



# **Support for data anonymization in IPFIX**

E. Boschi, B. Trammell

Hitachi Europe

# [ Background and history ]

- Support for anonymization is one of the requirements for IPFIX
  - RFC3917
  - Not addressed because still “area of research”
- Increasing need for it
- Should be addressed by the IPFIX WG
  - In the context of the mediators work
  - Needed by file

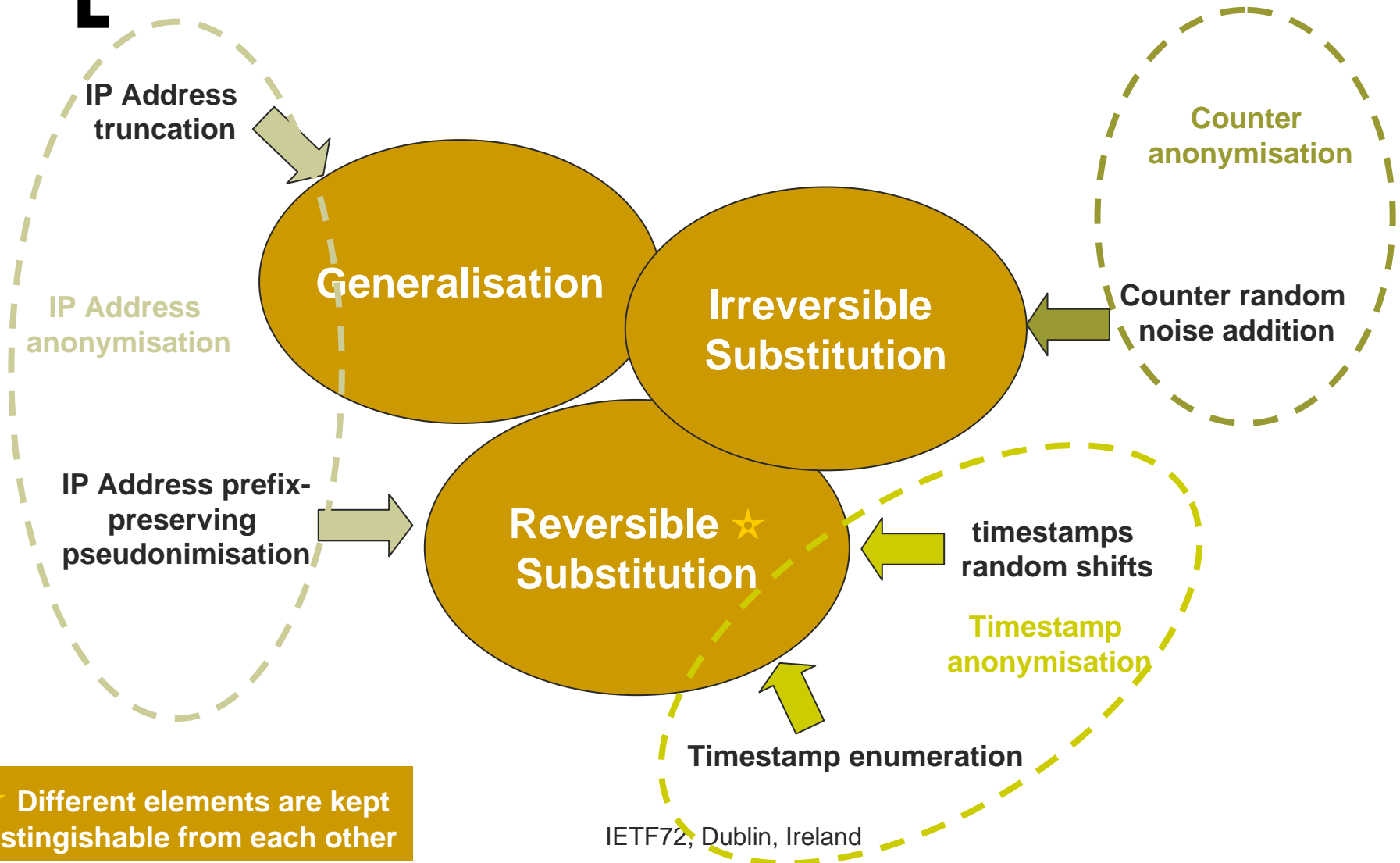
# [ Anonymization support draft ]

- “IP Flow Anonymisation Support”
  - draft-boschi-ipfix-anon-01
- Experimental
- Much like PSAMP techniques
- Using option templates scoped to Templateld to report information on the anonymized fields

# Table of Contents

- 1. Introduction
  - 1.1. IPFIX Protocol Overview
  - 1.2. IPFIX Documents Overview
- 2. Terminology
- 3. Categorisation of Anonymisation Techniques
- 4. Anonymisation of IP Flow Data
  - 4.1. IP Address Anonymisation
    - 4.1.1. Truncation
    - 4.1.2. Random Permutations
    - 4.1.3. Prefix-preserving Pseudonymisation
  - 4.2. Timestamp Anonymisation
    - 4.2.1. Precision Degradation
    - 4.2.2. Enumeration
    - 4.2.3. Random Time Shifts
  - 4.3. Counter Anonymisation
    - 4.3.1. Precision Degradation
    - 4.3.2. Binning
    - 4.3.3. Random Noise Addition
  - 4.4. Anonymisation of Other Flow Fields
- 5. Parameters for the Description of Anonymisation Techniques
- 6. Anonymisation Support in IPFIX
- 7. Security Considerations

# Categorisation of Anonymisation Techniques



# [ Next steps ]

- Incorporate comments and continue writing the document
  - IPFIX message versus flow data anonymisation
  - Anonymised data export technique
- Gain implementation experience
- Consider accepting it as WG item in the context of the mediator cluster