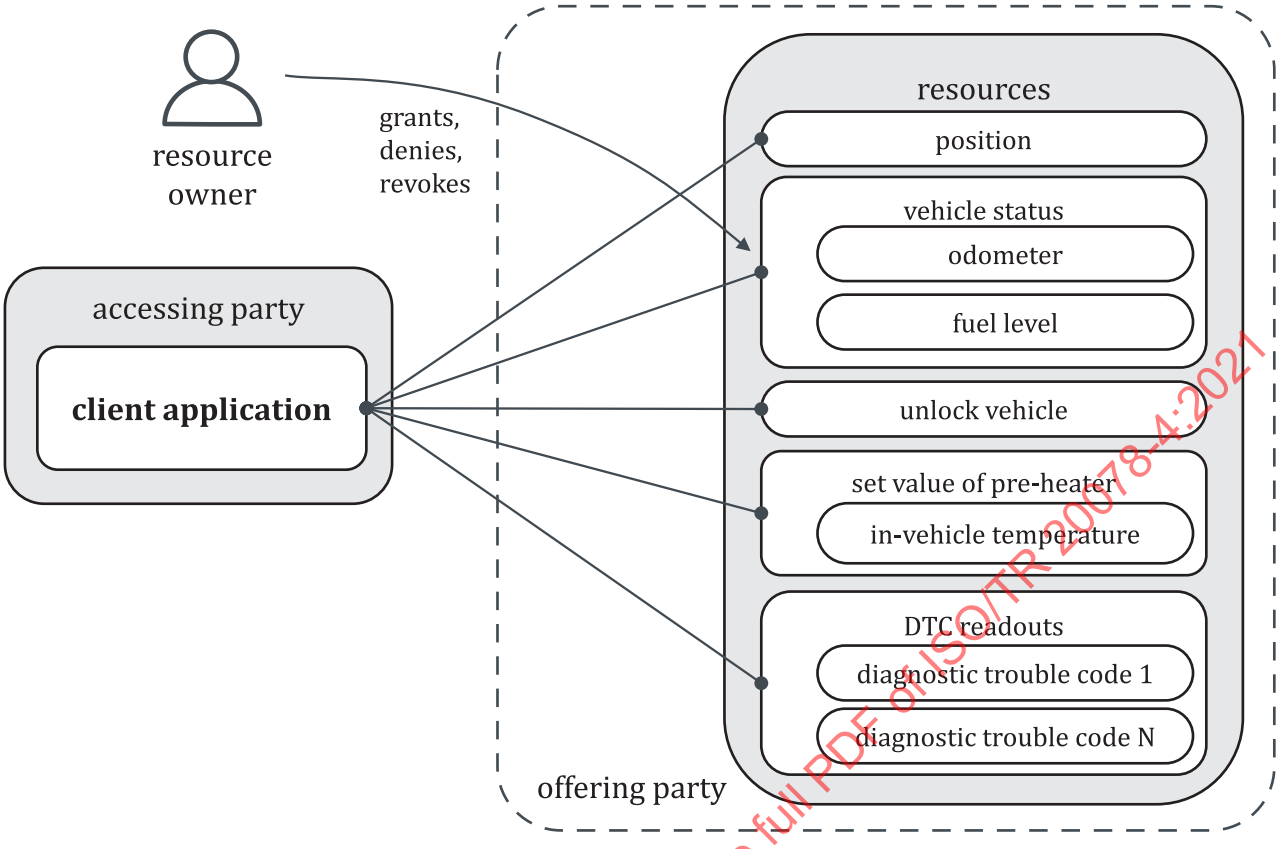

Figure 1 — The resource owner grants, denies or revokes access to resources

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.

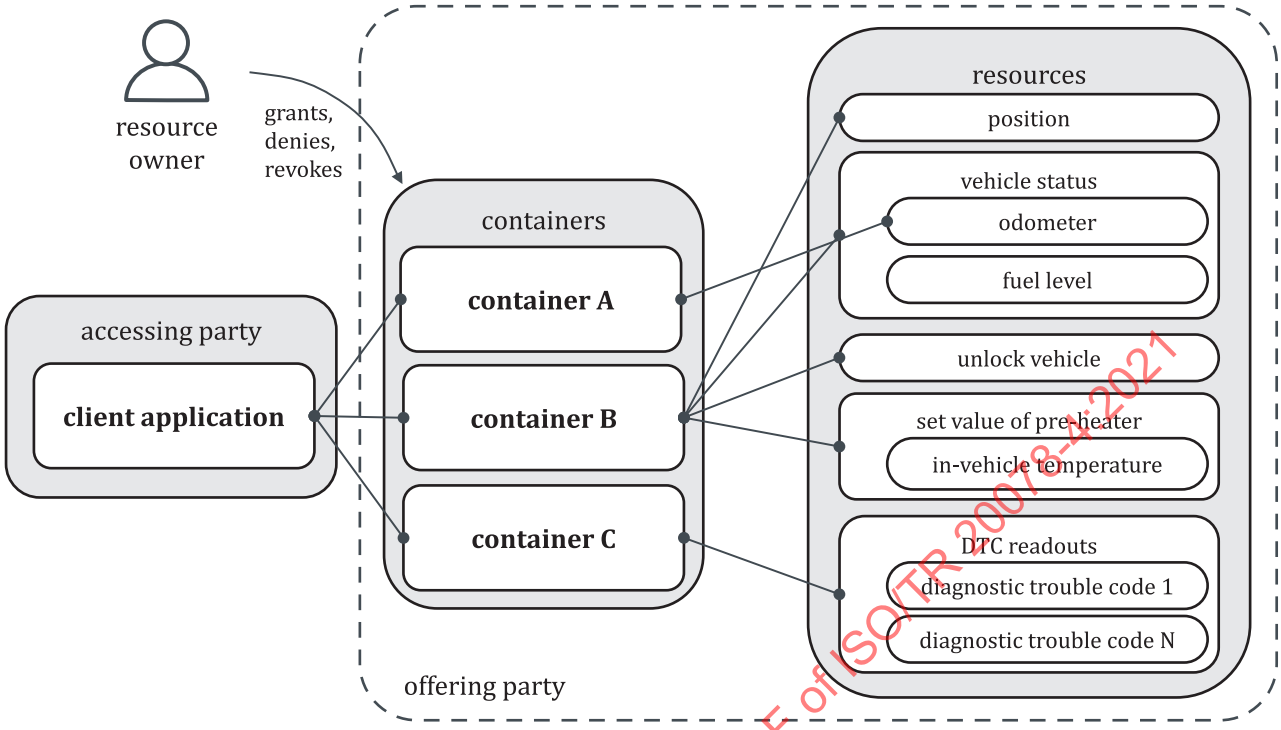

Figure 2 — The resource owner grants, denies or revokes access to containers

Figure 2 displays an example for one accessing party. The accessing party or the offering party defines containers, each identified by a unique container Id (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) in relation to a one or more vehicle identifiers (VINs) for not anonymized resources. Such decisions made by the resource owner are collectively called the request permission processes. Possible states or outcomes of these processes are the following.

— Granted: a certain container is defined by the accessing or the offering party. The resource owner grants access to the container (and if required in combination with a vehicle identifier) 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 party 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. 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 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 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.

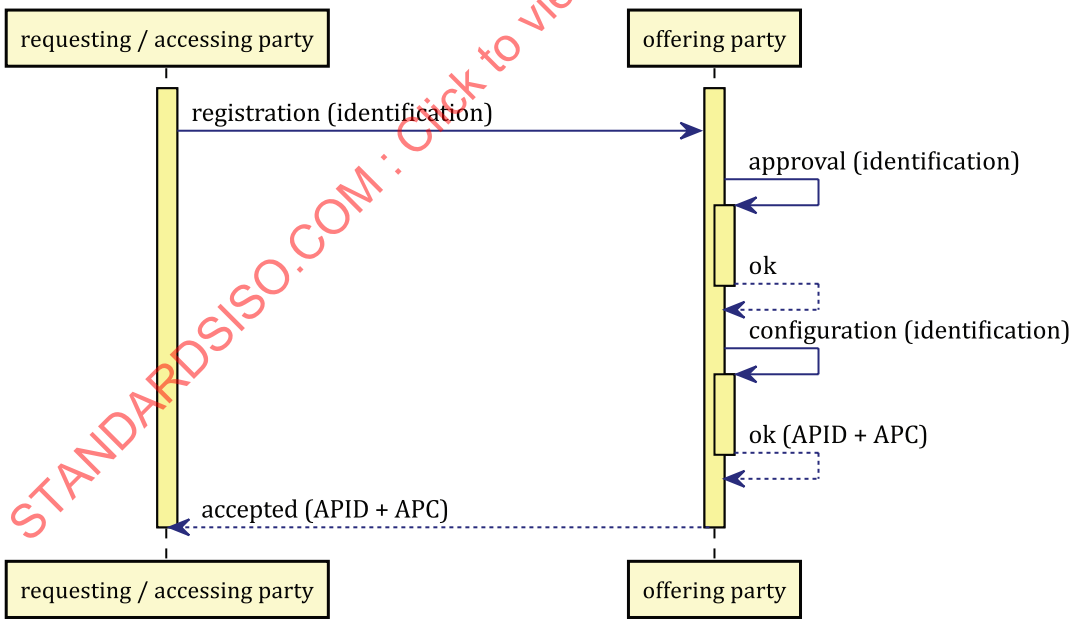

Figure 3 — Registration request of a requesting party accepted by the offering party

The approval of the registration is the 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 can (for example) create containers.

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

NOTE AccessingPartyID (APID) and AccessingPartyCredentials (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.

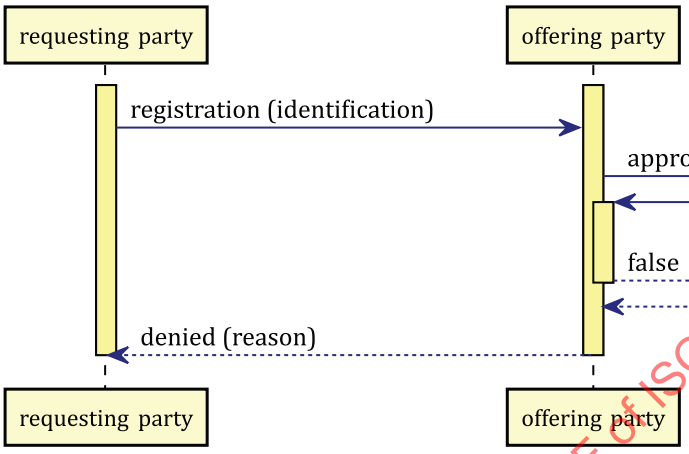

Figure 4 — Registration of a requesting party is rejected by the offering party

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 the 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.

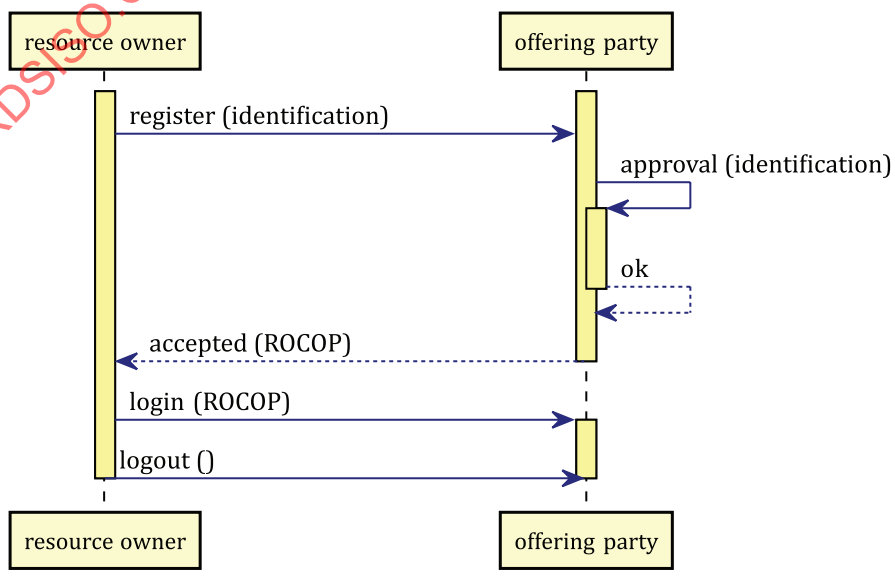

Figure 5 — Accepting registration of the resource owner at the offering party

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

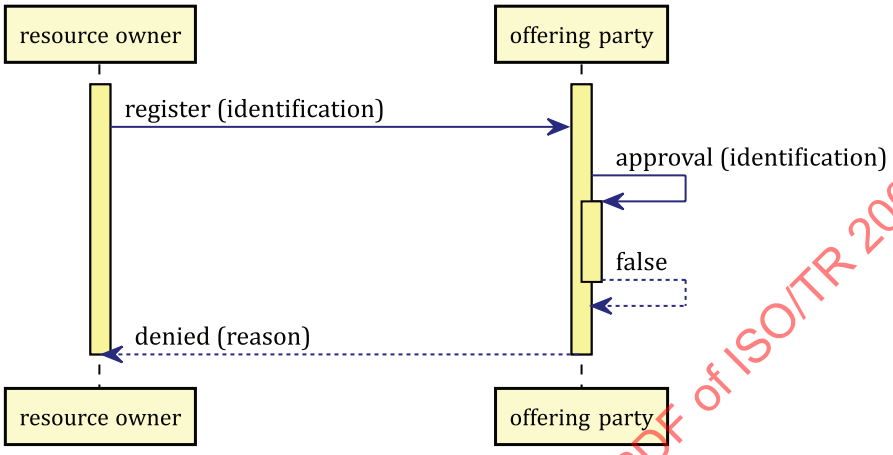

Figure 6 — Rejecting registration of the resource owner at the offering party

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.

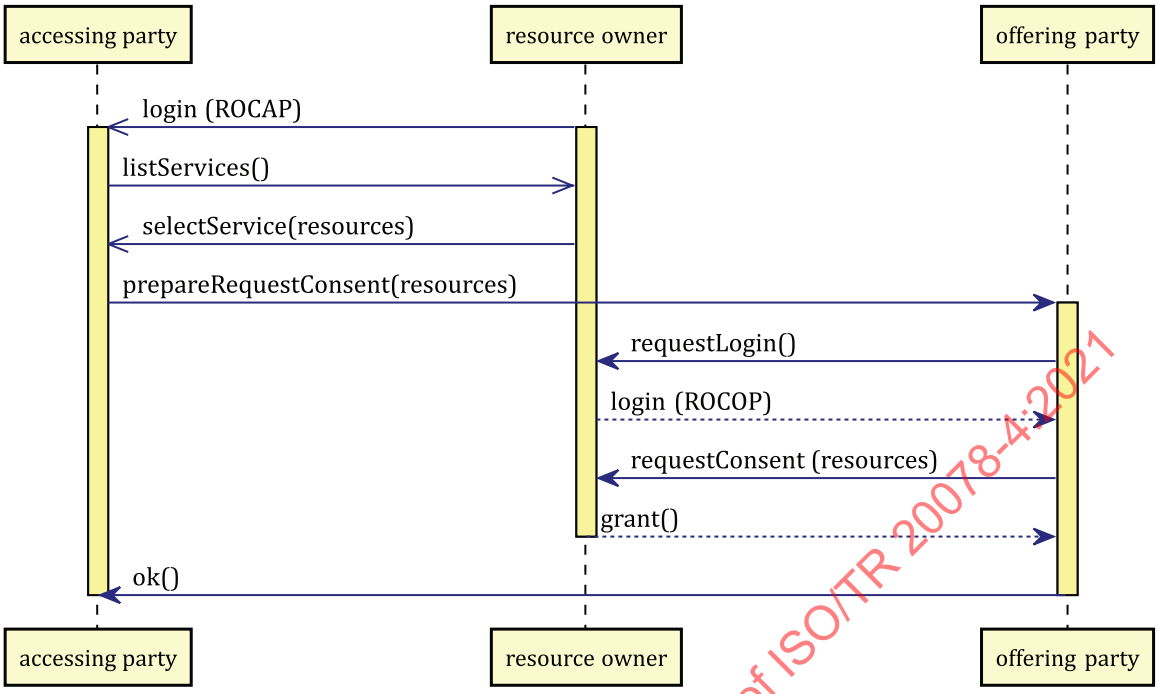

Figure 7 — Granting access to resources

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).

The process of Figure 7 can be simplified to an implicit grant.

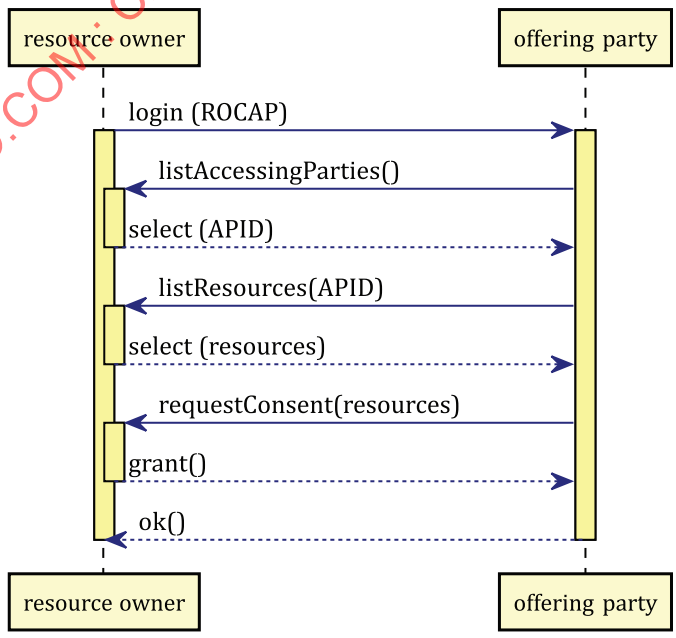

Figure 8 — Implicitly granting access to resources

Figure 8 shows the process for implicitly granting access to resources by the resource owner at the offering party. The resource owner starts at the offering party and authenticates using their ROCOP (ISO 20078-1) credentials. After authentication the resource owner lists the accessing parties and selects an accessing party. Whilst granting, the resource owner selects resources from a list and/or resource groups. The offering party requests consent for access to the chosen resources and/or resource groups for the selected accessing party. The resource owner grants this request.

NOTE 1 The accessing party is not (necessarily) in an active role at the process of Figure 8.

NOTE 2 The process of Figure 9 follows after the process of Figure 8.

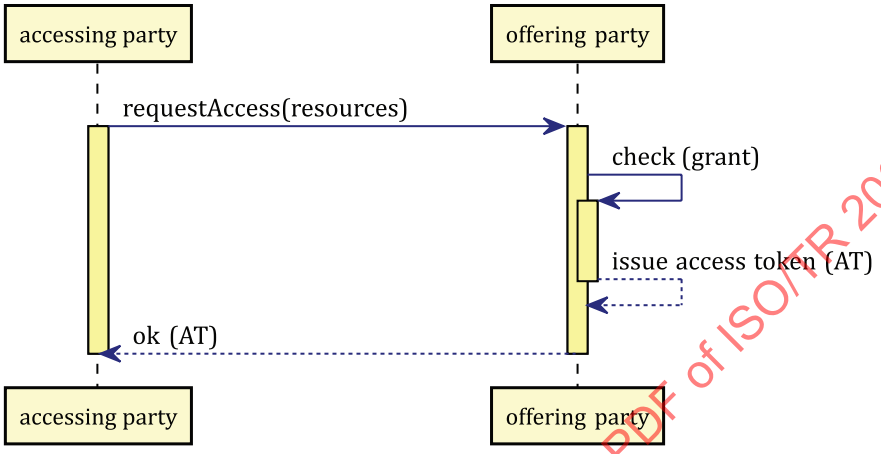

Figure 9 — Requesting access to resources

Figure 9 completes the implicit granting of Figure 8. The accessing party is requesting access to resources. The offering party checks the given consent (grant) for this request. If the request can be validated, an access token (AT; ISO 20078-1) is generated and transferred to the accessing party. This AT allows the accessing party to access resources at the resource provider (ISO 20078-3).

5.2.2 Reject access to resources

As shown by Figure 7 for granting access, the resource owner could also deny the request for access made by the accessing party.

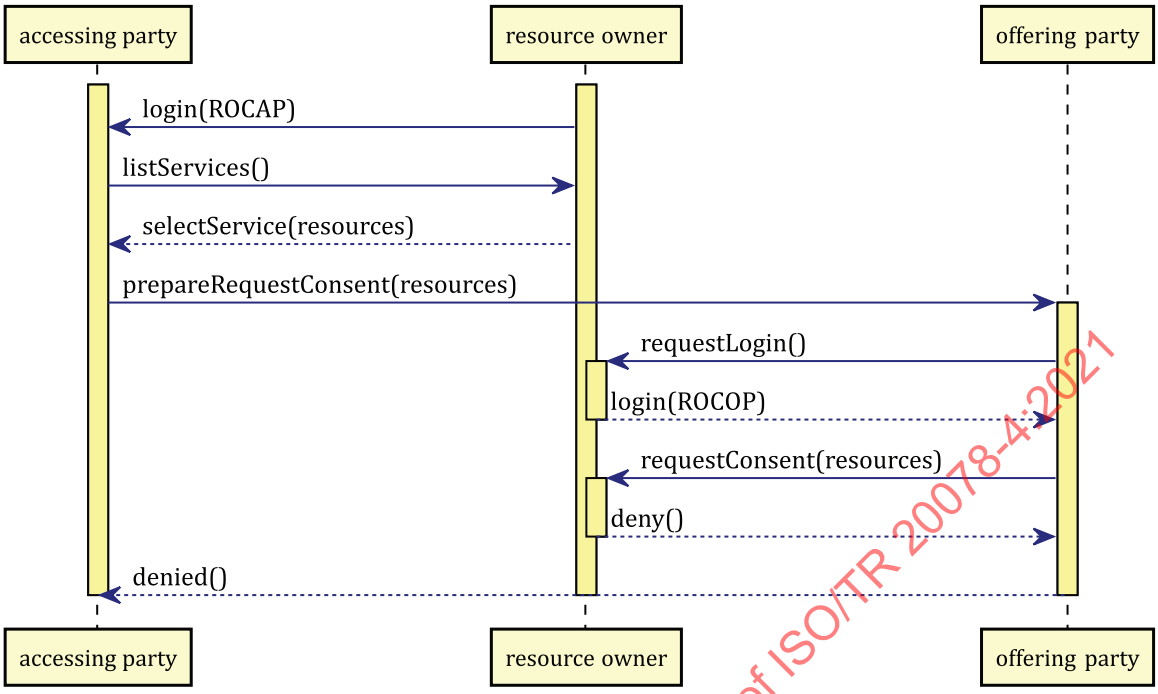

Figure 10 — Rejecting access to resources

Figure 10 displays the process for requesting access consent for resources that are denied by the resource owner at the offering party.

5.2.3 Ignore access request to resources

As shown by Figure 7 for granting access, the resource owner could also ignore the access consent request made by the accessing party for resources.

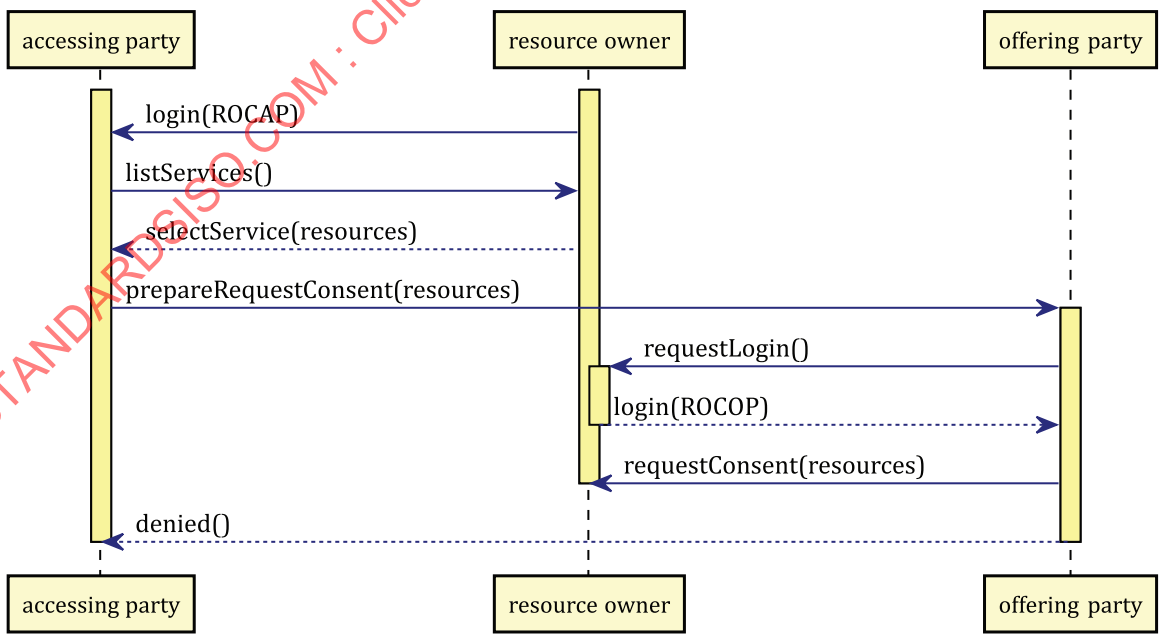

Figure 11 — Ignoring access request to resources

Figure 11 displays the process for requesting access consent for resources that are ignored by the resource owner at the offering party. The resource owner neither grants access nor rejects the request

for access. The offering party sets a time out (or time to live) interval that automatically rejects the request for access consent after a certain time period towards the accessing party.

5.2.4 Revoke access to resources

The resource owner revokes a granted access to resources at the offering party.

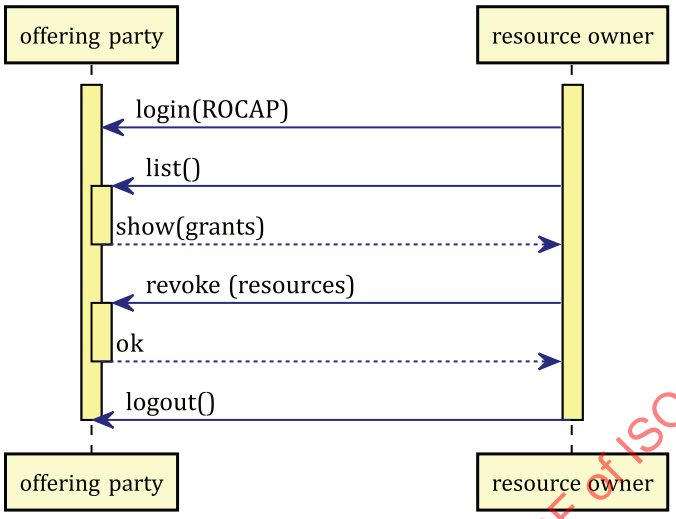

Figure 12 — Revoking access to resources

Figure 12 shows the process for the resource owner revoking access. The resource owner authenticates at the offering party by its ROCOP (ISO 20078-1). Afterwards the resource owner is able to list all grants on resources and is able to revoke a **selected** granted access on resources of an accessing party.

The revocation of access to resources is validated against the resource owner and it can be validated against the accessing party. During the next request for access, the accessing party immediately receives a notification of the revoked access by the offering party. The notification can be a response status code, e.g. a HTTP 403 "Forbidden" (ISO 20078-2).

5.3 Containers

5.3.1 Creation of a container

The following subclauses define the processes for creating and deleting containers by an accessing party or offering party, additionally granting, rejecting, ignoring as well as revoking access on resources grouped by containers.

Containers (ISO 20078-1) can be created out of a superset of resources with the container management API (ISO 20078-2).

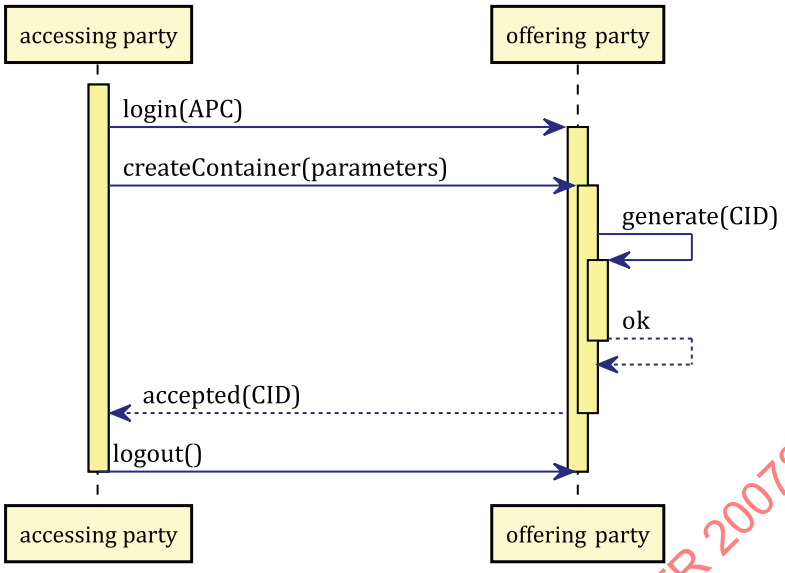

Figure 13 — Creating a container

Figure 13 displays the process for creating a container (ISO 20078-1) by the accessing party. The generated ContainerID (CID) and related internal parameters are stored at the offering party. The CID is passed securely to the accessing party and used for the purpose of container management.

The accessing party can repeat the process of Figure 13 or repeat it in parts [e.g. only createContainer(..)] by N times.

5.3.2 Deletion of a container

An accessing party can delete a certain container using its ContainerID by the following process.

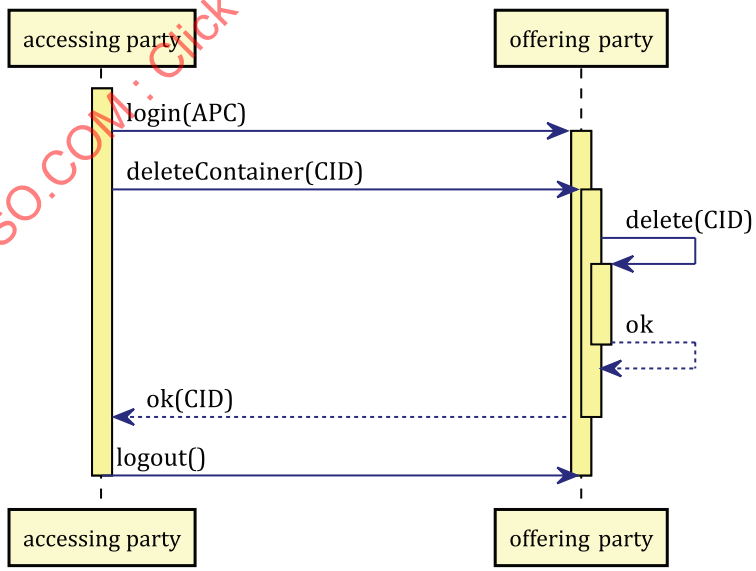

Figure 14 — Deleting a container

In Figure 14 the accessing party authenticates, is authorized, and selects or sends the CID (ISO 20078-1) to the offering party, indicating a request to delete the selected container. The offering party uses the transmitted CID to identify the container to be deleted.

The accessing party can repeat the process, or the relevant part deleteContainer(), of Figure 14; to delete more than one container.

5.3.3 Grant access to resources grouped by a container

After the creation of a certain container, the accessing party requests access permission (consent by resource owner) to the grouped resources. If resources are not anonymized, accessing party provides one or multiple vehicle identifiers. Connecting a vehicle with VIN(s) to a container allows the offering party to identify the resource owner and to request access permission for the given vehicle identifier, container resources, defined purpose and accessing party. It is possible for the resource owner to use the client application of the accessing party to initiate a grant. But to confirm and manage grants, the resource owner uses the client application of the offering party (see Figure 15).

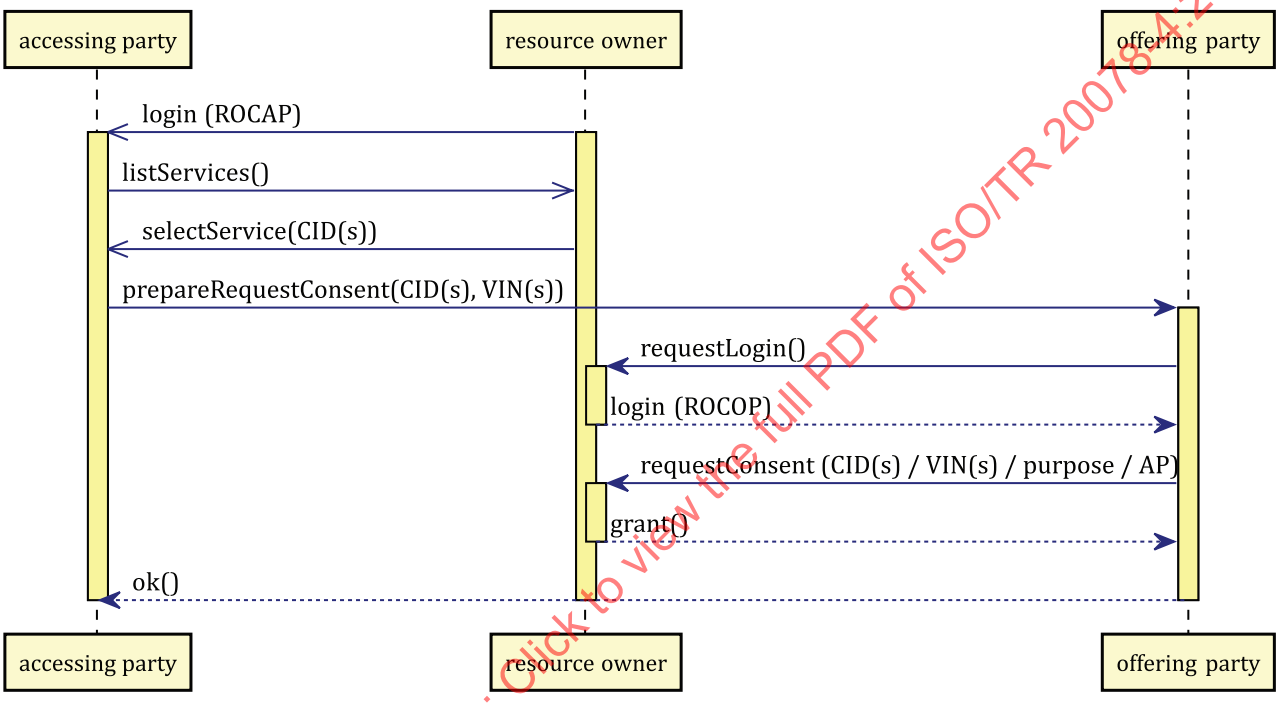

Figure 15 — Granting access to containers

Figure 15 shows the process for granting access to containers 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 accessing party side, these are the ROCAP credentials, and for the offering party these are the ROCOP (ISO 20078-1) credentials.

After authentication at the offering party, the resource owner checks the name and the purpose of the container, name of the accessing party, provided vehicle identifiers (VINs) as well as the covered resources to be granted.

The process of Figure 15 can be simplified to an implicit grant.

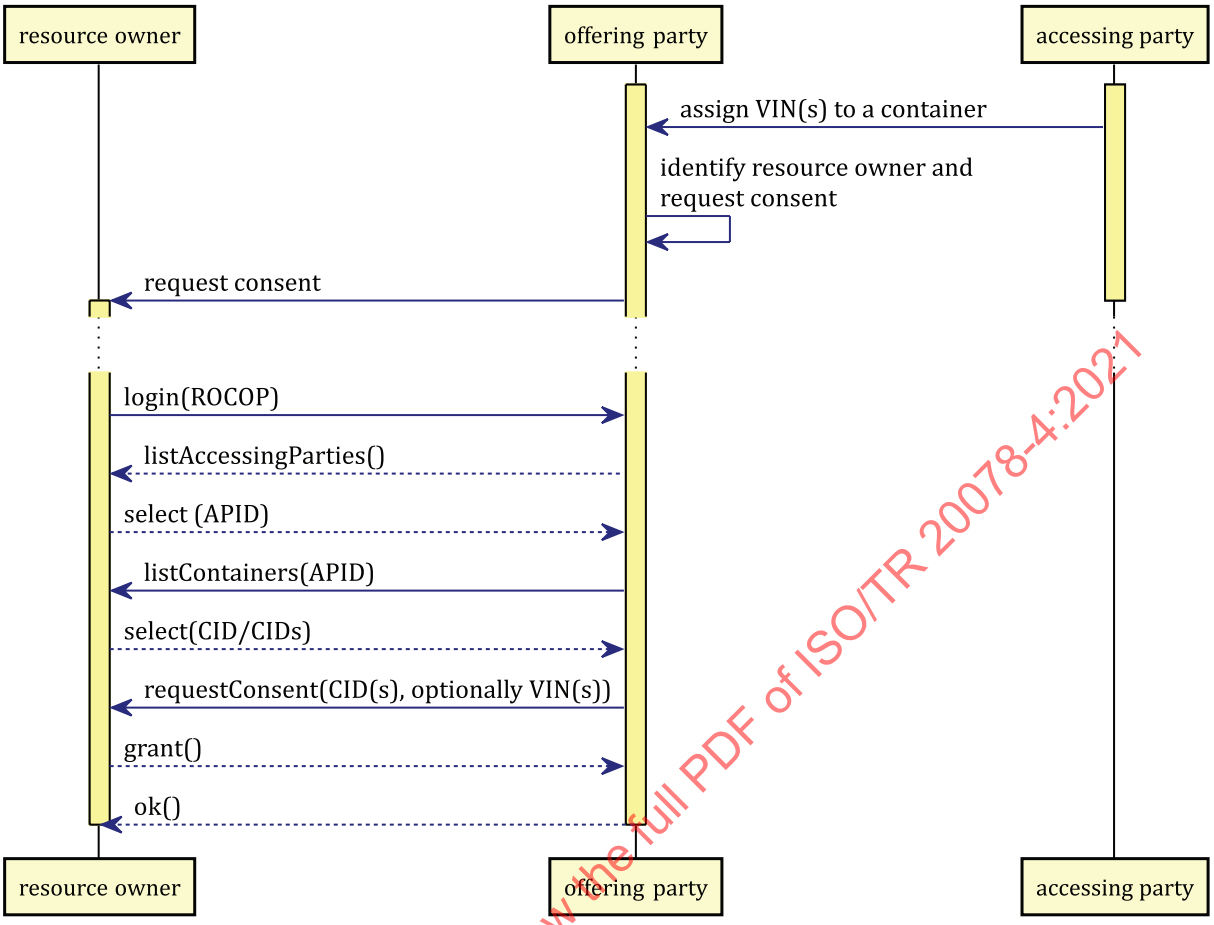

Figure 16 — Implicitly granting access to resources grouped by containers

Figure 16 shows the process for implicitly granting access to containers by the resource owner at the offering party. Based on assigned vehicle identifier to a container, offering party identifies the resource owner in order to request access to related resources.

The resource owner starts at the offering party and authenticates using their ROCOP (ISO 20078-1) credentials. After authentication, the resource owner selects an accessing party from the list. Next, the available container(s) are listed, where the resource owner selects from for granting. The offering party requests access consent to the selected container(s) and optionally vehicle resources for the selected accessing party. The resource owner grants this request.

NOTE 1 The accessing party is not (necessarily) in an active participating in the granting process of Figure 16 after assignment of vehicle identifier to a container.

NOTE 2 For not anonymized resources, consent is requested for specific vehicle identifiers (VINs).

NOTE 3 The process of Figure 17 follows after the process of Figure 16.

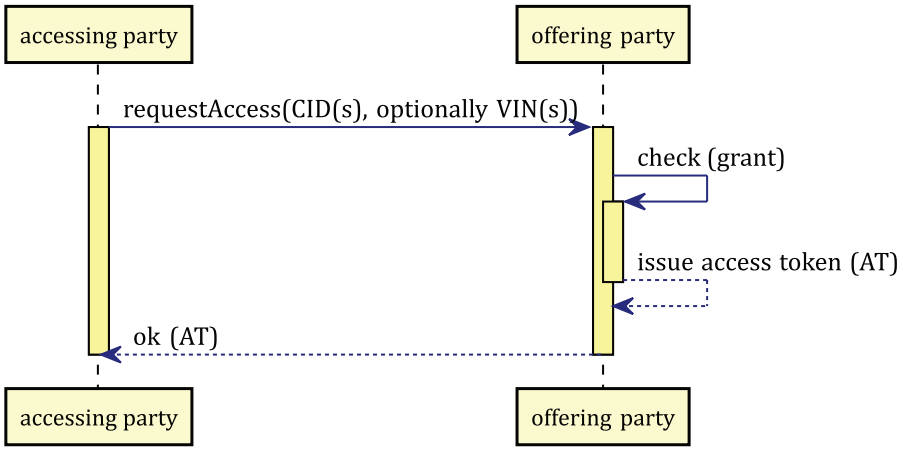

Figure 17 — Requesting access to resources

Figure 17 completes the implicit granting of Figure 16. The accessing party is requesting access to resources grouped by containers and providing vehicle identifiers (VINs) for not anonymized resources. The offering party checks the given consent (grant) for this request. If the request can be validated, an access token (AT; ISO 20078-1) is issued and transferred to the accessing party. This AT allows the accessing party to access resources at the resource provider (ISO 20078-3).

5.3.4 Reject access to containers

The resource owner could also deny the request for access permission of the accessing party.

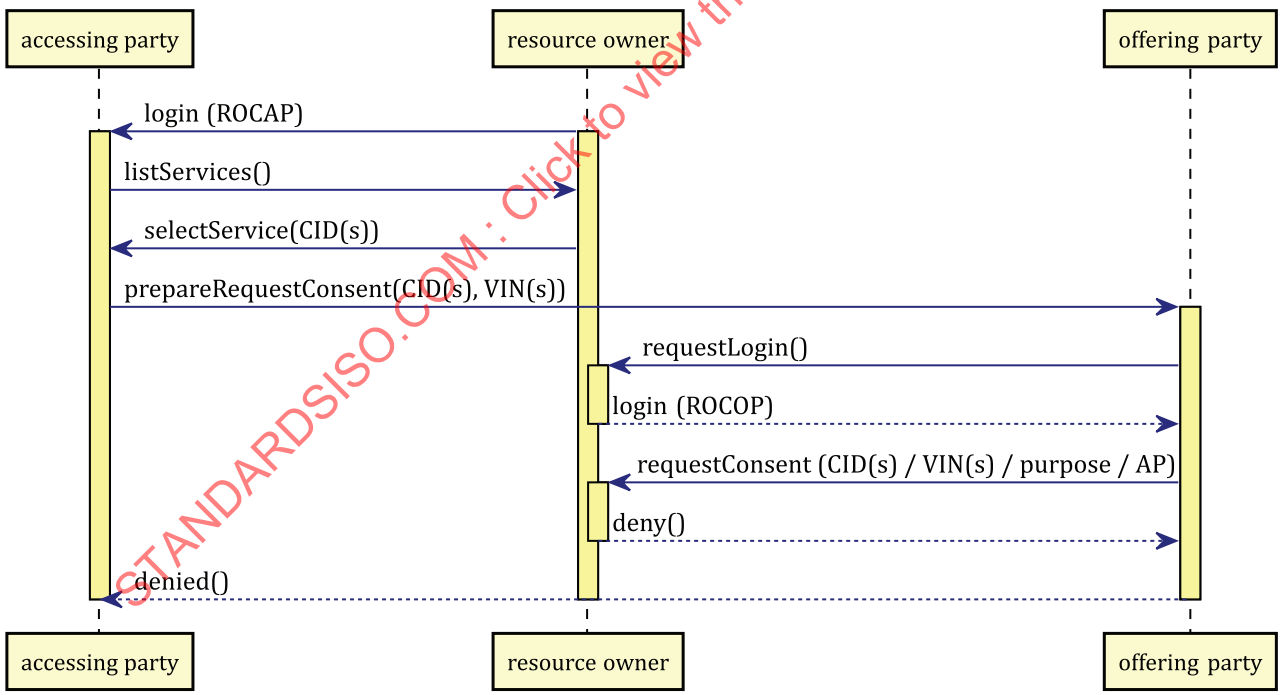

Figure 18 — Denying access to resources grouped by containers

Figure 18 displays the process for requesting access consent for access on resources grouped by containers and related to provided vehicle identifiers (VINs) that is denied by the resource owner at the offering party.

5.3.5 Ignore access request to containers

As shown by Figure 15 for granting access, the resource owner could also ignore the request for access consent to resource grouped by a container.

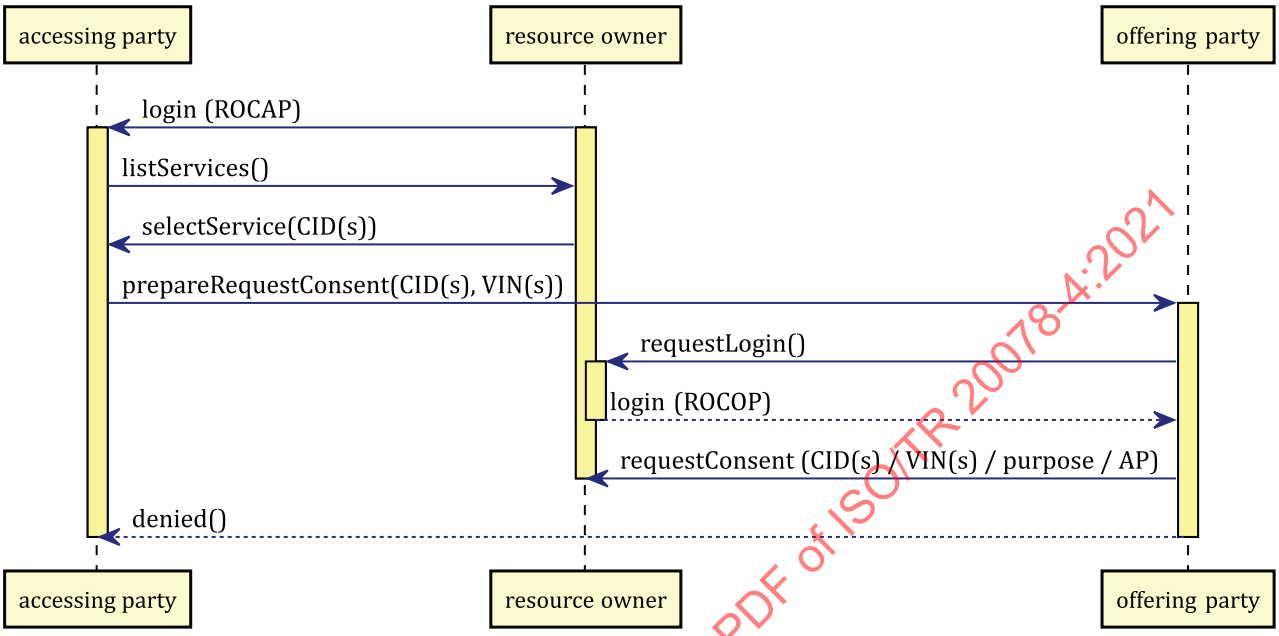

Figure 19 — Ignoring access request to resource grouped by containers

Figure 19 displays the process for requesting consent to access resources grouped by a container that is ignored by the resource owner at the offering party. It is possible for the resource owner to support its ROCOP (ISO 20078-1) towards the offering party but neither grant nor reject the request for access. The offering party sets a time out (or time to live) interval that automatically rejects the request for consent towards the accessing party after a certain time period.

5.3.6 Revoke access to containers

It is important that the resource owner is able to revoke a granted access to resources grouped by containers at the offering party.

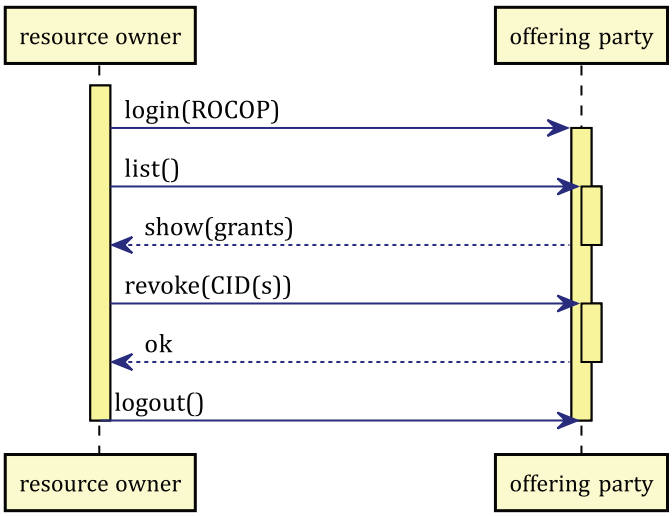

Figure 20 — Revoking access to resources grouped by containers

Figure 20 shows the process for the resource owner revoking access. The resource owner authenticates at the offering party by its ROCOP (ISO 20078-1). The resource owner is able to list all containers which relate to the granted access to resources. The resource owner revokes a granted access(es) by selecting a container.

The revocation of access to resources grouped by containers can be validated by the accessing party. During the next request for access, the accessing party immediately receives a notification of the revoked access by the offering party. The notification can be a response status code, e.g. HTTP 403 “Forbidden” (ISO 20078-2).

5.4 Resource access

5.4.1 Access

After being granted access, it is possible for the accessing party to request resources; see Figure 21. The accessing party accesses a resource URI by providing the access token containing the containerID, to retrieve data.

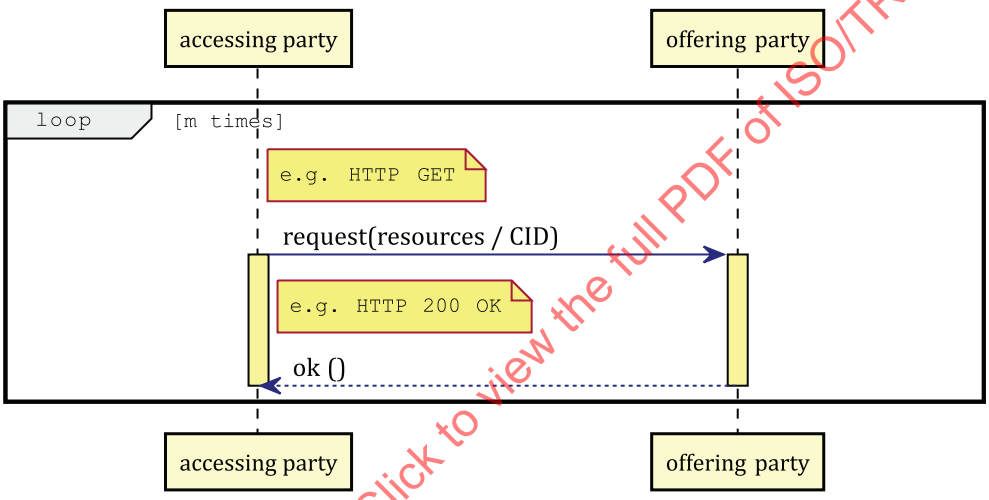

Figure 21 — Access to resources by the accessing party at the offering party

5.4.2 No access

The accessing party requests access to resources, where the access is either pending, ignored, denied or revoked by the resource owner. Such request is directly denied by the offering party.