SARS REQUEST FOR INFORMATION

BIOMETRIC SOLUTION FOR IDENTITY, VERIFICATION AND AUTHENTICATION OF TAXPAYERS

BUSINESS REQUIREMENTS SPECIFICATION

Contents

1. STRATEGIC CONTEXT

From SARS Vision 2024 our strategic intent is “to develop a tax and customs system based on Voluntary Compliance, and where required, enforce responsibly and decisively". In support of this vision, SARS has defined nine strategic objectives, including:

- To make it easy for Taxpayers & Traders to Comply & fulfil their obligations (Strategic Objective 2);
- Detect Taxpayers & Traders who do not Comply, and make non-compliance Hard & Costly (Strategic Objective 3); and
- Modernise our systems to provide digital & streamlined services (Strategic Objective 6).

As SARS services, solutions and capabilities continue to evolve and expand there is a continuous trade-off between (1) the need for absolute security, identification and verification of the taxpayer and /or SARS official party to a transaction; and (2) the need to balance this with taxpayer experience, taxpayer service levels, removing barriers to technology adoption and internal efficiency of SARS operations.

With this in mind, SARS regularly reviews the technology landscape for new platforms, tools and processes that would support SARS in achieving its strategic intent. SARS has identified Biometric Authentication as a technology enabler that would enhance the ability of SARS to perform on-site and remote biometric identity verification via available Digital Channels and improve the ability of SARS to safeguard taxpayer information and fully enable its Digital Channel landscape.

2. BACKGROUND

Safeguarding and protecting taxpayer information, as required by law, is of critical importance to SARS. The growing risks related to cyber-crime is a concern. To this end SARS must make all efforts to ensure that only authorised persons can access taxpayer information. This puts a large burden on SARS to perform adequate access control in all available channels, with specific focus on its Digital Channels (e.g. eFiling and SARS MobiApp) as well as authentication and / or identity verification prior to authorising / processing sensitive transactions such as “Banking Details Changes”.

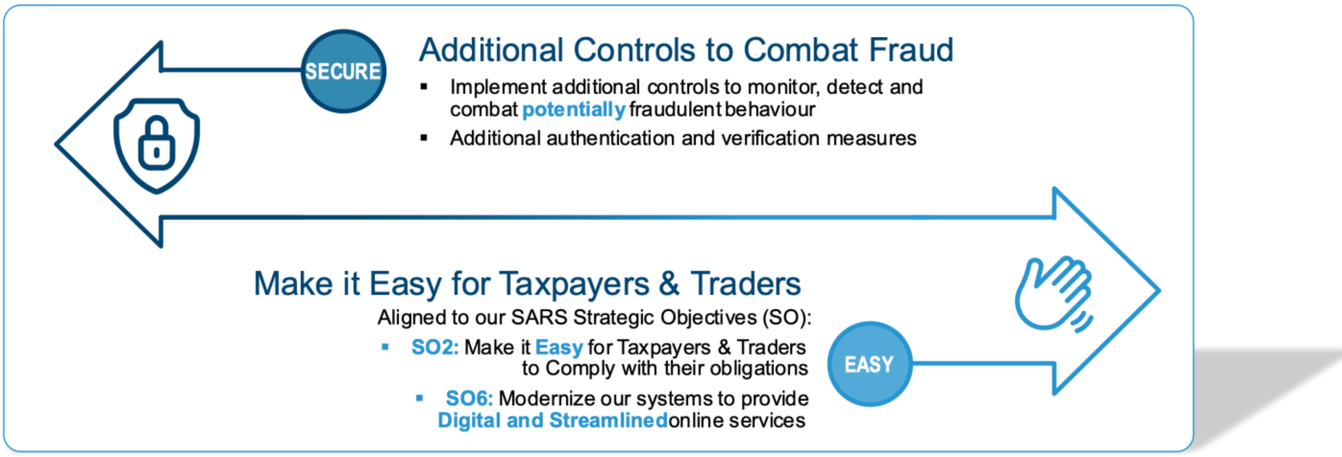
The best known method to ensure reliable and secure identity verification is the utilisation of biometric forms of verification, such as fingerprint verification, facial, iris and voice recognition. Multi-modal authentication combines these biometrics with other elements, including security tokens (trusted devices, device recognition and one-time PINs) and knowledge factors (Passwords, PINs and Security Questions).

While SARS has to some extent made previous investments in biometric identity verification, these have been largely tactical and limited to face-to-face transactions where the Taxpayer Verification (TPV) functionality was introduced to do biometric fingerprint verification with the Department of Home Affairs (DHA) in SARS branches.

Beyond specific processes, SARS has recognised the importance of person identity verification and authentication across the enterprise. This capability would be leveraged across taxpayer engagements, whether physical transactions at ports of entry, branch offices or SARS kiosks, or in the digital channels domain. Further, it would enable SARS internally to ensure system access is controlled and available to authorised and verified SARS officials only.

It is therefore envisaged that the requirements for such a multi-modal biometric verification and authentication capability be consolidated and SARS explore the possibility of a biometric authentication platform that could service the requirements of the enterprise, and provide a secure access management solution. This solution would integrate with SARS current technology solutions to enable both taxpayer and SARS official identity verification and authentication, both for on premise (SARS offices, branches and border posts) and remote channels (digital channels).

This will enable SARS to also seek the balance between implementing safeguards that, on the one hand provide additional controls that could combat fraud, whilst, as far as possible, making it easy for taxpayers and traders to engage with SARS and its channels, and comply with their obligations.



Additional Controls to Combat Fraud

- Implement additional controls to monitor, detect and combat **potentially** fraudulent behaviour
- Additional authentication and verification measures

Make it Easy for Taxpayers & Traders

Aligned to our SARS Strategic Objectives (SO):

- **SO2:** Make it **Easy** for Taxpayers & Traders to Comply with their obligations
- **SO6:** Modernize our systems to provide **Digital and Streamlined** online services

Figure 1 - Balancing the Need for Controls to Fight Fraud and Making it Easy for Taxpayers & Traders

SARS would therefore like to obtain information on available biometric authentication solutions and capabilities that are commercially available, and that could potentially be leveraged to meet SARS biometric authentication requirements.

3. REQUIREMENTS

SARS requires a solution to reliably and securely identify, verify and authenticate taxpayers and SARS officials to control authorised access management to its internal facing and external facing systems. It is anticipated that a biometric authentication such as fingerprint verification, facial-, iris- and voice recognition can meet these requirements. This will assist SARS combat fraud and other illicit activities, whilst providing an improved and secure user experience to taxpayers.

SARS is looking for a solution option that will support multi-modal biometric identity verification and authentication of taxpayers and officials performing transactions. While the organisation envisages prioritising facial recognition and voice recognition for the first phase of implementation, the solution should be capable of including other biometric modes thereafter.

3.1 ILLUSTRATIVE USE CASE – FACIAL RECOGNITION

Below is an illustrative use case outlining how SARS envisages the facial recognition solution be leveraged to improve the security of a user registering for the SARS online eFiling system. Note that SARS is looking at comprehensive solution to encompass multi-modal biometrics – the below example of facial recognition is provided for illustrative purposes.

- Facial Recognition must be introduced in the online channel in such a way that it is available as a service that can be incorporated into either an existing or new authentication process as and when required
- At a specified point in the User registration process, where authentication is required, Facial Recognition is incorporated as an authentication option.
- Where the transaction is not from a mobile device, the ability must exist to use a web-cam connected / built-in to the desktop or laptop. Where no webcam is present, the ability must exist to direct the person to a smartphone mobile app option. This could be achieved through “push-message” to SARS MobiApp or via SMS with a link to a browser option on the person’s mobile device or other secure options that may be available and practical to use in the SARS environment/ scenario.
- An image must be captured of the person transacting (Selfie) as the “Source” image. This process must incorporate the ability to detect that the person is a real, live human being (**liveliness detection**) and it is not just a static photograph presented to the image capturing function.
- The identification number of the person transacting must then be used to retrieve the associated image (hereafter referred to as the “Target” image) of the person from the reference database (e.g. DHA HANIS).
- The Source image must then be compared to the Target image to provide an identity verification / authentication result.

  - Successful comparison will enable the applicable process to continue and the relevant authentication level to be set.
  - Successful authentication via Facial Recognition must be identifiable by downstream processes and/ or activities in order to bring additional efficiencies in those processes (e.g. Facial Recognition success in eFiling user registration can eliminate eyeball cases and allow access to taxes without any further verification required)
  - Where it is practical in the specific process/ channel, an exception process must be available where a SARS staff member with applicable role will manually perform Facial Recognition by comparing the Source image with the Target image.
    - A complete evidence set of the Facial Recognition transaction and related channel information must be stored for purposes of non-repudiation when SARS needs to utilise the information in a court-of-law.
    - Sufficient data must be available for operational reporting on the utilisation and success of the Facial Recognition service

3.2 TO IMPROVE UNDERSTANDING OF AVAILABLE SOLUTION OPTIONS

- **Solution integration options**
  - SARS would like to understand how available biometric solutions are able to integrate with existing SARS existing applications and channels. What technologies, protocols or platforms are supported?

- **Expected Performance:**
  - Indication of Reliability and expected success rate for identity verification related to various biometric types:
    - Fingerprint (as captured by a typical fingerprint reader (e.g. Futronic FS80/81H)
    - Facial Recognition (using image capture from readily available sources such as 640x480, and 720p webcams, cell phone front-facing cameras)
    - Voice Recognition (required sample quality and sample length)
  - Typical Response time for a biometric verification (full cycle time, including capture, verification and response)
  - Experience and success rates using facial and voice recognition in the South African context
  - Against an expected database of 15 million subjects (expanding to 25 million over next 10 years)

- **Operational Requirements:**
    - What is required for enrolment?
        - What would the key implications and considerations be for SARS for each of the biometric types
        - Is there an ability to leverage existing data sources (e.g. facial recognition of captured image verified against DHA provided ID photos vs requiring taxpayers to be rephotographed)
        - Voice recognition – can previous contact centre engagement recordings be used?
    - Provide information on available options and solutions appropriate for contactless biometric verification
    - Provide information and available options and solutions for verification of a person's identity using online channels (e.g. taxpayers using eFiling)?
    - Indicate how the available solution can address concerns around and detection of spoofing and deepfakes as well as other anomaly detection options
    - Does the solution address non-repudiation and use of the biometric identity verification and authentication information in subsequent audit and, where applicable, legal court processes.
- **Implementation Considerations:**
    - Please provide an indication of typical hardware requirements. For performance indication, please consider a solution expected to complete ±30,000 face verifications per hour
    - Solution Delivery Models
        - Understand various business models by which a biometric solution meeting the above requirements would typically be delivered.
    - Solution Cost and Indicative Pricing
    - What ongoing technical support / vendor participation is typically required for the operation of the solution?
    - Typical Project Implementation Timeframes required to implement a solution