eCSIRT.net Common Language Specification

Arne Helme
www.stelvio.nl
Arne.Helme@stelvio.nl

Stelvio, The Netherlands

eCSIRT.net Common Language

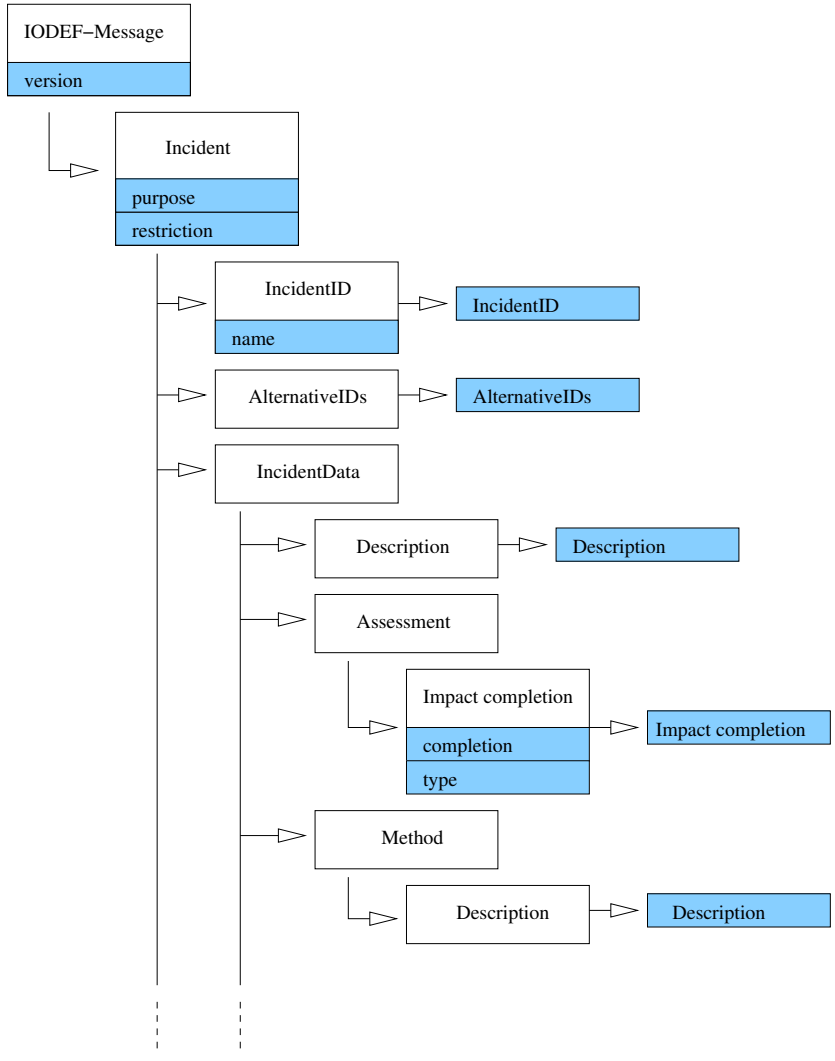
Overview:

- Covers syntax and sematics for the exchange of incident data between members (CSIRTs) of the project
- Based on INCH / IODEF

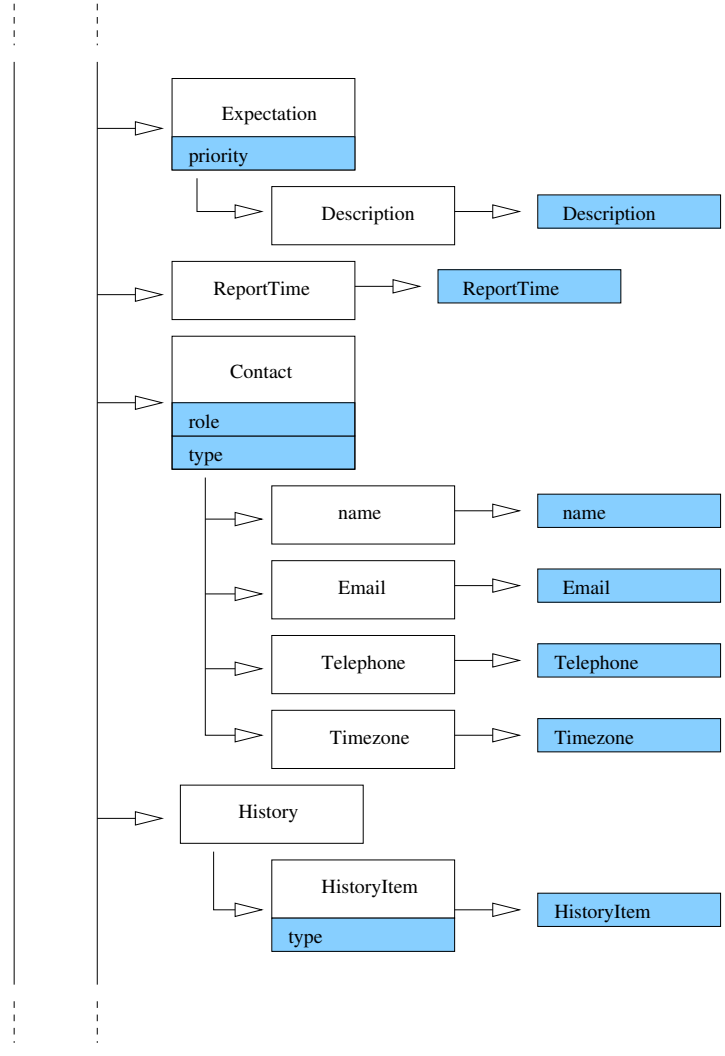
Common Language:

- Common Language profile:
  - Agreed upon subset of IODEF
  - Agreed upon message transport mechanism (email)
  - Agreed upon syntax and semantics for values and attributes

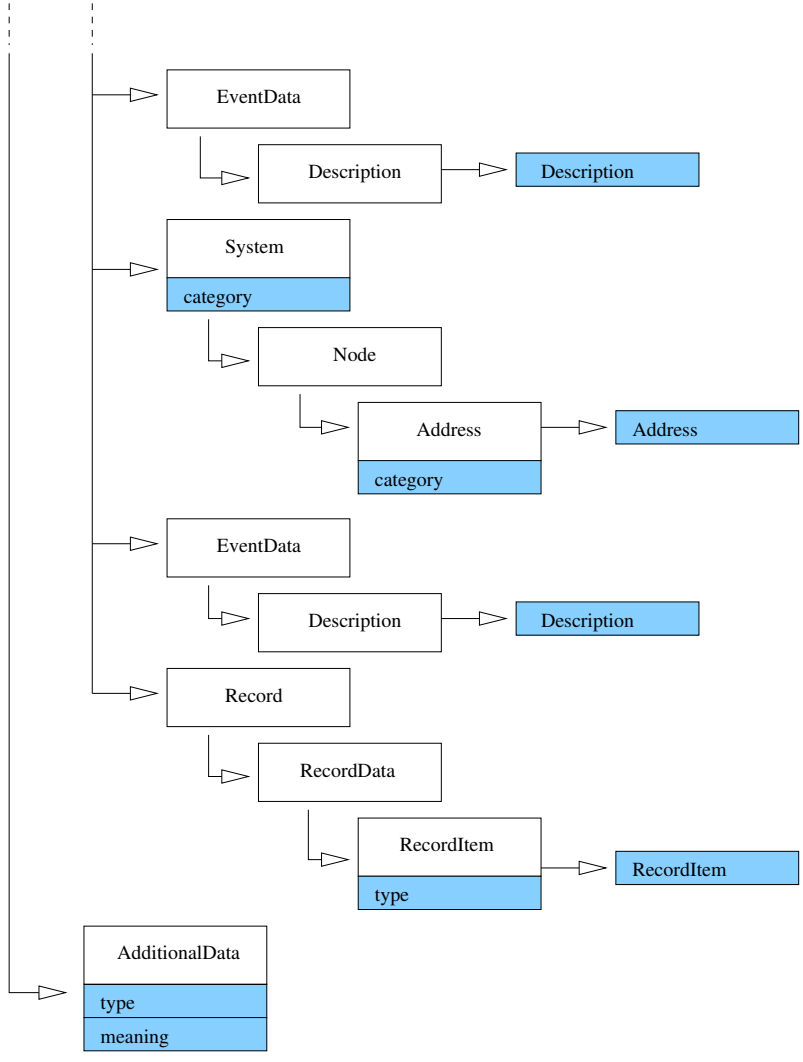
eCSIRT.net CL Profile (1)



eCSIRT.net CL Profile (2)



eCSIRT.net CL Profile (3)



INCH/IODEF Issues

CL Identifier:

- eCSIRT.net CL Profile identifier in AdditionalData:

```
<AdditionalData
  type="string"
  meaning="eCSIRT.net IODEF Profile Version 1.0">
  eCSIRT-net-IODEF-profile-v1.0
</AdditionalData>
```

Signalling:

- Current INCH/IODEF specification only covers incident data
- There is a need for a signalling mechanism / incident data exchange protocol