RFI06/2025 Document Authentication as Part of The Intelligent AI Verification Solution

Questions & Answers

#	Questions	Answers
8	**Hardware Requirements:** The RFI does not specify hardware expectations. Could SARS clarify whether the solution is expected to run on SARS-provided infrastructure, or if suppliers should propose hardware sizing (e.g., CPU, RAM, GPU, storage) for on-premise or hybrid deployment?	Refer to Q3 in the first set of questions and answers.
9	**Cloud vs On-Premise Preference:** Is there a preferred deployment model (cloud, on-premise, hybrid), or should suppliers propose multiple options?	Refer to Q3 in the first set of questions and answers.
10	**Integration Targets:** Are there existing systems (e.g., SIEM, SOC, document management platforms) that the solution must integrate with?	Core Business Systems: The solution must support integration with SARS's eFiling Portal and Case Management system via APIs. While integration specifics will be defined later, full deployment requires seamless connectivity with these platforms. During the PoV phase, integration is not mandatory, but future access to SARS's Document Management System (Documentum) is expected for retrieving and storing documents. Security and Identity Systems: The solution must integrate with SARS's Security Operations Centre (SOC) and feed logs into its SIEM platform. Please specify which platforms your solution can integrate with. It must operate within SARS's secure network (via enterprise web proxy) and support integration with Microsoft Active Directory for Single Sign-On and role-based access control, ensuring alignment with SARS's identity and access protocols.
11	**Volume Estimates:** Could SARS provide indicative volumes for document ingestion and	Refer to Q4 in the first set of questions and answers.

#	Questions	Answers
	fraud detection during full-scale rollout (beyond PoC)?	
12	**Document Ingestion:** Can SARS confirm whether encrypted or password-protected files are expected in live submissions, and whether manual review is acceptable for such cases?	SARS has not defined specific handling preferences for encrypted or password-protected files. Vendors are encouraged to describe available capabilities, including detection, flagging, decryption workflows, and audit support.
13	**Document Ingestion:** Should suppliers support real-time ingestion from mobile capture (e.g., taxpayer uploads via smartphone)?	SARS accepts supporting documents through multiple digital channels – the web-based eFiling portal and the SARS MobiApp (mobile app) – as well as other avenues like branch scanners and the online query system. All submitted documents, regardless of channel, are ultimately stored in SARS's enterprise Document Management System (Documentum).
14	**Document Ingestion:** Is there a minimum DPI or megapixel requirement for image-based documents?	SARS requires vendors to specify the minimum image quality—such as DPI or megapixel thresholds—necessary for their solution to effectively perform document fraud detection.
15	**Detection Capabilities:** Are there specific document types or fraud scenarios SARS considers high priority (e.g., ID forgery vs invoice tampering)?	SARS wants to know which document types your solution supports, out-of-the-box or through configuration, the effort required, and whether SARS can configure documents with vendor training or if the vendor must handle each configuration.
16	**Detection Capabilities:** Should the solution support detection of reused logos, watermarks, or signatures across unrelated documents?	Please describe all detection techniques employed, including image analysis, pattern recognition, and metadata comparison, to ensure comprehensive identification of reused visual elements.
17	**Detection Capabilities:** Is SARS interested in forensic comparison across multiple taxpayer submissions (e.g., duplicate documents reused fraudulently)?	SARS is interested to understand the solution's ability to detect and manage duplicate or reused documents across taxpayer submissions. Kindly detail all detection techniques utilized to ensure effective fraud identification.
18	**Performance Metrics:** Does SARS have target thresholds for acceptable false-positive or false-negative rates?	At this stage, SARS has not defined specific thresholds for these metrics. We recognize the importance of balancing accuracy and operational efficiency in intelligent AI verification solutions, and we anticipate that these parameters will be shaped further as we evaluate vendor capabilities

#	Questions	Answers
		and refine our deployment model. Vendors are encouraged to share their own benchmarks, performance expectations, and approaches to managing false-positive and false-negative rates, as this will help inform SARS's understanding and future requirements.
19	**Performance Metrics:** Should suppliers include benchmarking results from third-party evaluations or internal testing only?	Include benchmarking results from third-party evaluations and internal testing.
20	**Performance Metrics:** Is there a preferred format for presenting precision, recall, and F1-score metrics?	There is no mandated format for presenting precision, recall, and F1-score metrics. However, whichever format you choose should be easy to interpret and clearly structured.
21	**Output & Delivery:** Should the solution deliver fraud detection results via API, dashboard, or both?	Please describe all output mechanisms and capabilities, including integration options, data formats, and visualization features.
22	**Output & Delivery:** Is SARS expecting explainable AI outputs with annotated visuals or textual justifications?	SARS seeks to understand solution capabilities regarding explainable AI outputs, including annotated visuals and textual justifications. Please describe how your solution delivers fraud detection outcomes with interpretability features that support transparency, analysis, and informed decision-making.
23	**Technical & Compliance:** Are there specific regulatory standards (e.g., ISO, NIST, POPIA) SARS expects the solution to comply with?	Vendors are requested to provide details on the compliance of their solution with data protection and security regulations. Provide certification status, audit readiness and how regulatory requirements are embedded into the solution.
24	**Technical & Compliance:** Should suppliers propose a modular architecture that allows SARS to scale or swap components over time?	SARS requests details on the solution's architecture that supports scaling or component replacement. Indicate whether your solution uses modular services or other approaches that enable flexibility and long-term adaptability.