

RDAP Extension for Structured Reliability Assessment Metadata

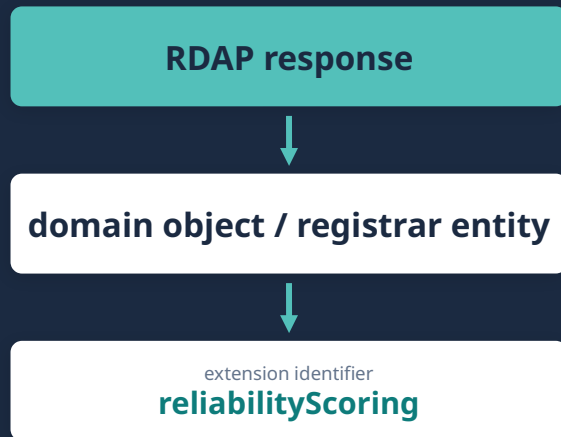
draft-bertoldi-regext-rdap-reliability-scoring-01

Presenter Simon Pietro Romano (UNINA)

Authors Alessandro Bertoldi (Bertoldi Cybersecurity), S. P. Romano

Individual draft, Experimental. Initial WG feedback, not adoption.

THE IDEA IN ONE PICTURE



an assessment envelope: points to the methodology and evidence, does not define them

Why we are here

Empirical research [DEEPSEC2025] keeps surfacing the same kind of weaknesses in registrar processes:

Credential recovery

Self-certification / weak recovery flows enabling account takeover

Identity verification

Bypassable with public registration data + social engineering

Email authentication

SPF / DKIM / DMARC present in theory, misconfigured in practice

EMPIRICAL MOTIVATION ONLY

6+ years

a flaw in a shared email platform left ~17,000 domains spoofable

Persistence, not novelty, is the point.

The underlying standards are not the gap. What is missing is a common, machine-readable way to expose whether a registrar / domain has been assessed.

Scope: an envelope, not a scoring system

Deliberate separation of concerns keeps the protocol layer neutral.



What it IS

- A structured assessment envelope inside RDAP responses
- Standardizes how results are transported and referenced
- For entity (registrar) and domain objects
- Fully conformant with RDAP core; fields individually OPTIONAL



What it is NOT

- Not a scoring methodology or algorithm
- Not thresholds, criteria, or a “pass / fail” mark
- Not a governance or accreditation framework
- Not an enforcement or abuse-mitigation mechanism

The protocol enables representation; the ecosystem decides how to populate and consume the fields.

The data model

`rdapConformance` carries `reliabilityScoring` · semantics defined by `scoreScheme`

scoreScheme

URI or identifier for the methodology; defines its semantics

scoreValue / scoreMaxValue

numeric result and its maximum

scoreDate

when assessed (RFC 3339)

scoreIssuer

opaque id of the assessor

evidenceUri

optional link to the supporting report

 example shape (values omitted)

```
"rdapConformance": [
  "rdap_level_0",
  "reliabilityScoring"
],
"reliabilityScoring_assessment": {
  "scoreScheme": "...",
  "scoreValue": 8,
  "scoreMaxValue": 10,
  "scoreDate": "...",
  "scoreIssuer": "...",
  "evidenceUri": "...
}
```

Fields individually OPTIONAL, with constraints. Omitting the member = no assessment metadata conveyed.

How it relates to existing work

verified-contacts

[draft-loffredo-...](#)

Orthogonal. That draft answers “which contact fields have been verified, and how?” Ours answers “what is the assessed security posture?” Designed to coexist in one response.

PIR AIP / QPI

[operational program](#)

A registry-specific operational program. The envelope is methodology-agnostic and COULD CARRY OUTPUTS from such programs, without standardizing them.

RDAP core

[RFC 7480/81](#) · [9082/83/9224](#)

Conformant with the RDAP core: reuses its JSON format, extensibility model, security framework, query format and service discovery. No core protocol changes.

Feedback we are asking for

These are open questions, including whether REGEXT is the right home at all.

1

Scope & fit

Is a generic assessment envelope appropriate work for REGEXT?

2

Namespacing

Prefixed top-level object with unprefix children (current): confirm namespacing and identifier?

3

Document status

Experimental: is that the right intended status?

4

Trust model

scoreIssuer / scoreScheme trust is out-of-band. Is the security & privacy text sufficient?

5

Field set

Are the six fields the right minimal set: too few, too many?

6

Coordination

How best to align / avoid overlap with verified-contacts?

What we are asking today

Initial WG feedback on an individual draft. **No adoption request**, no new-work-item decision, at this stage.

Draft datatracker.ietf.org/doc/draft-bertoldi-regext-rdap-reliability-scoring/

Comments regext@ietf.org · alessandro@bertoldicybersecurity.com · spromano@unina.it

Thank you, and thanks to Pawel Kowalik, Mario Loffredo, Maurizio Martinelli, James Gould and James Galvin for the early engagement at IETF 125.

Questions / comments welcome.

Full RDAP example (domain)

Illustrative only. Field semantics are defined by scoreScheme, not by this draft.

```
{
  "rdapConformance": [ "rdap_level_0", "reliabilityScoring" ],
  "objectClassName": "domain",
  "ldhName": "example.tld",
  "reliabilityScoring_assessment": {
    "scoreScheme": "urn:example:domain-security-posture:v2",
    "scoreValue": 9,
    "scoreMaxValue": 10,
    "scoreDate": "2026-01-01T00:00:00Z",
    "scoreIssuer": "example-assessor",
    "evidenceUri": "https://example-assessor.org/reports/example.tld"
  }
}
```