
dmARC-aggregate-parser

Documentation

Release 1.0

Dan Nielsen

Apr 28, 2020

Contents:

1	dmrcap package	1
1.1	dmrcap.auth_results module	1
1.2	dmrcap.identifiers module	2
1.3	dmrcap.meta_data module	2
1.4	dmrcap.parser module	3
1.5	dmrcap.policy_evaluated module	3
1.6	dmrcap.policy_published module	4
1.7	dmrcap.record module	5
1.8	dmrcap.report module	5
2	Indices and tables	7
	Python Module Index	9
	Index	11

1.1 dmarcap.auth_results module

dmarcap/auth_results.py - DMARC aggregate report AuthResultsType representation. Ref. <https://tools.ietf.org/html/rfc7489#appendix-C>

```
class dmarcap.auth_results.AuthResults
    Bases: future.types.newobject.newobject
    Representation of AuthResultsType

    dkim = None
        DkimAuthentication

    spf = None
        SpfAuthentication

class dmarcap.auth_results.Authentication (domain=None, result=None)
    Bases: future.types.newobject.newobject
    Base class for verification results

    domain = None
        Domain name represented in this verification

    result = None
        Verification result

class dmarcap.auth_results.DkimAuthentication (domain=None, result=None)
    Bases: dmrcap.auth_results.Authentication
    Representation of DkimAuthResultType

    human_result = None
        Any friendly, human-readable message.

    selector = None
        DKIM selector, e.g. k1, used in authentication
```

```
class dmarcap.auth_results.SpfaAuthentication (domain=None, result=None)
    Bases: dmarcap.auth_results.Authentication

    Representation of SpfAuthResultType

    scope = None
        SPF domain scope
```

1.2 dmarcap.identifiers module

dmARC/identifiers/py - DMARC aggregate report IdentifierType representation Ref. <https://tools.ietf.org/html/rfc7489#appendix-C>

```
class dmarcap.identifiers.Identifiers
    Bases: future.types.newobject.newobject

    Representation of the aggregate record IdentifierType

    envelope_from = None
        Envelope from of the evaluated message or SMTP transaction. E.g. MAIL
        FROM:<errors@example.com> or Return-Path: <errors@example.com>

    envelope_to = None
        Envelope recipient of the SMTP transaction. E.g RCPT TO: <jane@example.com>

    header_from = None
        From header field of the evaluated message
```

1.3 dmarcap.meta_data module

dmARC.py/meta_data.py - DMARC aggregate report meta data representation. Ref. <https://tools.ietf.org/html/rfc7489#appendix-C>

```
class dmarcap.meta_data.MetaData
    Bases: future.types.newobject.newobject

    Representation of aggregate report MetaDataType

    begin_localized_date_iso()
        Return report begin date in localtime ISO format

    begin_utc_date_iso()
        Returns report begin date in UTC ISO format

    date_range_begin = None
        Report date range beginning (unix timestamp).

    date_range_end = None
        Report date range ending (unix timestamp).

    email = None
        Organization contact email

    end_localized_date_iso()
        Return report end date in localtime ISO format

    end_utc_date_iso()
        Returns report end date in UTC ISO format
```

extra_contact_info = None
Additional organization contact info

org_name = None
Organization which generated the report

report_id = None
Unique report id

1.4 dmarcap.parser module

dmarcap/parser.py - Primary DMARC XML aggregate report parsing class

```
class dmarcap.parser.Parser(dmarc_report_xml_file)
    Bases: future.types.newobject.newobject
    Aggregate report parser base class

    parse_meta_data()
        Parse report meta data into MetaData

    parse_policy_published()
        Parse report published policy into PolicyPublished

    parse_report()
        Parse report into Report

    parse_report_records()
        Parse aggregate report records into a list of Record
```

1.5 dmarcap.policy_evaluated module

dmarcap/policy_evaluated.py - DMARC aggregate report evaluation policy representation. Ref. <https://tools.ietf.org/html/rfc7489#appendix-C>

```
class dmarcap.policy_evaluated.PolicyEvaluated
    Bases: future.types.newobject.newobject
    Representation of PolicyEvaluatedType

    disposition = None
        Disposition of the Record

    dkim = None
        Dkim result for the Record

    spf = None
        Spf result for the Record

class dmarcap.policy_evaluated.Reason(reason_type, reason_comment)
    Bases: future.types.newobject.newobject
    Representation of Reason in PolicyEvaluatedType

    comment = None
        Disposition of the Record

    type = None
        Disposition of the Record
```

1.6 dmarcap.policy_published module

dmarcap/policy_published.py - DMARC aggregate report published policy representation. Ref. <https://tools.ietf.org/html/rfc7489#appendix-C>

```
class dmarcap.policy_published.PolicyPublished
    Bases: future.types.newobject.newobject

    Representation of PolicyPublishedType

    adkim = None
        Dkim authentication mode

    aspf = None
        Spf authentication mode

    domain = None
        Domain publishing this policy

    failure_reporting_options = None
        Long format accessor for fo

    fo = None
        Failure reporting options

    p = None
        DMARC policy

    pct = None
        Policy percent, i.e. what percent of mail stream to apply the published policy to.

    percent = None
        Long format accessor for pct

    policy = None
        Long format accessor for p

    report_format = None
        Long format accessor for rf

    report_interval = None
        Long format accessor for ri

    report_uri_aggregate = None
        Long format accessor for rua

    report_uri_forensic = None
        Long format accessor for ruf

    rf = None
        Preferred report format

    ri = None
        Preferred report interval

    rua = None
        Aggregate report delivery URI

    ruf = None
        Forensic report delivery URI

    sp = None
        Sub domain policy
```

subdomain_policy = None
Long format accessor for *sp*

v = None
DMARC version

version = None
Long format accessor for *v*

1.7 dmarcap.record module

dmarcap/record.py - DMARC aggregate report RecordType representation. Ref. <https://tools.ietf.org/html/rfc7489#appendix-C>

class dmarcap.record.Record
Bases: `future.types.newobject.newobject`
Representation of an aggregate report record

auth_results = None
Message *AuthResults*

count = None
Number of messages received from this IP

identifiers = None
Message or SMTP *Identifiers*

policy_evaluated = None
Message *PolicyEvaluated*

source_ip = None
IP traffic source

1.8 dmarcap.report module

dmarclib/report.py - DMARC aggregate report representation. Ref. <https://tools.ietf.org/html/rfc7489#appendix-C>

class dmarcap.report.Report
Bases: `future.types.newobject.newobject`
DMARC aggregate report representation

dmarc_failures()
Returns a list of failed *Record*

meta_data = None
Aggregate report *MetaData*. Contains information about the reporting organization and the report range.

policy_published = None
Aggregate report *PolicyPublished*. Contains the policy and reporting values published in DNS by the domain owner. These were the policies used to evaluate incoming mail.

records = None
List of aggregate report *Record*. Contains all records from the aggregate report.

CHAPTER 2

Indices and tables

- `genindex`
- `modindex`
- `search`

d

- `dmарсap.auth_results`, 1
- `dmарсap.identifiers`, 2
- `dmарсap.meta_data`, 2
- `dmарсap.parser`, 3
- `dmарсap.policy_evaluated`, 3
- `dmарсap.policy_published`, 4
- `dmарсap.record`, 5
- `dmарсap.report`, 5

A

adkim (*dmarcap.policy_published.PolicyPublished* attribute), 4
 aspf (*dmarcap.policy_published.PolicyPublished* attribute), 4
 auth_results (*dmarcap.record.Record* attribute), 5
 Authentication (class in *dmarcap.auth_results*), 1
 AuthResults (class in *dmarcap.auth_results*), 1

B

begin_localized_date_iso() (*dmarcap.meta_data.MetaData* method), 2
 begin_utc_date_iso() (*dmarcap.meta_data.MetaData* method), 2

C

comment (*dmarcap.policy_evaluated.Reason* attribute), 3
 count (*dmarcap.record.Record* attribute), 5

D

date_range_begin (*dmarcap.meta_data.MetaData* attribute), 2
 date_range_end (*dmarcap.meta_data.MetaData* attribute), 2
 disposition (*dmarcap.policy_evaluated.PolicyEvaluated* attribute), 3
 dkim (*dmarcap.auth_results.AuthResults* attribute), 1
 dkim (*dmarcap.policy_evaluated.PolicyEvaluated* attribute), 3
 DkimAuthentication (class in *dmarcap.auth_results*), 1
 dmarc_failures() (*dmarcap.report.Report* method), 5
 dmarcap.auth_results (module), 1
 dmarcap.identifiers (module), 2
 dmarcap.meta_data (module), 2
 dmarcap.parser (module), 3

dmarcap.policy_evaluated (module), 3
 dmarcap.policy_published (module), 4
 dmarcap.record (module), 5
 dmarcap.report (module), 5
 domain (*dmarcap.auth_results.Authentication* attribute), 1
 domain (*dmarcap.policy_published.PolicyPublished* attribute), 4

E

email (*dmarcap.meta_data.MetaData* attribute), 2
 end_localized_date_iso() (*dmarcap.meta_data.MetaData* method), 2
 end_utc_date_iso() (*dmarcap.meta_data.MetaData* method), 2
 envelope_from (*dmarcap.identifiers.Identifiers* attribute), 2
 envelope_to (*dmarcap.identifiers.Identifiers* attribute), 2
 extra_contact_info (*dmarcap.meta_data.MetaData* attribute), 2

F

failure_reporting_options (*dmarcap.policy_published.PolicyPublished* attribute), 4
 fo (*dmarcap.policy_published.PolicyPublished* attribute), 4

H

header_from (*dmarcap.identifiers.Identifiers* attribute), 2
 human_result (*dmarcap.auth_results.DkimAuthentication* attribute), 1

I

Identifiers (class in *dmarcap.identifiers*), 2
 identifiers (*dmarcap.record.Record* attribute), 5

M

meta_data (*dmARCcap.report.Report* attribute), 5
 MetaData (class in *dmARCcap.meta_data*), 2

O

org_name (*dmARCcap.meta_data.MetaData* attribute), 3

P

p (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 parse_meta_data() (*dmARCcap.parser.Parser* method), 3
 parse_policy_published() (*dmARCcap.parser.Parser* method), 3
 parse_report() (*dmARCcap.parser.Parser* method), 3
 parse_report_records() (*dmARCcap.parser.Parser* method), 3
 Parser (class in *dmARCcap.parser*), 3
 pct (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 percent (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 policy (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 policy_evaluated (*dmARCcap.record.Record* attribute), 5
 policy_published (*dmARCcap.report.Report* attribute), 5
 PolicyEvaluated (class in *dmARCcap.policy_evaluated*), 3
 PolicyPublished (class in *dmARCcap.policy_published*), 4

R

Reason (class in *dmARCcap.policy_evaluated*), 3
 Record (class in *dmARCcap.record*), 5
 records (*dmARCcap.report.Report* attribute), 5
 Report (class in *dmARCcap.report*), 5
 report_format (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 report_id (*dmARCcap.meta_data.MetaData* attribute), 3
 report_interval (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 report_uri_aggregate (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 report_uri_forensic (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 result (*dmARCcap.auth_results.Authentication* attribute), 1

rf (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 ri (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 rua (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 ruf (*dmARCcap.policy_published.PolicyPublished* attribute), 4

S

scope (*dmARCcap.auth_results.SpfaAuthentication* attribute), 2
 selector (*dmARCcap.auth_results.DkimAuthentication* attribute), 1
 source_ip (*dmARCcap.record.Record* attribute), 5
 sp (*dmARCcap.policy_published.PolicyPublished* attribute), 4
 spf (*dmARCcap.auth_results.AuthResults* attribute), 1
 spf (*dmARCcap.policy_evaluated.PolicyEvaluated* attribute), 3
 SpfaAuthentication (class in *dmARCcap.auth_results*), 1
 subdomain_policy (*dmARCcap.policy_published.PolicyPublished* attribute), 4

T

type (*dmARCcap.policy_evaluated.Reason* attribute), 3

V

v (*dmARCcap.policy_published.PolicyPublished* attribute), 5
 version (*dmARCcap.policy_published.PolicyPublished* attribute), 5