

Modification proposal:	iGT UNC: "Password Protection Protocols for invoice supporting data and Portfolio Extracts" (iGT026V)		
Decision:	The Authority ¹ directs that this proposal be made		
Target audience:	Independent Gas Transporters (iGTs), Parties to the iGT UNC and other interested parties		
Date of publication:	29 April 2010	Implementation Date:	To be confirmed

Background to the modification proposal

The Data Protection Act 1998² requires companies to deploy 'appropriate technical and organisational measures' to protect personal data. Large amounts of commercially sensitive data pass between the Pipeline Operators and Pipeline Users who are parties to the iGT UNC, including data relating to invoicing and customer portfolios. This data currently transfers in various formats, including by portable media – CD/DVD – and by email, which are not protected and are considered insecure. The lack of security around this commercially sensitive data leaves it open to disclosure to, and potential misuse by, unintended recipients.

Modification proposal iGT026 was raised to address this defect through changes to the iGT UNC.

The modification proposal

EON UK (the proposer) raised iGT026 in October 2009. The proposer noted that the current practice by which data passes between Pipeline Operators and Users is not secure and could potentially be in breach of parties' data protection obligations. Some minor variations were made to the modification proposal before it was consulted on as iGT026V. The Modification aims to bring the current arrangements for transferring data into compliance with the data protection obligations:

- by stating that password protection is a requirement under Section K clause 23.2 of the iGT UNC (entitled 'Protected Information') which applies to portfolio extract data and invoice supporting data sent by email, CD or DVD; and
- by creating an iGT UNC Ancillary Document called Password Protection Protocol. The Protocol would explain the format of passwords to be used for the transferred data, how often they should change, and a preferred secure means of undertaking data transfers using password protection. Passwords would be provided by Users to Operators

The proposer recommended that the software used to secure files by password protection should be at least cost to assist small parties. The default software to be used (in the case of zipped files) would be WinZip7 which is available as a free download, although Users and Operators could agree an alternative.

Panel recommendation

The Panel was split equally between those recommending that the Modification is implemented and those who do not. The Panel therefore did not recommend approval of Modification iGT026V.

¹ The terms 'the Authority', 'Ofgem' and 'we' are used interchangeably in this document. Ofgem is the Office of the Gas and Electricity Markets Authority.

² Schedule 1 of Part 1.

All Panel Members agreed that the Modification would better meet code relevant objective (d) as it would introduce a security process into the iGT UNC that would reduce the potential for data to be passed on to competitors, thereby improving effective competition overall between shippers and suppliers.

Three Panel Members who supported the Modification agreed that it would also better meet code relevant objectives (a) and (f) by requiring the use of password protection to help secure sensitive data passed between parties. In their view, the effect of doing so would be to increase the efficiency of pipeline operation and increase efficient administration of the code arrangements by reducing the potential for erroneous communication between Pipeline Users and Operators.

The three Panel Members who voted against the Modification stated that it would not better meet relevant objectives (a) and (f), and that this outweighed their reason for supporting the Modification in relation to relevant objective (d). In their view the cost of implementing the new process would not necessarily provide a higher level of security and hence would be inefficient.

The Panel did not recommend an implementation date for the proposed changes. The proposer set out that the changes should take place no later than four months from the date of an Authority decision. This would ensure that data is secured as early as possible through password protection and minimise the risk that parties are in breach of data protection obligations.

The Authority's decision

The Authority has considered the issues raised by the modification proposal and the Final Modification Report (FMR) dated 24 March 2010. The Authority has concluded that:

1. implementation of the modification proposal would further the relevant objectives as defined in Standard Condition 9 of the Gas Transporters Licence³; and
2. directing that the modification be made is consistent with the Authority's principal objective and statutory duties.

Reasons for Authority decision

We consider that the Modification better meets code relevant objective (f) compared with the existing baseline. We provide our reasons below.

We note that those Panel members supporting the Modification also considered that code relevant objectives (a) (efficient and economic operation of the pipeline system) and (d) (securing effective competition between shippers and between suppliers) may be better met. However, in our view, there is a marginal impact on the efficiency of pipeline operation by securing sensitive data through password protection. We also regard the effect on competition to be marginal, although we do note that the mis-direction and subsequent misuse of sensitive data may have the potential to distort competition between shippers and between suppliers.

Code relevant objective (f) (the promotion of efficiency in the implementation and administration of the code)

We agree with the Panel and all consultation respondents who support the principle behind the Modification, namely, that commercially sensitive data ought to be secure. If data falls into the hands of those to whom it was not directed, and even if those parties disposed of the data without opening it, there may still be an adverse effect on the

³ http://epr.ofgem.gov.uk/document_fetch.php?documentid=13355

efficient administration of code arrangements. This principle is underpinned by the legal obligations that parties handling sensitive data need to meet under the Data Protection Act.

We agree that password protection offers some level of security over sensitive data and also allows parties to the iGT UNC to meet their wider legal obligations on securing data.

The proposed solution

We note that, despite full support for the principle of securing data through password protection, there is a difference of opinion on how best to achieve this. This difference rests on the balance between costs and security associated with the proposed solution.

We note the proposer's view that free (or very low cost) password protection software should be used to implement the solution. While it is preferable to develop as low cost a solution as possible, we note the concerns of some respondents that the software may not be sufficiently secure. Some respondents also suggested the use of a secure File Transfer Protocol (FTP) solution which, according to one respondent, costs a few hundred pounds but is regarded as more secure.

In our view, there is a balance required between the cost of the proposed solution and the level of security for sensitive data provided. We consider that the proposed Password Protection Protocol is drafted flexibly to allow Users and Operators to agree an alternative solution as a pragmatic approach but that an agreed baseline solution would be optimal.

We consider that the implementation of the Modification would ensure that the code arrangements are administered in an efficient way that effectively reduces the risk of data falling into the hands of unintended recipients at a reasonable cost. We therefore consider that the Modification does better meet code relevant objective (f).

We agree with the proposer that implementation of the Modification should take place as soon as possible and within four months of this decision. All iGT UNC parties should consider how best to implement the proposed solution during that period and seek to develop an agreed uniform baseline. A satisfactory resolution would ensure that password protection is deployed in the most effective way.

Decision notice

The Authority directs that modification proposal iGT026V: "Password Protection Protocols for invoice supporting data and Portfolio Extracts" be made.

Mark Cox

Associate Partner, Transmission and Governance

Signed on behalf of the Authority and authorised for that purpose.