interfront
Smart Systems. Better Borders.

REQUEST FOR INFORMATION (RFI) FOR

International Frontier Technologies State-Owned Company Limited

RFI subject: Request for Self-Sovereign Identification Initiative

RFI number: RFI-2023/24-07

YOU ARE HEREBY REQUESTED TO SUBMIT INFORMATION FOR THE REQUIREMENTS OF INTERFRONT			
RFQ NUMBER	**RFI-2023/23-07**		
DESCRIPTION OF GOODS/ SERVICES	**Request for Self-Sovereign Identification Initiative**		
DATE	**21 February 2024**		
CLOSING DATE & TIME	28 February 2024, 17h00pm		
COMPULSORY REQUIREMENTS	**None**		
ENQUIRIES	Enquiries must be addressed to: Name: Leanne Ross Contact number: 021 840 3400 e-mail: procurement@interfront.co.za (enquiries only, do not send quotes to this e-mail address)		
Response	Submit to procurement.quotes@interfront.co.za		
PHYSICAL ADDRESS	St Andrews Building Somerset Links Office Park De Beers Avenue Somerset West		
URGENCY:	Low ☐	Medium ☒	High ☐

1 Purpose

The purpose of this document (**RFI-2023/24-07**) is to invite prospective service providers in order for Interfront to collect information about the capabilities and services offered by various service providers / suppliers. A brief business requirement is described in paragraph 4 and 5. Interested service providers / suppliers are requested to send through detailed information which might lead to an informative discussion of what your company can offer in terms of paragraph 4 and 5 and to ascertain whether it will be suitable to Interfront requirements.

All bids, contracts or orders for goods or services shall be subject to the General Conditions of Contract as published by National Treasury of the Republic of South Africa. In the event of any conflict between the provisions contained in any contract or agreement in place as between Interfront and the supplier / contractor / service provider and the General Conditions of Contract, the provisions as contained in the General Conditions of Contract shall prevail. Kindly familiarise yourself with these provisions at www.treasury.gov.za

2 RFI is not a contract

This RFI does not constitute a contract or order with Interfront but merely serves to request information that may lead to a request for quotation.

3 Preparation Costs

The Service Provider will bear all its costs in preparing, submitting and presenting any response or proposal to this RFI and all other costs incurred by it throughout the RFI process.

4 Business Requirement Specification

Background:

Self-Sovereign Identity is a technology solution that allows individual citizens the capability to have autonomy and control of their own digital identity including all their personal information accompanies this digital identity.

All the information a customer typically shares with various organisations in their day-to-day life can be stored in the form of a digital wallet with all those credentials.

Trusted organisations such as banks, telcos or governments can provide verified information that the user can add to the wallet.

This approach then not only provides a way to safely store a digital identity and credentials, but SSI also enables trust on the validity of the data.

The digit wallet is only accessible by the citizen or authorised representative. The citizen can choose which organisations they are willing to share their credentials and SSI provides a technical solution to ensure sharing is done in the least intrusive manner.

SSI embraces decentralised identity systems, which distribute the authority and verification process across multiple entities or even individual users. These decentralised identity systems leverage technologies like blockchain, decentralised identifiers (DIDs), and verifiable credentials (VCs) enabling individuals to have greater autonomy and ownership over their identities.

SSI is built upon the foundation of decentralised identity systems and encompasses several fundamental technology elements.

Blockchain

Key to decentralised identity system is a blockchain, a distributed ledger shared among computers in a network. The blockchain records identity-related information in an immutable and tamper-resistant manner, making it incredibly difficult to change, hack, or cheat the system. The decentralised nature of the blockchain eliminates the need for a central authority, enhancing security and resilience. Blockchain does face challenges when it comes to scalability and privacy, another technology to keep an eye on is Directed Graph technology.

Decentralised Identifier (DID)

DIDs are unique identifiers generated on the blockchain, comprising a string of alphanumeric characters. DIDs contain essential details such as the public key and verification information associated with an individual's identity. By utilising DIDs, users can establish their digital presence in a secure and decentralised manner.

Decentralised Identity Wallet

A decentralised identity wallet is an application that empowers users to create and manage their decentralised identifiers (DIDs) and verifiable credentials. This wallet serves as a secure repository for users' identity information and grants them full control over its access and usage. Some examples of decentralised Identity wallets are Metamask, uPort, Sovrin and Blockstack which serve as a secure digital repository for users identity information.

Verifiable Credential (VC)

VCs are digital representations of both paper and digital credentials that individuals can present to organisations requiring verification. These credentials are cryptographically secured, enabling reliable verification and trust. The VC system involves three main parties:

- **Holder:** The individual who generates their decentralised identifier through a digital wallet application and obtains the verifiable credential. For example, a person could hold a verifiable credential as proof of their educational qualification, such as a university degree or a professional certification.

- **Issuer:** The entity that utilises their private key to sign a verifiable credential and subsequently grants it to the holder. Examples of issuers can include educational institutions, government agencies, or professional organisations. For instance, a university could issue a verifiable credential to certify a student's completion of a specific course or program.

- **Verifier:** An entity tasked with the verification of credentials. Verifiers have the ability to access the issuer's public DID on the blockchain to authenticate the legitimacy of the verifiable credential provided by the holder. For example, an employer may act as a verifier when verifying the job qualifications of a job applicant by verifying their educational credentials through a verifiable credential issued by a recognized institution.

From a technical perspective, SSI requires a number of concepts (like Trust Registries, keys, Decentralized Identifiers, Verifiable Credentials, authentication protocols)

Understanding SSI from a technological perspective requires the understanding of a few core concepts:

- **Trust Registries**, which serve as a shared and trusted record of certain information. In other words, they serve as a "layer of trust" and a "single source of truth".

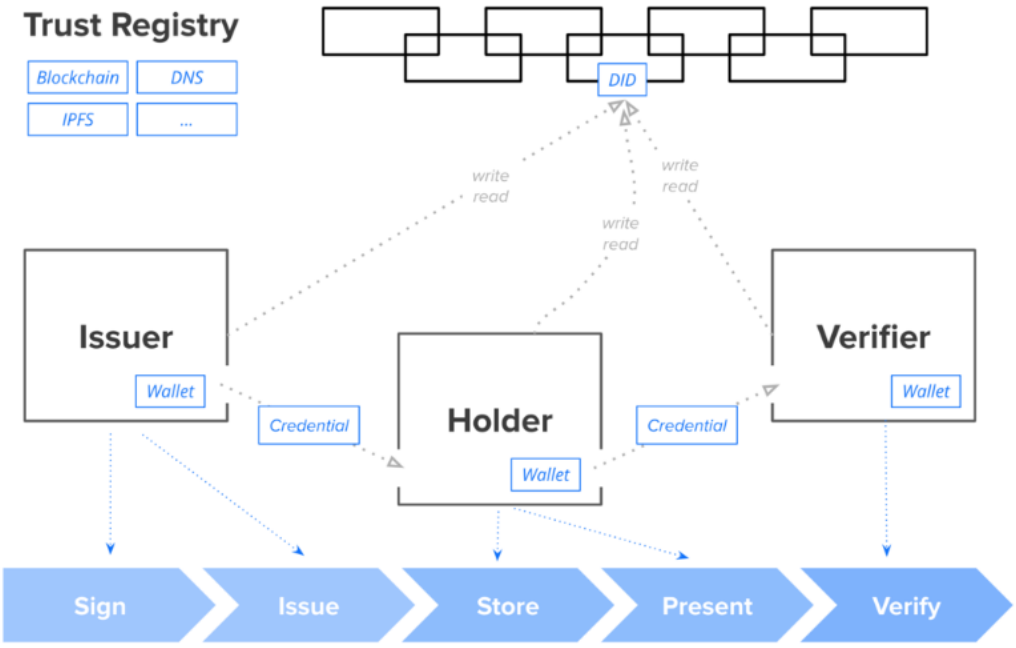
- **Cryptographic keys**, which convey control over digital identities and enable core functionality such as encryption and authentication.

- **Decentralized Identifiers (DIDs),** which establish a public key infrastructure by linking keys to unique identifiers that allow different parties to find and interact with each other.

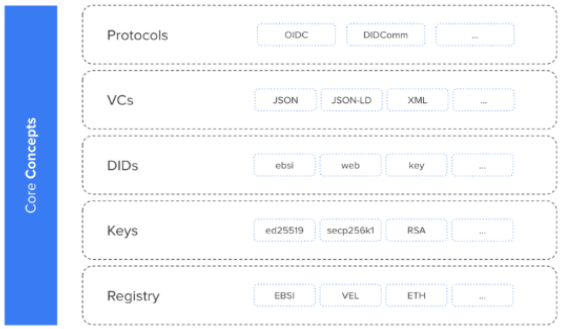
- **Verifiable Credentials (VCs)** which are digital identity documents that can easily and securely be shared with and verified (incl. validity, integrity, authenticity, provenance) by anyone in a privacy preserving way. Importantly, they are never (!) stored on a blockchain due to privacy and compliance reasons.

- **Wallets,** which store our keys (control) and VCs (identity data) and enable the management and sharing of our digital identities and data via easy-to-use applications.

Use of open standards (e.g. by the W3C, Decentralized Identity Foundation, OpenID Foundation and others) are vital.



Different technologies can be used to establish Trust Registries like blockchains (EBSI, Ethereum) or the domain name service (DNS). SSI even works (for certain use cases) without any Trust Registries but purely on a peer-to-peer basis. Similarly different types of DIDs, keys, proofs, credential formats, authentication and data exchange protocols can be used.



Information needed:

4.1 What are the protocols that are shaping the SSI environment and are being more broadly adapted by industry that are implementing SSI based solutions?

4.2 What skillsets are needed for project team members participating in SSI projects and initiatives to be part of the construction of SSI solution implementation?

4.3 What technology stacks would be ideally suited to SSI project implementation? Identify open-source options versus proprietary components or elements.

4.4 How many years of experience does your company have in similar Blockchain/SSI projects?

4.5 Company location - Is your company locally based in South Africa, outside of South Africa or does your company have a presence in South Africa?

4.6 Any additional information in your proposal will be an advantage.

A meeting can be arranged via MS Teams upon request before submitting a proposal.

5 Duration of engagement

To be determined

References:

https://www.linkedin.com/pulse/exploring-technology-behind-self-sovereign-identity-ssi-poelman/?trackingId=D4hFLICgRTie2u64RSXD%2FQ%3D%3D

https://www.linkedin.com/pulse/self-sovereign-identity-promise-safe-control-over-personal-poelman/