REGEXT
Internet-Draft
Intended status: Experimental
Expires: 15 October 2026

A. Bertoldi
Bertoldi Cybersecurity
S. P. Romano
UNINA

13 April 2026

RDAP Extension for Structured Reliability Assessment Metadata
draft-bertoldi-regext-rdap-reliability-scoring-00

Abstract

This document proposes an extension to the Registration Data Access Protocol (RDAP) that enables the representation and exchange of structured reliability assessment metadata for registrars and domain names. The extension defines a structured assessment envelope through which any registry, registrar, or third-party assessor can expose assessment results in a common, machine-readable format within RDAP responses.

The extension standardizes how assessment results are transported and referenced, not how they are computed. Scoring methodologies, thresholds, criteria, and governance frameworks are intentionally left to the operational and policy layer.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 15 October 2026.

Copyright Notice

Table of Contents

1. Introduction

The domain registration ecosystem relies on registrars as critical intermediaries between domain owners and the global DNS infrastructure. Research [DEEPSEC2025] has identified recurring systemic vulnerabilities in registrar processes, including credential recovery, identity verification, and email authentication configurations, that represent structural risks affecting large numbers of domains and their owners. These issues have in several cases remained unaddressed for extended periods despite responsible disclosure.

The Registration Data Access Protocol (RDAP), defined in [RFC7480], [RFC7481], [RFC9082], [RFC9083], and [RFC9224], was designed as the successor to WHOIS and introduces structured JSON responses, authentication and authorization support, and a well-defined extensibility model. These properties make RDAP a suitable foundation for exposing structured security and reliability metadata in a standardized, interoperable way.

This document defines an RDAP extension that provides an envelope for carrying assessment results related to the security posture and reliability of registrars and domain names. The extension standardizes the transport and referencing of such results; it does not define scoring methodologies, thresholds, or enforcement mechanisms. The protocol enables representation; the ecosystem decides how to populate and consume the exposed fields.

The proposal is intended as complementary to [I-D.loffredo-regext-rdap-verified-contacts], which establishes that contact data has been verified. The present extension adds a parallel layer: structured metadata about the security posture of the registrar and the domain itself.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following terms are used throughout this document:

Assessment Envelope: The structured set of fields defined by this

extension, representing the result of a security or reliability assessment of a registrar or domain. The envelope carries the result and points to the methodology; it does not define the methodology itself.

Score Scheme: An identifier or URI that denotes the scoring methodology used to produce an assessment result. The scheme defines the semantics of the score value, its range, and its criteria. Scheme definitions are maintained externally to this document.

Score Issuer: An opaque identifier for the entity that performed the assessment and produced the score value. The format and resolution of this identifier are defined by the scoreScheme.

Extension Identifier: The RDAP extension string registered in the IANA RDAP Extensions Registry that identifies this extension.

3. Motivation and Problem Statement

Research [DEEPSEC2025] has identified recurring systemic vulnerabilities in domain registrar processes that cannot be addressed by conventional technical security controls. These vulnerabilities arise from weaknesses in the interface between digital systems and human processes, and include deficiencies in credential recovery, identity verification, and email authentication configurations.

A notable characteristic of these vulnerabilities is their persistence: in several documented cases, exploitable issues remained unresolved for extended periods following responsible disclosure, reflecting diffuse accountability and the absence of structured incentives for timely remediation.

These findings suggest that while technical standards such as SPF [RFC7208], DKIM [RFC6376], and DMARC [RFC7489] are sound, their adoption and correct configuration cannot be reliably ensured without structured, machine-readable signaling mechanisms. The full technical details of the underlying research are documented in [DEEPSEC2025].

3.1. Why Protocol-Level Representation Helps

Structured representation of assessment metadata at the protocol level offers several complementary benefits relative to existing operational approaches.

First, publicly accessible, machine-readable assessment data creates reputational and commercial incentives for registrars and domain owners to adopt and maintain security best practices, analogous to the role of Certificate Transparency in the TLS ecosystem.

Second, a standardized RDAP extension enables any registry, registrar, browser, or security tool to consume assessment metadata through a common interface, eliminating dependency on proprietary or registry-specific systems.

Third, protocol-level representation does not replace operational scoring or enforcement programs. Rather, it provides a standardized channel through which the outputs of such programs can be expressed and consumed by the broader ecosystem.

4. Design Principles

The following principles guide the design of this extension.

Separation of concerns: This document defines the structured assessment envelope and extension points. The governance of who computes scores, the specific scoring methodology, any thresholds applied, and any enforcement actions based on scores belong to the operational and policy layer and are intentionally outside the scope of this document.

Envelope, not methodology: The extension standardizes how assessment results are transported and referenced within RDAP. It does not standardize how assessments are performed, what criteria are evaluated, or what thresholds apply.

Extensibility: The extension is designed to accommodate additional fields without breaking backward compatibility, consistent with RDAP’s existing extensibility model.

Interoperability: The extension is not tied to any specific registry, registrar, or policy framework. Any conformant RDAP server may implement it independently.

Complementarity: The extension is designed to coexist with and extend [I-D.loffredo-regext-rdap-verified-contacts], rather than replace or duplicate it.

5. RDAP Extension: Data Model

5.1. Extension Identifier

This extension is identified by the string "rdap_reliability_scoring", to be registered in the IANA RDAP Extensions Registry (see Section 9). RDAP responses that include this extension MUST include the extension identifier in the "rdapConformance" array.

5.2. Namespacing Approach

This version of the document groups all extension fields under a single top-level JSON object keyed by the extension identifier ("rdap_reliability_scoring"). This encoding is used for readability when the extension defines multiple related fields. The authors welcome working group guidance on the preferred namespacing approach; the encoding may be revised in subsequent versions based on working group feedback.

5.3. Assessment Envelope

The assessment envelope is a JSON object that MAY appear within entity objects (objectClassName: "entity") and domain objects (objectClassName: "domain"). An entity is considered to represent a registrar when its "roles" array includes the value "registrar" as defined in Section 10.2.4 of [RFC9083]. All fields within the envelope are OPTIONAL. Implementers SHOULD populate only those fields for which they have authoritative data.

The envelope carries the result of an external assessment and points to the methodology used. It does not define the methodology, the criteria, or the thresholds.

5.4. Field Definitions

The fields defined by this extension are described in the following table. All fields are OPTIONAL.

Field	Type	Description
scoreScheme	string (URI or identifier)	Identifies the scoring methodology used to produce the assessment. When expressed as a URI, it MUST conform to [RFC3986]. The scheme defines the semantics, range, and criteria of the score. Scheme definitions are maintained externally.
scoreValue	number or null	The non-negative numeric result of the assessment, as defined by the scoreScheme. If scoreMaxValue is present, scoreValue SHOULD NOT exceed scoreMaxValue unless the scoreScheme explicitly defines otherwise.
scoreMaxValue	number or null	The non-negative maximum possible value under the scoreScheme. Together with scoreValue, helps consumers interpret the numeric result.
scoreDate	string (date-time)	The date and time at which the assessment was last performed, in the format defined in [RFC3339].
scoreIssuer	string	An opaque identifier for the entity that performed the assessment and issued the score. The format and resolution of this identifier are defined by the scoreScheme; it may be a local name, a URI, or a registered identifier.
evidenceUri	string (URI) or null	An OPTIONAL URI pointing to supporting documentation, a detailed report, or the full assessment record maintained by the scoreIssuer.

Table 1

Implementers MUST NOT infer normative meaning from the illustrative field values used in the examples in this document or in Appendix B.

5.5. Registrar Object Extension

The following example illustrates how the assessment envelope MAY appear within an entity object representing a registrar.

```
{
  "rdapConformance": [
    "rdap_level_0",
    "rdap_reliability_scoring"
  ],
  "objectClassName": "entity",
  "handle": "REGISTRAR-EXAMPLE",
  "roles": ["registrar"],
  "rdap_reliability_scoring": {
    "scoreScheme": "urn:example:registrar-security-assessment:v1",
    "scoreValue": 8,
    "scoreMaxValue": 10,
    "scoreDate": "2026-01-15T10:30:00Z",
    "scoreIssuer": "example-assessor",
    "evidenceUri": "https://example-assessor.org/reports/reg-example"
  }
}
```

5.6. Domain Object Extension

The following example illustrates how the assessment envelope MAY appear within a domain object.

```
{
  "rdapConformance": [
    "rdap_level_0",
    "rdap_reliability_scoring"
  ],
  "objectClassName": "domain",
  "handle": "example.tld",
  "ldhName": "example.tld",
  "rdap_reliability_scoring": {
    "scoreScheme": "urn:example:domain-security-posture:v2",
    "scoreValue": 7,
    "scoreMaxValue": 10,
    "scoreDate": "2026-02-01T08:00:00Z",
    "scoreIssuer": "example-assessor",
    "evidenceUri": null
  },
  "events": [
    {
      "eventAction": "registration",
      "eventDate": "2024-01-01T00:00:00Z"
    }
  ]
}
```

6. Relationship to Existing Work

6.1. Relationship to draft-loffredo-regext-rdap-verified-contacts

The [I-D.loffredo-regext-rdap-verified-contacts] extension establishes that contact data associated with a domain or registrar has been verified. The present extension adds a complementary and orthogonal layer: structured metadata about the security posture of the registrar and the domain itself.

The two extensions answer different questions. The verified-contacts extension addresses whether the identity of the entity behind a domain has been confirmed. The reliability-scoring extension addresses what the assessed security posture of the entity managing that domain is. Both are expressible within the RDAP framework and are designed to coexist within the same RDAP response.

6.2. Relationship to PIR Abuse Intervention Program

PIR's Abuse Intervention Program (AIP) and Quality Performance Index (QPI) [PIR-AIP] represent an example of a registry-specific operational assessment program. This document does not standardize such a program; it defines a generic RDAP representation that could carry outputs produced by programs such as PIR/QPI or other assessment frameworks.

An operational scoring system such as PIR/QPI could, in principle, expose its outputs through the envelope defined in this document, enabling broader interoperability without modifying its internal methodology.

6.3. Relationship to RDAP Core Specifications

This extension is designed to be fully conformant with the RDAP core specifications [RFC7480] [RFC7481] [RFC9082] [RFC9083] [RFC9224]. It uses the JSON response format defined in [RFC9083], the extensibility model provided in [RFC7480], and the security framework of [RFC7481]. Query formats follow [RFC9082] and service discovery follows [RFC9224].

7. Security Considerations

The fields defined in this extension are informational. They do not constitute enforcement mechanisms and MUST NOT be interpreted as authoritative security certifications.

Score integrity: Without appropriate authentication of the scoring entity, assessment metadata fields are susceptible to manipulation. Access to fields that can be modified programmatically SHOULD require mutual TLS authentication between client and server.

Gaming and abuse: Any publicly visible scoring system creates incentives for gaming. The governance framework, which is outside the scope of this document, SHOULD address verification, audit, and revocation mechanisms.

False assurance: Consumers of assessment metadata MUST NOT treat scores as equivalent to security certifications. A high score value does not guarantee the absence of vulnerabilities. Consumers SHOULD treat scores as one signal among many and SHOULD NOT make high-stakes trust decisions based solely on RDAP assessment fields.

Staleness: Scores reflect the state at the time indicated by the

"scoreDate" field. Consumers SHOULD check the freshness of assessment data and SHOULD treat scores that have not been updated recently with appropriate skepticism. Implementers MAY define an expiration policy based on the scoreScheme.

Scheme trust: The reliability of assessment data depends on the trustworthiness of both the scoreIssuer and the scoreScheme. Consumers SHOULD establish out-of-band trust in the scoreIssuer before acting on assessment data.

Evidence URI: The resource identified by evidenceUri is maintained by the scoreIssuer and is outside the control of the RDAP server. Its content may change over time, may be subject to access control, and may become unavailable. Consumers SHOULD NOT assume that the evidence resource is publicly accessible or immutable.

8. Privacy Considerations

The fields defined in this extension describe security posture at the registrar and domain level and are not intended to expose personal data. They are designed to be compatible with the access control framework defined in [RFC7481].

Implementers MUST ensure that the presence or absence of assessment metadata does not inadvertently reveal information about the identity of natural persons. The separation between assessment metadata, which is intended to be publicly accessible, and contact data, which is subject to access control per [RFC7481], MUST be maintained in conformant implementations.

This extension is intended to be compatible with applicable data protection regulations, including the General Data Protection Regulation [GDPR] and equivalent frameworks.

The evidenceUri field, if populated, SHOULD NOT point to resources that expose personal data or operationally sensitive details beyond what is necessary for the consumer to understand the assessment result.

9. IANA Considerations

This document requests the registration of the following entry in the IANA RDAP Extensions Registry:

Extension identifier: rdap_reliability_scoring

Registry operator: IANA

Published specification: this document

Contact: Alessandro Bertoldi (alessandro@bertoldicybersecurity.com)

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/rfc/rfc3339>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[RFC7480] Newton, A., Ellacott, B., and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)", STD 95, RFC 7480, DOI 10.17487/RFC7480, March 2015, <https://www.rfc-editor.org/rfc/rfc7480>.

[RFC7481] Hollenbeck, S. and N. Kong, "Security Services for the Registration Data Access Protocol (RDAP)", STD 95, RFC 7481, DOI 10.17487/RFC7481, March 2015, <https://www.rfc-editor.org/rfc/rfc7481>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9082] Hollenbeck, S. and A. Newton, "Registration Data Access Protocol (RDAP) Query Format", STD 95, RFC 9082, DOI 10.17487/RFC9082, June 2021, <https://www.rfc-editor.org/rfc/rfc9082>.

[RFC9083] Hollenbeck, S. and A. Newton, "JSON Responses for the Registration Data Access Protocol (RDAP)", STD 95, RFC 9083, DOI 10.17487/RFC9083, June 2021, <https://www.rfc-editor.org/rfc/rfc9083>.

[RFC9224] Blanchet, M., "Finding the Authoritative Registration Data Access Protocol (RDAP) Service", STD 95, RFC 9224, DOI 10.17487/RFC9224, March 2022, <https://www.rfc-editor.org/rfc/rfc9224>.

10.2. Informative References

[DEEPSEC2025] Bertoldi, A. and S. P. Romano, "Forever-Day at Scale: Hijacking Registrars, Defeating 2FA and Spoofing 17,000+ Domains (Even with DMARC p=reject)", DeepSec Vienna 2025, 2025, <https://bcsec.io/research/deepsec2025/deepsec2025.pdf>.

[GDPR] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", April 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>.

[I-D.loffredo-regext-rdap-verified-contacts] Loffredo, M., Martinelli, M., Gould, J., and P. Kowalik, "Registration Data Access Protocol (RDAP) Extension for Verified Contact Information", Work in Progress, Internet-Draft, draft-loffredo-regext-rdap-verified-contacts-03, 23 February 2026, <https://datatracker.ietf.org/doc/html/draft-loffredo-regext-rdap-verified-contacts-03>.

[ISO27001] "Information security, cybersecurity and privacy protection -- Information security management systems -- Requirements", ISO/IEC 27001:2022, 2022.

[ISO27701] "Privacy information management systems -- Requirements and guidelines", ISO/IEC 27701:2025, 2025.

[PIR-AIP] Public Interest Registry, "PIR Abuse Intervention Program and Quality Performance Index", 2025, <https://icann85.sched.com/event/2GwoE/ssac-work-session-pir-abuse-intervention-program>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/rfc/rfc4033>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/rfc/rfc6376>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/rfc/rfc7208>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/rfc/rfc7489>.

Appendix A. Acknowledgments

The authors thank Pawel Kowalik, Mario Loffredo, Maurizio Martinelli, James Gould, and James Galvin for their early engagement and feedback during IETF 125.

Appendix B. Example RDAP Responses

The examples in this appendix are provided for illustrative purposes only. Score values, scheme identifiers, and issuer names are fictional.

B.1. Domain Lookup with Assessment

```
{
  "rdapConformance": [
    "rdap_level_0",
    "rdap_reliability_scoring"
  ],
  "objectClassName": "domain",
  "handle": "example.tld",
  "ldhName": "example.tld",
  "rdap_reliability_scoring": {
    "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"
  },
  "events": [
    {
      "eventAction": "registration",
      "eventDate": "2024-01-01T00:00:00Z"
    }
  ]
}
```


B.2. Registrar Entity Lookup with Assessment


```
{
  "rdapConformance": [
    "rdap_level_0",
    "rdap_reliability_scoring"
  ],
  "objectClassName": "entity",
  "handle": "REGISTRAR-EXAMPLE",
  "roles": ["registrar"],
  "rdap_reliability_scoring": {
    "scoreScheme": "urn:example:registrar-security-assessment:v1",
    "scoreValue": 10,
    "scoreMaxValue": 10,
    "scoreDate": "2026-01-01T00:00:00Z",
    "scoreIssuer": "example-assessor",
    "evidenceUri": null
  }
}
```


B.3. Domain Lookup without Assessment

An RDAP response for a domain that has not been assessed simply omits the extension member:

```
{
  "rdapConformance": [
    "rdap_level_0"
  ],
  "objectClassName": "domain",
  "handle": "unassessed.tld",
  "ldhName": "unassessed.tld",
  "events": [
    {
      "eventAction": "registration",
      "eventDate": "2025-06-01T00:00:00Z"
    }
  ]
}
```

Appendix C. Illustrative Scoring Dimensions

This appendix describes possible dimensions that an operational scoring program might evaluate when producing assessment results to be carried by the envelope defined in this document. This content is entirely non-normative. Nothing in this appendix constrains implementers or defines mandatory evaluation criteria.

The intent is to demonstrate that the envelope model is expressive enough to carry results from real-world assessment programs, including those derived from existing empirical research on registrar security posture [DEEPSEC2025].

C.1. Possible Registrar Assessment Dimensions

An operational program might evaluate registrars across dimensions such as: the strength of customer identity verification procedures; the adoption and enforcement of multi-factor authentication for customer-facing and internal systems; the possession of recognized information security certifications such as ISO/IEC 27001 [ISO27001] or ISO/IEC 27701 [ISO27701]; the correctness of email authentication configurations including SPF [RFC7208], DKIM [RFC6376], and DMARC [RFC7489] on registrar-operated domains; the existence of documented security policies; and the regularity of cybersecurity training programs for staff.

C.2. Possible Domain Assessment Dimensions

An operational program might evaluate individual domains across dimensions such as: the strength of owner identity verification at registration or renewal; the level of SSL/TLS certificate used; the correctness of SPF, DKIM, and DMARC configurations; the implementation of DNSSEC [RFC4033]; and the absence of the domain from monitored abuse blacklists over a defined observation period.

C.3. Note on Existing Operational Programs

Existing programs such as PIR's Quality Performance Index [PIR-AIP] focus on observable abuse outcomes and operational metrics within a single registry context. The assessment dimensions described above focus on structural security posture. The envelope defined in this document is agnostic to the methodology and could carry results from either type of program.

Authors' Addresses

Alessandro Bertoldi
Bertoldi Cybersecurity
Email: alessandro@bertoldicybersecurity.com

Simon Pietro Romano
Universita' degli Studi di Napoli Federico II
Via Claudio 21
80125 Naples
Italy
Email: spromano@unina.it