RSW-0011 — Security and Permissions

Revision 0.01 | Protocol rsw/1 | Format 1 | Experimental proposal

Developed by Pablo Murad — November 23, 2026 — pablo@pablomurad.com — https://rsw.works

Experimental Project Specification. This document is an experimental specification of the Really Small Web project. It is a work in progress and has not been published as an RFC or approved as an Internet Standard.

License: specifications CC0 1.0 (public domain); future reference implementation and official tools MIT.

RSW-0011 — Security and Permissions

Revision 0.01 | Protocol rsw/1 | Format 1

MVP — experimental normative proposal

Developed by Pablo Murad

Pablo Murad — November 23, 2026

pablo@pablomurad.com

MUST and MUST NOT indicate requirements of the described profile; SHOULD indicates a recommendation; MAY indicates an option. Experimental document, not yet ratified or implemented. The rules of RSW-0001 through RSW-0003 remain applicable.

01. Objective and Threat Model

Mandatory for the MVP. Attackers can control the PNG, ZIP, manifest, HTML, CSS, Markdown, URL, DNS, server, index, and content signed by their own key. They may attempt key access, file access, local services, tracking, exhaustion, and tampering. Authenticity is not equivalent to trust. Outside the guarantee: a compromised operating system, an unknown browser vulnerability, anonymity against a network observer, universal key recovery, and global availability. Do not promise an infallible sandbox.

02. Validation and Budgets

Apply RSW-0001/0002/0003 before rendering. Count real bytes, limit decompression, validate CRCs, paths, inventory, and hashes. Never open content in a browser pointed at an extracted directory. Do not allow special files or overwriting. Reject an invalid signature even in offline mode. Unsigned content is only accepted locally with a warning; it enables no additional privileges. Limit concurrent operations, memory, time, and disk; offer cancellation. A local policy may refuse a valid cartridge without marking it INVALID.

Renderable resources: .md, .html, .css, .png, .jpg, .jpeg; the remaining files are opaque data, without active display or automatic download. Local images: effectively decoded PNG or JPEG, at most 2048 x 2048 and 4,194,304 pixels per image; at most 16,777,216 pixels accumulated per page (count uses); reject animation or unsupported formats. Decode under a memory limit and re-encode into an inert representation for presentation; do not modify the original. SVG, fonts, GIF, audio/video, embedded PDF, plugins, and iframes are outside the safe profile. If a resource is unsupported, show a placeholder. Proposed per-page ceiling: 256 KiB of source text, 4096 rendered nodes, depth 32, 128 links, and 32 images. Presentation refusals do not invalidate the signature.

03. Text and Static Profiles

Text: CommonMark 0.31.2 Markdown, without active extensions; interpret the AST, treat raw HTML as text, do not render it directly. Static: parse HTML with an established parser, rebuild the allowed tree; never insert source text as HTML in the privileged interface. Allow semantic elements: p, h1..h6, div, span, section, article, header, footer, main, nav, blockquote, pre, code, em, strong, b, i, s, ul, ol, li, dl, dt, dd, hr, br, table, thead, tbody, tr, th, td, figure, figcaption, a, img. Remove active tags and subtrees of script, unprocessed style, iframe, object, embed, form, input, button, svg, math, template, meta, unauthorized link, base, and unknown elements; do not copy event attributes, srcset, target, download, nonce, data-*, or arbitrary URLs. Allowed attributes: id and class in a simple ASCII grammar, alt and title as text, local img src and a href analyzed per

RSW-0004. Anchor IDs must be valid and unique; discard later duplicates. Remove all other attributes. Non-admitted links appear inert.

CSS is optional for visual reading, but Static must allow restricted local styling. Read only a locally referenced .css explicitly referenced by the document's stylesheet, or a style element/attribute if the same safe parser is applied. Do not copy the original CSS. Accept only simple tag, .class, or #id selectors, without functions, pseudo-classes, or combinators; allow color, background-color (local list names or #RGB/#RRGGBB), font-weight (normal/bold/100..900), font-style (normal/italic), text-align (left/right/center), text-decoration (none/underline/line-through), font-size (8..48px), line-height (1..2.5), margin/padding (0..48px), border-width (0..4px), border-style (none/solid/dashed), border-color (allowed colors). Limit to 256 rules, 32 declarations per rule. Re-emit only validated values from a CSS parser; discard at-rules, functions, unvalidated escapes, url(), @import, variables, position, animation, and unknown properties. If there is no safe parser, omit CSS and report the visual limitation; never release raw CSS.

04. Reader Isolation

Reference architecture: a UI server on loopback and an OS-chosen port, a privileged interface separated from the content iframe. Empty sandbox iframe (without allow-scripts, allow-same-origin, allow-forms, allow-popups, or top-navigation). Render the rebuilt document with CSP: default-src 'none'; script-src 'none'; connect-src 'none'; object-src 'none'; base-uri 'none'; form-action 'none'; frame-src 'none'; img-src data:; style-src 'unsafe-inline'. Only reader-re-encoded images are converted to data:; do not accept data: from input. The re-emitted CSS contains no URLs. Prefer CSP by header on the isolated origin when possible; srcdoc may use an initial meta CSP plus sandbox and parent-origin controls. Do not treat CSP as a sanitizer substitute. The UI must present a list of links outside the iframe, with escaped labels and real destinations; in the iframe, represent links as inert numbered text, without remote href. Local fragments may be mediated by the UI. Do not use postMessage from static content as authority. External navigation requires explicit user action. The interface does not execute cartridge-provided HTML in its own origin.

05. Local API and Keys

Listen exclusively on 127.0.0.1 or ::1, on a non-public socket. Exact host of the created origin, exact Origin on mutating operations, CSPRNG session token of at least 128 bits, POST methods for changes, no permissive CORS. Validate Fetch Metadata when available; block UI framing (frame-ancestors 'none'); do not authenticate by IP address alone. Sensitive read operations also require a session. Do not expose arbitrary paths, secrets, a generic signing API, or shell access. Store keys outside the web root per RSW-0003; do not log sensitive content or secrets. Import, publication, and removal operations require explicit action and limits.

06. Transport and Privacy

Apply RSW-0005 to all remote fetching, including manually entered sources; prevent SSRF, DNS rebinding, redirects, and implicit proxies. Block traffic in offline mode. No prefetch, trackers, remote fonts, or external resources. No peer can trigger a download. External HTTPS opened by user request leaves the isolated area; do not attach identity, token, or history. Avoid telemetry by default. Store preferences locally, allow explicit clearing of history and cache without destroying keys.

07. Security Tests and Criteria

Fuzzing of PNG/ZIP/JSON/URI; exact limits and overflow; paths, symlinks, ZIP bombs, and CRCs; degenerate signatures; HTML with events, SVG, meta refresh, srcset, links, and remote CSS; CSS escapes; external and local requests; fake Host/Origin, CSRF, framing, and DNS rebinding; isolation between cartridges; offline test with monitored network. Verify that tokens, keys, and host files never appear in content. Test Linux, Windows, macOS, and supported browsers. Before public release, independent review and a disclosure process. Pending: implementation and proof of isolation; do not enable scripts through this proposal. References: CommonMark https://spec.commonmark.org/0.31.2/ ; CSP https://www.w3.org/TR/CSP3/ ; HTML https://html.spec.whatwg.org/ ; RSW-0001..0007/0012/0016.

License: CC0 1.0 (public domain dedication; see CC0-1.0.txt in the downloads area). Developed by Pablo Murad | pablo@pablomurad.com END — RSW-0011

Author's Address

Pablo Murad
Independent
pablo@pablomurad.com
https://pablomurad.com
Official project website: https://rsw.works

Small files. Independent worlds.