






Draft Workgroup Report	At what stage is this document in the process?
<h1>IGT130:</h1> <h2>Applying password protection encryption to electronic communication</h2>	<div>01 Modification</div> <div>02 Workgroup Report</div> <div>03 Draft Modification Report</div> <div>04 Final Modification Report</div>
<p>Purpose of Modification:</p> <p>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.</p>	
	<p>The Proposer recommends that this modification should:</p> <ul style="list-style-type: none"> • be subject to self-governance • be assessed by a Workgroup <p>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.</p>
	<p>High Impact:</p>
	<p>Medium Impact:</p>
	<p>Low Impact:</p> <p>IGTs, Shippers, CDSP</p>

Contents		 Any questions?
1	Summary	3
2	Governance	3
3	Why Change?	3
4	Code Specific Matters	4
5	Solution	5
6	Impacts & Other Considerations	7
7	Relevant Objectives	7
8	Implementation	8
9	Legal Text	8
10	Recommendations	9
Timetable		
The Proposer recommends the following timetable:		
Initial consideration by Workgroup	3 rd September 2019	
Amended Modification considered by Workgroup	14 th February 2020	
Workgroup Report presented to Panel	28 th February 2020	
Draft Modification Report issued for consultation	6 th March 2020	
Consultation Close-out for representations	27 th March 2020	
Variation Request presented to Panel		
Final Modification Report available for Panel	3 rd April 2020	
Modification Panel decision	24 th April 2020	



Any questions?

Contact:

Code Administrator



[IGTUNC@gemse
rv.com](mailto:IGTUNC@gemse
rv.com)



020 7090 1044

Proposer:

E.ON

Kirsty Dudley



[Kirsty.Dudley@eone
nergy.com](mailto:Kirsty.Dudley@eone
nergy.com)

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 and/or data which can relate to a consumer or premise 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.

Essentially there is now a need to provide a mechanism to ensure any information can be passed between Pipeline Operators and Pipeline Users in a secure manner when the sender determines that it is necessary, both to meet code requirements for commercial confidentiality for example and to meet the requirements of data protection regulations in respect of personal data for example.

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.

Where the sender of any communication determines that it requires encryption, the sender will do so in line with the Password Protection Protocol Ancillary Document, for example all communications containing MPRN level data in an email or contained within an attachment.

2 Governance

Justification for Self-Governance Procedures

This change should be classed as Authority decision as there could be consumer impacts.

Although the modification could be perceived as code housekeeping to align processes, the decision could impact Parties' ability to adhere to legislation on data protection. Security failures in how data is shared between parties could have a material impact on consumers and code should be drafted in a way which provides and enables Parties to protect consumers and their data.

It is suggested this is an Authority decision rather than Self-Governance.

Requested Next Steps

This modification should:

- be assessed by a Workgroup

Workgroup Comments

The workgroup supported the proposer's recommendation that the modification be subject to Authority decision.

3 Why Change?

What

The Password Protection Protocol Ancillary Document was amended under IGT118 (Amendments to the IGT UNC Password Protection 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 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 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 personal 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 opened up for use in any situation which the sender believes confidentiality and security warrant its use.

This aligns to information which the Information Commissioner's Office (ICO) provided when responding to the Competition and Market Authority's "Energy market investigation; Notice of possible remedies" (August 2015) – a summary of this guidance is:

- "The Data Protection Act (1998) (DPA) is concerned with the processing of "personal data". Personal data is data which relates to a living individual who can be identified from that data either itself, or in combination with other information".
- "An MPAN uniquely identifies an electricity supply point, which is often a particular property (or a commercial property, where the business owner is a sole trader), is likely to be personal data even if the name of the individual (or individuals) who live there is not known".

Although this guidance specifies electricity the principles would also apply in gas.

Additionally, Ofgem have confirmed that in conversations with the ICO (point 2.28 Page 10, Ofgem's [Retail Energy Code: Technical Specification approach consultation](#)) that "Metering Point Administration

Number (MPAN) and Metering Point Reference Number (MPRN) should be classified as Personal Data for the purposes of GDPR compliance.

Although not codified in the UNC or DSC in the detail proposed in this modification, communications which contain data which can relate to a person or premise are encrypted by the CDSP. The frequency of the password changes is more regular than those outlined in the Password Protection Protocols ancillary document, and they are applied to documents which require it and cover in some cases both GT and IGT supplies. The process to extend / introduce encryption into the IGT UNC would be an aligned approach to what is already delivered and would bring consistency in approach.

The SPAA and MRA have chosen to introduce a portal for Supplier to Supplier communications. Although this could be expanded to Transporter to Shipper communication the IGTs are not already using this and it would be a far greater development to introduce this portal compared to extending the use of the encryption and password protection processes already available under the IGT UNC

How

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

All communications containing personal 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.

4 Code Specific Matters

Technical Skillsets

IT security information may be required.

Knowledge of GDPR/Data Protection

5 Solution

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

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, the Password Protection Protocol should be expanded to include a provision for password protecting communications where the sender believes it is required including where it contains personal level data as defined in data protection legislation.

Emails and attachments containing personal level data as defined in data protection legislation should have password encryption applied.

Section K23 introduces a requirement for parties to accept the communication mechanism choice of the sender, so long as the mechanism is provided for within the code or through processes. The solution

does not place additional requirements on parties to use a mechanism in particular circumstances nor does it constrain the use of a mechanism.

The IGT UNC processes need to include a mechanism for securing communications and parties are free to use this mechanism when they feel it is appropriate both for the purpose of code requirements and for the purposes of data protection legislation.

The processes available must include encryption and if the information contained in the body of an email cannot be encrypted to the standard using passwords set out in the ancillary document, then an encrypted attachment will be the default. This, for example, could be an excel spreadsheet but is not limited to just that attachment type. The passwords applied are using the existing processes outlined in the Password Protection Protocol Ancillary Document.

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

Workgroup Comments

General observations supported by the whole Workgroup were that:

- The Master Registration Agreement (MRA) and Supply Point Administration Agreement (SPAA) have each brought in a secure portal in order to support secure communications. Currently the transporters are not part of the development of the platform in the MRA/SPAA, this is currently just for Suppliers. To introduce this into the IGT UNC was not deemed to be a cost-effective approach at this time.
- A period for implementation might be needed for this modification and a minimum period of 3 months was discussed. It was felt that multiple teams within organisations are likely to be impacted and that the complexity and issues arising from the briefings and training required would justify this. It was concluded that everyone should implement at the same time and not when individuals are ready.
- A codified mechanism for increased security for communications is needed to ensure that data protection considerations can be managed adequately and not through varied approaches per organisation.

Pipeline operators indicated that:

- The solution is too broad and is not seen as an efficient approach for the issue articulated in the modification. Nor is it seen to be in keeping with the existing Password Protection Protocols process.
- An increase in encrypted emails for all Parties, both Pipeline Operators and Users, is anticipated. This was not quantified, but it was expected that the increase would be difficult to manage in terms of operations and processes. It was suggested that more clarity around the process would be needed rather than taking a 'blanket approach'. There was concern that some shippers may struggle with encryption as there is evidence that some shippers are currently challenging the encryption applied to invoice backing data which is already outlined in the Password Protection Protocols.

The Proposer indicated that:

- The solution is an extension of a currently used process for sending backing / portfolio data as outlined already in the Password Protection Protocols rather than creating a brand-new process or being too prescriptive in code.

- The Central Data Service Provider (CDSP) applies a similar process for encrypting emails with consumer data which the proposal aligns to.
- The decision on when and whether data is subject to data protection legislation is a matter for the sender of the data and therefore the encryption decision is the responsibility of the Party wanting additional security / protection.

Pipeline users indicated that they had no additional comments and supported those of the proposer.

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

The proposed change supports Relevant Objective (F) as it seeks to enhance and improve the administration and security applied to individual or smaller subsets of data by adding clarity to the provisions within code. It ensures a consistent mechanism 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.

Workgroup Comments

There was no disagreement with the proposer's view.

It was noted that as the sender of the email determines when to use encryption, that some may choose not to use it and therefore that some parties may not implement this solution, and interpretation of GDPR could make the application of this change inconsistent for all parties.

However, there was agreement that the application of the solution would provide a mechanism to send data securely if the sender wished to do so.

8 Implementation

Next release following Authority decision.

Workgroup Comments

The proposer would be happy if the implementation period is between 3 and 6 months. This timeframe would allow a suitable window for Pipeline Operator and User teams to discuss and implement arrangements for the process going forwards.

The workgroup agreed that the implementation period should be a minimum of 3 months and that if this could not be achieved before the next scheduled code release, then the implementation should automatically be rolled into the one after that.

The group concluded that a phased delivery was not suitable and ideally all parties would implement at the same time to ensure readiness across Pipeline Operators and Pipeline Users.

9 Legal Text

Draft legal text can be found on the following links

[IGT UNC Part K Section 23](#)

[IGT UNC Ancillary Document "Password Protection Protocols"](#)

Workgroup Comments

The Workgroup agreed that the legal text met the intent of the change and there were no further comments.

10 Recommendations

Workgroup's Recommendation to Panel

The Workgroup asks Panel to agree that:

- this modification proposal is sufficiently developed to go out to consultation.

11 Appendix

[Amended 'Password Protection Protocols' Ancillary Document](#)