Internet-Draft
Intended status: Informational
Expires: 27 June 2026

Yoshio Murofushi
ZEROBANKX PTE. LTD.

January 10, 2026

Secure Resource Layer (SRL) Core
draft-zerobankx-srl-core-01

Abstract

This document defines the Secure Resource Layer (SRL), a global trust layer that verifies digital resources before they are accessed. SRL introduces governance, verification, and revocation mechanisms that complement existing URL, QR code, and short URL systems.

SRL is designed to be deployable incrementally and is already being validated through live resolver deployments without requiring changes to existing Internet standards.

1. Introduction

URLs, QR codes, and short URLs are widely used to reference digital resources. However, these mechanisms provide no native way to verify whether a referenced resource is trustworthy, revoked, or still valid at the time of access.

As a result, users and platforms face increasing risks, including phishing, malicious redirects, outdated links, and the distribution of unsafe or unauthorized content.

Despite widespread use of URLs and QR codes, the Internet currently lacks a standardized mechanism to express trust, governance, or revocation at the reference layer itself. Responsibility for link safety is fragmented across applications, platforms, and proprietary services, resulting in inconsistent security outcomes and limited accountability.

Secure Resource Layer (SRL) introduces a reference-layer trust model that operates independently of transport protocols and application platforms. SRL enables verification, governance, and revocation of

digital resources before they are accessed, while remaining backward compatible with existing Internet mechanisms.

This document defines the core concepts and architecture of SRL.

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.

SRL: Secure Resource Layer.
SRP: Secure Resolution Protocol.
Resource Identifier: An identifier referencing a digital resource.
Issuer: An entity that registers or publishes a resource.
Verifier: A component that validates SRL information.
Registry: A system that maintains trust and governance data.
Revocation: The act of invalidating a previously trusted resource.

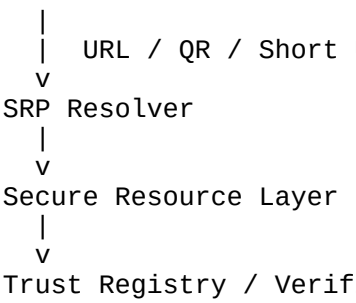
3. Design Goals

SRL is designed with the following goals:

- Platform and vendor neutrality
- Backward compatibility with existing Internet mechanisms
- Minimal disclosure of user information
- Explicit governance and accountability
- First-class support for revocation

4. Architecture Overview

SRL operates as a logical layer between resource references and resource access.



The architecture is implementation-agnostic and does not mandate a specific transport, programming language, or cryptographic mechanism.

4.1. Integration with Short URLs and QR Codes

SRL is designed to integrate seamlessly with existing short URL and QR code mechanisms, including managed short URL systems.

Trust validation, governance, and revocation are handled entirely by SRL prior to resource access. The QR code or short URL itself remains unchanged.

4.2. Deployment Model (Informative)

SRL is intended to be deployable without changes to existing Internet protocols, browsers, or operating systems.

Typical deployments include resolver-based validation prior to

redirection, platform-level verification for QR code scanners, and application-level trust checks for link previews.

An SRL deployment MAY operate as a local resolver, a network service, or an embedded component within an application.

5. Secure Resolution Protocol (SRP)

Secure Resolution Protocol (SRP) enables clients to query SRL for trust and validity information before accessing a resource.

SRP is transport-agnostic and MAY be carried over HTTPS, local inter-process communication, or other suitable mechanisms.

5.1. Protocol Model

SRP follows a request/response model. A client submits an SRP Request containing a resource identifier and optional metadata. SRL returns an SRP Response containing a trust decision.

5.2. Message Encoding

SRP messages are encoded using JSON [RFC8259] and MUST support UTF-8.

5.3. SRP Request Message

An SRP Request is a JSON object containing the following fields: srl_version (MUST), resource_id (MUST), issuer (SHOULD), timestamp (SHOULD), nonce (SHOULD), requested_action (MAY).

5.4. SRP Response Message

An SRP Response includes a status (MUST), resolved_url (MAY), expires_at (MAY), issuer_verified (MUST), and revocation_checked (MUST).

5.5. Error Handling

If an SRP Request cannot be processed, SRL SHOULD return an SRP Response with an appropriate status value.

5.6. Security Considerations for SRP

The absence of mandatory cryptographic signing in the current SRP design is an intentional design decision to prioritize deployability and early adoption.

6. Secure Resource Layer (SRL)

SRL evaluates SRP requests and determines the trust status of the referenced resource.

SRL explicitly separates resource trust from resource access. A positive trust decision does not imply endorsement of content, only that governance, issuer identity, and revocation status have been evaluated.

SRL MAY return trust decisions such as valid, revoked, expired, unknown, or blocked. Policy decisions MAY vary by deployment environment.

SRL does not require modification of the underlying resource, URL, or QR code.

7. Trust Registry and Governance

SRL relies on registries that maintain issuer information, trust status, and governance rules. Registries MAY be centralized, federated, or distributed.

Specific governance policies are intentionally out of scope for this document and may be defined by individual deployments.

8. Revocation Model

Revocation is a core feature of SRL. Supported models include immediate revocation, time-based expiration, and conditional revocation.

Revocation information MUST be retrievable by verifiers in a timely manner.

9. Security Considerations

SRL mitigates threats including phishing, redirect poisoning, replay attacks, and reference-layer spoofing. SRL complements, but does not replace, transport-layer security such as TLS.

SRL trust decisions do not constitute an endorsement or certification of the referenced content.

10. Privacy Considerations

SRL minimizes the collection of personal data. SRP requests SHOULD avoid including user-identifiable information.

11. Use Cases

SRL supports consumer web navigation, creator economies, medical information distribution, public administration, and platform-level link mediation.

12. IANA Considerations

This document has no IANA actions.

13. Normative References

[RFC2119] Bradner, S., RFC 2119.
[RFC8174] Leiba, B., RFC 8174.
[RFC8259] Bray, T., RFC 8259.

14. Future Work

Future specifications MAY define cryptographic signing, issuer-bound keys, and interoperability with existing PKI systems.

Authors’ Addresses

Yoshio Murofushi
ZEROBANKX PTE. LTD.
Email: fin.zerobankx@gmail.com