OCORA

Open CCS On-board Reference Architecture

Confidentiality Clause

Document ID: OCORA-BWS02-060

Version: 1.00

Release: Delta

Date: 30.06.2021

Revision history

Version	Change Description	Initial	Date of change
1.00	Final release, ready for pre-Delta publication	RM	29.01.2021
1.90	▪ Draft for Review in adjusted Template	RM	17.06.2021
2.00	Official version for OCORA Delta Release	RM	30.06.2021
	▪		
	▪		

Table of contents

References

Reader's note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). OCORA always reference to the latest available official version of the SUBSET, unless indicated differently.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS03-010 – Introduction to OCORA

[6] OCORA-BWS04-010 – Problem Statements

1 Introduction

1.1 Purpose of the document

This document aims to provide the reader the OCORA **Confidentiality Clause** as basis to serve started sector dialogue and RFIs.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

If you are a railway undertaking, you may find useful information to compile tenders for OCORA compliant CCS building blocks, for tendering complete on-board CCS system, or also for on-board CCS replacements for functional upgrades or for life-cycle reasons.

If you are an organization interested in developing on-board CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development.

1.2 Applicability of the document

The document is considered informative.

1.3 Context of the document

This document is published as part of the OCORA Delta release, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [5], and the Problem Statements [6]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

2 Confidentiality

2.1 The Parties shall not share Confidential Information that are sensitive commercial information. In particular, they shall not share any strategic information, including but not limited to information regarding their commercial policy, business plan or pricing strategy either towards their suppliers or towards their clients.

2.2 The Parties can share technical Confidential Information if this information is strictly needed for the purpose of the Cooperation. In such case, any Party receiving a Confidential Information grant it the same level of protection as it uses to protect its own Confidential Information.

2.3 The Parties are obliged to treat non-public company and business secrets of the other Parties, which become known to them on the basis of this COC, confidential towards third parties (**"Confidential Information"**). They will not make the Confidential Information of a technical and business nature accessible to third parties for the duration of the COC and for 5 years beyond, protect it from access by third parties, not make it the subject of their own application for industrial property rights and keep it in safe custody with due care. The meaningful use of the results by a Party must not, however, be impaired by this.

2.4 Under no circumstances may a Party use and exploit Confidential Information of another Party for its own business purposes (in particular not for the manufacture, use or sale of competing products) but exclusively for the purposes of this COC and to the extent necessary to achieve the purpose of this COC. For clarification purposes, the Parties state that the compliance with this obligation constitutes an essential contractual obligation of each Party.

2.5 The aforementioned obligation shall not apply to information which is generally known or which becomes apparent at a later point in time without the involvement of the respective Party or which has been independently compiled or lawfully obtained by third parties. In addition, each Party may disclose Confidential Information insofar as

the Party is obliged to do so by a judicial or official decision of a competent court or authority and insofar as the Party informs the other Parties of this at the earliest possible time and supports him in all reasonable steps to prevent publication, to the extent permitted by law.

2.6 Upon termination of this COC and/or a Party's participation in the OCORA Cooperation for any reason at all, each Party is obliged to return all Confidential Information to the other Party or destroy the Confidential Information, as requested by the other Party. This obligation shall also apply to records which a Party has made of Confidential Information in writing or on other data carriers, as well as to copies of Confidential Information, irrespective of the form in which they exist. Should the disclosure not be possible, for example because they are located on hard disks or similar data carriers, the corresponding data shall be deleted or destroyed in any other way. At the request of a Party, the respective other Party must within reasonable time confirm in writing that the above provisions and specifications have been complied with. The obligation to return or destroy Confidential Information shall not apply to the extent this is imposed by standard IT backup processes or internal bookkeeping requirements or in case retention of respective Confidential Information is required by mandatory law.

2.7 In case, a Party has disclosed Confidential Information in breach of its obligations set out in Part III, sections 2.1 to 2.6 (**"Unauthorized Disclosure"**), this Party shall use best efforts to ensure that the respective Confidential Information having been subject to such Unauthorized Disclosure will immediately be returned in full. All copies of such Unauthorized Disclosure will be irretrievably destroyed and reasonable evidence proving such irretrievable destruction will be provided without undue delay.