SPR MARKET-SOUNDING PACKAGE

Annex C
Data Provider Body Interface

High-Level, Outcome-Based Requirements

Technology-neutral market sounding | Non-binding | Vendor solution approach requested

Document field	Value
Version	2.0
Related document	SPR Market-Sounding Master Document
Issuing organization	Information Systems Agency of Armenia (ISAA)

Contents

How to read this annex

This annex intentionally defines business outcomes and non-negotiable boundaries rather than prescribing screens, form layouts, detailed workflows, API schemas or technical components. Vendors are expected to propose the implementation approach and identify assumptions, dependencies and alternatives.

1. Purpose and document status

This annex describes the required outcomes for a role-based interface and integration capability through which authorized data-provider bodies may submit or update State Population Register (SPR) data within their legal authority. It supports the market-sounding exercise and is not a final solution design or procurement specification.

- **Technology-neutral.** No specific low-code platform, product or architecture is mandatory for this annex.
- **Self-contained.** Vendors should be able to prepare an indicative response without receiving internal source documents.
- **Outcome-based.** The annex defines what the capability must achieve and the boundaries it must respect.
- **Non-binding.** The market-sounding exercise does not constitute a tender or commitment to procure.

2. Business objective

The objective is to give authorized government bodies a controlled way to provide SPR-related data while preserving legal data ownership, security, traceability and the authority of SPR Core. The capability should accommodate both human users and approved provider information systems.

Core business outcome

Each provider body must be able to submit only the data categories assigned to it, receive a clear processing result, correct or clarify returned submissions, and retain full traceability - without directly editing the SPR database.

3. Scope and boundaries

3.1 Mandatory baseline scope

- Secure access for authorized provider-body users and approved provider systems.
- Enforcement of provider organization, role and permitted data categories.
- Creation and submission of provider data submissions or updates.
- Basic validation, completeness checks and clear feedback before submission.
- Attachment or linkage of supporting evidence where required.
- Support for correction, clarification and resubmission.
- Provider-facing status and result tracking.

- Support for both case-based processing and an approved direct route to SPR Core.
- Exception handling when automated processing cannot complete successfully.
- Full audit, monitoring and administrative configuration.

3.2 Separately priced optional scope

- OCR or automatic extraction from provider-uploaded evidence documents, where proposed.
- Other optional functionality explicitly identified by the vendor and excluded from the baseline price.

3.3 Out of scope

- Document or certificate issuance.
- General government correspondence or generic request management.
- Unrestricted searching or browsing of the population register.
- Direct editing of the SPR database.
- Creation, selection or modification of a PSN outside SPR Core.
- Full automation of each provider body's internal business processes.

4. Users and required outcomes

User / channel	Required outcome
Provider-body user	Submit and follow data within the organization's approved authority; respond to correction or clarification requests.
Provider-body supervisor	Where required, oversee the organization's submissions, workload and internal approval responsibilities.
Provider information system	Submit approved data through a secure system-to-system mechanism and receive machine-readable outcomes.
Central administrator	Configure provider organizations, roles, data categories and other approved parameters without unrestricted access to business data.
Auditor / operational reviewer	Review authorized audit and transaction information without modification rights.

5. High-level capability areas

Capability area	Required business outcome
Access and organization control	Identify the user or system, resolve the provider organization and enforce the scope of permitted actions and data.
Data submission	Allow an authorized provider to prepare and submit data or updates within its approved categories.
Validation and quality	Check completeness, basic consistency and authority before accepting a submission; provide understandable correction information.
Evidence support	Allow evidence to be attached or referenced where required, while keeping actual files outside SPR Core.
Correction and resubmission	Allow returned submissions to be clarified, corrected and resubmitted without losing prior history.
Status and communication	Show the provider the permitted status, required actions and final result.

Capability area	Required business outcome
Routing and exception handling	Send transactions through the approved route and create or route exceptions for human review when necessary.
Administration and onboarding	Support controlled onboarding of provider organizations, users, permissions and approved data categories.
Reporting and audit	Provide organization-appropriate monitoring and full traceability of significant actions and outcomes.

Not prescribed at market-sounding stage

Exact screens, form layouts, field catalogues, workflow steps, status lists, routing algorithms, API schemas and technical products are not fixed by this annex. Vendors should propose a coherent approach and explain how it meets the required outcomes.

6. Processing routes and logical context

The solution must support different submission routes because provider bodies have different levels of technical maturity and different legal or operational requirements.

Route	High-level use
Provider UI route	For authorized users who enter or submit data through the role-based interface, including organizations without a mature source-system integration.
System-to-system route	For approved provider information systems that submit data through a secure integration mechanism.
Case-based route	Used where human review, evidence assessment, approval, clarification, conflict resolution or another case-management step is required.
Approved direct route	Used only for explicitly authorized providers, data categories and transactions where required validations pass and no human-review condition applies.
Exception route	Used when validation fails, a duplicate or conflict is detected, SPR Core rejects a transaction, evidence requires judgment, or another mandatory review condition applies.

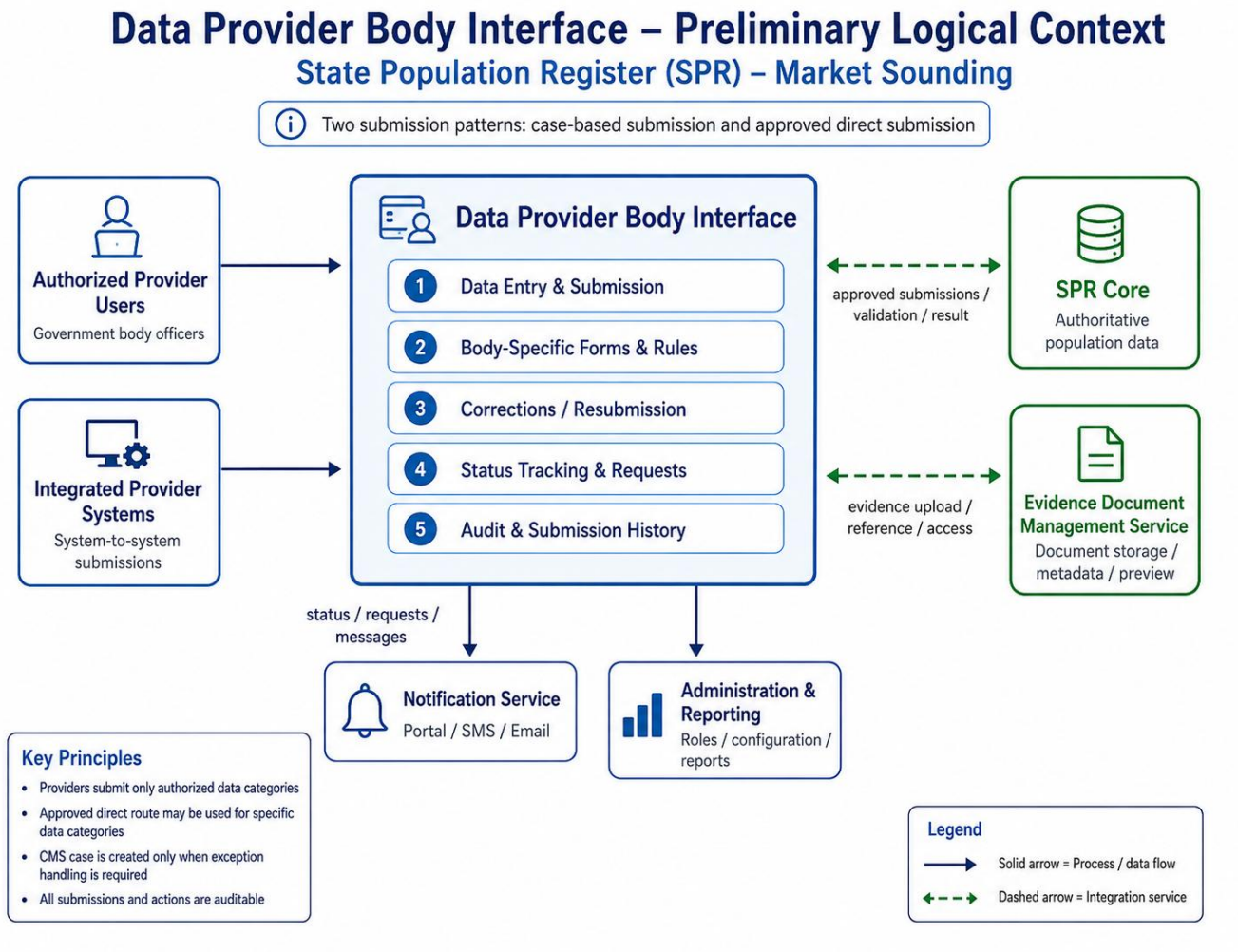

Figure 1. Preliminary logical context. The diagram is illustrative and does not prescribe a final technical architecture.

6.1 Non-negotiable route principles

- SPR Core remains the authoritative source of truth and performs the final authoritative update.
- Provider users and systems may act only within approved legal authority and data categories.
- No provider route may bypass SPR Core validation rules or directly edit the SPR database.
- Successful direct transactions must remain searchable and auditable even where no full CMS case is created.
- Exception conditions must be traceable and routed to the appropriate review or correction process.

7. Shared requirements

Area	High-level expectation
Security and privacy	Role- and organization-based access, least privilege, protection of personal data, secure human and machine authentication, and secure transmission.
Audit and traceability	Record significant user, system, submission, routing, evidence-access and outcome events in a protected audit history.
Usability and accessibility	Provide clear and understandable interactions for provider users and support approved government design and accessibility standards.
Configurability	Allow approved organizations, roles, data categories, rules and provider-facing messages to be configured without major redevelopment.

Area	High-level expectation
Reliability	Prevent unintended duplicate processing, support clear error handling, and provide recovery or reconciliation for interrupted transactions.
Interoperability	Use approved government integration mechanisms and allow vendor-proposed patterns that meet security, traceability and maintainability requirements.
Maintainability	Avoid unnecessary provider-specific duplication; support repeatable onboarding and controlled change management.

8. Integrations and dependencies

System / service	Purpose
SPR Core	Final validation, authoritative registration/update, PSN generation where applicable, and transaction result.
CMS / Back Office	Case-based review, approval, clarification and exception handling.
Evidence Document Management Service	Secure document storage, metadata, access and references.
IAM / SSO	Authentication, organization and role context for human users.
Notification capability	Provider-facing alerts and required-action notifications where included in the solution.
Audit / monitoring capability	Security, business and integration traceability.
Provider information systems	Approved system-to-system submission and outcome exchange.

Integration detail

Detailed API contracts, protocols, credentials, message schemas, retry rules and provider-specific connectors will be confirmed during analysis and design. Vendors must state their assumptions and propose a secure, maintainable integration approach.

9. Sizing and assumptions

Parameter	Current market-sounding baseline
Registered persons	300,000+
Provider organizations	10-30 organizations.
Back Office users	1,000+ programme baseline.
Concurrent users	200 programme-wide concurrent users.
Cases / transactions	100,000+ cases per year programme baseline. Provider-specific transaction volumes are not yet confirmed.
Growth	The proposed solution should scale beyond the baseline without major architectural redesign.

Where detailed provider-user, peak-load, document, notification or connector volumes are unknown, vendors shall provide reasonable assumptions and explain the impact on sizing, effort, cost and timeline.

10. Preliminary MVP and full implementation

10.1 Preliminary MVP

The vendor should propose a practical MVP that demonstrates an end-to-end provider submission capability while preserving the non-negotiable boundaries in this annex. The proposed MVP should cover, at minimum:

- authorized provider access and organization segregation;
- controlled submission within approved data categories;
- validation and understandable feedback;
- evidence attachment or reference where required;
- provider-facing status and correction/resubmission;
- at least one complete processing route with end-to-end traceability;
- audit and basic administration.

10.2 Full implementation

The full implementation should support repeatable onboarding of the expected provider organizations, both UI and approved system-to-system submissions, case-based and approved direct routes, exception processing, reporting, operational monitoring and scalable configuration.

11. Design-stage decisions

The following details are intentionally not finalized for market sounding. The required capability is part of the baseline; the exact configuration will be confirmed during analysis and design.

Decision area	To be confirmed
Provider catalogue	Final organizations, hierarchy, contacts, onboarding sequence and user numbers.
Data ownership and submission matrix	Authorized data categories, legal owner, submitting provider and permitted route.
Provider-facing data capture	Exact submission types, fields, mandatory data, reference values and help text.
Processing route	Case-based or approved direct route for each provider, data category and transaction.
Human review and approval	When provider or central review is required and who may approve.
Evidence requirements	Required document types, metadata, verification responsibility, visibility and retention rules.
Status and messages	Provider-facing statuses, correction reasons and disclosure limits.
Integration detail	Provider systems, protocols, API readiness, environments, certificates and connector sequence.
SLA and escalation	Provider response deadlines, reminders, escalation and pause rules.
Operational model	Support responsibilities, monitoring, reconciliation and incident handling.

12. Vendor response requirements

The vendor response should be concise but sufficiently detailed to support market comparison. Vendors should provide:

Response area	Requested information

Response area	Requested information
Understanding of need	Summary of the business problem, required outcomes and non-negotiable boundaries.
Proposed solution approach	High-level architecture, user experience, configuration approach and any reusable products or components.
Submission routes	Proposed treatment of UI, system-to-system, case-based, direct and exception routes.
Integration approach	Assumptions for SPR Core, CMS, evidence, IAM, notifications, audit and provider systems.
Security and audit	Approach to organization segregation, authorization, machine identities, personal-data protection and traceability.
MVP proposal	Recommended MVP scope, timeline, team, dependencies and limitations.
Full implementation	Indicative rollout and onboarding approach for 10-30 provider organizations.
Sizing assumptions	Provider users, peak load, transactions, evidence, notifications and storage assumptions.
Effort, timeline and cost	Indicative person-days, calendar duration, team composition and price in AMD with VAT treatment.
Warranty and support	Separate 12-month warranty/support scope and indicative price.
Risks and dependencies	Key assumptions, dependencies, unresolved questions and recommended decisions.
Deviations and alternatives	Any material deviation from the annex and proposed alternative with rationale.

Market-sounding principle

Vendors are not expected to reproduce a predefined solution. They are expected to demonstrate that their proposed approach can achieve the required business outcomes, respect the programme boundaries and be implemented at an indicative cost and timeline.

End of Annex C