

1) BRAND SUMMARY (max 10 bullets)

- Domain / brand: keylessssl.dev — security-first, API-first, developer-to-developer DCVaaS skin.
- Target persona: Devs, DevOps, CTOs building SaaS / multi-tenant custom domains; people who've been burned by cert automation.
- Positioning: Delegated DCV (DNS-01/ACME) that removes root DNS credentials from the pipeline; "Delegated DCV, not delegated trust."
- Primary conversion path: Generate API key (free for 3 domains) → add CNAME delegation → domain goes Verified/Validated → first cert issued → renewals stay boring.
- Primary CTA (persistent): "Get API Key — Free for 3 Domains" (header + repeated CTAs + footer).
- Key claims / pillars: Air-Gapped Validation, 47-Day Renewal Readiness/Future, Cloudflare-Powered Reliability/Arbitrage (edge execution, predictable validation).
- Trust posture language to keep: keys/tokens are scoped, shown once, stored hashed, rotatable, audit events/logs exist (or are planned in shared platform).
- Voice rules: short declarative sentences, protocols + failure modes, no "green padlock / peace of mind" fluff.
- Visual vibe: dark-first "infra UI", code + diagrams (RFC feel), line icons, minimal motion.
- SEO themes: ssl certificate api, wildcard ssl automation, delegated DCV, ACME, DNS-01 challenge, certbot alternative, DCVaaS.

2) THEME TOKENS

```
:root[data-brand="keylessssl.dev"]{
```

```
/* Brand identity */
```

--brand-name: "KeylessSSL";

--brand-domain: "keylessssl.dev";

color-scheme: dark;

/* Typography */

--font-sans: Inter, ui-sans-serif, system-ui, -apple-system, Segoe UI, Roboto, Helvetica, Arial, "Apple Color Emoji", "Segoe UI Emoji";

--font-mono: "JetBrains Mono", ui-monospace, SFMono-Regular, Menlo, Monaco, Consolas, "Liberation Mono", "Courier New", monospace;

/* Core colors (dark-first infra UI) */

--color-bg: #070A10; /* near-black w/ slight blue cast */

--color-bg-2: #0B0F17; /* depth gradient */

--color-surface: #0B1220; /* panels */

--color-surface-2: #0E1522; /* elevated panels */

--color-surface-3: rgba(0,0,0,.20); /* input fill / inset */

--color-text: #E7EEF9;

--color-text-muted: #A7B4C9;

--color-text-faint: #7F8AA0;

/* Lines / borders */

--color-border: rgba(255,255,255,.10);

--color-border-subtle: rgba(255,255,255,.06);

/* Brand accents */

```
--color-primary: #00D084;      /* secure green (primary action + success) */
--color-primary-weak: rgba(0,208,132,.18);
--color-primary-weak-2: rgba(0,208,132,.08);
--color-secondary: #39B7FF;     /* dev-blue (links + focus) */
--color-secondary-weak: rgba(57,183,255,.12);
--color-danger: #FF4D6D;
--color-danger-weak: rgba(255,77,109,.10);
--color-warning: #FFCD4A;       /* amber (pending) */
--color-warning-weak: rgba(255,205,74,.06);
```

```
/* On-colors */
```

```
--color-on-primary: var(--color-text);
--color-on-danger: var(--color-text);
```

```
/* Shadows */
```

```
--shadow-1: 0 1px 0 rgba(0,0,0,.35);
--shadow-2: 0 18px 50px rgba(0,0,0,.35);
--shadow-3: 0 20px 60px rgba(0,0,0,.55);
```

```
/* Radii */
```

```
--radius-xs: 10px;
--radius-sm: 12px; /* buttons/inputs */
--radius-md: 16px; /* cards */
--radius-lg: 22px; /* hero/price cards */
```

```
--radius-pill: 999px;
```

```
/* Spacing (4px base) */
```

```
--space-0: 0px;
```

```
--space-1: 4px;
```

```
--space-2: 8px;
```

```
--space-3: 12px;
```

```
--space-4: 16px;
```

```
--space-5: 20px;
```

```
--space-6: 24px;
```

```
--space-7: 32px;
```

```
--space-8: 40px;
```

```
--space-9: 48px;
```

```
--space-10: 64px;
```

```
--space-11: 80px;
```

```
/* Breakpoints + layout */
```

```
--container-max: 1140px;
```

```
--bp-sm: 640px;
```

```
--bp-md: 768px;
```

```
--bp-lg: 960px; /* matches collapse point in landing implementation */
```

```
--bp-xl: 1280px;
```

```
--app-sidebar-w: 280px;
```

```
--topbar-h: 56px;
```

```
/* Focus + motion */

--focus-ring: 0 0 0 4px rgba(57,183,255,.18);

--focus-border: rgba(57,183,255,.40);

--motion-fast: 80ms;

--motion-med: 120ms;


/* Iconography */

--icon-stroke: 1.8px;

}
```

3) TYPOGRAPHY + SPACING SCALE (concise)

Typography

- UI: var(--font-sans); code/DNS/API keys: var(--font-mono).
- Headings: tight line-height, slightly negative tracking; “infra tool” weight (650–900).
- Kicker labels (section eyebrow): mono, uppercase, wide tracking (RFC vibe).

Type scale mapping

- H1 (marketing hero): clamp(2.1rem, 4.6vw, 3.4rem) / 1.06
- H2: 1.7rem / 1.2–1.3
- H3: 1.08rem–1.15rem / 1.25
- Body: 1rem / 1.6 (marketing), 1.5 (app)

- Small: 0.9–0.95rem
- Micro/labels: 0.82–0.85rem (mono for headers + chips)

Spacing

- Base grid: 8px rhythm (use --space-2 multiples).
- Cards/tables: internal padding 12–18px (--space-3 to --space-5).
- Sections (marketing): vertical padding ~58px with thin dividers.

4) COMPONENT STYLE GUIDE (bulleted, grouped by component)

Buttons

- Base (.btn)
 - Height 40px desktop / 44px touch; radius --radius-sm; border 1px solid var(--color-border); background rgba(255,255,255,.02); weight 650; subtle press translateY(1px).
- Primary
 - Border tint: rgba(0,208,132,.45); background: green-tinted vertical gradient; shadow: green glow (rgba(0,208,132,.12)).
 - Hover: border rgba(0,208,132,.70), stronger gradient.
 - Use only for conversion actions: Get API Key, Verify DNS, Start Pro, Issue/Renew.
- Secondary

- Same as base button; used for “See integration”, “Integrate now”, “Docs”.
- Ghost
 - Border `--color-border-subtle`, transparent bg, muted text; used for “Sign in”, “Status”, tertiary links.
- Destructive
 - Danger border + danger wash background (`--color-danger-weak`), text `--color-text`; use for Rotate key confirmation, Disable domain. (Added)

Inputs (text/select/textarea)

- Background: `var(--color-surface-3)`; border 1px solid `var(--color-border-subtle)`; radius `--radius-sm`; monospace for domain, DNS records, API keys.
- Focus: border-color: `var(--focus-border)` + box-shadow: `var(--focus-ring)` (must apply on all inputs, search, table row focus, modal close).
- Inline help copy: technical and specific (“CNAME not found”, “points elsewhere”), no “Oops”.

Tables (Domains is the money screen)

- Sticky header with mono labels; subtle divider line.
- Rows: dense but scannable; hover = slight surface lift (`--color-border` stays).
- Domain + DNS values: monospace; allow horizontal scroll for long targets.
- Actions column: icon-only buttons with tooltips (View / Rotate token / Re-check DNS).

Status badges / chips (ops tooling style)

- Pill shape (--radius-pill), mono 0.82rem, dot indicator.
- Active / Verified: green dot + green wash.
- Pending: amber dot + amber wash.
- Error: danger dot + danger wash.
- Keep labels 1–2 words; expand details in diagnostics panel.

Cards

- Border: --color-border-subtle; bg: subtle white alpha gradient (no glass); shadow --shadow-2 only for hero/featured pricing; otherwise keep low.
- Card headers: title + small muted subtitle; include “chip” tag in mono for env/hostnames.

Navigation

- Marketing header
 - Sticky; condenses on scroll; CTA stays prominent.
 - Left: wordmark + glyph (key-with-slash inside shield).
 - Center (desktop): anchor links Architecture / Integration / Pricing / Docs.
 - Right: Status, Sign in, Get API Key — Free for 3 Domains.
- App shell
 - Left sidebar (desktop): keep required IA, but allow dev-expected items:
 - Core: Domains, Billing, Settings
 - Optional if supported: Certificates, API Keys, Webhooks, Audit Log, Usage/Rate Limits

- Mobile: sidebar → slide-over; keep a sticky primary action on Domains (“Add Domain”). (Added)

Modals

- Width 560–760px; mobile becomes full-screen sheet.
- Must: focus trap, Esc closes, close button keyboard reachable.
- Code blocks inside: mono, copy button, language chip label.

Alerts / callouts

- Root Key Vulnerability callout: danger border wash; short declarative statement; can include monospace emphasis.
- Verification instructions: info panel w/ clear record (host/type/target) + copy buttons + “Recheck DNS”.
- Respect prefers-reduced-motion.

Tooltips

- Dark surface, subtle border, shadow --shadow-2.
- Use for protocol hints + “keys shown once” reminders, not paragraphs.

Dashboard-specific components (must feel like a real infra console)

- Verification panel

- Shows the exact delegation record, copy host + target separately, and a single button: Verify DNS / Re-check DNS (polling + timeout states).
 - Diagnostics drawer/panel
 - Failure modes list (short): CNAME missing / wrong target / propagation delay / CA error / rate limit risk; show trace ID if present (Added; “trace IDs” mentioned as desired behavior).
 - API key display
 - Creation: show once, force a copy + “I’ve stored it” checkbox gate before continuing (if your existing flow supports multi-step).
 - After creation: masked `kssl_live_.....` style; copy still works (copies masked? no—copy should pull stored token only if backend returns; otherwise copy disabled) (Added; front-end constraint).
 - Copy-to-clipboard
 - Always present on code/DNS/API key fields; toast is minimal: “Copied”.
-

5) PAGE BLUEPRINTS

Home (marketing — one-page anchored scroll)

- Sticky header (wordmark + glyph, anchors, Status/Sign in, persistent CTA).
- Hero
 - Headline + subhead + CTA cluster + proof chips + architecture diagram (RFC style).
- Problem
 - Title “Root Key Vulnerability” + direct body + danger callout + threat model accordion (collapsed).

- Architecture
 - “Delegated DCV, not delegated trust.” + 3 pillars + 4-step flow.
- Integration
 - Inline 3 steps + “View integration” modal (tabs: curl, Terraform, GitHub Actions, Kubernetes).
- Dashboard preview
 - Domains table preview + “account health” metrics (optional).
- Pricing
 - Two cards (Hacker free, Pro \$15) + undercut note.
- Docs/Blog teaser
 - Two cards: Docs + Blog: certbot debt.
- Final CTA
 - High-contrast block + CTA button.
- Footer
 - Docs / API Reference / Security / Status / Contact / Terms / Privacy.

Pricing (route OR section on Home)

- If separate route exists: same two cards + FAQ + undercut note.
- If not: anchor to Home #pricing and keep plan cards identical.

How it Works (route OR sections: Architecture + Integration)

- “Delegated DCV via CNAME” diagram + 4-step flow.
- “Why certbot is technical debt” block (headline + short paragraph) and link to blog/docs.

Docs/Guides (if applicable)

- Quickstart: Generate API key → Add domain → Add CNAME → Verify → Issue via API.
- API reference + rate-limit semantics + domain lifecycle doc link (important for dev trust).

Login

- Minimal layout: logo + single-line purpose (no fluff); link to Docs/Quickstart.
- Optional: GitHub OAuth button only if already supported (Added/conditional).

Dashboard (Domains)

- Header line: Active Domains | Pending Verification | Rate Limit Status (must appear).
- Primary action: Add Domain.
- Main content: Domains table (Domain / Delegation / Cert / Next renewal / Last issuance / Actions).
- Side panel (or below on mobile): selected domain details:
 - Delegation record + copy buttons
 - Verification state + “Re-check DNS”
 - Cert state + last/next renewal
 - Diagnostics (failure mode bullets)

Add Domain modal

- Input placeholder: *.app.your-saas.com (must use).
- Instruction text (must use): “Add this CNAME record to your DNS provider once. We will handle rotations forever.”
- Display generated record:
 - Host: _acme-challenge.<domain>
 - Type: CNAME
 - Target: use backend-provided delegation target; show example format in helper text if needed (see conflicts section).
- Buttons: “Add domain” + “Verify DNS” (polling state).

Verification instructions (page or panel)

- Always show a single, copyable “one-time delegation” record and what success looks like (“Verified” chip goes green).
- Diagnostics states (Added, but aligned): NXDOMAIN / wrong target / propagation delay.

Billing

- Plan card (Hacker vs Pro) + domain usage meter.
- Keep language blunt: queue priority, rate limits, audit events/team access.

Settings

- API token/key management (keys shown once, rotation, scope).

- Minimal org/profile controls.
 - Include Security link prominently (matches trust narrative).
-

6) COPY PACK (marketing + in-app)

Marketing — Home hero

- Headline (verbatim across sources): “Stop leaking your DNS root keys to production servers.”
- Subhead (Merged; sourced wording, no new claims):

“KeylessSSL automates wildcard TLS via Delegated DCV. Delegate _acme-challenge once (CNAME). Your high-privilege DNS credentials stay air-gapped in your vault. Add one CNAME. Ship renewals forever.”
- Proof chips (verbatim):
 - “No DNS API keys in CI/CD”
 - “Built for 47-day renewal cycles”
 - “Cloudflare edge execution”
- Primary CTA (verbatim): “Get API Key — Free for 3 Domains”
- Secondary CTA (verbatim): “View integration” / “See integration” (opens snippet/modal).
- CTA microcopy (tooltip or below; merged): “No credit card. Key shown once. Tokens are hashed server-side. Rotate any time.”

Marketing — Problem block

- Title (verbatim): “Root Key Vulnerability”

- Body (verbatim concept; keep direct): Root DNS API keys on build agents/app servers/k8s secrets is “a zone takeover waiting to happen.”
- Anchor quote (verbatim): “If one server is compromised, your entire DNS zone is gone.”

Marketing — Architecture pillars

- Title (verbatim): “Delegated DCV, not delegated trust.”
- Pillars (verbatim headings + compressed copy):
 - Air-Gapped Validation — delegate only `_acme-challenge`; root keys never touch KeylessSSL / your servers / CI.
 - 47-Day Renewal Readiness — designed for high-frequency renewals, no cron glue.
 - Cloudflare-Powered Reliability — validation runs at the edge; predictable execution; “enterprise-grade uptime without the enterprise price tag.”

Marketing — Integration steps (inline)

1. Delegate validation
`_acme-challenge.example.com CNAME example-com.<tenant>.dcv.keylessssl.dev`
2. Issue via API (curl snippet)
3. Install (your way) “Nginx / Caddy / Traefik / ALB / Cloudflare — you decide.”

Marketing — Pricing cards

- Pricing section title (verbatim): “Pricing that doesn’t punish automation.”
- Plan 1: Hacker (Free) (verbatim lines)

- “\$0 / mo”
- “Up to 3 domains”
- “Wildcards included”
- “Delegated DCV”
- “Community queue”
- “Standard rate limits”
- CTA: “Get API Key — Free”
- Plan 2: Pro (verbatim lines)
 - “\$15 / mo”
 - “Up to 50 domains”
 - “Wildcards included”
 - “Priority queue”
 - “Higher rate limits”
 - “Team access + audit events”
 - CTA: “Start Pro”
- Undercut note (verbatim): “Cheaper than BrandSSL’s \$29/mo starter — without shipping your root keys.”

Marketing — Docs/Blog teaser

- Title (verbatim): “Built by people who’ve been burned by cert automation.”
- Links (verbatim):
 - “Docs: ACME + DNS-01 via Delegated DCV”

- “Blog: Why certbot is technical debt”

In-app — required strings (verbatim from brand bible)

- Dashboard header: “Active Domains | Pending Verification | Rate Limit Status”
- Add Domain modal:
 - Placeholder: *.app.your-saas.com
 - Instruction: “Add this CNAME record to your DNS provider once. We will handle rotations forever.”
- API token page CTA + warning (verbatim):

“Generate Scoped API Token. Warning: This token is shown only once. It is hashed using SHA-256 before storage.”

In-app — status microcopy (Added; aligned to ops tone)

- Active: “Auto-renewing. Next renewal scheduled. Last issuance logged.”
- Pending: “Delegation not detected. Confirm _acme-challenge CNAME target.”
- Error: “Validation failed. Open diagnostics for exact failure mode + trace.”
- Toasts: “Copied.” / “Saved.” / “Domain queued.”

7) IMPLEMENTATION CHECKLIST (10-20 checkboxes)

- Implement hostname → brand resolver and set
document.documentElement.dataset.brand = "keylessssl.dev".

- Load the token set via `:root[data-brand="keylessssl.dev"] { ... }`; remove component-level hardcoded colors.
- Enforce dark-first (color-scheme: dark) and verify AA contrast for text, muted text, links, chips.
- Apply focus styles globally using `--focus-ring + --focus-border` (buttons, inputs, tabs, table rows, modal close).
- Keep marketing header behavior: sticky, condense on scroll, CTA stays full-size; center anchors on desktop only.
- Implement “copy-to-clipboard done right”: copy button + “Copied” toast on DNS records, code blocks, API key display.
- Build Integration modal with code tabs (curl / Terraform / GitHub Actions / Kubernetes) and include “Tokens are scoped... shown once...” footer microcopy.
- Ensure signup/API key UX honors “shown once” (mask after creation) and uses the exact SHA-256 warning string on token page.
- Domains screen: implement status chips (Active/Pending/Error/Disabled) that look like ops tooling.
- Verification UX: one clear CNAME record + “Verify/Re-check DNS” button + polling + timeout messaging (front-end only; consume existing endpoints).
- Surface rate limit info somewhere visible (dashboard header already includes Rate Limit Status).
- Keep IA intact (Login, Dashboard, Domains, Add Domain, Verification, Billing, Settings). Add extra nav items only if the backend already exposes them.
- Marketing SEO: set title/meta/OG from landing spec (technical tone).
- Respect prefers-reduced-motion; no heavy animations; hover/focus only.
- Regression guard: no auth/billing/API behavior changes; theming + copy + layout only.

Vance Mercer check (ruthless):

This merged spec is usable. It keeps the product's knife-edge message: root keys in prod = catastrophic blast radius and the UI reads like infra, not a brochure. The only place you can still sabotage conversion is ambiguity: hardcode nothing you don't control (CNAME target), and don't lie about rate limits. Make "Get API Key" unavoidable, make "Verify DNS" idiot-proof, and ship the Security page link early — devs buy threat models, not vibes.