Joint consultation by the German gas transmission system operators

as part of an application to the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (below referred to as "Bundesnetzagentur") under Article 23(2) of Regulation (EU) 2015/703 (Network Code on Interoperability and Data Exchange) for permission to continue to use the data exchange solutions in place between the transmission system operators and the counterparties concerned on the date of entry into force of Regulation (EU) No 2015/703

Consultation conducted by:

bayernets GmbH

Fluxys Deutschland GmbH

Fluxys TENP GmbH

GASCADE Gastransport GmbH

Gastransport Nord GmbH

Gasunie Deutschland Transport Services GmbH

GRTGaz Deutschland GmbH

jordgasTransport GmbH

Lubmin-Brandov Gastransport GmbH

NEL Gastransport GmbH

Nowega GmbH

ONTRAS Gastransport GmbH

OPAL Gastransport GmbH & Co. KG

Open Grid Europe GmbH

terranets bw GmbH

Thyssengas GmbH

Table of contents

1. Introduction 3

2. Background and context of this consultation 3

3. Scope of application of the relevant provisions and analysis of existing solutions 5

3.1. Personal scope 5

3.2. Material scope 5

4. Discussion of the intended scope of the TSOs' applications to Bundesnetzagentur under Article 23(2) for permission to continue to use existing data exchange solutions during a transitional period 7

5. Analysis of the data exchange solutions AS2 and edifact as to their compliance with the requirements set out in Articles 20(2) and 22 8

5.1. Compliance with Article 20(2) 8

5.2. Compliance with Article 22 8

5.2.1. Definition of relevant scope 8

5.2.2. Appropriateness of the transfer protocol AS2 to secure the communication chain 9

5.2.2.1. Security through encryption and message signing 9

5.2.2.2. Traceability through acknowledgements of delivery and receipt 10

5.2.3. Conclusions concerning the compliance of the data exchange solutions AS2 and edifact with the requirements set out in Articles 20(2) and 22 10

1. Introduction

The Network Code on Interoperability and Data Exchange (NC INT) was adopted on 30 April 2015 and, given its legal effects as directly applicable legislation, came into force in all EU member states on 21 May 2015. According to Article 26[1] its provisions apply from 1 May 2016.

NC INT was adopted to reach an appropriate level of harmonisation across the various gas transmission systems in technical, operational and communications matters. The aim is to avoid the emergence of potential barriers to efficient gas trading and transport within the European Union so as to support the completion and functioning of the European internal gas market, security of supply, and appropriate and secure access to information.[2] NC INT thus provides rules and procedures to, inter alia, harmonise data exchange between the gas transmission system operators (TSOs) themselves as well as between the TSOs and their communication partners (throughout this text referred to as "counterparties" in line with the terminology used in the network code).

2. Background and context of this consultation

Article 20(2) operating in conjunction with Articles 21 and 23(1) requires the TSOs and the counterparties concerned to implement common data exchange solutions by 1 May 2016 and to use them from that date. This obligation applies with respect to document-based, integrated and interactive types of data exchange (see Article 21(1)) but depending on the requirements imposed by the regulations listed in Article 20(2). Specifically, Article 21(2) sets out the protocol, data format and network to be used for each type of communication. An overview is provided in the table below:

	Document-based data exchange	Integrated data exchange	Interactive data exchange
Protocol	AS4	HTTP/S	HTTP/S
Data format	Edig@s XML	Edig@s XML	not specified
Network	Internet	Internet	Internet

Table 1: Common data exchange solutions pursuant to Article 21(2)

All data exchange solutions used for communication purposes must also meet the security and availability requirements for data exchange systems set out in Article 22.

Article 23(2) provides that any data exchange solution in place between TSOs and the counterparties concerned on the date of the Regulation's entry into force may continue to apply after consultation of network users and subject to the approval of the TSOs' national regulatory authority, provided that the existing data exchange solutions meet the security requirements set out in Article 22 and that they are compatible with the data exchange requirements under Article 20(2).

[1] Except where otherwise indicated all references to articles made in this text relate to Commission Regulation (EU) 2015/703 of 30 April 2015 establishing a Network Code on Interoperability and Data Exchange Rules as published in the Official Journal of the European Union (OJ L 113, 1.5.2015, p. 13).
[2] Whereas clauses (3) and (8).

This means in practice that all existing data exchange solutions falling within the scope of Regulation (EU) 2015/703 other than those specified in Article 21(2) need to be consulted and approved by 1 May 2016 or they may no longer be applied from 1 May 2016.

The German gas TSOs therefore intend to apply to Bundesnetzagentur under Article 23(2) for permission to continue to use the common data exchange solutions currently in place with network users for a limited period of time. The TSOs are running this consultation to seek the views of all counterparties concerned on the common data exchange solutions they think should continue to be used and in respect of which the TSOs are going to seek the approval of Bundesnetzagentur.

Structure of the consultation

In chapter 3 the TSOs first discuss the personal and material scope of the relevant provisions, i.e. the TSO-counterparty communications that are subject to the harmonisation requirements of Regulation (EU) 2015/703, before describing the respective solutions currently in place.

In chapter 4 the TSOs discuss which of the existing solutions they intend to include in their application to Bundesnetzagentur and what transition period they propose for their continued use.

Chapter 5 provides the reasons why the solutions to be included in the application are considered to meet the requirements set out in Articles 20(2) and 22.

A questionnaire for the counterparties consulted is provided as an appendix to this consultation document.

Please submit your response by emailing the feedback form to Transport@gasunie.de by 22 January 2016 at the latest. Your answers will be taken into account by the TSOs when drafting their applications for continued use of the existing data exchange solutions and submitted to Bundesnetzagentur in unredacted form. Please also send an additional version of your response that is suitable for publication (i.e. a non-confidential version not containing any commercially sensitive or confidential information) to info@fnb-gas.de. All responses submitted to the TSO association Fernleitungsnetzbetreiber e.V. will be published on the association's website.

3. Scope of application of the relevant provisions and analysis of existing solutions

3.1. Personal scope

According to Article 20 the relevant provisions apply to communications between "transmission system operators" and "counterparties". Article 20(1) states that a counterparty means any network user who is active at a) interconnection points or b) both interconnections points and virtual trading points.

The TSOs therefore consider that the personal scope of NC INT extends to communications

- between TSOs,
- between TSOs and counterparties, and
- between the capacity allocation platform PRISMA and counterparties (where and to the extent that PRISMA handles processes and acts on behalf of the TSOs).

The TSOs understand the term "counterparty" in relation to any TSO as comprising all network users registered with and admitted as a user by that TSO on 1 May 2016, i.e.

- shippers and their authorised agents (including market area managers where they act as shippers in the context of their operational balancing activities), and
- balancing group managers,

where and to the extent that they operate across national or market area borders.

Conversely, it can be inferred from the wording in Article 20(1)(a) and (b) that traders who only execute trades on the virtual trading point (VTP) do not fall within the personal scope of the relevant provisions.

3.2. Material scope

According to Article 1(2), sentence 1, NC INT applies at "interconnection points" (in the German text referred to as "*Netzkopplungspunkt*"). The term "interconnection point" is not defined in NC INT itself. Article 2, however, expressly states that the definitions provided in the Network Code on Capacity Allocation Mechanisms in Gas Transmission Systems (NC CAM) shall apply for the purposes of NC INT. According to Article 3(10) of NC CAM an "interconnection point" (in the German text here referred to as a "*Kopplungspunkt*", as opposed to "*Netzkopplungspunkt*") means a point that connects adjacent entry/exit systems. Other language versions of NC CAM and NC INT use identical terms (e.g. "interconnection point" in English), which had also been the intention at the time of drafting the text so as to ensure a consistent framework for interactions between the network codes. The term "interconnection point" (and thus the German term "*Netzkopplungspunkt*" as used in NC INT) is therefore understood to apply to both interconnection points that provide a connection between different German market areas (market area interconnection point) and interconnection points that provide a connection between a German market area and a market area in another country (cross-border interconnection points).

With regard to the common data exchange solutions described in chapter V, NC INT serves a support function in that it ultimately facilitates the implementation of other regulations.[3] The material scope of the data exchange solutions described in Article 21 and the implementation and application obligations arising in relation thereto are therefore determined by the data exchange requirements set out in the regulations referred to in Article 20(2).[4]

The table below provides an overview of the processes that are necessary to implement the regulations referred to in Article 20(2).

- Column 4 lists the communication processes between TSOs/counterparties that are affected by this consultation.
- Column 5 indicates what type of data exchange they involve according to the categories provided in Article 21(1).
- Column 6 lists the protocols and formats currently used by the parties.
- Column 7 lists the protocols and formats to be implemented under Article 21(2).

No.	Topic	Legislative reference Article 20(2) NC INT	Communication processes	Type of data exchange according to Article 21(1) NC INT	Solutions currently in place		Solutions to be implemented under Article 21(2) NC INT	
	2	3	4	5	6		7	
					Format	Protocol	Format	Protocol
1	Congestion management	No 2.2 Annex I Regulation (EC) No 715/2009 (CMP)	Capacity surrender process pursuant to No 2.2.4 between PRISMA and network users	Interactive data exchange (browser-based graphical user interface (GUI))	(n/a)	HTTP/S	(n/a)	HTTP/S
	Congestion management	No 2.2 Annex I Regulation (EC) No 715/2009 (CMP)	Notification of renomination limit from TSOs to network users where required to implement renomination restrictions under No 2.2.3	Document-based data exchange	edifact (primarily CHACAP message)	AS2 and (un)encrypted email via SMTP	edig@s-XML	AS4
2	Capacity allocation	Regulation (EU) No 984/2013 (NC CAM)	All processes required to book capacity at market area and cross-border interconnection points on the capacity allocation platform PRISMA	Interactive data exchange (browser-based graphical user interface (GUI))	(n/a)	HTTP/S	(n/a)	HTTP/S
3	Balancing	Regulation (EU) No 312/2014 (NC BAL)	(Re-)nominations and confirmations thereof	Document-based data exchange	edifact (primarily NOMINT and NOMRES messages)	AS2 and (un)encrypted email via SMTP	edig@s-XML	AS4

[3] NC INT thus facilitates the implementation and application of the Union regulations listed in Article 20(2), i.e. provisions adopted in the fields of congestion management procedures (CMP; No 2.2 of Annex I Regulation (EC) No 715/2009 as amended by commission decision of 24 August 2012, OJ L 231, 28.8.2012, p. 16), capacity allocation (NC CAM; Regulation (EU) No 984/2013 of 14 October 2013 establishing a Network Code on Capacity Allocation Mechanisms in Gas Transmission Systems and supplementing Regulation (EC) No 715/2009, OJ L 273, 15.10.2013, p. 5), balancing (NC BAL; Regulation (EU) No 312/2014 of 26 March 2014 establishing a Network Code on Gas Balancing in Transmission Networks, OJ L 91, 27.3.2014, p. 15) and NC INT itself as well as the regulation on wholesale energy market integrity and transparency (REMIT; Regulation (EU) No 1227/2011 of 25 October 2011 on Wholesale Energy Market Integrity and Transparency, OJ L 326, 8.12.2011, p. 1), by introducing harmonised data exchange solutions for data-based communications required between the market participants involved.

[4] This is stated clearly in Articles 21(1) and 23(1), where implementation and use of the relevant data exchange solutions is required "depending on the data exchange requirements under Article 20(2)".

Table 2: Existing and required data exchange solutions for communications between TSOs (including PRISMA booking platform) and counterparties

Explanatory notes:

a) General notes on the message types included in the table

The TSOs consider that only the format pursuant to Article 21(2) that is to be included in the application for continued use would have had to be consulted. In that case merely the trade mark or brand name as such would have had to be stated, as was done in NC INT, where the specification runs to "edig@s-XML". However, to facilitate a better understanding of this consultation for the network users consulted, especially which parts of the message formats are affected, the TSOs considered it useful to also indicate the relevant message types. Still, in their applications for permission to continue to use the existing formats the TSOs will merely request continued use of the format "edifact".

b) Notes on No. 1 and No. 2 of the table (congestion management and capacity allocation)

In connection with the processes the booking platform PRISMA handles on behalf of the TSOs it should be noted that all data exchange requirements for communications with shippers (option to book capacity, publication of auction results etc.; see Articles 5 and 11(10) of NC CAM)[5] have been fully implemented by PRISMA via a browser-based graphical user interface (GUI) provided for that purpose. This makes it an interactive data exchange within the meaning of Article 21(1)(c), which is carried out via Internet using the HTTP/S protocol.

c) Notes on other provisions referred to in Article 20(2)

Any other communication requirements according to NC INT or the REMIT Regulation that do not affect communications between TSOs and/or PRISMA and counterparties (e.g. matching according to NC INT or data reporting to ACER according to REMIT) are not part of this consultation.

4. Discussion of the intended scope of the TSOs' applications to Bundesnetzagentur under Article 23(2) for permission to continue to use existing data exchange solutions during a transitional period

In consideration of the above remarks the TSOs intend to apply for permission to continue to use

- the format "edifact"
- and the protocol "AS2"

at market area and cross-border interconnection points during a transitional period until 31 January 2018 in TSO-counterparty communications.

[5] See footnote No. 3.

The application will not include a request for continued use of unencrypted email communications for application of the regulations listed in Article 20(2) given that this type of communication does not meet the security requirements set out in Article 22. Yet according to Article 23(2) that would be a prerequisite for this exception to be requested. From 1 May 2016, unencrypted email can thus no longer be used in data exchange processes falling within the scope of NC INT.

The TSOs believe that the existing solutions should continue to be available for a limited period of time that is identical for all parties and that the solutions to be continued under the exception to be applied for should be the same throughout the market. **The TSOs therefore propose to apply for approval of the above-mentioned transition period until 31 January 2018 for continued use of the solutions currently in place**. In view of the experiences made in connection with the switch from ISDN/FTP to AS2 the TSOs believe that a period of one and a half years starting from the potential effective date of any decision approving the exception is a reasonable time.

The TSOs are of the view that if the existing solutions are approved for continued use, this will have the effect described below. Where a TSO had established communications on the basis of edifact and AS2 with at least one network user on 21 May 2015 (date of the Regulation's entry into force, see exact wording of Article 23(2)), this will have the following implications for network users:

- Network users already communicating with that TSO on the basis of edifact and AS2 will have the option to continue to use this type of communication for the duration of the approved transition period.
- Network users communicating with that TSO on the basis of any other data exchange solution will have the option to switch to edifact and AS2 during the approved transition period.
- Network users who have not yet established communications with that TSO will have the option to establish new communications on the basis of edifact and AS2 with that TSO during the approved transition period.

5. Analysis of the data exchange solutions AS2 and edifact as to their compliance with the requirements set out in Articles 20(2) and 22

5.1. Compliance with Article 20(2)

Approval for continued use of existing solutions can only be granted if the data exchange solutions in place are capable of meeting the requirements set out in the regulations referred to in Article 20(2). In relation to the TSO-counterparty communications which are the subject of this consultation that is indeed the case. All relevant capacity allocation, congestion management and balancing processes were implemented within the applicable time limits provided in the respective regulations[6] and have been operated using edifact formats and the AS2 protocol ever since.

5.2. Compliance with Article 22

5.2.1. Definition of relevant scope

Article 22 sets out the security and availability requirements data exchange systems must meet. For the sake of clarification the TSOs would like to point out that the term “data exchange system” as

[6] See the references provided in footnote No. 3.

used in Article 22 has a broader meaning than the term "data exchange solution" which is the subject of this consultation. The TSOs consider a data exchange system to mean a combination of physical IT infrastructure and the intangible data exchange solution (primarily format and protocol) addressed in this consultation. Accordingly, the text below only discusses why the data exchange solutions that are the subject of this consultation comply with the requirements of Article 22(1)(a), i.e. why they are appropriate to "secure the communication chain".

Neither the security criteria set out in Article 22(1)(b) and (c) nor the availability requirements for IT infrastructure set out in Article 22(2) are part of this consultation but will have to be ensured through appropriate physical security measures to be taken by the TSOs and their respective counterparties.

5.2.2. Appropriateness of the transfer protocol AS2 to secure the communication chain

When it comes to securing the communication chain in data transmissions a key factor lies in selecting an appropriate communications protocol, which can be understood as representing a (secured) envelope for the messages to be sent/received. One such communications protocol is AS2, a standard protocol widely used for data exchange purposes in the energy industry.[7]

The security of all data transmissions via AS2 is achieved by means of 3DES message encryption, unique sender authentication and non-repudiation through use of signatures. To further increase security, all encryption and signature certificates are changed on a regular basis.

Moreover, in its cost/benefit analysis carried out to support the final choice of standard transfer protocol to be included in NC INT (below referred to as the "CBA")[8] ENTSOG also examined the security aspects of data exchanges solely by looking at the transfer protocol used (see section 6.4 of the CBA). Hence, the CBA focused on the specific aspects of achieving

- security through encryption and message signing, and
- traceability through acknowledgements of delivery and receipt

which are discussed below by way of a comparison between AS4 and AS2. For the purpose of that comparison it was assumed that the AS4 protocol, being as it is the standard solution envisaged in NC INT, can be deemed appropriate to "secure the communication chain".

5.2.2.1. Security through encryption and message signing

After analysing the transfer protocols AS4, AS2 and ebMS v3[9] in its above-mentioned CBA, ENTSOG concluded its analysis by proposing AS4 as the standard transfer protocol to be included in NC INT. The reason given in the CBA for this proposal is that AS4 uses more up-to-date encryption algorithms and signatures than AS2, which furthers the "security" element described above. The ENTSOG CBA does not, however, categorise AS2 as an unsecure transfer protocol.

[7] https://www.bdew.de/internet.nsf/id/DE_Vereinbarung-elektronischer-Datenaustausch-EDI (German only).
[8] ENTSOG Cost-Benefit Analysis study (CBA) – Document for the selection of a harmonised data exchange solution between gas transmission system operators in Europe and with their counter parties, http://www.entsog.eu/public/uploads/files/publications/INT%20Network%20Code/2013/INT0414%20CBA%20DataExchange-final.pdf.
[9] ebMS v3 will not be discussed further as AS4 builds on ebMS v3 and both protocols can be considered to provide an equivalent level of security.

In this context it should be noted that Article 23(2) does not require existing data exchange solutions to provide an equivalent level of protection to the solutions set out in NC INT but merely to be "compatible with Article 22". Of course if this were not the case, it would hardly be possible to approve any existing data exchange solution, given that NC INT introduced the most up-to-date, state of the art technology for harmonisation purposes to provide a basis for future developments.

The statement that AS4 uses a more up-to-date encryption algorithm specifically relates to the use of AES encryption, which has the advantage of a longer maximum key length compared to the above-mentioned 3DES encryption, which is used in AS2 communications. Various studies[10,11] have shown, though, that the 3DES algorithm still provides an "appropriate" level of security even today. The fact that 3DES – alongside AES – remains the encryption method most commonly used in the financial industry also supports the assumption that AS2 meets current security standards.[12]

5.2.2.2. Traceability through acknowledgements of delivery and receipt

Both AS4 and AS2 are synchronous data transfer methods and as such provide the possibility of verifying successful delivery of data transmissions (similar to registered letters where the recipient is required to sign on delivery[13]), which is a key criterion to establish the security of a communication chain. Thanks to its consistent acknowledgement management, the synchronous data transfer protocol AS2 ensures that it can be verified whether messages are correctly transferred between the sending and receiving parties both physically and syntactically.[14] Digital certificates guarantee that the sender cannot repudiate the origin of sent messages.

5.2.3. Conclusions concerning the compliance of the data exchange solutions AS2 and edifact with the requirements set out in Articles 20(2) and 22

Given that all relevant capacity allocation, congestion management and balancing processes were implemented within the applicable time limits provided in the respective regulations and have been operated using the edifact formats and the AS2 protocol ever since, it can be concluded that these data exchange solutions meet the requirements set out in the relevant provisions. The TSOs further believe that the existing data exchange solutions proposed for continued use (subject to the approval of Bundesnetzagentur) are appropriate to secure the communication chain as required under Article 22(1)(a) of NC INT due to their use of the AS2 protocol.

[10] Bhanot/Hans (2015), A Review and Comparative Analysis of Various Encryption Algorithms, International Journal of Security and Its Applications, http://www.sersc.org/journals/IJSIA/vol9_no4_2015/27.pdf.
[11] Princy (2015), A Comparison of symmetric key algorithms DES, AES, BLOWFISH, RC4, RC6: A SURVEY, International Journal of Computer Science & Engineering Technology, http://www.ijcset.com/docs/IJCSET15-06-05-055.pdf.
[12] "Within the financial industry, triple DES and AES are the most commonly used block ciphers.", European Payment Council (2014), Guidelines on Algorithms Usage and Key Management, http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/guidelines-on-algorithms-usage-and-key-management/epc342-08-guidelines-on-algorithms-usage-and-key-management-v40/.
[13] http://edi-wissen.de/edi/kommunikationswege-datenquellen-senken/eher-offentliche-wege/as2/ (German only).
[14] BDEW (2009), Study on secure web-based transmission channels. Security recommendations for external electronic communications connections via Internet for Electronic Data Interchange in the German energy industry (German only), https://www.bdew.de/internet.nsf/id/1D5238ECBAFA1677C12578BE004CAE55/$file/2009-11-05_Energie-Info_Studie_Sichere%20webbasierte%20%C3%9Cbertragungswege_V%202.1.pdf.