Terms of Reference (ToR) for
ETSI ISG Encrypted Traffic Integration (ETI)

Approved by the Director-General on **26 June 2020,** following ETSI Board consultation

Scope

The Encrypted Traffic Integration Industry Specification Group (ISG ETI) will develop Group Specifications (GS) and Group Reports (GR) that define the requirements and that identify the use cases of ETI techniques to mitigate against threats to networks and users arising from the deployment of encrypted traffic, and where applicable define detailed specification of mitigation measures with a view to their further development in ETSI TCs that are identified as appropriate for their adoption.
As a pre-standardisation activity, the ISG ETI is intended to frame the security concerns arising from widespread adoption of encryption by default in networks and to build the foundation of a longer-term response to the threats arising from the encrypted by default paradigm. In part this will be achieved by sponsoring the future development of normative technical specifications in relevant groups from the initial activity in ISG ETI to provide detailed specification of mitigation measures.
The underlying rationale for ISG ETI is that a paradigm of "encrypted by default" has been adopted by many network and service providers without taking due account of any threats to network resilience and security. The network management oversight that is accepted for non-encrypted traffic may be lost when an all encrypted paradigm is adopted. Thus the aim of ISG ETI is to be able to better describe the issues and to establish essential requirements to allow for the integration of such traffic to all aspects of network operation.

Areas of Activity

The ISG ETI will produce both informative documents (Group Reports) and normative documents (Group Specifications). The ISG's work will initially focus on the following deliverables which will also be used to help refine the future direction of the ISG work programme.
ISG ETI will initially focus its activity on identifying candidate encrypted traffic integration processes, procedures, protocols and techniques against a set of requirements to be developed as a baseline. The ETI requirements shall be developed as GR taking into account the following scope of study:

- Existing and new transport, network and application layer and management plane protocols, such as DNS and server name identifier encryption
- ETI candidate approaches to achieving visibility, analysis, and control or encrypted traffic, such as middlebox-based solutions
- Public and enterprise networks, cloud data centres, network slicing, 5G, MEC, and NFV/SDN
- Integration of ETI solutions with automated cyber defence platforms
- The role of ETI in the presence of hardware acceleration and AI implementations

ISG ETI intends to work on:

- Documenting requirements ETI protocols and techniques
- Means for ETI visibility and analysis of encrypted traffic for cyber security purposes
- Use of ETI information to mitigate attacks and threats
- ETI for both end users and network operators, including privacy.

As the detail of the work programme will evolve as the initial research studies are undertaken the relative effort applied to each of the listed areas of activity will also evolve.

Outreach and engagement (collaboration with other stakeholders)

On the understanding that ISG ETI is a unique global venue that builds relationships between standards and R&D communities it is considered essential that the ISG engages as much as possible with representatives from the following classes of organisation:

- Member R&D and professional employees not devoted to standards development
- Non-member academic institutions and activities
- Other standards body research arms and activities
- ISG ETI provides an opportunity for fast, timely participation by researchers now only met by major academic conferences of ACM and IEEE.

Annex (informative): collaboration with other bodies

ISG ETI will set up appropriate communication channels to the following groups:

ETSI groups

- ETSI PP 3GPP (especially each of SA2, SA3, SA3-LI)
- ETSI PP oneM2M
- TC CYBER
- TC LI
- SC SAGE
- ISG ENI
- ISG F5G
- ISG MEC
- ISG NFV
- ISG NIN
- ISG SAI
- ISG ZSM

and others as identified during the progression of the work.

External groups

- ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information)
- CCDB (ISO Common Criteria Development Board)
- EC Horizon Europe programme
- IACD Community (Integrated Adaptive Cyber Defense)
- IEEE and ACM Conference Committees
- ISO/IEC JTC 27 WG3
- ENISA
- ITU-T (especially SG13, SG11, SG16 and SG17)
- OASIS (especially TCs CTI, CACAO, OpenC2)
- Relevant University Centres of Excellence
- ISACs and Threat Exchange organizations

and others as identified during the progression of the work.