TECHNICAL REPORT

ISO/TR 23791

First edition
2019-09

Road vehicles — Extended vehicle (ExVe) web services — Result of the risk assessment on ISO 20078 series

Véhicules routiers — Web services du véhicule étendu (ExVe) — Résultats de l'évaluation des risques de la série de normes ISO 20078

Reference number
ISO/TR 23791:2019(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*.

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

The ISO 20078 series specifies a possible web service to implement a certain web interface of the Extended Vehicle, depending on the concerned use case.

The development of this series has revealed several fears about possible risks related to safety, security, competition, liability, and data protection that may originate from that interface.

To address these fears, a list of criteria was first developed to be considered independently of the considered interface. This list is the object of ISO/TR 23786.

This list was then used for assessing the risks originating from the ISO 20078 series and concept to issue this document.

Finally, the risk assessment demonstrated that there are no risks resulting from the ISO 20078 series itself, however, there may be risks resulting from an implementation of that series.

Road vehicles — Extended vehicle (ExVe) web services — Result of the risk assessment on ISO 20078 series

1 Scope

This document presents the assessment of the safety, security, competition, responsibilities, and data protection risks that can originate from the ISO 20078 series.

In particular, the following risks are outside the scope of this assessment, because they relate to elements that are excluded from the scope of the ISO 20078 series:

— the risks associated with the implementation of the ISO 20078 series;

— the risks associated with the process that the accessing parties or any other parties would later on use to communicate the information they obtained;

— the risks associated with the process used by the resource owner to provide, modify, or revoke their authorization to pass information;

— the risks associated with the mitigation of the risks, should such a mitigation be necessary.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 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 http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1.1
accessing party
entity which accesses *resources* (3.1.8) via *web services* (3.1.11)

[SOURCE: ISO 20078-1:2019, 3.1.6, modified — Notes to entry have been deleted.]

3.1.2
authorization provider
entity at the *offering party* (3.1.7) that manages the access rights to resources and *resource owner* (3.1.9) information

[SOURCE: ISO 20078-1:2019, 3.1.9, modified —Note 1 to entry has been deleted.]

3.1.3
extended vehicle
ExVe
entity, still in accordance with the specifications of the vehicle manufacturer, that extends beyond the physical boundaries of the road vehicle and consists of the road vehicle, off-board systems, external interfaces, and the data communication between the road-vehicle and the off-board systems

[SOURCE: ISO 20077-1:2017, 3.5, modified — Note 1 to entry has been deleted.]

3.1.4
ExVe manufacturer
vehicle manufacturer responsible for the *extended vehicle* (3.1.3)

[SOURCE: ISO 20077-1:2017, 3.6]

3.1.5
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.

[SOURCE: ISO 20078-1:2019, 3.1.7, modified —Note 2 to entry has been deleted.]

3.1.6
intermediate body
party that manages the authorizations given by the *resource owner* (3.1.9) to communicate resources to the *accessing party* (3.1.1) via *web service* (3.1.11)

3.1.7
offering party
entity who provides *web services* (3.1.11) access to *resources* (3.1.8)

[SOURCE: ISO 20078-1:2019, 3.1.3.]

3.1.8
resource
data, aggregated information or functionalities of the connected vehicle

[SOURCE: ISO 20078-1:201, 3.2.1, modified —Note 1 to entry has been deleted.]

3.1.9
resource owner
responsible party for the *resource(s)* (3.1.8)

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.

[SOURCE: ISO 20078-1:2019, 3.1.4.]

3.1.10
resource provider
entity at the *offering party* (3.1.7) that protects and provides *resources* (3.1.8)

[SOURCE: ISO 20078-1:2019, 3.1.8.]

3.1.11
web service
software system, with an interface described in a machine-processable format, and designed to support interoperable machine-to-machine interaction over a network

[SOURCE: ISO 20077-1:2017, 3.21.]

3.2 Abbreviated terms

ExVe Extended Vehicle

VM Vehicle Manufacturer

4 General result of the risk assessment

This document presents a risk assessment of the ISO 20078 series. This means it intends to answer to the following question: "Does the ISO 20078 series generate any safety, security, competition, responsibility, liability, or data protection risks?"

The answer is NO: The ISO 20078 series does not generate any safety, security, competition, responsibility, liability, or data protection risks.

Nevertheless, the risk assessment did not consider the manner the ISO 20078 series is implemented. Therefore, there may be safety, security, competition, responsibility, liability, or data protection risks resulting from implementation.

It is therefore recommended to conduct a risk assessment by the vehicle manufacturer on safety, security, competition, responsibility, liability, or data protection for the individual implemented solution.

5 Categories of the assessed risks

In this document, the risks that have been assessed are the one listed in ISO/TR 23786. They are regrouped as follows:

— safety risks: risks related to the safety of persons and goods during the vehicle life cycle;

— security risks: risks associated to the security of the vehicle communication system;

— competition risks: risks associated to the fair competition among the concerned actors;

— responsibility and liability risks: risks related to the responsibility and liability of the concerned actors;

— data protection risks: risks related to the protection of the resources owned by the resource owner.

More precisely, the assessment results from the answer to the following question: "Can the ExVe web service interface, when designed according to the ISO 20078 series for a certain use case, present safety, security, competition, responsibility, liability, or data protection risks originating from that series?"

The risks resulting from the implementation of the ISO 20078 series are excluded from the assessment. In particular, when implementing the ISO 20078 series, the ExVe manufacturer will design all the arbitration mechanisms, including the mechanisms aiming at mitigating the risks. To address these risks the ExVe manufacturer is invited to apply the design methodology specified in ISO 20077-2.

6 Assessment of the risks related to the safety of the persons and the goods during the ExVe life cycle

6.1 Safety risks considered

"Can the ExVe web service interface, when designed according to the ISO 20078 series for a certain use case, present safety risks originating from that series?"

The safety risks considered for this assessment are the following:

— overload safety risks that are not resulting from cybersecurity issues or problems:
  — SAFE 1. Possible overload of the electronic system of the moving vehicle (numerous simultaneous requests);
  — SAFE 2. Possible overload of the electronic system of the moving vehicle (frequent requests);
  — SAFE 3. Possible overload of the electronic system of the moving vehicle (unexpected requests);
  — SAFE 4. Possible illicit or malicious remote control of vehicles;
  — SAFE 5. Lack of compatibility with the existing systems and mechanisms;
  — SAFE 6. Failures of the remote communication solution itself of the ExVe (including the VM back-end server when applicable);
  — SAFE 7. Lack of consideration of the complete vehicle life cycle;
  — SAFE 8. Risks related to the design validation process;
  — SAFE 9. Lack of misuse prevention;
— safety risks that are resulting from cybersecurity issues or problems:
  — SAFE 10. Lack of, or inappropriate measures aiming at reducing the risks in case of illicit or malicious remote control of vehicles;
  — SAFE 11. Other safety risks resulting from cybersecurity issues or problems.

NOTE In these two lists the electronic system encompasses both the hardware and the software.

6.2 Analysis of the situation presented by the ISO 20078 series

6.2.1 SAFE 1: Possible overload of the electronic system of the moving vehicle (numerous requests)

To the question:

“Does the ISO 20078 series generate safety risks related to a possible overload of the electronic system of the moving vehicle in the case of several requests at the same time?”

The answer is NO.

The safety risks related to a possible overload of the electronic system of the moving vehicle in the case of several requests at the same time are only related to the implementation of the ISO 20078 series.

The series reduces these risks because it introduces the interface at the backend server of the manufacturer. However, the ISO 20078 series does not provide any recommendation regarding that implementation. It is suggested that the ISO 20078 series could recommend designing this implementation according to the methodology specified in ISO 20077-2.

The detailed analysis addressing this question can be found in Annex A.

6.2.2 SAFE 2: Possible overload of the electronic system of the moving vehicle (frequent requests)

To the question:

“Does the ISO 20078 series generate risks related to highly frequently repeated requests?”

The answer is NO.

The safety risks related to a possible overload of the electronic system of the moving vehicle in the case of frequently repeated requests are only related to the implementation of the ISO 20078 series.

The series reduces these risks because it introduces the interface at the backend server of the manufacturer. However, the ISO 20078 series does not provide any recommendation regarding that implementation. It is suggested that the ISO 20078 series could recommend designing this implementation according to the methodology specified in ISO 20077-2.

The detailed analysis addressing this question can be found in Annex A.

6.2.3 SAFE 3: Possible overload of the electronic system of the moving vehicle (unexpected requests)

To the question:

"Does the ISO 20078 series generate risks related to unexpected requests?"

The answer is NO.

The safety risks related to a possible overload of the electronic system of the moving vehicle in the case of unexpected requests are only related to the implementation of the ISO 20078 series.

The ISO 20078 concept, by introducing the web-service communication via the back-end server of the vehicle manufacturer, enables a possible substantial reduction of these risks, should the vehicle manufacturer appropriately design this backend server.

It is recommended unexpected requests be denied. However, the ISO 20078 series does not provide any such recommendation. It is suggested that the ISO 20078 series could recommend designing this implementation according to the methodology specified in ISO 20077-2.

The detailed analysis addressing this question may be found in Annex A.

6.2.4 SAFE 4: Possible illicit or malicious remote control of vehicles

To the question:

"Does the ISO 20078 series prohibit illicit or malicious remote control of vehicles, or an illicit or malicious remote activation of systems and components? Actively?"

The answer is NO.

The safety risks related to a possible illicit or malicious remote control of vehicles, or an illicit or malicious remote activation of systems and components are only related to the implementation of the ISO 20078 series.

The ISO 20078 concept, by introducing the web-service communication via the back-end server of the vehicle manufacturer, enables a possible substantial reduction of these risks, should the vehicle manufacturer appropriately design this backend server.

However, the ISO 20078 series introduces concepts that may facilitate the introduction of mechanisms aiming at actively preventing or limiting uncontrolled or malicious remote take of control of vehicles, or an uncontrolled or malicious remote activation of systems and components.

The detailed analysis addressing this question can be found in Annex A.

6.2.5 SAFE 5: Lack of compatibility with the existing systems and mechanisms

To the question:

"Does the ISO 20078 series generate risks related the lack of compatibility with the existing design of the vehicle?"

The answer is NO.

To the question:

“Does the ISO 20078 concept address the risks related to the lack of compatibility with the existing design of the vehicle?”

The answer is YES.

The ISO 20078 concept, by introducing the web-service communication via the back-end server of the vehicle manufacturer, enables a possible substantial reduction of these risks, should the vehicle manufacturer appropriately design this backend server.

The detailed analysis addressing this question can be found in Annex A.

6.2.6 SAFE 6: Failures of the remote communication solution itself of the ExVe (including the back-end system of the manufacturer)

To the question:

“Does the ISO 20078 series generate safety risks in the case when e.g. the back-end server is down (internal failures, hacking, etc…)?”

The answer is NO.

The detailed analysis addressing this question can be found in Annex A.

6.2.7 SAFE 7: Lack of consideration of the complete ExVe life cycle

To the question:

“Does the ISO 20078 series generate safety risks related to requests that are inappropriate in the actual life cycle phase of the running vehicle?”

The answer is NO.

However, such safety issues may occur in the case of a dysfunction of the processes informing the authorization provider of a change of the life cycle stage (manufacturing, sales, operation, maintenance and repair, end of life).

The detailed analysis addressing this question can be found in Annex A.

6.2.8 SAFE 8: Risks related to the design validation process

To the question:

“Does the ISO 20078 series generate safety risks related to the validation of the design process and its traceability?”

The answer is NO.

The detailed analysis addressing this question can be found in Annex A.

6.2.9 SAFE 9: Lack of misuse prevention

To the question:

“Does the ISO 20078 concept permit a limitation of the passed information to avoid safety issues?”

The answer is YES.

To the question:

"Does the ISO 20078 series specify or recommend a limitation of the passed information to avoid safety issues?"

The answer is NO.

Addressing the issue is left by the ISO 20078 series to external actors (for example those involved at the implementation stage of the series or at the specification of the considered use-cases).

The detailed analysis addressing this question can be found in Annex A.

6.2.10 SAFE 10: Lack of, or inappropriate measures aiming at reducing the risks in case of illicit or malicious remote control of vehicles

To the question:

"Does the ISO 20078 series contain mechanisms or processes reducing the safety risks presented by a remote control"?

The answer is YES.

However, the ISO 20078 series only partially addresses these risks because, while there is no guarantee that the accessing party is free from impersonation risks (e.g. ID theft upstream its own accessing request), the ISO 20078 series does not contain any recommendation for considering and possibly limiting these risks (out of scope).

The ISO 20078 concept, by introducing the web-service communication via the back-end server of the vehicle manufacturer, enables a possible substantial reduction of these risks, should the vehicle manufacturer appropriately design this backend server.

The detailed analysis addressing these questions can be found in Annex A.

6.3 Conclusion: Assessment of the safety risks possibly originating from the ISO 20078 series

The analysis of the ISO 20078 series regarding the possible safety risks considered in this document have permitted to demonstrate:

— that the ISO 20078 concept per se, by introducing the concept of communicating via the back-end server of the manufacturer, enables the vehicle manufacturer to endorse its full responsibility for ensuring the safety of the persons and the goods during the ExVe life cycle;

— that the ISO 20078 series does not generate any risk relative to the persons and the goods during the ExVe life cycle;

— that some of the risks relative to the safety of the persons and the goods are related to the way the ISO 20078 series is implemented (see e.g. the arbitration mechanisms) and not to the ISO 20078 series per se (it has not been possible to find a safety risk originating from the ISO 20078 series itself);

— that the ISO 20078 series does not address these implementation risks; in particular, the ISO 20078 series does not recommend any measure that may help preventing these risks, such as, but not limited to the use of the design methodology specified in ISO 20077-2 for designing this implementation.

7 Assessment of the risks associated to the security of the ExVe communication system

7.1 Security risks considered

"Can the ExVe web service interface, when designed according to the ISO 20078 series, present security risks originating from the series?"

The security risks considered for this assessment are the following:

— SEC 1. Risks related to integrity and authenticity;

— SEC 2. Risks at vehicle systems that are not located at the moving vehicle;

— SEC 3. Risks related to the consequences of a complete or partial cybersecurity breach (this includes safety, security, competition, confidentiality and data protection risks);

— SEC 4. Lack of misuse prevention measures.

7.2 Analysis of the situation presented by the ISO 20078 series

7.2.1 General considerations relative to the specification of the OAuth2 framework

The ISO 20078 series specifies that the web service interface shall be designed according to the OAuth2 framework. This may be considered as the major contribution of the series to address the security risks according to the 2018 state-of-the-art.

ISO 20078-3 references several cyber-security guidelines and relevant material for considering the security risks.

The detailed analysis addressing this question can be found in Annex B.

7.2.2 General consideration related to cybersecurity

To the question:

"Does the ISO 20078 series address the 2018 state-of-the-art cybersecurity risks?"

The answer is YES.

The ISO 20078 series addresses the 2018 state-of-the-art cybersecurity risks. Nevertheless, due to its scope, the ISO 20078 series does not address the state-of-the-art cybersecurity risks at all stages of the communication between the vehicle and the service provider who is directly in contact with the vehicle operator.

Recommending (without requiring) the ExVe manufacturer that implements the ISO 20078 series to design this implementation according to the ISO 20077-2 methodology may help better addressing the cybersecurity risks.

The detailed analysis addressing this question can be found in Annex B.

7.2.3 SEC 1: Risks related to integrity and authenticity

To the question:

"Does the solution prevent the manipulation of the system (e.g. regarding integrity and authenticity)?"

The answer is YES.

However, the final level of integrity and authenticity, that involves all actors in the process, is conditioned by implementation of the ISO 20078 series.

The detailed analysis addressing this question can be found in Annex B.

7.2.4 SEC 2: Security risks at vehicle systems that are not located at the moving vehicle

To the question:

"Does the ISO 20078 series address security risks at other places than the vehicle itself?"

The answer is YES.

The ISO 20078 series addresses the security risks related to the communication between the back-end server of the manufacturer and the accessing party.

To the question:

"Does the ISO 20078 series address all security risks at other places than at the vehicle itself?"

The answer is NO.

The ISO 20078 series only specifies a web service solution at the back-end server of the manufacturer. The off-board components of the extended vehicle (including the back-end system itself) as well as the equipment of the accessing parties are outside the scope of the ISO 20078 series.

There may be security risks related to these components but the manner to address them is outside of the scope of the ISO 20078 series.

The detailed analysis addressing this question can be found in Annex B.

7.2.5 SEC 3: Risks related to the consequences of a complete or partial cybersecurity breach (this includes safety, security, competition, confidentiality and data protection risks)

To the question:

"Does the ISO 20078 series include measures that limit the consequences of a security breach?"

The answer is YES.

These measures are mainly specified in ISO 20078-2.

The detailed analysis addressing this question can be found in Annex B.

7.2.6 SEC 4: Lack of misuse prevention measures

To the question:

"Does the ISO 20078 series include misuse prevention measures?"

The answer is YES.

This answer is primarily based on the fact that the ISO 20078 series is based on the OAuth2 framework, but there are also important other technical measures that complete this assertion.

The detailed analysis addressing this question can be found in Annex B.

7.3 Conclusion: Assessment of the security risks possibly originating from the ISO 20078 series

The analysis of the ISO 20078 series regarding the possible security risks considered in this document have permitted to demonstrate:

— that the ISO 20078 series mainly addresses the security risks by specifying the OAuth2 framework;

— that the ISO 20078 series does not address nor provide any recommendation for addressing the security risks related to its implementation and to the components or communication systems outside its scope.

8 Assessment of the risks associated to the fair competition among the concerned actors

8.1 Competition risks considered

"Can the ExVe web service interface, when designed according to the ISO 20078 series for a certain use case, present competition risks originating from the series?"

The competition risks considered for this assessment are the following:

— FAIR 1. Possible misuse of the acquired knowledge;

— FAIR 2. Possible gaining of unique knowledge of the market through monitoring;

— FAIR 3. Possible gaining of unique knowledge of the customer's behaviour through monitoring;

— FAIR 4. Competition risks among the involved parties;

— FAIR 5. Risk of excluding competitors from playing roles;

— FAIR 6. Risks related to the development of new after-sales applications;

— FAIR 7. Competition risks among manufacturers.

8.2 Analysis of the situation presented by the ISO 20078 series

8.2.1 Involved actors

To address these risks, it should be first considered who are the involved parties that can be affected by an unfair competition situation. This is illustrated in Figure 1.

As the ISO 20078 series is fundamentally based on the OAuth2 process to secure the communication according to the 2018 state-of-art, the ExVe manufacturer is always resource provider, authorization provider, and in case of the personal data of the resource owner also identity provider. The difference between the two cases illustrated in Figure 1 lies in the magnitude of the authorization managed by the vehicle manufacturer in its role of authorization provider.

The ISO 20078 series mainly focuses on the case when the full authorization role is given to the vehicle manufacturer (see example in green in Figure 1). In this case, it verifies for each and every request that the resource owner has authorized to provide the requested information to the concerned party(ies) and under the actual circumstances.

The ISO 20078 series is also fully compatible with use-cases where the main authorization role is given to one or several intermediate bodies (see example in red in Figure 1). In the example of Figure 1 the ExVe manufacturer only knows for each and every request who is the intermediate body, what is the information that is requested. It only verifies that the resource owner has authorized the concerned intermediate body

to receive information. Such use-cases are nevertheless not technically described in the ISO 20078 series and may be additionally defined by a description/specification for an intermediate body.

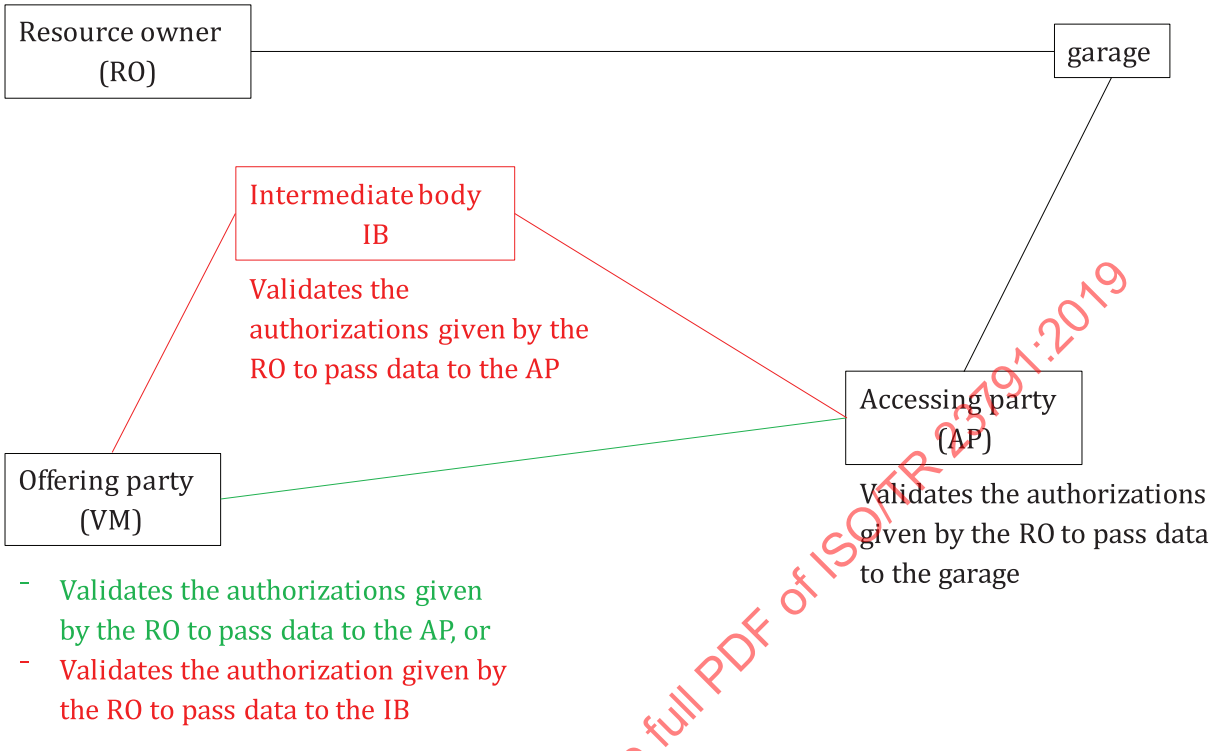

Figure 1 — Two communication cases: With and without an intermediate body

8.2.2 FAIR 1: Possible misuse of the acquired knowledge

To the question:

"Does the ISO 20078 series generates or address competition risks related to the ability for any of the involved parties to misuse the data they have knowledge of due to their role(s) in the specified process?"

The answer is NO.

The detailed analysis addressing this question can be found in Annex C.

8.2.3 FAIR 2: Possible gaining of unique knowledge of the market through monitoring

To the question:

"Does the ISO 20078 series generate or address competition risks because, through monitoring, the ExVe manufacturer gains unique knowledge of the market (for a certain, e.g. brand specific, after-sales service)?"

The answer is NO.

The ISO 20078 series neither generates nor addresses the considered competition risk. This risk is related to the manner the ExVe manufacturer implements the ISO 20078 series. This risk is not limited to the ExVe manufacturer.

The detailed analysis addressing this question can be found in Annex C.

8.2.4 FAIR 3: Possible gaining of unique knowledge of the customer's behaviour through monitoring

To the question:

"Does the ISO 20078 series generate or address competition risks because, through monitoring, the ExVe manufacturer gains unique knowledge of the customer's behaviour?"

The answer is NO.

The ISO 20078 series neither generates nor addresses the considered competition risk. This risk is related to the manner the ExVe manufacturer implements the ISO 20078 series. This risk is not limited to the ExVe manufacturer.

In fact, the risk is not specific to the ISO 20078 series because, through monitoring, several competing parties may have a unique knowledge of the customer's behaviour.

The detailed analysis addressing this question can be found in Annex C.

8.2.5 FAIR 4: Competition risks among the involved parties

To the question:

"Does the ISO 20078 series generate or address competition risks among the actors involved in the series?"

The answer is NO.

The ISO 20078 series neither generates nor addresses competition risks among the actors involved in the series. These risks are linked with:

— the manner the ExVe manufacturer implements the ISO 20078 series, and

— the manner the accessing party and/or the intermediate body manage the knowledge they may have acquired through monitoring.

The detailed analysis addressing this question can be found in Annex C.

8.2.6 FAIR 5: Risk of excluding competitors from playing roles

To the question:

"Does the ISO 20078 series exclude competitors from the market place to become, e.g. authorization provider, without technical justifications?"

The answer is NO.

The ISO 20078 series does not preclude any party to be an intermediate body and to have accordingly access to the competition sensitive information.

The detailed analysis addressing this question can be found in Annex C.

8.2.7 FAIR 6: Risks related to the development of new after-sales applications

To the question:

"Does the ISO 20078 series impact the competition risks among the parties aiming at the development of similar but different applications?"

The answer is NO.

To the question:

"Does the ISO 20078 series impact the competition risks related to the availability in a non-discriminatory manner of information that is necessary for developing new services and that has not yet been made available?"

The answer is NO.

The ISO 20078 series is not impacting these risks.

The detailed analysis addressing this question can be found in Annex C.

8.2.8 FAIR 7: Competition risks among manufacturers and/or vehicle components (systems) suppliers

To the question:

"Does the ISO 20078 series generate risks related to the competition among vehicle manufacturers and/or vehicle components (systems) suppliers?"

The answer is NO.

To the question:

"Does the ISO 20078 series generate risks of communicating private know-how data without the full agreement of its owner (vehicle or system manufacturers, suppliers, etc.)?"

The answer is NO.

The ISO 20078 series is nevertheless impacting these risks because it introduces provisions that can permit the safeguard of the private know-how data of the vehicle manufacturer or component suppliers.

The detailed analysis addressing this question can be found in Annex C.

8.3 Conclusion: Assessment of the competition risks possibly originating from the ISO 20078 series

The analysis of the ISO 20078 series regarding the possible competition risks considered in this document have permitted to demonstrate:

— that most of these risks are related to the way the ISO 20078 series is implemented and not to the series per se (it has not been possible to find a competition risk originating from the series itself);

— that, while the ISO 20078 series does not address the implementation process, the ISO 20078 series neither recommends any measure that may help preventing the competition risks originating from that implementation. One possible option to do it would be to recommend the use of the design methodology specified in ISO 20077-2.

It has also been demonstrated that if several of the competition risks are related to the manufacturer behaviour, these risks are also very much related to the behaviour of the other actors, in particular of the accessing party or, when present in the process, the intermediate bodies.

9 Assessment of the risks related to the responsibility of the concerned actors

9.1 Liability and responsibility

Liability is a concept that is either connected to legislation or connected to business agreements but that is always based on a principle of responsibility.

Therefore, this document reports about the assessment of the risks that are related to the responsibility of the concerned actors and may potentially lead to liability risks, as follows:

— RESP 1. Does the ISO 20078 series introduce responsibilities without allocating them to any identified party?

— RESP 2. Does the ISO 20078 series confuse the share of responsibilities?

9.2 Analysis of the situation presented by the ISO 20078 series

The ISO 20078 series specifies a web service interface of an Extended Vehicle, where the requested resource is provided by the back-end server of the manufacturer to the accessing party.

Through this interface, there is no direct connection between the accessing or intermediate parties and the vehicle. In the ISO 20078 concept, the responsibility for getting information from the vehicle is not shared and solely allocated to the ExVe manufacturer. One can thereby consider that the ISO 20078 concept itself prevents potential responsibility issues regarding the design and the manufacture of the extended vehicle.

The ISO 20078 series, and particularly ISO 20078-1, specifies who are the actors and which are their roles. These roles are not overlapping.

Details of this analysis can be found in Annex D.

9.3 Conclusion: Assessment of the risks related to the responsibility of the concerned actors possibly originating from the ISO 20078 series

The analysis of the ISO 20078 series regarding the possible risks related to the responsibility of the concerned actors and considered in this document have permitted to demonstrate:

— that the ISO 20078 concept potentially prevents some responsibility risks because the responsibility for getting information from the vehicle is not shared and solely allocated to the ExVe manufacturer;

— that the ISO 20078 series specifies roles and responsibilities and systematically allocate them to a defined party;

— that the ISO 20078 series never introduces confusion in the share of responsibilities.

The ISO 20078 series however strictly addresses responsibilities within its scope and does not address responsibilities for the parts of the communication process that is located outside of that scope.

10 Assessment of the risks related to the protection of the resources owned by the resource owner (data protection)

10.1 Data protection risks considered

"Can the ExVe web service interface, when designed according to the ISO 20078 series for a certain use case, present risks related to the protection of the resources own by the resource owner (data protection)?"

The data protection risks considered in the risks assessment are the following:

— PROT 1. Negative impact on the ability of the resource owner to decide on the transmitted information;

— PROT 2. Negative impact on the ability for the resource owner to select/reject any of the involved parties (accessing party, service provider, etc.);

— PROT 3. Negative impact on the ability for the resource owner to permit/reject in a timely manner communication depending on the circumstances;

— PROT 4. Negative impact on the ability for the resource owner to select/reject different parties for different use-cases;

— PROT 5. Negative impact on the ability for the resource owner to monitor the information requests made on his behalf;

— PROT 6. Negative impact on the possibility to limit the passed information to permit protection of data privacy (data misuse prevention).

10.2 Analysis of the situation presented by the ISO 20078 series

The ISO 20078 series specifies a web service interface of an extended vehicle, where the requested resource is provided by the back-end server of the manufacturer to the accessing party or to an intermediate body between the extended vehicle and the accessing party for a certain use case.

This communication is based on the OAuth2 framework, where an authorization provider controls that the resource (data) owner has effectively authorized the concerned resource (data) to be communicated to the requesting party under the given circumstances. Once this verification made, the authorization provider enables the communication itself by emitting a token to the accessing party.

The ISO 20078 series focuses on the main case where a direct communication exists between the back-end server of the manufacturer and the accessing party or intermediate body. In that case the vehicle manufacturer has been informed of the complete set of authorizations and controls accordingly the communication of the resources (data) to the accessing party.

The ISO 20078 series also considers a side-case where the communication between the back-end server of the manufacturer and the accessing party is indirect and is made through an intermediate body (or intermediate parties). In that case the resource owner has authorized the intermediate body at the vehicle manufacturer and the vehicle manufacturer has been informed of the authorization to communicate the resource (data) to the accessing party (ies).

In both cases the ISO 20078 series disregards important data protection risks, these risks being supposed to be addressed by the accessing party.

Details of this analysis can be found in Annex E.

10.3 Conclusion: Assessment of the risks related to the protection of the resources owned by the resource owner and possibly originating from the ISO 20078 series (data protection risks)

The analysis of the ISO 20078 series regarding the possible data protection risks considered in this document have permitted to demonstrate:

— that the ISO 20078 concept does not generate data protection risks because it is fundamentally based on authorizations received from the data owner;

— that the ISO 20078 series fully addresses the data protection risks in the case of a direct communication between the VM back-end server and the accessing party;

— that the ISO 20078 series fully addresses the data protection risks in the case of a direct communication between the VM back-end server and the intermediate body;

— that the ISO 20078 series only partly addresses the data protection risks in the case of intermediate bodies;

— that the ISO 20078 series does not take into consideration (by conditions, recommendations, etc.) that the complete data protection are also impacted by the manner the other parties are involved.

Annex A
(informative)

Assessment of safety risks

A.1 Possible overload of the electronic system of the moving vehicle (numerous requests)

Description of the risk	Does the ISO 20078 series generate safety risks related to a possible overload of the electronic system of the moving vehicle in the case of several requests at the same time?
Analysis	The considered safety risk is related to the existence and the logic of prioritization mechanism(s) in the final solution. The ISO 20078 series does not specify any prioritization logic or criterion. This logic is left to the choice of the designer of the Extended vehicle. The ISO 20078 series specifies that the communication interface involves a backend server of the manufacturer. This permits the ExVe manufacturer to develop appropriate prioritization mechanisms that are not limited by the available computing resources of the moving vehicle. NOTE — To reduce the risk, this choice can be performed according to the ISO 20077-2 design methodology, but the ISO 20078 series does not specify to do it. — To reduce the risk, the ExVe manufacturer may decide not to forward several requests to the moving vehicle at the same time. — In the case that the logic is located in the backend server of the manufacturer, each backend may have its own specific logic. — The ISO 20078 series includes a mechanism that enables the requester to know how its request is taken into account.
Conclusion	To the question: “Does the ISO 20078 series generate safety risks related to a possible overload of the electronic system of the moving vehicle in the case of several requests at the same time?” the answer is NO. The safety risks related to a possible overload of the electronic system of the moving vehicle in the case of several requests at the same time are only related to the implementation of the ISO 20078 series. The series reduces these risks because it introduces the backend server in the interface. However, the ISO 20078 series does not provide any recommendation regarding that implementation. ISO 20077-2 would be recommendable to help containing this overload risk.

A.2 Possible overload of the electronic system of the moving vehicle (repeated requests)

Description of the risk	Does the solution present risks due to highly frequently repeated requests? NOTE This is also a security issue.
Analysis	The considered safety risk is related to the existence and the logic of prioritization mechanism(s) in the final solution. The ISO 20078 series does not specify any prioritization logic or criterion. This logic is left to the choice of the designer of the extended vehicle. The ISO 20078 series specifies that the communication interface involves a backend server of the manufacturer. This permits the ExVe manufacturer to develop appropriate prioritization mechanisms that are not limited by the available computing resources of the moving vehicle. NOTE — To reduce the risk, this choice may be performed according to the 20077–2 design methodology but the ISO 20078 series does not specify to do it. — To reduce the risk, the ExVe manufacturer may decide not to forward several requests to the moving vehicle at the same time. — In the case that the logic is located in the backend server of the manufacturer, each backend may have its own specific logic. — The ISO 20078 series includes a mechanism that enables the requester to know how its request is taken into account.
Conclusion	To the question: "Does the ISO 20078 series generate risks related to highly frequently repeated requests?" the answer is NO. The safety risks related to a possible overload of the electronic system of the moving vehicle in the case of frequently repeated requests are only related to the implementation of the ISO 20078 series. The series reduces these risks because it introduces the backend server in the interface. However, the ISO 20078 series does not provide any recommendation regarding that implementation. ISO 20077-2 would be recommendable to help containing this overload risk.

A.3 Possible overload of the electronic system of the moving vehicle (unexpected requests)

Description of the risk	Does the solution present risks due to unexpected requests?
Analysis	Implementation should be done according to the state of the art (unexpected request should be denied). The considered safety risk is related to the existence of a mechanism in the final solution that addresses the case of unexpected requests and of its logic. The ISO 20078 series does not specify any such logic neither request it. This logic is implicitly left to the choice of the designer of the extended vehicle. It is recommended that unexpected requests be denied, however this recommendation is not mentioned in the ISO 20078 series.
Conclusion	To the question: "Does the ISO 20078 series generate risks related to unexpected requests?" the answer is NO. The safety risks related to a possible overload of the electronic system of the moving vehicle in the case of unexpected requests are only related to the implementation of the ISO 20078 series. It is recommended that unexpected requests be denied. However, the ISO 20078 series does not provide any such recommendation.

A.4 Possible illicit or malicious remote control of vehicles (prevention)

Description of the risk	Does the solution prohibit illicit or malicious remote control of vehicles, or an illicit or malicious remote activation of systems and components? Actively?
Analysis	The ISO 20078 series specifies that communication to the vehicle is made via the backend server of the manufacturer. This enables a possible technical validation by the backend server of the requests aiming at a taking of control. In addition, the ISO 20078 series introduces the OAuth2 concept of authorization provider that controls that the requester is entitled to emit its request. The risk is therefore strongly depending on the manner that the backend and the authorization system are designed. NOTE To reduce the risk, this design can be performed according to the ISO 20077-2 design methodology but the ISO 20078 series does not specify to do it.
Conclusion	To the questions: "Does the ISO 20078 series prohibit uncontrolled or malicious remote take of control of vehicles, or an uncontrolled or malicious remote activation of systems and components? Actively?" the answers are NO. The safety risks related to a possible uncontrolled or malicious remote take of control of vehicles, or an uncontrolled or malicious remote activation of systems and components are only related to the implementation of the ISO 20078 series. However, the ISO 20078 series introduces concepts that may facilitate the introduction of mechanisms aiming at actively preventing or limiting uncontrolled or malicious remote take of control of vehicles, or an uncontrolled or malicious remote activation of systems and components.

A.5 Illicit or malicious remote control of vehicles (reduction of the risks)

Description of the risk	Does the solution contain mechanisms or processes reducing the safety risks presented by a remote control?
Analysis	The ISO 20078 series is based on the OAuth2 concept where an authorization provider controls that the requester is entitled to emit its request. The authorization provider concept and the access control process (through token) reduce together the risk according the current state of the art. NOTE — The usage of the OAuth2 concept does not reduce in any manner the potential technical risks presented by a remote take of control. — The ISO 20078 series only requests the usage of the OAuth2 concept for the communication with the backend server of the manufacturer; it however does not request the usage of OAuth2 for the other communication mechanisms involved in the complete request process.
Conclusion	To the question: "Does the ISO 20078 series contain mechanisms or processes reducing the safety risks presented by a remote take of control?" the answer is YES. However, the ISO 20078 series only partially addresses these risks because, while there is no guarantee that the accessing party is free from impersonation risks (e.g. ID theft upstream its own request), the ISO 20078 series does not contain any recommendation for considering and possibly limiting these risks.

A.6 Lack of compatibility with the existing systems and mechanisms

Description of the risk	Has the compatibility with the existing design of the vehicle been thoroughly checked and addressed? (When applicable) is the already existing design tolerant to retrofit or reconfiguration?
Analysis	The ISO 20078 series specifies that the communication is made via the backend server of the manufacturer and according to Oauth2 framework. This backend is an abstraction layer for the running vehicle. The ISO 20078 technology embraces the different designs (physical implementations), e.g. different manufacturers, different generations of vehicles, etc. Direct communication with the running vehicle is achieved by the backend server. It is the role of the ExVe designer to secure that compatibility is achieved at that level, including in the case of retrofit or reconfiguration. It is strongly supported that each manufacturer uses the Oauth2 framework as a common embracement of the different manufacturer backend systems.
Conclusion	To the question: "Does the ISO 20078 series generate risks related the compatibility with the existing design of the running vehicle?", the answer is NO. To the question: "Does the ISO 20078 concept address the risks related the compatibility with the existing design of the running vehicle?", the answer is YES. The ISO 20078 concept, by introducing the web-service communication via the back-end server of the vehicle manufacturer, enables a possible substantial reduction of these risks, should the vehicle manufacturer appropriately design this backend server.

A.7 Failures of the remote communication solution itself of the ExVe (including the VM back-end server)

Description of the risk	Does the solution present a safety risk in the case when the back-end server is down (internal failures, hacking, etc.)?
Analysis	In the case the backend server is down, the communication between that backend server and the accessing party may be affected. This malfunction nevertheless does not present per se any safety risk to the running vehicle. When it deals with the communication between the backend server and the running vehicle, the communication with the running vehicle may be stopped (there are survey mechanisms internal to the systems in case e.g. of predictable failures). This communication and these mechanisms are totally outside the ISO 20078 series. NOTE The history of communication technology has shown in several examples, e.g. telephone communication, the benefit in term of complexity of first centralising before distributing a communication network.
Conclusion	To the question: "Does the ISO 20078 series generate safety risks in the case when the backend server is down (internal failures, hacking, etc.)?", the answer is NO.

A.8 Lack of consideration of the complete ExVe life cycle

Description of the risk	Does the solution present safety risks related to requests that are inappropriate in the actual life cycle phase of the running vehicle?: — Manufacturing — Sales — Operation — Maintenance and repair (e.g. does the solution permits reparability for ensuring safety upon time?) — End of life
Analysis	The considered risks are typically related to the facts that — at each life cycle stage, the vehicle has one (or several) owner(s) that may be different from its owner at a different stage; — what is permitted at one stage may not be at another. These aspects are described in ISO 20077-2. The ISO 20078 series enables communication on the basis of authorizations and exchanged tokens (OAuth2 concept). If the authorizations change between 2 stages, the ISO 20078 series can address that change. The processes for initialisation/transfer/revocation of authorizations are nevertheless outside the ISO 20078 series. The ISO 20078 series is only looking for an authorization (whoever is the owner of the ExVe). For example, the authorization provider may only invalidate the token related to the normal "operation stage" when the vehicle is taken out of the market, if the customer has informed the authorization provider of the change. NOTE The example relative to the repair and maintenance stage is typically outside the scope of ISO 20078 series, although it can be included in the scope of standard relative to use-case clusters, such as in ISO 20080.
Conclusion	To the question: "Does the ISO 20078 series generate safety risks related to requests that are inappropriate in the actual life cycle phase of the running vehicle?", the answer is NO. However, such safety issues may occur in the case of a dysfunction of the processes informing the authorization provider of a change of the life cycle stage (manufacturing, sales, operation, maintenance and repair, end of life).

A.9 Risks related to the design validation process

Description of the risk	Has the validation of the design process been sufficiently exhaustive? Is there a sufficient traceability of this validation?
Analysis	As seen before, the ISO 20078 series presents features that enable a design of the extended vehicle that may substantially reduce safety risks. It does not specify the manner that design shall be done. Accordingly, the validation of the measures taken to reduce the risks related to the safety of persons and goods is strongly related to implementation of the ISO 20078 series. NOTE The validation of the request itself is done by the backend (e.g. the data structure, type of the data, etc.).
Conclusion	To the question: "Does the ISO 20078 series generate safety risks related to the validation of the design process and its traceability?", the answer is NO.

A.10 Lack of misuse prevention

Description of the risk	Does the solution permit a limitation of the passed information to avoid safety issues?
Analysis	The ISO 20078 series is deliberately enabling such a limitation. However, it does not specify such a limitation. The decision to introduce such a limitation may be taken at the implementation level (per decision of the ExVe designer), possibly further to external specification (e.g. in ISO 20080, actuators use-cases may restrict the passed information because of safety risks).
Conclusion	To the question: "Does the ISO 20078 concept permit a limitation of the passed information to avoid safety issues?", the answer is YES. To the question: "Does the ISO 20078 series specify or recommend a limitation of the passed information to avoid safety issues?", the answer is NO. Addressing the issue is left by the ISO 20078 series to external actors (e.g. those involved at the implementation stage of the series or at the specification of the considered use-cases).

Annex B
(informative)

Assessment of security risks

B.1 Cybersecurity risks (general)

Description of the risk	Does the solution address at all stages (i.e. involving all actors) the state-of-the-art cybersecurity risks (e.g. by considering ISO/SAE 21434 and Reference [9])?
Analysis	The ISO 20078 series specifies that the communication between the accessing party and the manufacturer backend server shall be done according to the OAuth2 specifications. At the time when the series is developed the OAuth2 framework is considered as one of the state-of-the-art manner to address cybersecurity risks. The ISO 20078 series only specifies clauses that lie within the scope of the project. In particular: — the ISO 20078 series partly specifies cybersecurity requirements related to the implementation of the series. For example, the ISO 20078 series addresses encryption of the information (TLS), duration of the token validity, etc.; — the ISO 20078 series does specify or recommend any condition related to cybersecurity for a accessing party be considered as an agreeable accessing party.
Conclusion	To the question: “Does the ISO 20078 series address the 2018 state-of-the-art cybersecurity risks?” the answer is YES. The ISO 20078 series address the 2018 state-of-the-art cybersecurity risks. Nevertheless, due to its scope, the ISO 20078 series does not fully address the state-of-the-art cybersecurity risks at all stages of the communication between the vehicle and the service provider who is directly in contact with the vehicle operator. Recommending (without requiring) the ExVe manufacturer that implements the ISO 20078 series to design that implementation according to the ISO 20077-2 methodology may help better addressing the cybersecurity risks.

B.2 Risks related to integrity and authenticity

Description of the risk	Does the solution prevent at all stages (i.e. involving all actors) the manipulation of the system (e.g. Re integrity and authenticity)?
Analysis	The ISO 20078 series requires an OAuth2 based communication between the accessing party and the manufacturer backend server. The Oauth2 framework is state of the art for authenticity. Furthermore ISO 20078-2 requires the TLS 1.2 or higher for transport layer security for encryption.
Conclusion	To the question: "Does the solution prevent the manipulation of the system (e.g. Re integrity and authenticity)?" the answer is YES. However, the final level of integrity and authenticity, that involves all actors in the process, is conditioned by implementation of the ISO 20078 series.

B.3 Risks at vehicle systems that are not located at the moving vehicle

Description of the risk	Does the solution present security risks at vehicle systems that are not located at the vehicle itself? For example: — At the accessing party? — At the off-board components of the vehicle (in the case of an extended vehicle)?
Analysis	The ISO 20078 series specifies web services for extended vehicles that communicate with the accessing party(ies) through the back-end server of the vehicle manufacturer. The ISO 20078 series addresses the security risks related to these web services (see the other items of this analysis). The off-board components of the ExVe, including the back-end server itself, as well as the communication equipment of the accessing party and/or the intermediate parties are outside the field of application of the ISO 20078 series.
Conclusion	To the question: "Does the ISO 20078 series address security risks at other places than at the vehicle itself?" the answer is YES. The ISO 20078 series addresses the security risks related to the communication between the back-end server of the manufacturer and the accessing party. To the question: "Does the ISO 20078 series address all security risks at other places than at the vehicle itself?" the answer is NO. The ISO 20078 series only specifies a web service solution at the back-end server of the vehicle manufacturer. The off-board components of the Extended Vehicle (including the back-end system itself) as well as the equipment of the accessing parties are outside the scope of ISO 20078 series. There may be security risks related to these components but the manner to address them is outside of the scope of the ISO 20078 series.

B.4 Consequences of a security breach

Description of the risk	Does the solution include measures that limit the consequences of a security breach?
Analysis	This issue is addressed in ISO 20078-2. For example: — There is a clause in ISO 20078-2 dealing with the rate limits of requests. — ISO 20078-2 requires TLS 1.2 or higher for transport layer security. By this way there are other measures that are specified.
Conclusion	To the question: "Does the ISO 20078 series include measures that limit the consequences of a security breach?" the answer is YES. These measures are mainly specified in ISO 20078-2.

B.5 Misuse prevention measures

Description of the risk	Does the solution include misuse prevention measures? For example: — in permitting in-use a controlled access arbitration; — in permitting an efficient limitation of the passed information; — in permitting a monitoring of the passed information; — in only communicating with trustable parties.
Analysis	The ISO 20078 series specifies using the OAuth2 framework for communication. In this framework it is the role of the authorization provider to control in-use the access to the resources of the extended vehicle. This control is founded on actual authorizations given by the resource owner (e.g. the vehicle owner) to solely communicate resources to selected parties in selected use-cases and use-cases scenarios. This control is conditioned by the information provided by the identity provider in charge of the authentication (identification) of the resource owners. The ISO 20078 series also includes more technical clauses that address misuse prevention, for example: — ISO 20078-2 considers a rate-limit of the requests, and thereby permits an efficient limitation of the passed information, it is included a security framework of the web service ("watchdog") that permits a monitoring of the passed information.
Conclusion	To the question: "Does the ISO 20078 series include misuse prevention measures?" the answer is YES. This answer is primarily based on the fact that the ISO 20078 series is based on the OAuth2 framework, but there are also important other technical measures that complete this assertion.

Annex C
(informative)

Assessment of competition risks

C.1 Possible misuse of the acquired knowledge

Description of the risk	Does the solution present competition risks related to the ability for one of the involved parties to misuse the data he has knowledge of due to its role(s) in the specified process, whether or not other parties have that knowledge?
Analysis	The ISO 20078 series specifies the web service interface between an accessing party and the extended vehicle (the back-end server of the ExVe manufacturer). It neither specifies the manner this interface is implemented nor the conditions for that implementation. Therefore, it does not specify any specific condition for ensuring a fair attitude of the concerned parties regarding the usage they may have access to due to their role in the communication process. The ISO 20078 series specifies that the ExVe manufacturer has the role of resource, identity and authorization provider. The ExVe manufacturer acquires thereby an accumulated knowledge it may or may not use for competition purposes. In the same manner any other party involved in the complete communication process (from the ExVe to the final customer) may or may not misuse the knowledge he has got by its own role(s).
Conclusion	To the question: "Does the ISO 20078 series address competition risks related to the ability for one of the involved parties to misuse the data he has knowledge of due to its role(s) in the specified process?" the answer is NO. To the question: "Does the ISO 20078 series generate specific competition risks related to the ability for one of the involved parties to misuse the data he has knowledge of due to its role(s) in the specified process?" the answer is NO. The ISO 20078 series neither generates nor addresses the considered competition risks.

C.2 Possible gaining of unique knowledge of the market through monitoring

Description of the risk	Does the solution present competition risks because, through monitoring, some competing parties gain unique knowledge of the market (for a certain, e.g. brand specific, after-sales service)? In particular: — because of their role of resource provider; — because of their role of authorization provider; — because of their role of identity provider.

Analysis	In the communication scheme considered in the ISO 20078 series, — the ExVe manufacturer has typically the roles of resource, identity, and authorization provider regarding the resources provided to the accessing party; — the accessing party has typically the roles of resource, identity, and authorization provider regarding the resources provided to other parties such as the service provider directly in contact with the customer or any other intermediate body; — there may be other intermediate bodies between the accessing party and the final customer that may also have the roles of resource, identity and authorization provider. This demonstrates that, while the ISO 20078 series specifies the clauses relative to the first step of that communication scheme (the communication between the back-end server of the manufacturer and the accessing party), the risk that, through monitoring, some competing parties have a knowledge of the market (for a certain, e.g. brand specific, after-sales service) other might not have, is not specific to the ISO 20078 series. It is true that the knowledge resulting from the accumulation of the information known by the resource, authorization, and identity provider may create competition risks when it is used for after-sales purpose. This accumulation may result from the fact that the resource, identity and authorization provider belong to the same company. This accumulation may also occur when an after-sales party acquires the cumulated information with resource, identity and authorization provider, although each of them belongs to a different company. This demonstrates that, while the ISO 20078 series considers that the vehicle manufacturer has typically the roles of resource, identity and authorization provider, the risk is not specific to the ISO 20078 series because, through monitoring, several other competing parties may have a unique knowledge of the market (for a certain, e.g. brand specific, after-sales service).
Conclusion	To the question: “Does the ISO 20078 series generate competition risks because, through monitoring, the ExVe manufacturer gains a unique knowledge of the market (for a certain, e.g. brand specific, after-sales service)?” the answer is NO. To the question: “Does the ISO 20078 series address competition risks when, through monitoring, the ExVe manufacturer gains a unique knowledge of the market (for a certain, e.g. brand specific, after-sales service)?” the answer is NO. The ISO 20078 series neither generates nor addresses the considered competition risk. This risk is related to the manner the ExVe manufacturer implements the ISO 20078 series. This risk is not limited to the ExVe manufacturer.