draft-ietf-mile-rfc5070-bis-10

Roman Danyliw <rdd@cert.org>

IETF 91

November 10, 2014

What is IODEFv2?

- An XML format to represent data elements commonly exchanged by CSIRTs:
  - Computer security incident reports
  - Cyber security indicators
- IODEFv2 is an update to the Incident Object Description Exchange Format (IODEF)/RFC5070
- IODEF is extended by various extensions
  - RFC 5901 (Phishing)
  - RFC 7203 (Structured Cybersecurity Information)
  - draft-murillo-mile-cps-00 (Cyber Physical Incidents)
  - draft-schaad-mile-iodef-plasma-00 (Policy Framework)
  - draft-suzuki-mile-darknet-00 (Darknet Monitoring)
- IODEFv2 is exchanged with RID (RFC 6545) and ROILE (draft-field-mile-rolie)

Drafts Since IETF 90 (Toronto)

- -08 (2014-08-05)
- -09 (2014-10-21)
- -10 (2014-11-10)

Issues Closed in -08, -09, -10

#3	Review implementation of extending enumerated values	-10	2013-06-14
#6	Harmonize the specification for Reference with other WG activity	-09	2013-06-14
#10	Review completeness of Impact@type	-10	2013-06-14
#20	Review how to provide a list of file and email indicators	-10	2013-08-21
#25	Clarify what type attribute of HashInformation should be used to represent a TLS certificate	-10	2013-08-29
#29	Clarifying the scope of HashInformation@valid	-10	2013-08-29
#37	Add intended purpose of attack to Assessment	-10	2013-10-16
#40	Reference@attacktype documentation	-09	2014-02-26
#43	{Application,OperatingSystem}@user-agent documentation	-09	2014-02-26
#44	HashData/{ds:Signature,ds:KeyInfo,ds:KeyReference} documentation	-10	2014-02-26
#45	Clarifying the computation of a file and email hash	-08	2014-02-27
#46	Missing data elements from NIST SP800-61 and CERT's Handbook for CSIRTs	5 of 7	2014-02-27

All post-IETF-87 survey items are complete

http://trac.tools.ietf.org/wg/mile/trac/report/1?asc=1&sort=ticket

Incompatibilities with v1

- IODEF-Document@version="1.00" → "2.00"
- Service@ip_protocol → @ip-protocol
- Node/Name → Node/DomainData/Name
- Node/DataTime → Node/DomainData/DateTime
- NodeRole moved to System (from Node)
- Reference class is now defined by draft-ietf-mile-enum-reference-format-09
- No more "ext-" extension attributes
- Impact v1 class is now SystemImpact and IncidentCategory classes.

Issue #3: Extending Attributes

- Old Way

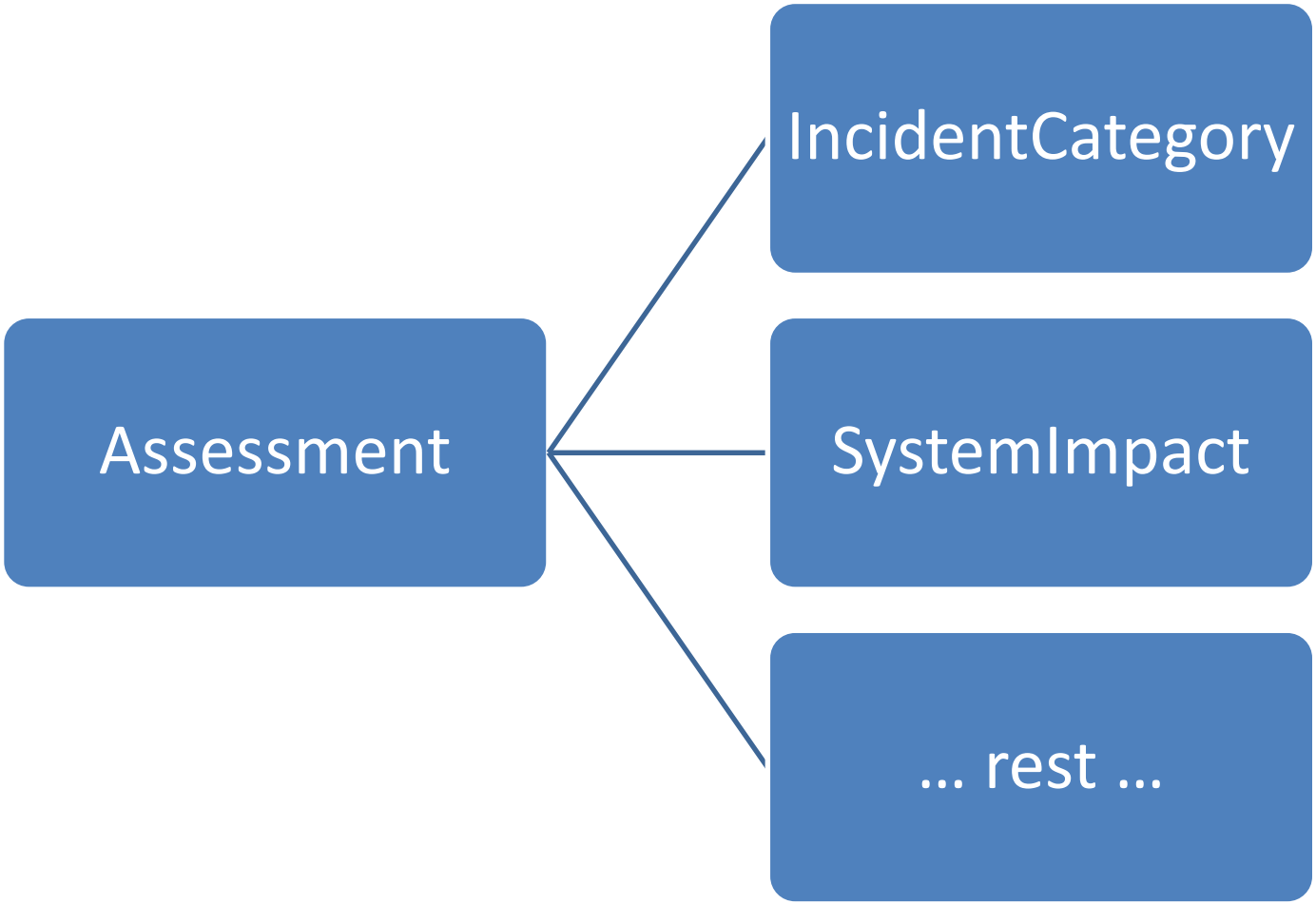
```
<NodeRole category="ext-value"
          ext-category="extension value"
```

- New Way
  - IANA Registry "IODEFv2→NodeRole-category"
  - Each registry is a

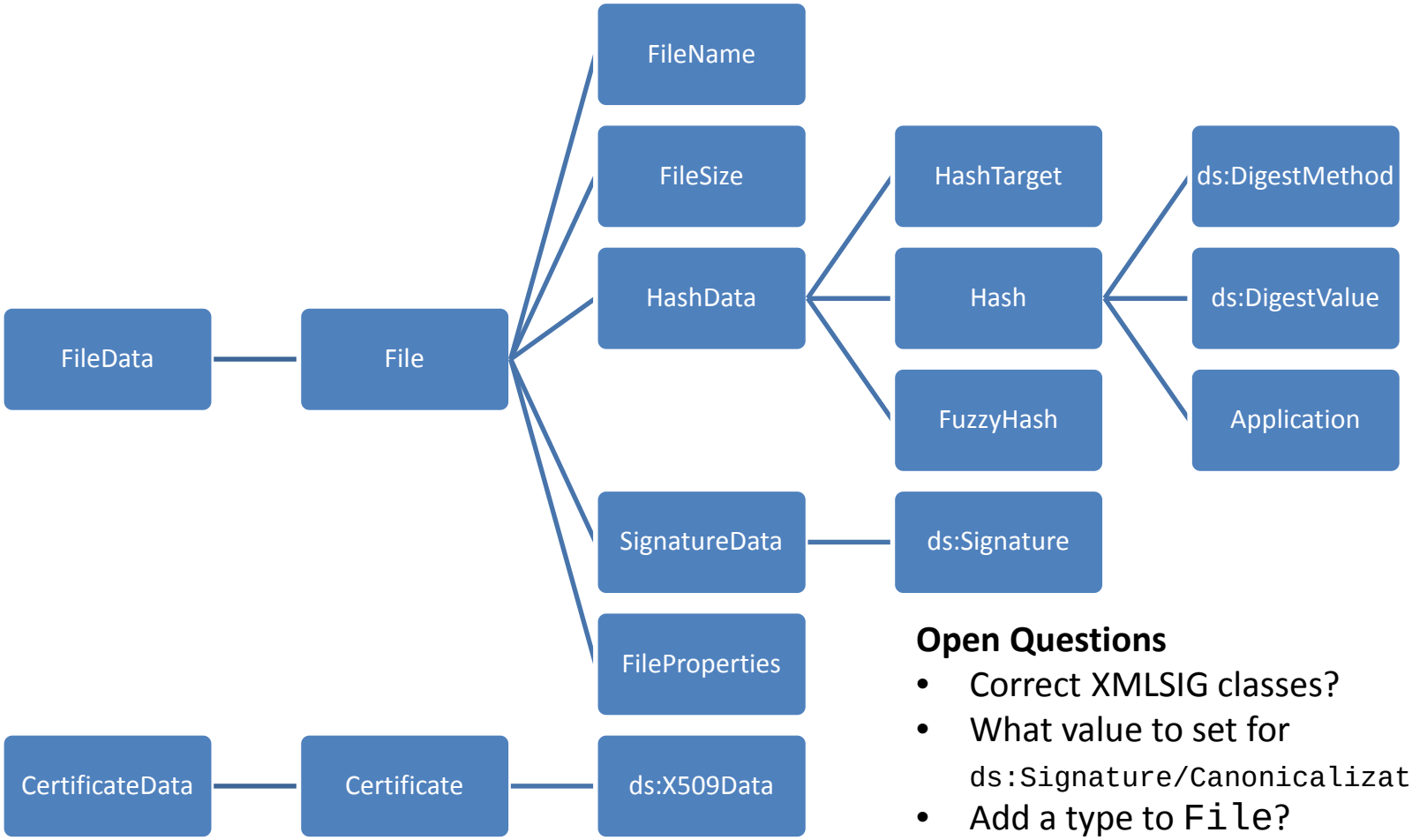
    RegistryName

    Value | Description | Reference
  - Allocation through Expert Review

Issue #10: `Impact@type`



Rethinking `HashData` (Issue #20,25,29,44)



Open Questions

- Correct XMLSIG classes?
- What value to set for `ds:Signature/CanonicalizationMethod`?
- Add a type to `File`?
- Specify `FuzzyHash`?
- Move `FileData`, `CertificateData`, etc. to `System`?

`HashData` and `Signature` also added to `EmailData`

Issue #29: Scope of `HashData@valid`

Text before -10

- HashData@valid
- “Indicates if the signature or hash is valid.”

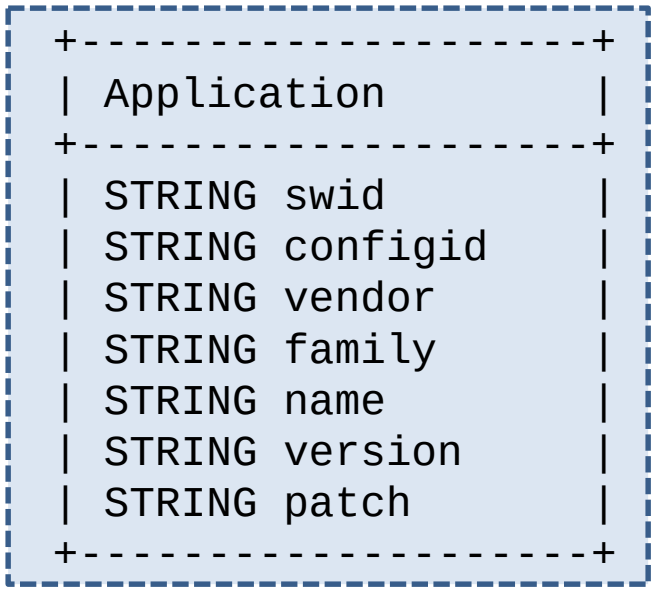
Text in -10

- Certificate@valid
- “Indicates whether a given certificate has a valid signature. An invalid signature may be due to an invalid certificate chain, a signature not decoding properly, or a certificate contents not matching the hash.”

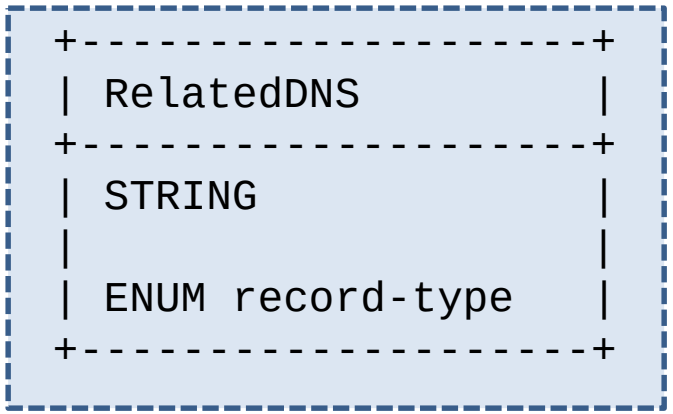
Outstanding Issues

#1	Fix internationalization	TODO	2013-06-14
#38	Improve example in Section 7	TODO	2014-01-08
#39	RelatedDNS documentation	PROPOSAL	2014-02-26
#46	Missing data elements from NIST SP800-61 and CERT's Handbook for CSIRTs	2 of 7 left	2014-02-27
#47	Clarify definition of iodef:SoftwareType	TODO	2014-10-23

iodef:SoftwareType



RelatedDNS



http://trac.tools.ietf.org/wg/mile/trac/report/1?asc=1&sort=ticket

Discussion