





IGT UNC Request Workgroup Report	At what stage is this document in the process?
<h1>RG007:</h1> <h2>Secure measures of sending electronic communication and password protection</h2>	<div> <div>01</div> <div>Modification</div> </div> <div> <div>02</div> <div>Workgroup Report</div> </div> <div> <div>03</div> <div>Draft Modification Report</div> </div> <div> <div>04</div> <div>Final Modification Report</div> </div>
<p><b>Purpose of Request:</b></p> <p>Following the implementation of IGT118 it became apparent that the password protection protocol needs to be given a wider scope to cover additional measures that are currently not within this scope. The aim of this Review Group was to address these issues and widen the scope of the protocol.</p>	
	<p>The Panel will consider this Workgroup Report on 20<sup>th</sup> September 2019. The Panel will consider the recommendations and determine the appropriate next steps.</p>
	<p>High Impact:</p> <p>Pipeline Users, Pipeline Operators</p>
	<p>Medium Impact:</p> <p>N/A</p>
	<p>Low Impact:</p> <p>N/A</p>

## Contents

<b>1</b>	<b>Request Summary</b>	<b>3</b>
<b>2</b>	<b>Impacts and Costs</b>	<b>4</b>
<b>3</b>	<b>Terms of Reference</b>	<b>5</b>
<b>4</b>	<b>Review Group Update</b>	<b>6</b>
<b>5</b>	<b>Modifications</b>	<b>7</b>
<b>6</b>	<b>Recommendations</b>	<b>7</b>
<b>7</b>	<b>Appendix 1</b>	<b>7</b>

## About this document:

This document is a Workgroup report which recommends that Review Group (RG) 007 has now completed its requested action. This will be presented to the Panel on 20<sup>th</sup> September 2019.

The Panel will consider the Workgroups recommendations and conclusions with respect to any subsequent modifications needed in light of the findings of the RG.



**Any questions?**

Contact:

**Code Administrator**



[IGTUNC@Gemserv.com](mailto:IGTUNC@Gemserv.com)



**02070901044**

Proposer:

**Radhika Kalra**

**E.ON**



[radhika.kalra@eonergergy.com](mailto:radhika.kalra@eonergergy.com)



**07971810459**

## 1 Request Summary

### Why is the Request being made?

This RG was requested following discussions that took place with IGT118 which sought to widen the scope of that modification. However, the objective of IGT118 was to bring the Password Protection Protocol up to date with references to technology and the mechanisms by which protected information is sent. Discussions at the Workgroup on IGT118 highlighted additional areas where password protection should be used in order to offer wider protection when confidential information is being sent from one organisation to another.

### Scope

The proposed scope of this review was to consider the updated Password Protection Protocol as well as ideas that arose from the workgroup discussions regarding IGT118 to widen the scope of the protocols, and any additional parts of the IGT UNC which contain processes by which confidential information is sent between industry parties and may need to be sent in a more secure format. Consideration was given to Part K 23.2A of the main body to determine whether it needed to be revised to point only to the protocols.

### Recommendations

#### Objectives

- To consider the information which is currently sent between parties which falls within the scope of the Password Protection Protocols and to determine whether there is additional information that is sent between parties that does not fall under the scope of the protocols
- To determine whether the Password Protection Protocol needs to have a wider scope to cover the information type and the mechanisms by which confidential information is sent between IGT UNC parties
- To review the legal text to determine whether it needs to be revised in light of the Password Protection Protocols

### Additional Information

None

## 2 Impacts and Costs

### Consideration of Wider Industry Impacts

#### Impacts & Costs

No direct impacts or costs were envisaged as a result of the proposed work for this RG, but there are likely to be impacts seen in the mechanism of sending confidential information to parties across the industry by inclusion of a password or alternative document delivery mechanism(s).

#### Impacts

Impact on Central Systems and Process	
Central System/Process	Potential impact
UK Link	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Operational Processes	<ul style="list-style-type: none"> <li>The addition of a password when sending electronic communications to other parties containing commercially sensitive data</li> </ul>

Impact on Users	
Area of Users' business	Potential impact
Administrative and operational	<ul style="list-style-type: none"> <li>The addition of a password when sending electronic communications to other parties containing commercially sensitive data</li> </ul>
Development, capital and operating costs	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Contractual risks	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Legislative, regulatory and contractual obligations and relationships	<ul style="list-style-type: none"> <li>Password protection measures for electronic communication may be updated in the IGT UNC</li> </ul>

Impact on Transporters	
Area of IGT business	Potential impact
System operation	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Development, capital and operating costs	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Recovery of costs	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Price regulation	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Contractual risks	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Legislative, regulatory and contractual obligations and relationships	<ul style="list-style-type: none"> <li>Password protection measures for electronic communication may be updated in the IGT UNC</li> </ul>
Standards of service	<ul style="list-style-type: none"> <li>N/A</li> </ul>

#### Impact on Code Administration

Area of Code Administration	Potential impact
Modification Rules	<ul style="list-style-type: none"> <li>N/A</li> </ul>
iGT UNC Panel	<ul style="list-style-type: none"> <li>N/A</li> </ul>
General administration	<ul style="list-style-type: none"> <li>Involvement in communicating updated passwords</li> </ul>

#### Impact on Code

Code section	Potential impact
IGT Network Codes	<ul style="list-style-type: none"> <li>Part K 23.2A of the main body</li> </ul>

#### Impact on iGT UNC Related Documents and Other Referenced Documents

Related Document(s)	Potential impact
IGT UNC Ancillary & Guidance Documents	<ul style="list-style-type: none"> <li>Password Protection Protocol</li> </ul>

#### Other Impacts

Item impacted	Potential impact
Security of Supply	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Operation of the Total System	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Industry fragmentation	<ul style="list-style-type: none"> <li>N/A</li> </ul>

## 3 Terms of Reference

### Background

The proposed scope of this review was to consider the updated Password Protection Protocol as well as ideas that arose from the workgroup discussions regarding IGT118 to widen the scope of the protocols, and any additional parts of the IGT UNC which contain processes by which confidential information is sent between industry parties and may need to be sent in a more secure format. Consideration was given to Part K 23.2A of the main body to determine whether it needs to be revised to point only to the protocols.

#### Objectives

- To consider the information which is currently sent between parties which falls within the scope of the Password Protection Protocols and to determine whether there is additional information that is sent between parties that does not fall under the scope of the protocols
- To determine whether the Password Protection Protocol needs to have a wider scope to cover the information type and the mechanisms by which confidential information is sent between IGT UNC parties

- To review the legal text to determine whether it needs to be revised in light of the Password Protection Protocols

## Topics for Discussion

- Understanding the objectives
- Assessment of alternative means to achieve the objectives
- Development of Solution (including business rules if appropriate)
- Assessment of potential impacts of the Request
- Benefit of alignment with UNC
- Assessment of legal text.

## Outputs

Produce a Workgroup Report for submission to the Modification Panel, containing the assessment and recommendations of the Workgroup including a draft modification where appropriate.

## Composition of Workgroup

The Workgroup was open to any party that wished to attend or participate.

A Workgroup meeting will be quorate provided at least two Transporter and two User representatives are present.

## Meeting Arrangements

Meetings were administered by Gemserv and conducted in accordance with the Code Administration Code of Practice.

# 4 Review Group Update

## Workgroup Update

At the first meeting for RG007, members discussed varying solutions in regards to protecting personal information. Attendees agreed that a breach of personal information would constitute a compliance issue with respect to the General Data Protection Regulation (GDPR). The RG Proposer indicated that they sought a single standard codified process that protects personal data at a baseline level. The Proposer asked RG members to review internal processes and in particular how they handled 'Protected Information' and feed this back to the second meeting.

At the second meeting held on 6<sup>th</sup> August 2019, the Proposer presented a draft modification proposal. The Proposer indicated that the draft modification proposal solution states that any MPRN level data should be encrypted. The Review Group members concluded that it was important to protect data sent to and from Pipeline Operators/Users. From these findings, the Review Group Proposer formally submitted [IGT130 – Applying password protection to electronic communication containing MPRNs](#) on 12<sup>th</sup> August 2019 for Panel review.

At the third meeting on 3<sup>rd</sup> September 2019, the RG attendees agreed - that through the raising of IGT130 – the objectives of the RG had been met, and the recommendation could be made to the IGT UNC Modification Panel to formally close the RG.

## 5 Modifications

### Potential Modifications needed

The Review Group Proposer drafted a modification proposal as a result of the findings from the first review group held on 2<sup>nd</sup> July 2019. The draft modification proposal for [IGT130 – Applying password protection to electronic communication containing MPRNs](#) was reviewed at the review group on 6<sup>th</sup> August 2019. From these findings, the Review Group Proposer formally submitted [IGT130 – Applying password protection to electronic communication containing MPRNs](#) on 12<sup>th</sup> August 2019 for Panel review.

## 6 Recommendations

### Workgroup's Recommendation to Panel

The Workgroup asks Panel to:

- Accept the findings in this report;
- Close the Review Group

## 7 Appendix 1

Below is a list of relevant documents produced by the Review group:

- [IGT130 – Applying password protection to electronic communication containing MPRNs](#)