

# Specifications of the Protocol for IPFIX Mediations

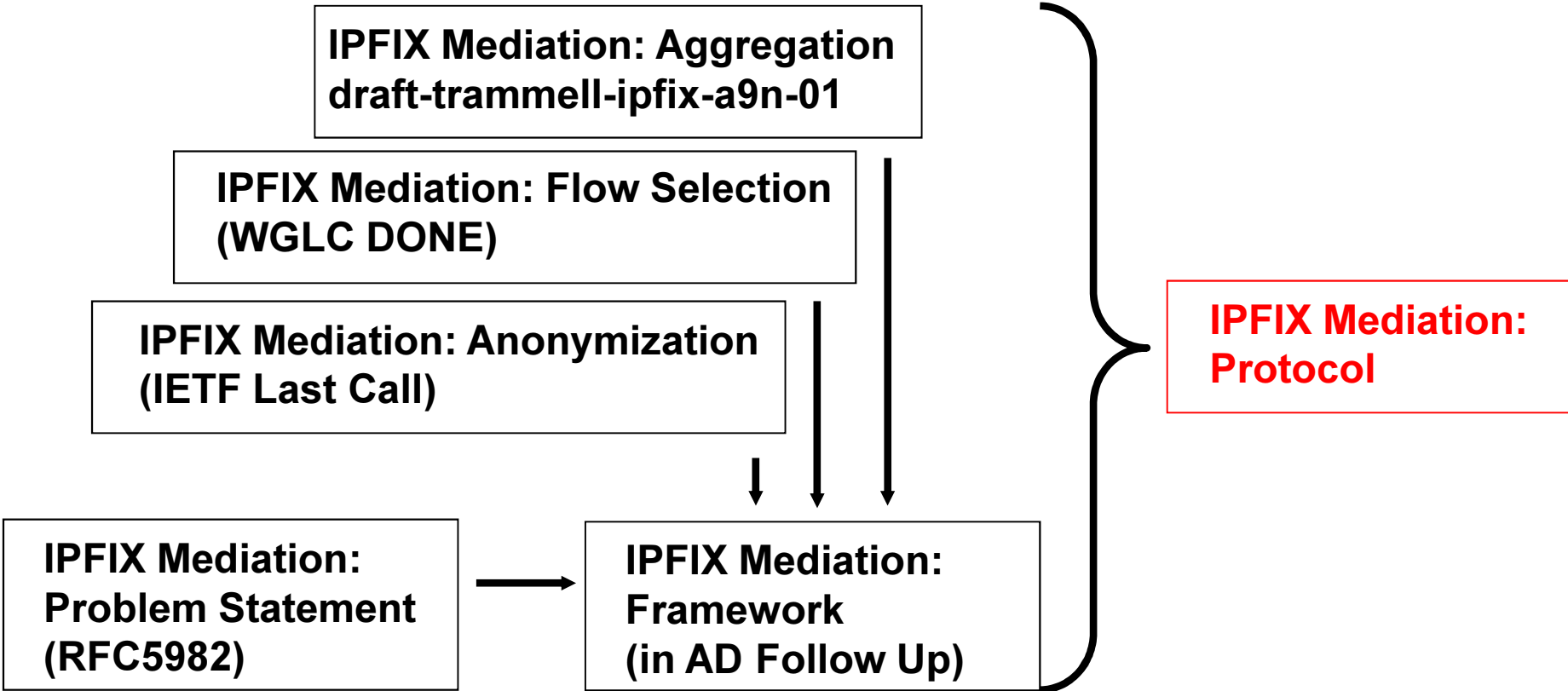
IETF-79 Beijing, 2010

<draft-claise-ipfix-mediation-protocol-02.txt>

Atsushi Kobayashi, Brian Trammell, Benoit Claise

# Work Justification

---



**Sometimes some generic solutions for all Intermediate Process Types**

**Sometimes some specific solutions per Intermediate Process Type**

# Introduction

---

- **Clearly differentiate the aggregation case (in draft-trammell-ipfix-a9n-01) versus what is generic for all IPFIX Mediation (Intermediate Process Type)**

**Happy because most cases dealt with in previous version dealt with aggregation**

- **Not a complete new protocol, but a series of conventions on the top of the IPFIX protocol RFC5101**

# New in this Version

---

- **When required, refer to or copy the terminology from the different drafts.**

**"IPFIX Mediation: Problem Statement" [RFC5982],  
Informational -> copy**

**[IPFIX-MED-FMWK], Informational -> copy**

**[IPFIX-MED-ANON], Experimental -> copy**

**[IPFIX-MED-FLOWSEL], Standards Track -> refer**

**[IPFIX-MED-AGGR], Standards Track -> refer**

# New in this Version

---

- For a specific Intermediate Process, the specifications in the following reference **MUST** be followed, on the top of the specifications in this document:
  - For the Intermediate Aggregation Process, the specifications in [IPFIX-MED-AGGR] **MUST** be followed.
  - For the Intermediate Selection Process, the specifications in [IPFIX-MED-FLOWSEL] **MUST** be followed.  
**EDITOR'S NOTE: actually, there is no MUST/SHOULD/MAY in [IPFIX-MED-FLOWSEL]. Seems to be just a list of required Information Elements.**
  - For the Intermediate Anonymization Process, the specifications in [IPFIX-MED-ANON] should be considered as guidelines as [IPFIX-MED-ANON] is an experimental RFC.
- Note that no specific document deals with the Intermediate Conversion Process at the time of this publication.

# Technical Table of Content

---

## 3. Specifications

### 3.1. Encoding of IPFIX Message Header

### 3.2. Template Management

#### 3.2.1. Template Management Without Template Record Change

#### 3.2.2. Template Management With Template Record Change

### 3.3. Time Management

### 3.4. Observation Point Management

#### 3.4.1. Observation Domain Management

### 3.5. Specific Reporting Requirements

#### 3.5.1. The Flow Keys Options Template

#### 3.5.2. IPFIX Protocol Options Template

#### 3.5.3. IPFIX Mediator Options Template

### 3.6. The Collecting Process's Side

### 3.7. Sampling Management

## 4. New Information Elements

## 5. Security Considerations

### 5.1. Avoiding Security Downgrade

### 5.2. End-to-End Assertions for Mediators

# Technical Content

---

- **Time management:**
  - “It is **RECOMMENDED** that Mediators handle time using absolute timestamps”
- **Observation Point Management**
  - New IEs: originalExporterIPv4Address and originalExporterIPv6Address**
  - IPFIX Structured MUST be used to represent any complex observation point (list of something)**

# Technical Content

---

- **Observation Domain management**

**Intermediate Processes that maintain the O.D.**

**Intermediate Processes that don't maintain the O.D. (ex: aggregation from multiple exporters)**

**“The Observation Domain ID SHOULD be 0 when no specific Observation Domain ID is relevant for the entire IPFIX Message.”**

- **Flow keys Management**

**Like in RFC5101, with an Options Template Record**



# Technical Content

---

- **Sampling Management**

**“In an IPFIX Mediation, aggregation for Flow Records with same sampling rate and same sampling algorithm is recommended. In that case, an IPFIX Mediator can export this sampling rate and sampling algorithm, and other accuracy statistics data, part of the PSAMP Report Interpretation [[RFC5476](#)]. “**

**Otherwise, “some more research is required to determine the right sampling function and/or sampling rate to export from the IPFIX Mediator”**

**Maybe something from [IPFIX-MED-FLOWSEL] or maybe [IPFIX-MED-AGGR]?**

# TO DO

---

- **A couple of EDITOR'S NOTE in the draft**
- **Check that all documents (this one, [IPFIX-MED-ANON], [IPFIX- MED-FLOWSEL], [IPFIX-MED-AGGR]) all fit together.**

**[IPFIX-MED-AGGR], mainly done**

**[IPFIX-MED-ANON], on its way**

**[IPFIX-MED-FLOWSEL], no done**

**And obviously [IPFIX-MED-FMWK]**