Statement on the Finnish Government's review of the EU's balanced approach to encryption

The Finnish Parliament's Transport and Communications Committee has requested a statement from FiCom concerning the Government's review of a proposal by the EU Presidency on the Union's balanced approach to encryption and the ability of competent authorities to obtain access to encrypted data, within their remit, in individual cases. FiCom thanks the committee for the opportunity to make a statement and respectfully proposes the following:

In October 2020, the United States, the United Kingdom, Australia, New Zealand, Canada, India and Japan published the international statement "End-To-End Encryption and Public Safety", in which the countries of the Five Eyes intelligence alliance, supported by India and Japan, demand legal access to content in a readable and usable format. The countries stated that they support strong encryption because it plays "a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security. It also serves a vital purpose in repressive states to protect journalists, human rights defenders and other vulnerable people, as stated in the 2017 resolution of the UN Human Rights Council". In spite of all this, the countries still urge the technology industry to consider methods of allowing access to encrypted content.

In late 2020, Germany, which held the presidency of the European Council, called for "security through encryption and security despite encryption" in a resolution. The oxymoron in this statement reflects the difficulty in finding a balance between safeguarding the privacy and security of electronic communications through strong encryption, and providing access to competent authorities.

The German resolution emphasises the fact that the EU supports the use of effective encryption technology to ensure the fulfilment of security, as well as of fundamental and human rights, while at the same time highlighting the problems faced by law enforcement authorities in obtaining the information they need due to encryption solutions based on such technology. According to the resolution, governments, authorities, the technology industry, communication service providers, higher education institutions and other relevant stakeholders should work together to identify technical solutions to permit legal access to data, complying with the principles of legality, transparency, necessity and proportionality, and assuming the protection of personal data by default. Because there is no single method for achieving these given objectives, collaboration with the industry would be necessary to find the required balance.

To promote the resolution, a document has been issued with recommendations for consequent measures, according to which there is a need "to review the effects arising from different relevant regulatory frameworks in order to develop further a consistent regulatory framework across the EU that would allow competent authorities to carry out their operational tasks effectively." The document does not, however, specify what these regulatory frameworks and new technical solutions actually comprise. The document states a determination to "maintain a close exchange with the initiators of the 'International Statement: End-

to-End Encryption and Public Safety' (UK, USA, Australia, New Zealand, Canada, India, Japan) and other relevant international actors."

FiCom's member companies continuously work with law enforcement authorities to make the internet safer for companies and individuals alike. At the same time, however, FiCom supports strong encryption which, in a democratic society, plays a central role in ensuring cyber security and user privacy.

Germany's resolution does not specify at which actors the proposed measures would be directed. Finland's statement notes that a significant proportion of communications takes place on platforms that bypass telecommunication providers (so-called OTT platforms), but that this does not mean that potential legislative proposals would fail to apply to telecom companies.

End-to-end encryption of communication services, as well as cryptographic protocols such as TLS (Transport Layer Security) and HTTPS (Hypertext Transfer Protocol Secure) are crucial for the trustworthiness of the internet. The objective of the proposed actions is to leave a backdoor in encryption, providing law enforcement authorities with access to private communications. International experiences have shown that malicious hackers will always make use of such options, which reduces both cyber security and the online privacy of users and companies. This, in turn, would diminish trust in the internet and could slow down the adoption of online services in the EU. Neither the Finnish Government's review nor the German resolution makes any business impact assessments, focusing entirely on the impact on official operations.

Operators are prepared to continue collaborating with the law enforcement authorities, but the benefits to society of the encryption of online content and the negative impacts of weakening this encryption are so significant that FiCom must object to the adoption of mandatory backdoors for the authorities based on EU law. If any such backdoors are even considered, the national authorities of the countries in which service providers are located must assess the legality of measures, and these measures must be sufficiently closely defined and correctly proportioned. The approach must be balanced and technologically neutral, and it must observe privacy and data protection. The confidentiality of communications must be safeguarded under all circumstances.