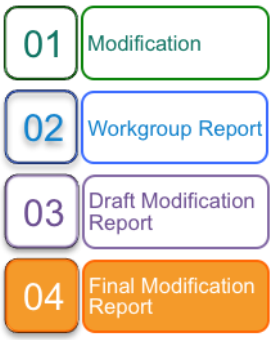
IGT | UNC

Final Modification Report	At what stage is this document in the process?

IGT130: Applying password protection encryption to electronic communication



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.

	Panel consideration is due on 24th April 2020 The Panel has decided to implement under self-governance rules.
	
	High Impact: None
	Medium Impact: None
	Low Impact: IGTs, Shippers, CDSP

IGT | UNC

Contents

Timeline

The Proposer recommends the following timetable:

Initial consideration by Workgroup	3rd September 2019
Amended Modification considered by Workgroup	14th February 2020
Workgroup Report presented to Panel	28th February 2020
Draft Modification Report issued for consultation	13th March 2020
Consultation Close-out for representations	3rd April 2020
Variation Request presented to Panel	
Final Modification Report available for Panel	17th April 2020
Modification Panel decision	24th April 2020

Any questions?

Contact:
Code Administrator

iGTUNC@gemserv.com

020 7090 1044

Proposer:
Kirsty Dudley

Kirsty.Dudley@eonenergy.com

07816 172 645

Any questions?

Comments

The proposer has changed their initial recommendation to the Panel that the modification be subject to Self-Governance and would now like the modification to be subject to Authority Decision.

The Panel are particularly interested to receive the views of Parties on the Governance of this modification (whether it should be subject to Self-Governance or Authority Decision) and the justification / reasons for their views and have asked that this be highlighted to respondents.

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 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 subject to Authority decision
- 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 legalisation.

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 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 the 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

Suggested Text

IGT UNC Part K section 38

Ancillary Document "password protection controls"

Workgroup Comments

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

10 Consultation

Representations were received from the following parties:

Organisation	Response	Relevant Objectives	Key Points
BUUK	Do not support	No objectives met	• The Modification lacks certainty. Due to the proposer making the decision as to whether the email requires encryption or not, there is bound to be a lack of uniformity for code operations. As a result, we are unable to anticipate how many encrypted emails we will need to facilitate. The issue here doesn't solely apply to IGTs as it is suggested some Shippers already struggle with the encryption applied through the password protection protocols. • The solution attempts to apply an existing mechanism for processes to a type of data. In itself creating inconsistencies but this also fails to consider existing duties and operations from parties to meet GDPR obligations. Measures can already be taken to improve communication between industry parties without the need for stringent password protection protocols. • We ultimately believe that the modification adds no value to the code and paves the way to greater levels of uncertainty surrounding encryption. Parties should therefore rely on existing processes and trust in abilities of other parties to meet GDPR obligations until a more practical and useful solution can be brought to the table • Mod governance - We are neutral in our outlook on this matter. • The implementation of this modification seeks to enhance the administration and security of the mechanism by which the code proscribes protected information sent between code parties. However due to the proposer determining whether to encrypt or not this solution may not be uniformly implemented and thus cause inefficiencies by parties making resources available for emails that they will not receive. It is therefore felt that the

			objectives are not met from this change as the proposed solution can provide no certainty as to the impact on parties. • Due to uncertainty with regards to the scope of what will and will not be encrypted, and from whom, it is very difficult to predict development and ongoing costs if this modification is implemented. As there is no certainty, we cannot predict the levels of time and resource required to deal with the effects of this change. This isn't just anticipated as an issue for us, but also for other IGT and Shipper parties where the inconsistency created from the proposed solution has the potential to cause issues for multiple industry parties, and thus fail to meet the intent of the change. • Should the modification be implemented, we would like to see an extended implementation period of at least 3 to 6 months in order for preparations to be put in place to deal with the encryption. This would allow IGT and Shipper operational staff to discuss with one another plans and suitable communication routes for sending such information. It should be noted however that this approach of cooperation between parties can be utilised in the world today without the need to follow strict password protection protocols that were intended for specific processes, rather than types of data. • Yes, we agree the drafted legal text meets the solution put forward. • We would like to reinforce our view that it is not the intent of the change we have issue with. We support the proposer's intent to ensure the protection of customer data. However, we feel that the GDPR requirements mandate such assurance and that this proposal adds nothing more. Protection of personal data is of upmost importance and should be treated thusly. However, it is not felt that the solution this change puts forward will have a beneficial effect on such arrangements. The open-ended nature has the potential to cause

			additional problems and inconsistencies for companies. Failing to take into account real world company operations and adherence to GDPR obligations, which require efficient and safe use of personal data. Without the need for additional steps such as those proposed by this change. • It's unfortunate that the review group which formed the basis of this change was unable to yield a better solution proposal, but that is not seen as a valid reason to continue with an approach that will do more harm than good.
ESP Utilities Group	Supports	(F) positive impact	• ESP supports this modification as it will improve consistency in the application of security protocols for incoming and outgoing communications that are deemed to require encryption by one or both parties. • Mod Governance - Yes, we agree that this should be a self-governance modification. • This modification will positively impact the administration of the code by adding a mechanism that facilitates consistency of encrypted communications between code parties. • We would not face any direct costs if this modification were implemented. We note that the modification may potentially mean some communications fall under the password protection protocols that did not fit the relevant criteria prior to implementation. If the volume of reclassified communications is high, this will likely require increased resource to manage. • We agree with the proposer that a lead time of three to six months would be sufficient for parties to put processes in place to meet the requirements. • Yes, we believe the legal text will satisfactorily deliver the intent of the modification.
Indigo Pipelines	Do not support	(F) negative impact	• We feel the proposed solution is heavy-handed and not proportionate to the risk.

			Existing data protection regulations, including GDPR, adequately address the issue identified. • There are very few scenarios in which Shippers actually need to send customers' personal data to the Transporter, and these should already be by protected means. For example, Special Needs and Emergency Contact details are exchanged via Xoserve's secure IX network and meter works booking forms are already emailed as password protected attachments. • Where Shippers are sending more general enquires, such as Supply Point or Meter data enquiries, there should be no need to send customer's personal data in the query. All parties should already be educating staff about data protection and ensuring they limit the exchange of personal data. • An MPRN is the unique reference number assigned to a gas service pipe, by itself it does not identify an individual or business occupying the property that is served by the gas service pipe; the occupier does not 'own' the MPRN and does not take it with them when they move out, as such the MPRN is 'neutral' to the identity of the occupier. • We feel that mandating password protection of all and any communications containing an MPRN is not necessary as MPRNs are in the public domain and do not by themselves identify an individual. Where the MPRN is being exchanged in conjunction with personal data then it must be protected, in compliance with existing rules. • Mod Governance - Yes, it should be self-governance • This proposal impact Objective F (Efficiency in the Implementation and Administration of the Code) but we do not agree with the Proposer that it is a Positive impact. We feel that the additional burden will hinder efficiency in administration of the Code. • This would make communications between parties more complicated and time-

			consuming, potentially necessitating additional staff to manage the process due the additional tasks involved in encrypting/decrypting files, exchanging additional emails with password information, etc. Shippers will need to share their passwords internally more widely than they currently do to ensure all departments who might send queries to the Transporter are fully briefed and aware of the new process and passwords • This could be implemented 3 months after approval • The draft legal text meets the intent of the Modification.
SSE Business Energy	Supports	(F) positive impact	• We support this modification to provide a mechanism to send data securely, encouraging use of password/ encryption processes to protect confidential data for the good of iGT UNC parties and customers. • We agree with the proposer's amended recommendation to the Panel that the modification be subject to Authority decision. • We agree that the modification furthers relevant objective F in promoting efficiency in implementation and administration of the Code. • We do not anticipate development or ongoing costs relating to this modification. • We would support a 3 – 6 month lead time to implementation in order to communicate internally for awareness of the change. • Are you satisfied that the legal text will deliver the intent of the modification? Yes.
E.ON	Supports	(F) positive impact	• As the proposers of the modification we support the implementation of these changes. It seeks to ensure a robust approach to data encryption and not just applying encryption to larger data transfers such as the portfolios but to smaller subsets of data too. • Protection of consumer data is at the heart of this change and the mod has not mirrored the supplier approach by introducing a portal but

			instead it has extended the current protocols which in a time of unprecedented change e.g. Switching and Code Consolidation SCRs we believe is sensible. • The modification allows the sender of the data to be the decision maker on 'if' the protocols are needed, which is hoped to be a less resource intensive approach and in line with the GDPR principles. The approach proposed is lighter touch because it isn't saying all communication containing MPRs 'must' be encrypted, this is because there are some processes in the IGT UNC which wouldn't require encryption so could have made it cumbersome. • We support codifying the sender driven decision making approach because it is robust enough clarify the encryption used rather than everyone doing something different, but sensible enough not to force an overhaul of either Pipeline Operator or Pipeline User processes by overengineering the encryption process. • We support the change being Authority decision due to the legislative links to GDPR and how the application of this modification could have impacts on consumer data. Although we recognise this could have been seen as a housekeeping modification, we believe robust Authority decision making is required. • We also recognise the divide in the views of the Pipeline Operators against those of the Pipeline Users and with the current unequal weighting of the IGT UNC Panel we believe that an Authority decision is a fair and transparent approach for the modification. Although unpredicted we believe this is the correct approach, we would like to stress we do not believe that the IGTs would intentionally use the uneven weighting to their advantage, but we still believe Authority decision is a fairer approach especially with the clearly split constituency views on this modification. • The modification supports Objective (F)

			because it seeks to introduce a consistent data encryption approach regardless of the size of the data set which is being shared. • We have identified that manual process changes will occur to either decrypt or encrypt the data shared, we have noted this as a 'low cost' change. As our organisation forward plan passwords it would be a low cost impact to us. • To allow parties readiness we would be happy to deliver this within 3-6 months of Authority approval, we would ideally like an earlier implementation but recognise that November 2020 is a likely candidate and we believe even with the amount of change occurring in the industry that it is a deliverable date. • Are you satisfied that the legal text will deliver the intent of the modification? Yes, no comments.

In summary:

- Five responses were received to the consultation for IGT30 from three Pipelines Operators and two Pipeline Users.
- Three respondents offered support for and two respondents did not support this modification.
- Three respondents agreed that the modification had a positive impact on relevant objective (F) Promotion of efficiency in the implementation and administration of the Code and one respondent believed it had a negative impact on (F). Another respondent believed that none of the relevant objectives were met by the modification.
- All respondents agreed that implementation should be 3 to 6 months after approval of the modification.
- All respondents believed that the legal text met the intent of the modification.
- Two respondents challenged the efficiency of the solution and indicated that the intent of the modification could be met in another way.

With regards to the Panel's enquiry for views on the governance of the modification:

- Two respondents agreed that this should be an authority decision.
- Two respondents noted that the modification should be subject to self-governance.
- One respondent noted they were neutral

11 Panel Discussions

Discussion

The Panel members reviewed why the proposer had recommended that the modification be an Authority Decision along with the views expressed in the consultation responses and those of the workgroup on this matter. The Panel and the Ofgem representative discussed whether the modification fulfilled the self-governance criteria and all present concluded that it did.

The Panel did not all agree that the mod would have a positive impact on the promotion of efficiency in the implementation and administration of the Code and some believed that there could be a negative impact due to the solution not being efficient or no impact due to Parties already being subject to and required to comply with General Data Protection Regulations.

The Panel considered the timing of implementation. All consultation respondents indicated that they required between 3 and 6 months to implement the modification. However, the Panel considered the new circumstances of the current Covid lockdown and felt that the implementation would now need a longer period. The Panel agreed that to ensure sufficient time for implementation the mod should be incorporated within the February 2021 Code release.

Consideration of the Relevant Objectives

The Panel agreed that relevant objective (f) Promotion of efficiency in the implementation and administration of the Code was impacted by the modification but were not in agreement that the impact was positive.

Determinations

The Panel determined that this modification be subject to Self-Governance decision.

The Panel determined that this modification be implemented.

The Panel determined that this modification be implemented in the February 2021 release.

12 Recommendations

Panel Determination under Self-Governance

Members agreed:

- that Modification 130 should be subject to Self-governance and implemented.