SPR MARKET-SOUNDING PACKAGE

Annex D

Evidence Document Management Service

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
Module	Evidence Document Management Service
Issuing organization	Information Systems Agency of Armenia (ISAA)

Contents

How to read this annex / This annex intentionally defines required business outcomes and non-negotiable boundaries. It does not prescribe a storage product, screen layout, exact metadata schema, document-status catalogue, API contract, workflow design or infrastructure topology. Vendors are expected to propose a coherent, secure and supportable approach.

1. Purpose and document status

This annex describes the required outcomes for the Evidence Document Management Service supporting SPR cases and data submissions. It supports market sounding and is not a final solution design or procurement specification.

- **Technology-neutral.** No specific storage product, document-management platform, cloud service or implementation 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 service 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 provide a shared, secure and traceable capability for receiving, storing, classifying, accessing, reviewing and linking evidence used in SPR applications, cases and provider submissions, while keeping actual document files outside SPR Core.

Core business outcome / Authorized users and systems can provide and use evidence for an SPR case or submission, and the evidence remains securely stored, correctly linked and fully traceable. SPR Core receives only approved references or metadata, not the actual file.

3. Scope and boundaries

3.1 Mandatory baseline scope

- Evidence intake from the SPR Portal, CMS / Back Office, Data Provider Body Interface and approved integrated systems.
- Secure storage of actual evidence files outside SPR Core.
- Unique identification, classification and metadata sufficient to find, understand and govern each evidence item.
- Controlled preview, retrieval and permitted download or temporary access.
- Linkage to the relevant case, application, provider submission and approved person or SPR Core references.
- Support for review, verification status, rejection or acceptance outcomes and additional evidence.
- Lifecycle, retention, replacement/addition history and lawful deletion exceptions.
- Role-, organization-, task-, case- and purpose-aware access control.
- Audit, operational monitoring, reporting and controlled administration.
- Secure integration and reference exchange with the other SPR solution modules and SPR Core.

3.2 Separately priced optional scope

- OCR or automatic extraction of data from evidence documents.
- Automated comparison of extracted document content with submitted application or case data.
- Other optional capabilities explicitly proposed by the vendor and excluded from the baseline price.

3.3 Out of scope

- A general government-wide document or records-management platform.
- Document or certificate issuance functionality.
- Storage of actual evidence files in the SPR Core database.
- Direct alteration of authoritative SPR data by the evidence service.
- Creation of legal retention, archival or disclosure policy; the service must implement approved policy.
- Construction of external identity, notification, audit or provider systems, except for required integrations.

4. Users and required outcomes

User / source	Required outcome
SPR Subject through the Portal	Provide required evidence, view permitted evidence and respond to additional-evidence requests in the subject's own context.
Back Office officer / reviewer	Access case-relevant evidence, review or verify it, record outcomes and preserve decision traceability.
Data Provider Body user	Provide evidence within the organization's authorized data and submission context and access only permitted items.
Approved integrated system	Submit evidence or references through approved machine-to-machine mechanisms with identity, authorization and traceability.
Administrator / support user	Manage approved configuration and technical operations without automatic unrestricted access to evidence content.
Auditor / security reviewer	Review authorized evidence-access and lifecycle history without modifying business records.

5. High-level capability areas

Capability area	Required business outcome
Evidence intake	Accept evidence from approved users and systems in the correct case or submission context and return a reliable reference.
Storage and integrity	Protect files and associated information from loss, corruption, malware, unauthorized alteration and unauthorized disclosure.
Classification and metadata	Maintain sufficient configurable information to identify, govern, search and interpret evidence without imposing one universal metadata model on every document type.
Access and preview	Allow authorized users to securely view or retrieve evidence while enforcing role, organization, task, sensitivity and legal-basis restrictions.
Review and verification	Support the responsible user or body in recording whether evidence has been reviewed, accepted, rejected or requires follow-up.
Linkage and references	Preserve clear relationships between evidence, cases, applications, provider submissions, decisions and approved person/Core references.
Lifecycle and retention	Preserve submitted and processed evidence according to approved rules, including additional/replaced evidence and controlled exceptions.
Audit and oversight	Provide traceable evidence history, access history, operational monitoring, reporting and controlled configuration.
Integration	Exchange document references, metadata, status and approved access mechanisms with the relevant SPR modules and services.

Not prescribed at market-sounding stage / The Customer is not fixing a storage product, repository technology, screen design, document-status catalogue, exact metadata fields, preview/download mechanism, API schema or infrastructure topology at this stage. Vendors should propose an approach and clearly explain assumptions, dependencies and recurring costs.

6. Service model and logical context

The Evidence Document Management Service is a shared capability used by the SPR Portal, CMS / Back Office, the Data Provider Body Interface and approved integrations. The diagram below is illustrative and does not prescribe a final technical architecture.

Processing principle	High-level treatment
Files outside SPR Core	Actual evidence files are stored in the evidence service or its approved secure storage; SPR Core receives approved references or metadata only.
Evidence has context	Each evidence item is associated with at least one approved application, case or data submission and retains its source and uploader context.
Submitted history is preserved	After final submission, evidence is not silently overwritten. Additional or corrected evidence is added in a way that preserves prior history.
Access is purpose-limited	Access depends on role, organization, assigned work, case/submission context, sensitivity, legal basis and visibility rules.
Verification is controlled	Manual review is the baseline where evidence judgment is required; optional OCR or extraction does not replace approved decision responsibility.
All material actions are traceable	Upload, access, review, linkage, lifecycle and administrative actions are auditable.

6.1 Non-negotiable service principles

- The Evidence Document Management Service is not the authoritative source for population data.
- Actual evidence files must not be stored in the SPR Core database.
- The service must not directly edit authoritative SPR data or create a PSN.
- Evidence access must follow least privilege and approved legal/business purpose.
- Evidence must remain linked to the relevant case or submission and remain traceable through its lifecycle.
- Mandatory configurable capability remains baseline even where exact metadata, retention or access rules are finalized during design.

6.2 Preliminary logical context

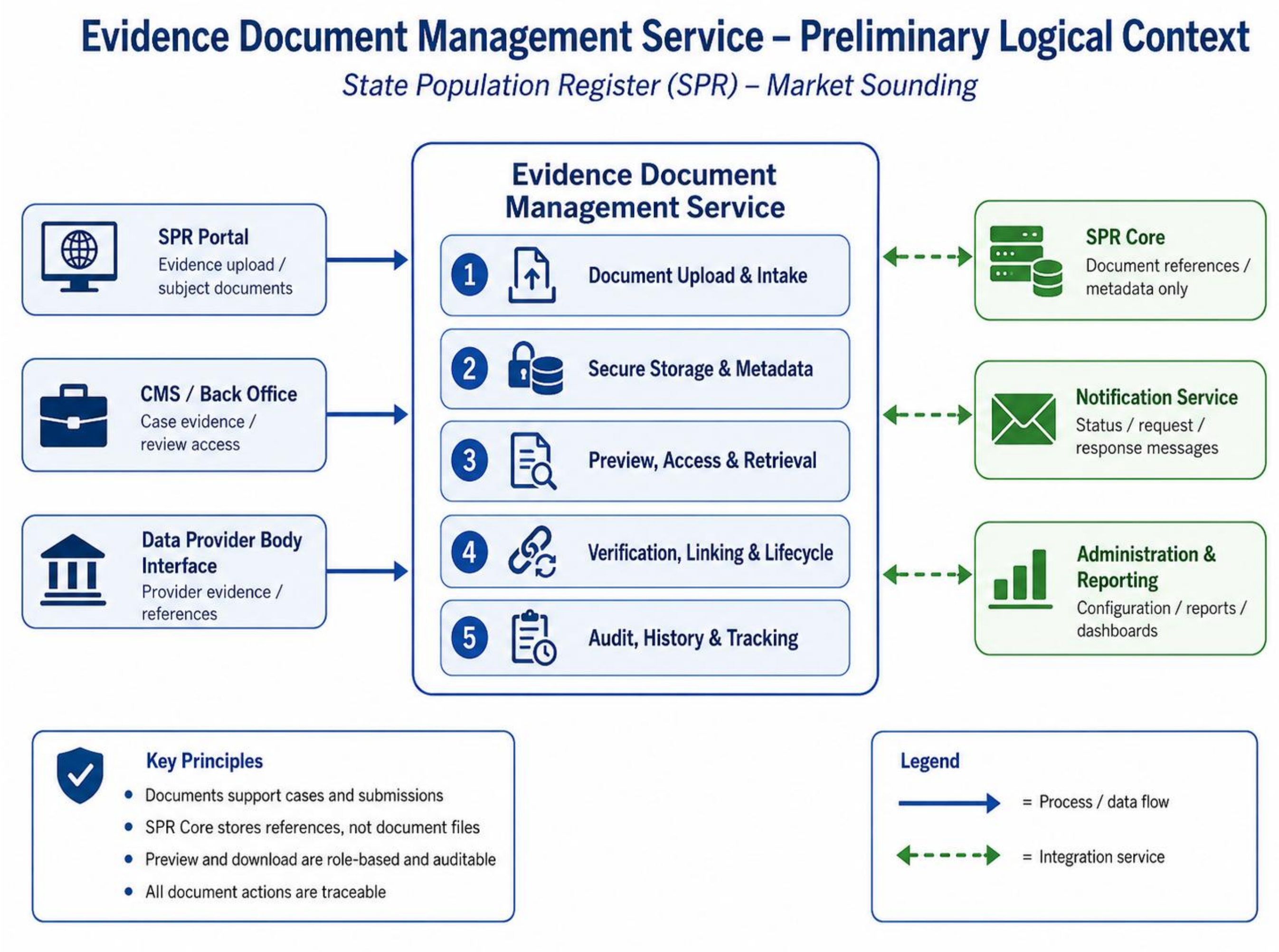

Figure 1. Preliminary logical context. The diagram shows the main users of the shared evidence capability and its relationship with SPR Core and shared services.

Interpretation / The diagram describes responsibility boundaries and information flows only. It does not define the final storage technology, deployment topology, user interface, API design or document workflow.

7. Shared requirements

Area	High-level expectation
Security and privacy	Role-, organization-, task-, case-, sensitivity- and purpose-aware access; least privilege; encryption and protection against data leakage.
Integrity and durability	Reliable storage, integrity checking, backup/recovery and protection against unauthorized alteration or loss.
Audit and accountability	Traceable actor/system, action, evidence item, context, time, reason and outcome for significant activity.
Usability	Practical evidence upload, review, preview and retrieval for subjects, officers and provider users within their permitted contexts.
Configurability	Document types, metadata, evidence requirements, statuses, access, visibility, size/format limits and retention exceptions should be configurable where appropriate.
Reliability and recoverability	Controlled upload failures, scan failures, retries, service recovery and prevention of duplicate or orphaned evidence.
Maintainability	Documented interfaces, supportable components, controlled releases and clear operational responsibilities.
Observability	Monitoring of availability, capacity, upload/preview failures, security scanning, access denials and integration errors with actionable alerts.
Data portability and exit	The vendor should explain how documents, metadata, configuration and audit history can be transferred or exported under an approved transition.

8. Integrations and dependencies

System / service	Purpose
SPR Portal	Subject evidence submission, additional evidence, permitted preview and subject-visible status.
CMS / Back Office	Case linkage, evidence review, verification status, additional-evidence handling and decision traceability.
Data Provider Body Interface / systems	Provider evidence submission, linkage, correction/resubmission and organization-scoped access.
SPR Core	Receive approved document references or metadata associated with registration or update transactions; not actual files.
IAM / SSO	User/system identity, role and organization context for access control.
Audit / monitoring platform	Security events, service health, capacity, alerts and centralized traceability where applicable.
Approved integrated systems	System-to-system evidence submission or reference exchange where authorized.

Integration detail / Detailed API contracts, preview/download mechanisms, credentials, message patterns, error handling, idempotency, retry and reconciliation rules are design-stage decisions. Vendors must state assumptions and propose a secure, supportable approach.

9. Sizing and assumptions

Parameter	Current market-sounding baseline / treatment
Registered persons	300,000+ programme population baseline.
Back Office users	1,000+.
Provider organizations	10-30.
Concurrent users	200 across the integrated solution.
Cases per year	100,000+ programme baseline.
Documents and storage growth	Not yet confirmed; vendor must propose and justify assumptions.
Peak upload / preview / API volumes	Not yet confirmed; vendor must state assumptions and capacity impact.
Retention horizon	Exact periods and exceptions require legal/business confirmation; vendor must explain storage impact under stated assumptions.

Sizing instruction / Unknown document counts, average sizes, peak loads, retention periods and annual storage growth shall not be invented. Vendors shall provide transparent assumptions, identify cost and capacity drivers, and explain how the service scales after the design-stage sizing model is approved.

10. Preliminary MVP and full implementation

10.1 Preliminary MVP

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

- evidence intake from the SPR Portal, CMS / Back Office and Data Provider Body Interface;
- unique document reference, basic configurable metadata and secure storage outside SPR Core;
- file validation, integrity and malware/security handling;
- controlled preview/access and role-based authorization;
- linkage to a representative case or provider submission;
- manual review/verification outcome and additional-evidence handling;
- reference/metadata transfer to SPR Core for a representative transaction;
- audit, basic administration, operational monitoring and a credible storage/capacity model.

10.2 Full implementation

The full implementation should support the approved evidence and document catalogue, all agreed upload sources, configurable metadata and access rules, final lifecycle and retention rules, required integrations, operational reporting, monitoring, recovery and scalable capacity for the confirmed programme baseline.

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
Storage implementation	Whether to build a dedicated service or integrate with an approved existing service; storage component, topology, encryption/key management, backup/recovery and tiering.
Document catalogue	Initial and full document types/categories and their mapping to case and provider-submission types.
Metadata	Exact mandatory and optional fields by document type, including foreign and archival evidence where applicable.
Evidence requirements matrix	Required/optional evidence by case type, data category, provider, workflow step and legal basis.
Verification model	Responsible reviewer or data owner, statuses, reasons/codes, deadlines and whether automatic checks are advisory or determinative.
Access and visibility	Subject-, provider-, officer-, auditor- and administrator-visible content; masking; additional permissions for sensitive evidence.
Preview and download	Default preview model, download restrictions, temporary secure links and permitted exports.
Lifecycle and retention	Retention periods, legal holds, withdrawal rules, deletion exceptions, expiry, technical tiering and archival treatment.
File policy and sizing	Final formats, limits, documents per case/submission, peak volumes and growth assumptions.
Integration contracts	Detailed upload/reference APIs, status exchange, error handling, retries, idempotency, reconciliation and monitoring.
Notification boundary	Whether evidence-status messages are owned directly by this service or triggered through Portal/CMS/provider modules.
Optional automation	Scope and accuracy expectations for OCR, extraction or automated comparison if ordered.

Baseline protection / Mandatory configurable capability shall not be treated as optional scope or a chargeable change merely because its final configuration is confirmed during design.

12. Vendor response requirements

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

Response area	Requested information
Understanding of need	Summary of the evidence-management problem, intended outcomes and important programme boundaries.
Proposed solution approach	High-level service architecture, storage model, major components, technology choices and boundaries with the other modules.
Storage and capacity	Capacity assumptions, included storage, scale model, durability, backup/recovery, retention impact, recurring costs and lock-in considerations.
Evidence handling	Upload, validation, malware/integrity controls, metadata, review, linkage, additional/replaced evidence and lifecycle approach.
Access and security	Identity, role/organization/task/case access, sensitivity controls, preview/download restrictions, encryption and data-leakage protection.
Integration approach	Portal, CMS / Back Office, provider channels, SPR Core, IAM/SSO, audit/monitoring and approved integration assumptions.
Audit and operations	Audit protection, monitoring, alerting, operational support, administration and transition/export approach.
Sizing and performance	Capacity model using the confirmed baseline and justified assumptions for unknown document and peak volumes.
MVP proposal	Recommended scope, sequencing, calendar duration, person-days, team and total price in AMD with VAT treatment.
Full implementation	Calendar duration, person-days, team composition and total price in AMD with VAT treatment.
Optional scope	Separate effort, duration and price for OCR/automatic extraction and any other optional items.
Warranty and support	Separate 12-month service description and price, including storage, incident and security-fix assumptions.
Risks and dependencies	Key legal, data, storage, infrastructure, Core, provider and decision dependencies; risks and mitigation.
Deviations and alternatives	Any unsupported requirement, exclusion, alternative or condition affecting price, timeline or recurring cost.

Market-sounding principle / Vendors are not expected to reproduce a predefined document-management product or architecture. They are expected to show how their approach achieves the required outcomes, respects the programme boundaries and provides credible capacity, effort, cost and operational assumptions.

End of Annex D