South African Revenue Service

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

Questions & Answers

#	Questions	Answers
1	**Scope Clarification:** Please confirm whether SARS intends to authenticate only supporting documents submitted by taxpayers, or whether internal documents (e.g., correspondence, audit reports) also form part of the scope. .	The scope of document authentication for the Intelligent AI Verification Solution is currently focused on supporting documents submitted by taxpayers. Internal documents, such as correspondence or audit reports, are not included in the scope at this stage.
2	**Integration Points:** Which core systems should the solution integrate with during the PoV (e.g., Case Management, eFiling Portal, SARS Document Management System)?	At this stage, there are no integration requirements with core systems during the Proof of Value (PoV) phase. All input data will be provided separately or manually.
3	**Data Residency and Hosting:** Will SARS permit cloud processing within Microsoft Azure South Africa Region, or must all data remain on-premise during the PoV phase?	Processing of sensitive bulk documents including (taxpayer supporting documentation residing in Documentum) for fraud detection will require a strategic approach that balances security, compliance, integration and operational efficiency. SARS would prefer a Hybrid solution deployment which combines on-premises infrastructure with cloud services, allowing SARS to keep sensitive data within our data centre, whilst leveraging cloud capabilities for scalabilities and advanced analytics. This approach will offer flexibility and allow SARS to build and integrate the solution with security and compliance requirements in mind. The processing of such sensitive information should be performed in such a way that duplication of such data is avoid as far as possible, that any sensitive information is not stored in a public cloud environment (private cloud environment would be strongly advised), that any cloud AI analytic

#	Questions	Answers
		capabilities comply with RSA data residency requirements, and that integration between the on-premises and cloud environments is performed through a dedicated API channel. This should also be true for the PoV phase to ensure operability of the solution.
4	**Volume Metrics:** Please confirm anticipated monthly document volume for PoV and full rollout to enable accurate sizing and indicative pricing.	Should a Proof of Value phase be pursued, SARS anticipates that approximately 20,000–30,000 documents may be processed through the solution. For the broader rollout, rather than specifying a fixed monthly volume at this stage, please outline the volumes your solution is capable of handling along with indicative pricing.
5	**Model Training Data:** Will SARS provide anonymized historical document samples to train fraud detection models during the PoV phase? .	If a Proof of Value phase is undertaken, the solution would need to ensure robust data protection throughout model training. In such a case, SARS may provide original document samples—rather than anonymized historical data—to support accurate fraud detection model development, while maintaining strict data security protocols.
6	**Preferred Output Formats:** Should fraud detection results be exported in JSON, XML, or CSV format for system integration?	Fraud detection results should ideally be exported in JSON format, as this aligns with industry standards and is widely supported by modern cloud-based solutions. XML can be considered for integration with legacy systems. CSV is less preferred because it requires manual ingestion and is not ideal for automated integration. However, the choice of format should ultimately depend on the capabilities of your solution. On our side, SARS will evaluate the integration requirements of our systems and select the most suitable option based on compatibility.
7	**GRC Alignment:** Section 6.2.1 of the RFI mentions an “integrated Governance, Risk and Compliance (GRC) solution.” Should the RFI response address document authentication only or include broader GRC interoperability features?	The primary focus of the RFI response should be on document authentication. However, if your proposed solution includes other GRC interoperability features, you may certainly provide more details about these features and how SARS may benefit from them.