# Original Client Specifications

I want a simple webpage where people can give feedback about our product or service. People should be able to leave feedback anonymously, but it would be good if they have an option to add their email in case we want to follow up. Each piece of feedback should show when it was submitted. There should be a simple way for me or someone else to log in securely to see all the feedback that has been left. We also need to be able to delete feedback if necessary, but it should ask for confirmation before deleting anything. It’s important that people's email addresses and the login information for managing the feedback are kept safe and secure. We also need to let people know how their email addresses will be used if they provide them, to keep everything compliant with privacy laws like GDPR. The page should be simple and easy to use, and it should look good and work smoothly on different web browsers like Chrome, Firefox, and Edge.

# Macro Iteration 02

## Phase: Initiating

### Artifact 1.1.0 final (mini 02) — Input

|  |  |  |
| --- | --- | --- |
| Input Item | Details | Related Reqs |
| Client specification (summary) | Simple webpage for anonymous feedback, optional email, admin view, delete with confirm, GDPR notice, responsive | [PLACEHOLDER-AUTO] |
| Anonymous feedback | Allow anonymous submissions; store feedback text plus minimal metadata: submission\_id, timestamp, ip-hash | [PLACEHOLDER-AUTO] |
| Optional email capture | Optional email field; encrypt at rest, mark contact\_intent flag, do not require for submit | [PLACEHOLDER-AUTO] |
| Submission timestamp | Record ISO-8601 UTC timestamp for each submission and surface in admin UI | [PLACEHOLDER-AUTO] |
| Admin authentication | Least-privilege admin roles, strong password + MFA, session rotation with rotatedAt and TTL | [PLACEHOLDER-AUTO] |
| Delete with confirmation | Admin delete requires explicit confirmation UI; record deletion event with actor\_id and timestamp | [PLACEHOLDER-AUTO] |
| Data protection for emails and credentials | Encrypt emails and admin credentials at rest; TLS for transport; role-based access and audit logs | [PLACEHOLDER-AUTO] |
| Privacy / GDPR notice | Show brief notice when email requested covering usage, retention and opt-out; link to full policy | [PLACEHOLDER-AUTO] |
| Responsive cross-browser UI | Accessible UI, keyboard navigable, responsive across desktop and mobile widths | [PLACEHOLDER-AUTO] |
| Initial user scenario: submit feedback | Anon user opens page, enters feedback, optionally adds email, submits, sees confirmation receipt | [PLACEHOLDER-AUTO] |
| Initial user scenario: admin review | Admin logs in, views list sorted by timestamp, filters, inspects feedback, may delete with confirm | [PLACEHOLDER-AUTO] |
| Success metric: submission reliability | Submission success rate >= 99.0 % over PT30D for production submissions; source: API-Service logs | [PLACEHOLDER-AUTO] |
| Success metric: UI performance | Median first-contentful-paint <= 2.0 s over PT30D measured in production RUM | [PLACEHOLDER-AUTO] |
| Identifier strategy | Use time-sortable UUID identifiers (time-ordered UUIDs) for feedback and admin actions | [PLACEHOLDER-AUTO] |
| Security baseline | Session cookie flags Secure/HttpOnly/SameSite, idle timeout PT30M, MFA for admin, retention P365D, audit logs | [PLACEHOLDER-AUTO] |
| Rate-limit for submissions | POST /feedback rate-limit 10 requests per IP per PT1M with exponential backoff; instrumented metric owner=SRE | [PLACEHOLDER-AUTO] |
| Session rotation policy | Issue session tokens with rotatedAt timestamp and TTL PT8H; renew on privileged action | [PLACEHOLDER-AUTO] |
| CSRF and anti-forgery | Admin flows require anti-CSRF token or SameSite=Strict for admin cookies; validate server-side | [PLACEHOLDER-AUTO] |
| Minimal DevSecOps checklist | Enforce TLS, secret rotation, dependency vuln scan, audit logging, least-privilege IAM entries | [PLACEHOLDER-AUTO] |
| Instrumentation owner for rate-limit metric | Owner: SRE team; metric source: API-Service request counters and throttles; alert on >1% throttle PT1H | [PLACEHOLDER-AUTO] |

### Artifact 1.1.1 final (mini 02) — Main Scenario Table with N modules

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Module ID | Module | Action 1 | Action 2 | Action 3 | Action 4 | Action n | Related Reqs | DevSecOps / Security |
| M-1 | Public Feedback Form | Open feedback page (responsive, accessible) | Enter feedback text | Optional email field + contact\_intent checkbox | Show GDPR/privacy notice and consent checkbox | Submit feedback with ISO-8601 UTC timestamp | FR-005 | POST /feedback rate-limit 10 req per IP per PT1M; metric owner=SRE; source=API-Service counters; 429+exp backoff; TLS; input validation; log throttle events |
| M-2 | Submission Processing | Validate feedback payload server-side | Sanitize content for display | Mark contact\_intent if email present; hash email before persist | Enqueue for storage and notify admin UI | Return success/failure to client with id | FR-022 | Server-side validation; XSS sanitization; hash email before persist; audit write on submit; retry idempotency for ingest |
| M-3 | Storage | Store feedback records in SQL RDBMS | Encrypt sensitive fields at rest (email, ip-hash) | Enforce least-privilege DB access | Backup cadence PT24H | Retention policy P365D enforcement and secure deletion | [PLACEHOLDER-AUTO] | Field-level encryption at rest; TLS in transit; DB access via least-privilege roles; access logs for reads/writes; retention enforcement job |
| M-4 | Admin UI | Admin login screen (responsive) | List feedback sorted by timestamp | Inspect feedback details | Delete feedback with confirm dialog | Log deletion actor ID and ISO-8601 timestamp | [PLACEHOLDER-AUTO] | RBAC for UI actions; CSRF tokens or SameSite=Strict cookies for admin flows; audit trail for deletes; session idle timeout PT30M |
| M-5 | Admin Authentication | Authenticate admins via OIDC IdP capability | Enforce session cookie flags Secure/HttpOnly/SameSite | Enforce MFA for admin accounts | Rotate sessions on privileged actions and record rotatedAt | Session TTL PT8H; renew on privileged action | FR-025 | OIDC IdP capability; session TTL PT8H; rotatedAt timestamp; idle timeout PT30M; MFA enforcement; secrets rotation policy |
| M-6 | Privacy & GDPR | Display email-use notice when email requested | Capture consent and contact-intent flags | Provide data access and deletion request process | Support verified data deletion and record event | Surface retention disclosure to admins | [PLACEHOLDER-AUTO] | Record consent and processing purpose in audit logs; encrypt email at rest; deletion audit event with actor\_id and timestamp; retention disclosure |

## Phase: FeasibilityStudy

### Artifact 1.1.1.1 final (mini 02) — Modules Components Description Table

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Requirement ID | Module | Component | Description | Interface | Potential Metrics | V&V focus | Related Reqs | DevSecOps / Security | Metric Owner |
| FR-001 | Public Feedback Form | Open feedback page (responsive) | Serve responsive feedback page across desktop and mobile | I-1: GET /feedback page | Median FCP <=2.0 s PT30D; percentile: p50; source=RUM | Cross-browser rendering, accessibility | FR-001 | TLS; CSP; input validation; RUM instrumentation; deploy pipeline scans | Frontend |
| FR-002 | Public Feedback Form | Enter feedback text | Input accepts freeform feedback text, client-side length limit 5000 chars | I-2: feedback textarea | Validation error rate <=0.5% PT30D; source=Frontend logs | Input validation, XSS sanitization | FR-002 | Client-side sanitization; server-side validation; dependency vuln scans | Frontend |
| FR-003 | Public Feedback Form | Optional email input | Optional email field; flag contact\_intent when present; store encrypted using field-level envelope encryption (KMS) | I-3: email input (optional) | % submissions with email PT30D (vanity) ; Encrypted-at-rest verified 100% PT30D; source=API-Service | Email optionality, encryption correctness, contact\_intent flag | FR-003 | Field-level envelope encryption (KMS); least-privilege DB access; consent capture; audit on access | Product |
| FR-004 | Public Feedback Form | Show GDPR/privacy notice and consent checkbox | Display brief email-use notice and consent capture when email requested | I-4: consent checkbox UI | Consent capture rate when email present 100% PT30D; source=Frontend | Consent recorded and auditable | FR-004 | Consent logged immutably; retention disclosure; privacy text audit | Product |
| FR-005 | Public Feedback Form | Submit feedback with ISO-8601 UTC timestamp | POST feedback; server assigns UUIDv7 id and ISO-8601 UTC timestamp | I-5: POST /feedback | Submission success rate >=99.0% PT30D; rate-limit throttles <=1% PT30D; source=API-Service logs | Id assignment, timestamp accuracy, rate-limit enforcement | FR-005 | Rate-limit 10 req/IP/PT1M; 429 on exceed; TLS; request logging; abuse alerts | SRE |
| FR-006 | Public Feedback Form | Show submission confirmation | Client shows success/failure message after submit | I-6: submission UI response | Median time-to-confirm <=1.5 s PT30D; source=RUM | User feedback and error handling | FR-006 | Consistent HTTP status codes; client telemetry for failures | Frontend |
| FR-007 | Submission Processing | Validate feedback payload server-side | Server-side schema validation and duplicate detection | I-7: POST /feedback validation | Rejected payload rate <=1.0% PT30D; source=API-Service | Schema validation, duplicate suppression | FR-007 | Server-side validation; input shaping; request schema tests | Backend |
| FR-008 | Submission Processing | Sanitize content for display | Sanitize stored content to prevent XSS on admin views | I-8: sanitize pipeline | XSS vulnerability count =0 (scan) PT30D; source=Security scans | Sanitizer test coverage | FR-008 | Output encoding; sanitizer library pinned; security scans | Security |
| FR-009 | Submission Processing | Mark contact\_intent if email present | Set contact\_intent boolean when optional email provided | I-9: contact\_intent flag in payload | Flag consistency 100% PT30D (audit); source=DB audit | Flag persistence, audit logs | FR-009 | Audit log on flag set; encrypted email field access controls | Backend |
| FR-010 | Submission Processing | Encrypt email before persist | Apply field-level envelope encryption (KMS) to emails prior to storage | I-10: crypto module | Encrypted-at-rest verified 100% (audit) PT30D; source=Security | Encryption key usage, KMS integration tests | FR-010 | KMS policy; key rotation; access limited to service role; decrypt audits | Security |
| FR-011 | Submission Processing | Persist record with time-sortable UUID | Persist feedback record with UUIDv7 primary id | I-11: DB insert API | Insert success rate >=99.0% PT30D; source=DB metrics | ID format, DB ACID write tests | FR-011 | DB least-privilege role; input sanitization; write-audit | Storage |
| FR-012 | Submission Processing | Return success/failure to client | Return clear HTTP status and error codes; retry-safe | I-12: POST /feedback response codes | Proper HTTP success code on valid submit 100% PT30D; source=API-Service | Status code correctness, idempotency | FR-012 | Idempotency tokens where needed; structured error codes | Backend |
| FR-013 | Storage | Store feedback records in SQL RDBMS | Persist feedback rows in SQL RDBMS with least-privilege access | I-13: DB schema feedback table | DB write latency p95 <=200 ms PT30D; source=DB metrics | Schema correctness, access controls | FR-013 | DB roles; TLS to DB; audit logging for writes | Storage |
| FR-014 | Storage | Encrypt sensitive fields at rest | Encrypt emails and credentials at rest using field-level envelope encryption | I-14: encryption-at-rest policy | Encrypted fields coverage 100% (audit) PT30D; source=Security audit | Encryption verification, key rotation tests | FR-014 | KMS keys; key rotation schedule; encryption audit | Security |
| FR-015 | Storage | Apply least-privilege DB access | DB accounts scoped by role; app uses minimal privileges | I-15: DB access roles | Role violation incidents =0 PT90D; source=IAM audit | Access control audits | FR-015 | IAM role reviews; automated permission drift alerts | InfraSec |
| FR-016 | Storage | Retention policy P365D enforcement | Automated deletion of records older than P365D unless exempt | I-16: retention job | Retention enforcement rate 100% monthly; source=Retention job logs | Retention job correctness, delete logs | FR-016 | Automated deletion job; deletion audit entries | Storage |
| FR-017 | Storage | Audit-write deletion events | Log deletion actor id and ISO-8601 timestamp immutably | I-17: deletion audit log | Deletion audit entries 100% per delete; source=Audit store | Audit integrity and append-only writes | FR-017 | Append-only audit store; retention for audit logs | Compliance |
| FR-018 | Storage | Periodic backups of dataset | Perform regular backups with retention and restore tests | I-18: backup schedule | Daily backup success rate >=99.0% PT30D; source=Backup logs | Backup restore verification | FR-018 | Encrypted backups; restore drills; access controls | Storage |
| FR-019 | Admin UI | Admin login screen (responsive) | Responsive admin login with session handling | I-19: GET/POST /admin/login | Median admin login time <=2.0 s PT30D; source=RUM | Auth flow and UI accessibility | FR-019 | OIDC flows; MFA prompt; CSRF protection on login forms; TLS | AdminUX |
| FR-020 | Admin UI | List feedback sorted by timestamp | Admin list view sorted newest-first using UUIDv7 ordering | I-20: GET /admin/feedback?sort=time | List latency p95 <=300 ms PT30D; source=API-Service | Sorting correctness, pagination | FR-020 | RBAC checks; query rate-limits; audit read logs; CSRF tokens for admin actions | AdminUX |
| FR-021 | Admin UI | View full feedback details | Detail view shows text, timestamp, contact\_intent, encrypted email marker | I-21: GET /admin/feedback/{id} | Detail retrieval success 100% PT30D; source=API-Service | Decryption/display rules, masking | FR-021 | Decryption via authorized role; masking for emails; access audit; CSRF protection | AdminUX |
| FR-022 | Admin UI | Delete feedback with confirm dialog | Admin delete requires explicit confirm and second-step verification | I-22: DELETE /admin/feedback/{id} | Confirmed-deletes ratio >=99% PT30D; source=Audit logs | Confirm dialog enforcement, race conditions | FR-022 | DeletionNonce TTL PT15M; audit log actor id; RBAC and CSRF tokens; confirmation UI | AdminOps |
| FR-023 | Admin UI | Log deletion actor ID and ISO-8601 timestamp | Record actor id and timestamp in audit log on delete | I-23: deletion audit entry | Audit entry present 100% per deletion; source=Audit store | Audit consistency and tamper-evidence | FR-023 | Immutable audit store; retention and access controls | Compliance |
| FR-024 | Admin UI | Search and export feedback list | Admin can search and export CSV with permission checks | I-24: GET /admin/feedback?query & export | Export success rate >=99.0% PT30D; source=API-Service | Permission enforcement, export data masking | FR-024 | Export masking; RBAC; export job audit; CSRF tokens on export actions | AdminUX |
| FR-025 | Admin Authentication | Authenticate admins via OIDC IdP capability | Admin auth via OIDC-capable IdP; support MFA | I-25: OIDC flow endpoints | Admin auth failure rate <=1.0% PT30D; source=Auth logs | OIDC flow conformance, token validation | FR-025 | OIDC capability; token validation; MFA enforcement; secret rotation | Auth |
| FR-026 | Admin Authentication | Enforce session cookie flags Secure/HttpOnly/SameSite | Set Secure, HttpOnly, SameSite on admin session cookies | I-26: session cookie policy | Cookies with flags 100% (audit) PT30D; source=Auth audit | Cookie attribute verification | FR-026 | Cookie flags enforced; SameSite=Strict for admin; cookie audits | Auth |
| FR-027 | Admin Authentication | Idle session timeout PT30M | Idle admin sessions expire after PT30M inactivity | I-27: session timeout policy | Idle session expiry enforcement 100% daily audit; source=Session store | Timeout enforcement | FR-027 | Session store TTL PT30M; inactivity checks; session rotation | Auth |
| FR-028 | Admin Authentication | Enforce MFA for admin accounts | Require MFA for all admin logins | I-28: MFA enrollment and challenge | MFA enabled rate 100% for admin accounts; source=Auth | MFA enforcement tests | FR-028 | MFA challenge on auth; backup codes; enrollment audit | Auth |
| FR-029 | Admin Authentication | Role-based access control for UI actions | RBAC for admin UI actions and exports | I-29: RBAC policy checks | Unauthorized access attempts =0 PT90D; source=Auth audit | RBAC policy correctness | FR-029 | RBAC enforcement; policy tests; permission audit logs | Auth |
| FR-030 | Admin Authentication | Audit admin login and privilege changes | Log admin login events and role changes with actor id and timestamp | I-30: admin audit log | Admin audit entries 100% per event; source=Audit store | Audit completeness and integrity | FR-030 | Append-only admin audit; alert on suspicious changes | Compliance |
| FR-031 | Privacy & GDPR | Display email-use notice when email requested | Show notice explaining email use, retention and opt-out | I-31: privacy notice UI | Notice shown on email field 100% (UI test) PT30D; source=UI tests | Notice visibility and content accuracy | FR-031 | Privacy text versioning; UI tests; consent link to policy | Product |
| FR-032 | Privacy & GDPR | Capture consent and contact-intent flags | Store consent and contact\_intent flags with timestamp and actor id | I-32: consent storage API | Consent recorded 100% when checkbox checked; source=DB audit | Consent auditability | FR-032 | Immutable consent records; linkage to submissions; audit | Product |
| FR-033 | Privacy & GDPR | Provide data access and deletion request process | Admin process and API to fulfill access/deletion requests | I-33: data subject request endpoints | DSR fulfillment time <=30 days per request; source=Compliance logs | Request verification and completion | FR-033 | Verified request workflow; audit trail; auth for DSRs | Compliance |
| FR-034 | Privacy & GDPR | Support data deletion upon verified request | Delete or anonymize records on verified deletion requests, log action | I-34: verified delete workflow | Verified deletions completed within 30 days; source=Audit store | Deletion verification and audit | FR-034 | DeletionNonce verification; deletion audit entries | Compliance |
| FR-035 | Privacy & GDPR | Expose retention period to admins | Display retention policy and next-delete dates in admin UI | I-35: retention info UI | Retention info accuracy 100% (audit) PT30D; source=Storage | Retention metadata correctness | FR-035 | Retention metadata generation; UI access controls | Storage |
| FR-036 | Privacy & GDPR | Record consent and processing purpose in audit logs | Append consent and processing purpose to audit trail immutably | I-36: consent audit entries | Consent audit entries 100% per consent; source=Audit store | Audit linkage and immutability | FR-036 | Append-only audit; retention and access control | Compliance |
| FR-037 | Admin Authentication | Session rotation policy and rotatedAt field | Rotate session tokens on privilege change and record rotatedAt ISO-8601 | I-27b: session rotation endpoint /session/rotate | Session rotation performed 100% on privilege change; source=Auth logs | Rotation enforcement, rotatedAt timestamp correctness | FR-037 | Rotate tokens on privilege change; record rotatedAt; rotation tests | Auth |
| FR-038 | Submission Processing | DeletionNonce TTL verification | Verify deletionNonce TTL before accepting admin delete requests | I-22b: deletionNonce verification in DELETE /admin/feedback/{id} | Rejected deletes due to expired nonce <=0% PT30D; source=API-Service | Nonce TTL correctness, rejection behavior | FR-038 | DeletionNonce TTL PT15M; verify server-side; audit rejection events; CSRF tokens for admin delete | AdminOps |

### Artifact 1.1.2 final (mini 02) — Domain Context Table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Category | Details | Quality Attributes | Potential Metrics | DevSecOps / Security | Related Reqs | Metric Owner |
| Admin Access & Auth | Admin login via OIDC-capable IdP; RBAC and MFA required | Confidentiality, Least-Privilege, Availability | MFA enabled rate =100 % PT30D; admin auth failure rate <=1.0 % PT30D; source=Auth logs | OIDC capability; MFA enforcement; Secure/HttpOnly/SameSite=Strict; CSRF tokens for admin flows; secret rotation | FR-025, FR-026, FR-028, FR-029, FR-030 | Auth |
| Backup & Restore | Periodic backups with retention and restore verification | Durability, Recoverability, Integrity | Daily backup success rate >=99.0 % PT30D; restore drill success >=95 % PT90D; source=Backup logs | Encrypted backups; access-limited key material; restore drills; backup retention policy | FR-018 | Storage |
| Feedback Submission | Public POST /feedback accepts freeform text; server assigns UUIDv7 id and ISO-8601 timestamp | Reliability, Availability, Input Validation, Abuse-resistance | Submission success rate >=99.0 % PT30D; rate-limit throttle rate <=1 % PT30D; source=API-Service logs | Server-side schema validation; XSS sanitization; TLS; rate-limit enforcement; request logging; vuln scans | FR-001, FR-005, FR-007, FR-008 | SRE |
| Identifier Strategy | Time-sortable UUIDv7 for feedback and admin actions | Ordering, Uniqueness, Traceability | UUID collision rate =0 observed PT90D; source=DB/ID-gen logs | Server-side UUIDv7 generation; include id in audit entries; monitor collisions | FR-005, FR-011 | Storage |
| Monitoring & Metrics | Collect service, DB and auth metrics; alert on key SLO breaches | Observability, Operability, SLA compliance | Alert when submission success rate <99.0 % over PT30D; dashboard RBAC audit PT90D; source=Monitoring | Secure metrics ingestion; RBAC for dashboards; metrics retention PT90D; pipeline scans | FR-012, FR-030 | SRE |
| Optional Email | Optional email field; store only when provided; mark contact\_intent | Privacy, Data Minimization, Integrity | % submissions with email PT30D (vanity); encrypted-at-rest verified 100 % PT30D; source=API-Service | Deterministic field-level envelope encryption for emails; TLS in transit; access audit; mask in exports | FR-003, FR-010, FR-009 | Security |
| Privacy & Consent | Show email-use notice and capture consent when email requested | Privacy, Legal Compliance, Transparency | Consent recorded =100 % when checkbox checked PT30D; source=DB audit | Store consent timestamp and purpose immutably; expose opt-out; consent audit trails | FR-004, FR-031, FR-032, FR-036 | Product |
| Retention & Deletion | Automated retention P365D; support verified deletion requests and retain deletion audit | Compliance, Auditability, Recoverability | Retention enforcement rate =100 % monthly; verified deletion completion <=30 days per request; source=Retention logs | Retention job with immutable deletion audit entries; deletionNonce TTL PT15M; RBAC for delete actions | FR-016, FR-017, FR-033, FR-034 | Storage |
| Search & Export | Admin search and CSV export with permission checks and masking | Correctness, Performance, Data Minimization | Export success rate >=99.0 % PT30D; masked fields present 100 % PT30D; source=API-Service | Permission enforcement; mask encrypted emails in exports; audit export events; CSRF tokens on export actions | FR-024 | AdminUX |
| Storage & Persistence | Persist feedback in SQL RDBMS with least-privilege DB accounts | Durability, Consistency, Performance | DB write latency p95 <=200 ms PT30D; insert success rate >=99.0 % PT30D; source=DB metrics | Encrypt sensitive fields at rest via envelope encryption; scoped DB roles; daily backups; TLS to DB | FR-013, FR-014, FR-015, FR-018 | Storage |
| Admin UI: Feedback Management | List and detail views sorted newest-first; delete requires confirm and deletionNonce verification | Usability, Performance, Safety, Tamper-resistance | List latency p95 <=300 ms PT30D; confirmed-deletes ratio >=99 % PT30D; source=API-Service and Audit store | Confirm dialog; server verifies deletionNonce TTL PT15M; log deletion actor id and ISO-8601 timestamp immutably; CSRF tokens on admin forms | FR-020, FR-021, FR-022, FR-023, FR-038 | AdminOps |
| Submission Processing | Server-side schema validation, duplicate detection, sanitization, idempotent responses | Correctness, Safety, Idempotency | Rejected payload rate <=1.0 % PT30D; XSS vulnerability count =0 PT30D; source=Security scans | Sanitize content for admin views; duplicate suppression; idempotency-safe error codes; sanitizer library pinning | FR-007, FR-008, FR-009, FR-012 | Backend |
| Session Rotation | Rotate session tokens on privilege change and record rotatedAt ISO-8601; rotation TTL PT8H | Security, Traceability | Session rotation performed =100 % on privilege change PT30D; rotatedAt present for rotated sessions PT30D; source=Auth logs | Rotate tokens on privilege change; rotation endpoint; session TTL PT8H; audit rotation events | FR-037 | Auth |