IGT | UNC

Modification	At what stage is this document in the process?

IGT130:

Applying password protection encryption to electronic communication containing MPRNs

01	Modification
02	Workgroup Report
03	Draft Modification Report
04	Final Modification Report

Purpose of Modification:

The purpose of this modification is widening the scope of encryption requirements building on those approved via IGT118. The developments and discussions have been completed through RG007 which was set up to determine the need and scope for this modification.

The Proposer recommends that this modification should:

- be subject to self-governance
- be assessed by a Workgroup

This modification will be presented by the Proposer to the Panel on 16th August 2019. The Panel will consider the Proposer's recommendation and determine the appropriate route.

High Impact:

Medium Impact:

Low Impact:

IGTs, Shippers, CDSP

12th August 201929th October 2019

Formatted: Superscript

IGT | UNC

Contents

? Any questions?

Contact:
Code Administrator

iGTUNC@gemserv.com

020 7090 1044

Proposer:
E.ON
Radhika Kalra

radhika.kalra@eonenergy.com

07971810459

Alternative:
E.ON
Kirsty Dudley

Kirsty.Dudley@eonenergy.com

07816172645

Timetable

The Proposer recommends the following timetable:

Initial consideration by Workgroup	3rd September 2019
Amended Modification considered by Workgroup	
Workgroup Report presented to Panel	20th September22nd November 2019
Draft Modification Report issued for consultation	25th November23rd September 2019
Consultation Close-out for representations	16th December 2019 14th October 2019
Variation Request presented to Panel	
Final Modification Report available for Panel	19th December15th October 2019
Modification Panel decision	17th January 202022nd November 2019

Formatted: Superscript

Formatted: Superscript

Formatted: Superscript

Formatted: Superscript

Formatted: Superscript

12th August 201929th October 2019

1 Summary

What

The Password Protection Protocol Ancillary Document was amended under IGT118 to bring the provisions up to date with the information technology and mechanisms by which protected information is sent between the Pipeline User and Pipeline Operators within the industry for the portfolio and invoicing data. During the Working Group discussions for IGT118 it became apparent that more Protected Information was sent than the portfolio and invoicing data. Therefore, the scope needed to be widened because further consideration is needed to Section K23.2 of the IGT UNC e.g. how requests which contain MPRNs are sent and if they should be encrypted. To avoid delays in development to IGT118 the additional scope discussions were separated and were taken to a Review Group, which then formed the basis of this modification.

Why

Now that the Password Protection Protocol has been amended, Section K23.2 is out of date and needs to be brought in line to the amendments made under IGT118 to ensure transparency, clarity and consistency are applied to encrypting data which is sent under the IGT UNC.

In addition, there have been instances when MPRNs are sent across the industry which is deemed to be customer information for the purposes of Data Protection and is subject to the General Data Protection Regulation (GDPR). It would be considered as good governance to ensure that processes outlined in the IGT UNC are in line with the regulations and are clearly outlined for both Pipeline Operators and Pipeline Users ensuring that processes remain up to date and robust.

How

Amendments are to be made to Section K23.2 to keep them in line with those made to the Password Protection Protocol under IGT118.

All communications containing MPRN level data in an email or contained within an attachment will have encryption applied in line with the Password Protection Protocol Ancillary Document.

2 Governance

Please state clearly which governance procedures apply and why, referring to the relevant criteria (reproduced by the Code Administrator below):

Justification for Self-Governance Procedures

This change should be classed as Self-Governance as it does not propose any changes which would have a material impact to Parties as it doesn't have any impact to competition, security of the network but instead relates to how data is shared between Pipeline Operators and Pipeline Users of the IGT UNC.

Formatted: Superscript

Requested Next Steps

This modification should:

- be assessed by a Workgroup

3 Why Change?

What

The Password Protection Protocol Ancillary Document was amended under IGT118 (Amendments to the IGT UNC Password Protocols) to bring the provisions up to date with the information technology and mechanisms by which protected information is sent between the Pipeline User and Pipeline Operators within the industry for the portfolio and invoicing data. During the Working Group discussions for IGT118 it became apparent that more Protected Information was sent than the portfolio and invoicing data. Therefore, the scope needed to be widened because further consideration is needed to Section K23.2 of the IGT UNC e.g. how requests which contain MPRNs are sent and if they should be encrypted. To avoid delays in development to IGT118 the additional scope discussions were separated and were taken to a Review Group, which then formed the basis of this modification.

Why

Now that the Password Protection Protocol has been amended, Section K23.2 is out of date and needs to be brought in line to the amendments made under IGT118 to ensure transparency, clarity and consistency are applied to encrypting data which is sent under the IGT UNC.

In addition, there have been instances when MPRNs are sent across the industry which is deemed to be customerpersonal information for the purposes of Data Protection and is subject to the General Data Protection Regulation (GDPR). It would be considered as good governance to ensure that processes outlined in the IGT UNC are in line with the regulations and are clearly outlined for both Pipeline Operators and Pipeline Users ensuring that processes remain up to date and robust.

How

Amendments are to be made to Section K23.2 to keep them in line with those made to the Password Protection Protocol under IGT118.

All communications containing personalMPRN level data (including the MPRN, an address and/or Consumer information) in an email or contained within an attachment will have encryption applied in line with the Password Protection Protocol Ancillary Document.

The application of the password will be decided by the issuing organisation but where applied will be using the password and processes outlined in the Password Protection Protocol Ancillary Document.

Formatted: Superscript

4 Code Specific Matters

Technical Skillsets

IT security information may be required.

Knowledge of GDPR/Data Protection

5 Solution

To amend Section K23.2 in consideration of what is meant by 'Protected Information' and be clearer on the password encryption applied to communications (emails or within an attachment) containing MPRN data.

To continue with the consistent and robust transfer of data between the Pipeline Operator and the Pipeline User or the Pipeline User and the Pipeline Operator, we believe the scope of the Password Protection Protocol should be widened to include a provision for password protecting communications where it contains personal level data as defined in data protection legislationcontaining MPRN level data.

Where possible all emails and attachments containing personal level data as defined in data protection legislation should have a password encryption applied. The decision on whether password encryption should be applied will be at the sole discretion of the 'sending' organisation.

Section K23.2 has a requirement to encrypt the email or the attachment as a minimum to protect 'Protected Information'. And iIf the information contained in the body of an email cannot be encrypted to the standard and using passwords set out in the ancillary document then an encrypted attachment will be athe default. This, for example, could be an excel spreadsheet but is not limited to just that attachment type. The passwords applied are using existing processes outlined the Password Protection Protocol Ancillary Document.

Where the premise is a new connection and is part of a developer's portfolio it will be out of scope and therefore PSA/PSB will not require encryption, however, once a Consumer begins occupancy then encryption will be required to protect their data.

Any further consequential changes to the IGT UNC Ancillary Document (Password Protection Protocols) will be considered during the development of the solution.

Where personal information is not protected appropriately by the sender, the recipient of the information may seek to report it to the Information Commissioner's Office (ICO).

6 Impacts & Other Considerations

N/A

7 Relevant Objectives

Impact of the modification on the Relevant Objectives:

Relevant Objective	Identified impact
(A) Efficient and economic operation of the pipe-line system	None
(B) Co-ordinated, efficient and economic operation of (i) the combined pipe-line system; and/or (ii) the pipe-line system of one or more other relevant gas transporters	None
(C) Efficient discharge of the licensee's obligations	None
(D) Securing of effective competition: (i) between relevant shippers; (ii) between relevant suppliers; and/or (iii) between DN operators (who have entered into transportation agreements with other relevant gas transporters) and relevant shippers	None
(E) Provision of reasonable economic incentives for relevant suppliers to secure that the domestic customer supply security standards… are satisfied as respects the availability of gas to their domestic customers	None
(F) Promotion of efficiency in the implementation and administration of the Code	Positive
(G) Compliance with the Regulation and any relevant legally binding decisions of the European Commission and/or the Agency for the Cooperation of Energy Regulators	None

We believe Tthe proposed change supportsfalls within Relevant Objective (F) as it seeks to enhance and improve the administration and security applied to individual or small subsets of data by adding clarity to the provisions within code. It ensures a consistent mechanism as well as improving the secure means by which protected information is sent between the Pipeline User and the Pipeline Operator (and vice versa).

Although GDPR clearly articulates the legal standard the improvement to code drafting reduces ambiguity and possible misunderstanding, it also uses the password process which has already been created for an established process so it utilises an existing process rather than creating something brand new.

8 Implementation

February 2020

9 Legal Text

Part K Section 23 Legal Text for IGT130

Formatted: Superscript

The Proposer is welcome to put forward suggested legal text. If this is a proposed Fast Track Self-Governance modification then legal drafting and commentary must be provided. Otherwise the legal representative when requested to do so by the Modification Panel will provide formal legal text and commentary.

Text Commentary

In support of the legal text provided, the legal representative will provide a plain English explanatory note setting out the approach taken to converting the Solution into legal text, illustrating how the legal text delivers the intent of the Solution.

To be provided by the Transporters.

[Suggested] Text

The legal representative will provide the Text (to be inserted into Code) with instructions for the Code Administrator. The Text can be published alongside the main document.

Insert text here

10 Recommendations

Proposer's Recommendation to Panel

Panel is asked to:

- Agree that Self Governance procedures should apply; and
- Refer this proposal to a Workgroup for assessment.

11 Appendix 1

Amended 'Password Protection Protocols' Ancillary Document

Formatted: Superscript