TOTSCo Bulletin No 12 – Amended on 12 July to include responses we received

DATE: 12 June 2023

SUBJECT: End-to-End Encryption ("E2EE") at One-Touch Switch ("OTS") Go-Live

We have amended this Bulletin on 12 July to include the responses we received. To respect confidentiality and privacy, we have not included the names of the respondents. We have admitted responses from those that asked for their response to be confidential.

Introduction

Several Communications Providers ("CPs") have asked TOTSCo to consider implementing, at OTS go-live, the end-to-end encryption of messages sent through the TOTSCo Hub ("the Hub"), to reduce the risk of a loss of personal information contained in these messages.

In considering this request, TOTSCo:

- Drew on the knowledge and experience of its staff and others engaged in the OTS project,
- Consulted external technical experts,
- Consulted Hub users through a Request for Feedback, dated 14th April 2023,
- Consulted Tech Mahindra, the Hub design and operate partner.

TOTSCo focused its considerations on the following questions:

1. Is the level of security provided by the Hub without E2EE sufficient to meet regulatory requirements for the protection of the personal information contained in OTS messages? If not, then E2EE and /or other measures would become a necessity.
2. If so, are there additional reasons for the introduction of E2EE that would outweigh any risks or problems?

Hub Security

Given the timings of the Hub procurement process, we were unable to share in the E2EE request for feedback any description of the Hub's security architecture and other arrangements. However, these are an important consideration, and we can now share some details.

The key components of the security architecture and organisational measures include:

- TLS 1.3 encryption between the CP and the TOTSCo Hub,
- Strong encryption of the TOTSCo Hub database, protecting message processing, and
- A layered security approach within the TOTSCo Hub infrastructure to cover multiple threat vectors.

Messages between the CP and the Hub are protected using TLS 1.3, which encrypts the communication tunnel between the two parties, and allows messages to be sent uninterrupted into and out of the Hub in a secured state. TOTSCo have heavily engineered the security model for our infrastructure to prevent an attacker from penetrating the Hub infrastructure and deploying code to collect the messages as they pass through. Multiple layers of anti-virus, anti-malware, host firewalling and web security have been implemented to restrict both forward and lateral movement inside the infrastructure layer. Even authorised staff accessing the environment must connect to a secured virtual desktop that has no internet connectivity, from there they "jump" to the OTS servers; this creates a secure gap between their own machine and the servers, over which files and code cannot be transferred. All jump sessions are monitored and recorded and can be audited by TOTSCo at any time to ensure even authorised staff are behaving as prescribed, mitigating against both external and insider risk.

The Hub infrastructure itself is protected by advanced firewalls. These analyse the traffic coming from CPs and ensure the stream is only the messaging text we expect and not malicious code or sessions attempting to travel through the messaging streams. An additional layer of protection is the web application firewall. This protects the Hub application itself and enables TOTSCo to define valid sessions; so, it becomes possible to define valid messages that can pass to and from the Hub and block all other un-solicited traffic.

The protection layers that TOTSCo have engineered into the infrastructure are designed to provide a layered approach for security and lock down all functionality to only approved behaviours and activity, blocking any other transactions and sessions. This is how online banking protect their environments on a day-to-day basis.

It is TOTSCo's assessment that this design, together with the organisational measures which will be detailed in TOTSCo's Security Policy, amount to a very high level of security that is like that typically seen in applications involving very sensitive personal data.

Statutory Obligations

Under GDPR, organisations are required to adopt appropriate technical and organisational security measures to protect personal data that they control. They are also required to comply with requirements relating to data minimisation, data storage limitation, integrity & confidentiality and privacy by design and default requirements. When a third party (such as TOTSCo) processes data on behalf of CPs, the CPs must ensure such processing is carried out subject to an appropriate contract, including obligations to keep personal data secure.

Appropriate technical measures to keep personal data secure could include, but are not limited to, encryption in transit, encryption at rest, and/or end-to-end encryption. The regulator, ICO explains:

> *"Are we required to encrypt personal data? The UK GDPR includes encryption as an example of a technical measure that can be appropriate to protect the personal data you hold. Ultimately, whether or not encryption is the right measure to put in place depends on your circumstances—the sort of processing you are undertaking, the risks that may be posed to individuals' rights and freedoms, and the state of the art of technology available to you to protect that data"*

The draft User Agreement includes a provision that TOTSCo will comply with applicable data protection law and will contain a standard data controller-processor schedule setting out the various contractual obligations on TOTSCo (including data security) in circumstances in which TOTSCo processes CPs customers' personal data.

OTS messages do not contain any "special categories" of personal data, or information such as bank account or credit card details.

Potential Risks of E2EE Implementation

TOTSCo's initial assessment identified that E2EE implementation risked introducing some potential operational complications and development delays arising from:

- Encryption-key management
- Encryption-key backwards compatibility
- Development and maintenance of encryption and decryption code
- Complications for Third Party Integrators ("TPIs")
- Additional failure modes in testing and real-time operation
- Complications in cases where troubleshooting is required

Stakeholder Consultation

Given the complexity of the issues involved, on 14 April TOTSCo published a "request for feedback" on the subject (https://totsco.org.uk/wp-content/uploads/2023/04/Message-Encryption-Request-for-Feedback.pdf). The responses demonstrated a large divergence of views from respondents.

Many respondents felt that E2EE implementation would, at worst, cause negligible problems. Some stated that they viewed E2EE as obligatory for statutory reasons, or that E2EE would simplify development and reduce development times. These respondents all favoured implementing E2EE from OTS go-live.

However, other respondents echoed some, or all, of the risks listed above, and a small number were concerned about the processing power being required to encrypt and decrypt messages, with a possible impact on meeting 60-second SLAs. Some of these respondents felt that E2EE should nonetheless be implemented from go-live, while others felt that it was unnecessary or should be considered only after OTS go-live.

In general, the larger the respondent, the greater their propensity to raise concerns about development delays and operational risks.

Tech Mahindra, our technical partner, has indicated that the deployment of E2EE would lead to a delay in the Hub go-live.

TOTSCo conclude, that while there is support from a number of CPs, the implementation of E2EE at Hub go-live would result in a significant risk of operational complications and a probability that OTS go-live would be delayed.

Conclusions and next steps

After considering the issues outlined in this note, TOTSCo have concluded that:

1. The Hub's baseline specification, i.e. without E2EE, meets and even exceeds the threshold of "appropriate … measures to protect personal data." E2EE implementation is not therefore required to satisfy GDPR.

2. While there is an appetite from many stakeholders to implement E2EE at OTS go-live, this will result in a delay to go-live, and there is a risk that it would introduce operational complications which could impact on consumer experience.

TOTSCo believe that implementing E2EE when there is no statutory obligation to do so is not justified given the risk of delay to OTS go-live. TOTSCo has therefore concluded that E2EE will not be implemented at OTS go-live.

However, given the significant expression of interest in E2EE, we will continue to engage with industry on the topic. We invite interested stakeholders to share any evidence and/or analysis which shows why industry might benefit from further consideration of E2EE implementation post-OTS launch.

End

The One Touch Switching Company Limited (TOTSCo) is a not-for-profit private company limited by guarantee, founded by the UK telecommunications industry to deliver switching processes for fixed voice and broadband services. Registered number 14115273. Registered office Gresham House 5-7 St Pauls Street, Leeds LS1 2JG