Understanding the level of encryption required for TOTSCo

There has recently been some debate about what type and level of encryption would be necessary and appropriate for TOTSCo. There are several different drivers for what data should be encrypted and to what extent.
Below is an outline description of the issues as I understand them. Please get back to me with your views and inputs.

Gita Sorensen
TOTSCo Director – New infrastructure providers constituency
You can reach me on gita.sorensen@totsco.org.uk

The TOTSCo RFP states that:

"The 3rd Party must ensure that TOTSCo Information classified as confidential or higher, is appropriately encrypted (in transit and at rest) and all encryption shall be accomplished with strong, modern cryptographic algorithms and ciphers employing robust integrity protection mechanisms and in accordance with industry standards for secure key and protocol negotiation and key management. For data in transit the following TLS options are not allowed: TLS v1.0, TLS v1.1, v6.0, TLS v6.1 and SSL (any version). Encryption will be to a minimum of TLS v1.2."

The vendor will implement encryption at "Rest" – which means that the data will be stored (for a brief) moment in the "Mailbox" in an encrypted form. TLS (the padlock on websites) will also add another layer of encryption which is used when the data is in "transit", which has never been broken/hacked and therefore is safe from "bad actors/hackers" reading the message data.

With "end to end" encryption ("E2EE"), **some or all** of the message is encrypted by the sender and, facilitated by an exchange of keys, only the ultimate recipient can read it. Thus, data encrypted in this way cannot be read by the Hub. Access to some of the message is necessary for routing of messages.

We can set the E2EE to apply to all or just some parts of the message, e.g. personal data only.

The sensitivities expressed by CPs are:

1. Visibility of Personal Data: If we use transport layer encryption only and therefore data is unencrypted while in the Hub, then we TOTSCo can "see" personal data (name, address, telephone number, services consumed etc). This means that TOTSCo is treated as a data processor and CPs and TOTSCo need to put the right risk-assessments and agreements in place and manage any risks. (E2EE of some or all of the message solves this issue.) In addition, TOTSCo can see the message type (see below) from which commercially sensitive information can be generated.
2. Visibility of Commercially Sensitive Data: Even where E2EE is used, but only to encrypt the personal data and nothing else, the "message type" is still visible to TOTSCo. This means that TOTSCo can generate reports which could be commercially sensitive, e.g. who is winning business and from whom. We could also monitor some forms of SLA compliance (e.g. if any CP is rejecting a higher than average share of match requests, or is taking longer than 60

seconds to respond). There are a number of message types, corresponding to the three sets of message exchanges around which the IP is built (i.e. match request, switch order, switch complete).

The argument against using E2EE at any level is that it introduces operational complications and new failure modes. The system requires each CP to upload a "public key" to the directory of the Hub. Any CP sending a message has to encrypt that message using the recipient's key, which they download from the directory. The recipient uses their "private key" – which is known only to them - to de-crypt the message. (Public and private keys are generated as a set and they are refreshed at intervals – typically months but potentially more or less.)

The decision on encryption is a balance between operational simplicity on one hand, and risks around data protection and security on the other. TOTSCo has generated a Failure Mode and Effect Analysis (FMEA) to assess the operational fragility issues. The other side of the equation is an assessment of the way in which personal data could leak from the Hub. The transitory nature of the data in the Hub is helpful in reducing the risk. CPs' views of data protection are of course important. However, note that E2EE was not required by the OTS Steering Group when designing the Industry Process, and this Group would have been well aware of data protection issues.

The "what should we report to Ofcom?" is largely an independent question to that of encryption. We could use either method of encryption and still have the ability to generate the data. Only in the case where E2EE is used to encrypt the whole message would we not be in a situation to generate any commercially sensitive information.

The data is very secure by design from a OTS hub point of view. The breaches may occur at the CP level whereby their data may be at risk whilst it being prepared or read in their systems, but this is outside the scope of the HUB. There are elements of the message that the hub must see in order to function as intended. This includes routing information and other salient attributes used by the Hub.