TERMS OF REFERENCE

Invitation for Expressions of Interest for Implementation and Operation of Smart Africa Trust Alliance Data Interoperability Platform (SATA-DIP)

Client Address	**Smart Africa Secretariat** 10th Floor, Career Centre Building KG 541 ST, Kigali, Rwanda, PO Box: 4913 Tel: +250784013646| +250 788-300-581 Email: tenderenquiries@smartafrica.org www.smartafrica.org
EOI#:	090/SA/EOI/03/2023
Release date:	07th March, 2023
Closing date:	07th April, 2023; 5pm (Local time, Kigali)
Contact	For any questions or enquiries, please write to: tenderenquiries@smartafrica.org For Proposal Submissions: procurement@smartafrica.org

1. ORGANISATION BACKGROUND

Smart Africa is a bold and innovative commitment from African Heads of State and Government to accelerate sustainable socio-economic development on the continent, ushering Africa into a knowledge economy through affordable access to Broadband and usage of Information and Communications Technologies.

In 2013 in Kigali Rwanda, 7 African Heads of State (Rwanda, Kenya, Uganda, South Sudan, Mali, Gabon, Burkina Faso) adopted the Smart Africa Manifesto in recognition of the need to adopt a harmonized digital transformation process in Africa. In 2014, all Heads of State and the Government of the African Union endorsed the Smart Africa Manifesto at the 22nd Ordinary Session of the Assembly of the African Union in Addis Ababa.

The Smart Africa Alliance has since grown to include 36 African Heads of State and countries that represent close to 1.1 billion people: Algeria, Angola, Benin, Burkina Faso, Burundi, Cameroon, Cape Verde, Chad, Congo, DR Congo, Côte d'Ivoire, Djibouti, Egypt, Gabon, Ghana, Guinea, Kenya, Madagascar, Mali, Mauritania, Morocco, Niger, Nigeria, Rwanda, Sao Tome & Principe, Sierra Leone, Senegal, South Africa, South Sudan, Sudan, Togo, Tunisia, Uganda, Zambia, and Zimbabwe. The Alliance is also a partnership bringing together all African countries adhering to the Manifesto, the African Union (AU), the International Telecommunication Union (ITU), the World Bank, the African Development Bank (AfDB), the GSMA, ICANN, academia, and the Private Sector. Besides its initial membership, other organizations and countries sharing the same vision, interests, and goals will be admitted to the Alliance.

Smart Africa's vision is to transform Africa into a single digital market by 2030. This vision will be reached by delivery towards 3 strategic objectives:

1) build resilient and sustainable digital Infrastructure for Africa,
2) drive agile policy and regulatory harmonization to attract investment to the African digital landscape, and
3) leverage technology to accelerate the inclusive uptake of digital public goods and services across Africa.

Smart Africa strategy for years 2023-2025 features concrete action plan to realize the objectives. Among the strategic initiatives and priorities, the development of digital identity interoperability and data interoperability through the Smart Africa Trust Alliance (SATA) are central. These will be the backbones of Africa's transformation into a single digital market, as identity and data exchange are the basic enablers for cross-border digital trade and services.

2. SATA DATA INTEROPERABILITY PLATFORM (SATA-DIP) BACKGROUND

Africa has a market size of 50+ countries with a population of 1.4 billion, the world's youngest population profile, and the highest growth rates. However, digital markets are developing mostly in a national level and do not (yet) benefit from the scale of the continent. Currently, intra-Africa trade represents approximately 16.6% of Africa's GDP only, while intra-European trade represents 69% of the European Union's GDP, for instance. One reason for this is the coexistence of 50+ separate and distinct national regulatory frameworks in Africa, and the lack of a system to establish mutual trust and recognition across national digital ID schemes and private sector solutions.

According to the World Bank, an estimated 1 billion people worldwide cannot officially prove their identity, making it difficult or impossible to vote, bank, travel, or buy property. Of the 1 billion people without proof of identity, nearly half those people, approximately 500 million, are estimated to live in sub-Saharan Africa.

Without proof of identity, millions of African people are missing out on basic legal, social, and economic rights and opportunities. Faced with these challenges to sustainable development, African countries are considering the most effective solutions to identify their citizens and residents and adapted to the realities of the continent. One promising solution is already being deployed in some countries: Digital or Electronic Identification. Identity is a crucial element for each individual as it defines a set of traits to uniquely identify a

person. Similarly, digital identity is equally important as it helps establish confidence in user identities presented digitally to a system.

Smart Africa's audacious vision is to build a single digital market by 2030, with digital products and services accessible easily throughout the continent and operate seamlessly with the rest of the world. Digital identity represents the backbone of Africa's transformation into a single digital market, as it is a basic building block for access to both public and private services.

On February 11, 2019, at the 7th meeting of Smart Africa's Board in Addis, Ethiopia, the board requested the Smart Africa Council of ICT Ministers to spearhead and coordinate the collaboration of key public and private sector stakeholders to develop a blueprint for a continental framework that could assist Member States in designing and implementing interoperable individual digital ID schemes in a manner that would facilitate and enable trusted cross-border transactions across Africa by leveraging the public sector where appropriate.

This would be a key practical contributor to the future success of the African Continental Free Trade Agreement (AfCFTA) as digital ID schemes designed to facilitate cross-border recognition will undoubtedly promote national financial and economic inclusion, enhance public services, and create wide-ranging new economic opportunities in their home markets and across Africa.

In line with the instructions of the Board, the Smart Africa Secretariat (SAS) launched a Working Group to provide a platform for collaboration with and among a range of stakeholders. The Working Group developed the digital ID blueprint as well as a continental concept – named the Smart Africa Trust Alliance (SATA) – to establish institutional ownership and accountability combined with a trust framework based on standards and trust assurance mechanisms to facilitate cross-border interactions.

In order to bring cross-border digital ID to life, the first stage of SATA will be to interconnect the national digital registers and other information systems following a set of mutually agreed data-sharing rules and technical standards by Smart Africa Member States and supported by a certification and evaluation system, plus a shared data exchange platform. This will be in line with SATA's objectives to contribute to the transformation of Africa into a single digital market.

In addition to the digital ID cross-border use, SATA data exchange framework will support single digital market more widely by allowing dataflows across the borders between governments, government-to-business and vice versa, also business-to-business and business-to-customer in a trusted and efficient ways.

In 2022-23, SAS has developed a more detailed concept, strategy as well as implementation roadmap of SATA and the data exchange framework. Among the first steps will be the implementation of a Data Interoperability Platform (SATA-DIP), as the building block for cross-border digital ID and wider data exchange in the next years. The first use case identified for initial implementation of SATA-DIP is cross-border Mobile SIM card registration, and currently 4 Smart Africa Member States have expressed willingness to be the piloting partners: Benin, Ghana, Senegal and Togo. More countries may join the process.

3. EXPRESSION OF INTEREST (EOI) OBJECTIVE AND SCOPE

Smart Africa Secretariat (SAS) seeks for a Data Interoperability Platform Technology Solution (**Technology**) and a potential partner (**Provider**) to implement, operate and support the Smart Africa Trust Alliance Data Interoperability Platform (**SATA-DIP**) as the first SATA solution.

This process will serve as a pre-qualification process with-which selected applicants will be invited to a final process that shall lead to contract negotiation and signing.

The selected **Provider will be remunerated or reimbursed based on the Commercial Model** proposed by Provider and agreed upon with the Smart Africa Secretariat and key SATA members. SAS intent is to find a Provider who would be willing to take up **maximum possible initial and ongoing financial investment into launching and operations of SATA-DIP**, in return the provider should secure the return on investment (ROI) based on cost reimbursement and/or revenue sharing model in later stages of operations. In essence, SAS seeks a Public-Private Partnership (PPP) engagement with the Provider.

SATA – DIP must be designed and deployed as a **highly scalable technical solution as a service** that will be hosted in Africa from the pilot stage to the full scale and operation stage. The environment for the Technology should be a self-contained cloud installation.

Technology should support the achievement of the first use-case goals and targets, but be easily scalable to any use-cases. The first use-case of the SATA-DIP will be the Cross-border SIM registration through SATA. The next use cases and the relevant data exchange volumes will be agreed and are to be implemented in course of SATA implementation and scaling. SAS expects that within course of 3 years, at the very least 5 more high-impact cross-border data exchange use-cases will be implemented between interested Member States on top of SATA-DIP.

4. OBLIGATIONS OF THE PROVIDER

The Provider proposing the Technology implementation, operation and support for SATA-DIP is expected to perform the following activities:

1. Setup of cloud resources for the solution;
2. Installation and configuration of all required components;
3. Testing of the solution;
4. Creation of operational manuals;
5. Training of the operations and users' technical teams;
6. Support of the users' integrations.
7. Support of the Technology during the course of operations;
8. Processing of certificate signing and revocation requests;
9. Processing of member registration and deletion;
10. Monitoring and periodic reporting of the solution usage, compliance, performance and support;
11. Knowledge transfer to SAS team and other relevant stakeholders
12. Participation and support in scaling of SATA-IP uptake among African countries, the relevant promotion and development of use-cases.
13. The **timeframe for the engagement** is expected to be as follows:

    - **Implementation of Technology and set-up Customer Support** with the first use-case – maximum **5 months** from contract signing (Phases 1-2 below);
    - **Total duration of the engagement**, i.e. for operations and support of SATA-DIP – **36 months** from contract signing.

More concretely, the Provider should ensure the delivery of following deliverables by the stages as envisioned here:

Phase 1 Platform Set-Up

- Creation of the SATA-DIP environment incl. cloud resources, necessary installation and configurations;
- Creation of operation manuals for the Technology;
- Creation of a detailed management plan for the key technical sub-components
- Creation of operation manuals incl. for each sub-component
- Creation of the testing descriptions
- Creation of the Technology training plan

Phase 2 Customer Support Set-up

- Training of SAS and users' technical teams.
- Support of the users' integrations.
- Support of the acceptance tests.
- Support the use case and data exchange service development.

Phase 3 Operations

- Support of the additional integrations and conduct of additional users trainings.
- Support of the additional acceptance tests.
- Transfer of the Technology operations knowledge to Smart Africa Secretariat (SAS)
- Processing of certificate signing and revocation requests.
- Processing of member registration and deletion.
- Monitoring and periodic reporting of the solution usage, compliance, performance and support.
- Inputs to and participation in SATA-DIP promotion work and use-cases development.

5. TECHNOLOGY REQUIREMENTS

Based on the market study of best practices and data exchange solutions in-use globally, SAS is expecting to receive offers from Providers having experience and expertise with open-source solutions such as the X-Road technology, e-Delivery technology, or any other **open-source technology complying with High-Level Technical Requirements detailed in Appendix 1**.

More detailed Technical Requirements in case the e-Delivery is the solution offered are detailed in Appendix 2, and for the X-Road in Appendix 3. In submission of Proposal, potential Provider has to provide a description of how their Technological solution will meet the requirements from Appendix 2 or 3 accordingly.

Among the High-Level Technical Requirements, the Base Requirements are mandatory for qualification and Additional Requirements are preferred qualities of the Technology.

In case the Provider will propose any other Technology the information about the Technology should be detailed in accordance with the requested information detailed in Appendix 4. Please note that both the e-Delivery and the X-Road-specific mandatory technology requirements are described in the relevant Appendixes 2 and 3. In case a different Technology is proposed, the Provider should also in a proper manner present information about the mandatory technical requirements as requested in Appendix 4.

The Provider candidates are expected to list additional features, that could make the solution's Operations more effective and what should be considered/implemented during the post-Pilot phase for the full-scale operations. The proposed solution should be adapted to hosting relocation when needed for the scale-up phase and the Provider should have the ability to support the full localization of the Technology at the infrastructure provided by the SAS when need be and adequately accommodated.

6. COMMERCIAL MODEL REQUIREMENTS

An interested party should build up and suggest a Commercial Model that incorporates and clearly indicates the total cost of the Solution, plus the split between different types of payment and stages of the project.

As part of the Commercial Model, the potential Supplier should present a share of the total cost of the project Supplier is ready to discount from the Implementation and Support phase and take an opportunity to earn a revenue share or be reimbursed in the future.

The supplier should count on no more than 3 years period for the PPP model to earn from the revenue share or receive reimbursement, and should define the maximum amount to be received, including the risk margin for the initial discount.

For clarification, there is no current definite Business Plan and Pricing Model for the SATA Pilot from SAS side. There is a potential to launch pricing and to earn revenues with future use-cases, but most probably not earlier than 12-18 from the start of the contract.

The Commercial Model should be shown in USD, with all sums inclusive of VAT or Rwanda withholding tax (WHT).

The following is the format for the Commercial Model submission:

1) Direct Expense for SAS

	Without revenue sharing or later reimbursement	With revenue sharing or later reimbursement (discounted expense proposal)
Total cost for 36 months *Including:*	… USD	… USD
1. Payment for the Implementation phase (one-time payment), *including:*	… USD	… USD
1.1 Payment at the start of the project	… USD	… USD
1.2 Payments during the implementation process	… USD	… USD
1.3 Payment for the delivery and acceptance of the solution	… USD	… USD
2. Ongoing operations and support for up to 36 months, including:	… US	… USD
2.1. Minimum monthly payment for SLA delivery (fixed price)	… USD monthly	… USD monthly
2.2 Additional payment for the additional necessary support (hourly rate in case of extra work needed)	… USD	… USD

2) Future payment proposal for the discounted expense proposal

Present/submit as applicable either option 1 or 2.

Option 1: Revenue sharing

Minimum total amount expected as revenues for duration of contract	… USD
Ongoing payment or end-of-contract result fee	… (choose as appropriate)
Expected payment frequency	Annual/quarterly/monthly (choose as appropriate)
Expected start of ongoing payments (if applicable)	Month / year
In case of fixed transaction fee model preference:	… USD per … DIP member / user / data exchange transaction (choose as appropriate)
In case of revenue total share model preference:	… % of SATA-DIP revenues
Any additional conditions / expectations from Provider side	

Option 2: Later reimbursement

Total amount expected as revenues for duration of contract	… USD
Ongoing payment or end-of-contract result fee	… (choose as appropriate)
Expected payment frequency	Annual/quarterly/monthly (choose as appropriate)
Expected start of ongoing payments (if applicable)	Month / year

Any additional conditions / expectations from Provider side	

7. OUTLINE OF THE SELECTION PROCESS

The process for the selection of the Provider:

Step 1: Terms of Reference published
Step 2: After receiving Offers, SAS creates an evaluation committee made up of key Smart Africa Secretariat staff, Member States representatives and possible external advisors.
Step 3: Pre-qualification of maximum 3 Qualified Providers/suppliers.
Step 4: Final Interviews / Meetings with Qualified Providers/suppliers.
Step 5: Selection of Most Qualified Provider/supplier and engagement negotiations

8. EVALUATION CRITERIA

The following model will be used to evaluate all respondents and proposals submitted:

Item	Evaluation Notes
No tax arrears	*Mandatory Requirement: Automatic disqualification if not met*
Depth and extent of Provider experience: • With the proposed Technology (as most important factor) • With similar public-private partnerships • With similar commercial models	*To be scored based on criteria by evaluation committee as this is a pre-qualification process*
Technology that meets High-Level Requirements (per Appendix 1) and is open source	*Mandatory Requirement: Automatic disqualification if not met*
Technology suitability to expected set-up (per Appendix 2 or 3 or 4)	*To be scored based on criteria by evaluation committee as this is a pre-qualification process*
Suitability of mission team set-up and experience	*To be scored based on criteria by evaluation committee as this is a pre-qualification process*
Commercial model, including: • Cost for SAS • Suitability of future payments model proposal	*To be scored based on criteria by evaluation committee – based on comparison of proposals*
Suitability of high-level work-plan	*To be scored based on criteria by evaluation committee as this is a pre-qualification process*

9. SUBMISSION REQUIREMENTS

A specific outline must be followed to facilitate the Smart Africa Secretariat's review and evaluation of the responses received.

A response to this expression of interest must include the following sections in the order listed:

a. A cover letter confirming the firm's interest in providing the services and entering the required partnerships
b. Administrative document: Company registration certificates, and Tax clearance certificates). *Failure to submit will lead to automatic disqualification of the offer.*
c. A technical proposal containing the following content:
    - Company's experience with the Technology proposed, with similar partnerships and similar commercial models – list concrete references for each aspect (project names, short descriptions)
    - Technology and solution details (as highlighted above in Section)
    - Mission team set-up and experience:
        - core team structure and roles

    - profiles/bios of key personnel for the roles, highlighting relevant experience and providing concrete references (project names, short descriptions)
- Commercial Model (as highlighted above)
- High-level workplan, indicating Provider's potential time schedule and readiness to deliver the deliverables within the indicated timeframe.
- A technology compliance form as seen in Appendix 4 of this EOI document

Note: *The details of the technical proposal should help SAS to understand that the applicants has the technology, the resources and the relevant team to deliver the project.*

10. SUBMISSION PROCESS

Soft copies of proposals must be submitted to procurement@smartafrica.org in PDF format indicating as e-mail title "***Expressions of Interest for Implementation and Operation of Smart Africa Trust Alliance Data Interoperability Platform (SATA-DIP)*** " not later than **07th April 2023 at 5:00 pm** Kigali time.

To facilitate the success of this pre-qualification process, please ensure that all submission requirements are clearly met. More details on various requirements are found in the appendix section.

Late submissions will be rejected.

11. VALIDITY:

Proposals and quotes must remain valid for 180 days after the date of closing noted above. After, the closing date and time, all proposals received by the Smart Africa Secretariat become its property.

12. ANTI-CORRUPTION:

Smart Africa is committed to preventing and not tolerating any act of corruption and other malpractices and expects that all bidders will adhere to the same ethical principles.

13. ENQUIRES:

Any enquires will be received and addressed 5 days or mor before the closing date for the submission of any proposal through tenderenquiries@smartafrica.org .

14. RIGHTS RESERVED:

a. This REOI does not obligate the Smart Africa Secretariat (SAS) to complete the REOI process.
b. SAS reserves the right to amend any segment of the REOI prior to the announcement of a selected provider .
c. SAS also reserves the right to remove one or more of the services from consideration for this contract should the evaluation show that it is in SAS's best interest to do so.
d. SAS also may, at its discretion, issue a separate contract for any service or groups of services included in this REOI. SAS may negotiate a compensation package and additional provisions to the contract awarded under this REOI.
e. Smart Africa reserves the right to debrief the applicants after the completion of the process due to the expected high volume of applications and avoiding the compromise of the process.

APPENDIX 1

HIGH-LEVEL TECHNICAL REQUIREMENTS

MANDATORY REQUIREMENTS	**YES / NO**
Single common data exchange environment	YES
Federation Support	YES
Data Sovereignty	YES
Open Standards	YES
Privacy by Design	YES
Non-domain-specific	YES
Secure communication	YES
Secure systems	YES
Suitable for public Internet use	YES
High Availability	YES
Open Source Licence	YES
Centralized Governance Model	YES
Decentralized Data Exchange	YES
Fine-grained access control	YES
Centralized Monitoring	YES
Digitally signed, logged and timestamped data exchanges	YES
Real-time request-response	YES
Secure Audit Trail	YES
Compatible with high LOA digital signatures	YES
Centralized collection of statistics and reporting	YES

ADDITIONAL REQUIREMENTS	**YES / NO**
Fast Scalability	YES
Supports RESTful Web Services	YES

DEFINITIONS AND ADDITIONAL INFORMATION

Mandatory Requirements

Feature	Comments
Single common data exchange environment	The technology provided must provide one environment for the interconnection of data exchange participants. This unifies data exchange methods and optimises expansion costs.
Federation Support	Multiple installations (e.g., country-level and pan-African environments) can be interlinked to facilitate national and international interoperability using the same technology.
Data Sovereignty	The data owner/service provider must have sole control over data storage and use. Ensures data stays within the set boundaries and mechanisms are in place in case of misconduct
Open Standards	Use non-proprietary standards and systems. Must be agnostic to information system technology, allowing integration with different systems.
Privacy by Design	Privacy of personal data is not compromised
Non-domain-specific	Suitable for any kind of data
Secure communication	Cybersecurity focus. Ability to specify cryptographic keys at the required level (AES 256/512, RSA 2048). Use of standard protocols (TLS 1.3)
Secure systems	Cybersecurity focus. Encryption of data at rest (AES256/512)
Suitable for public Internet use	Cost-effective
High Availability	Resilient to failures of components and network connectivity
Open Source	Open-source systems have the source code freely available, enabling anyone to analyse and modify it. The software license must permit proprietary modifications. Expanding the service provider range removes single provider risk.
Centralized Governance Model	The Governing Authority can regulate the use of the platform and make sure that parties follow agreed rules.
Decentralized Data Exchange	Allows to move of data directly between parties (countries), and supports data sovereignty.
Fine-grained access control	Service access can be controlled on the service level by the service provider (usually the party responsible for data security), allowing participants from multiple domains and varying access levels to use one system.
Centralized monitoring	A single tech support team can monitor the system, including adherence to standards
Digitally signed, logged and timestamped data	Provide non-repudiation in case of disputes if and

exchanges	when information was provided.
Real-time request-response	No significant latency is introduced by the data exchange environment. Able to provide immediate replies to requests.
Secure Audit Trail	Message logs must be stored in a way that prohibits any undetectable tampering with the log.
Compatible with high LOA digital signatures	High LOA digital signatures (as defined by the EU eIDAS legislation) must be supported by the environment.
Centralized collection of statistics and reporting	Provides oversight of system use. Allows unified reporting to regulators and other third-party stakeholders.

Additional Requirements

Feature	**Comments**
Fast scalability	New members and services are easy to add
Supports RESTful Web Services	RESTful web services are currently the most common API technology. Supporting this will considerably ease integrations as well as the re-use of existing services.

APPENDIX 2

TECHNICAL REQUIREMENTS FOR e-Delivery TECHNOLOGY

The components described here are installed as one cloud environment for the SATA-DIP Pilot Project. This approach minimizes the maintenance effort and resource requirements.

The architecture and technical requirements described in this Appendix 2 are considered mandatory to qualify for the evaluation.

e-Delivery

Data interoperability solution (e-Delivery) is standardized by Connecting Europe Facility (CEF).

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery

Infrastructure Overview

The SATA-DIP environment uses open-source e-Delivery software (e.g., Domibus or Harmony e-Delivery Access), with PKI services provided by EJBCA Community Edition software. The environment consists of central components managed by Smart Africa Secretariat (SAS) and components used by each party connected to the environment (the Customers' Access Points).

While there are multiple ways to deploy e-Delivery, SATA-DIP uses one specific model:

- 4-corner network model;
- PKI with one dedicated Certification Authority;
- Message exchange using e-SENS AS4 Profile;
- Dynamic service discovery with SML and SMP;
- Service Metadata Locator (SML) Service;
- One Service Metadata Publisher (SMP) service for all members' services.

The whole system is depicted in the diagram below (Figure 1).

All components including Access Points (except the Customer Backends) are installed in a single dedicated cloud environment with VPN access to the web and terminal interfaces.

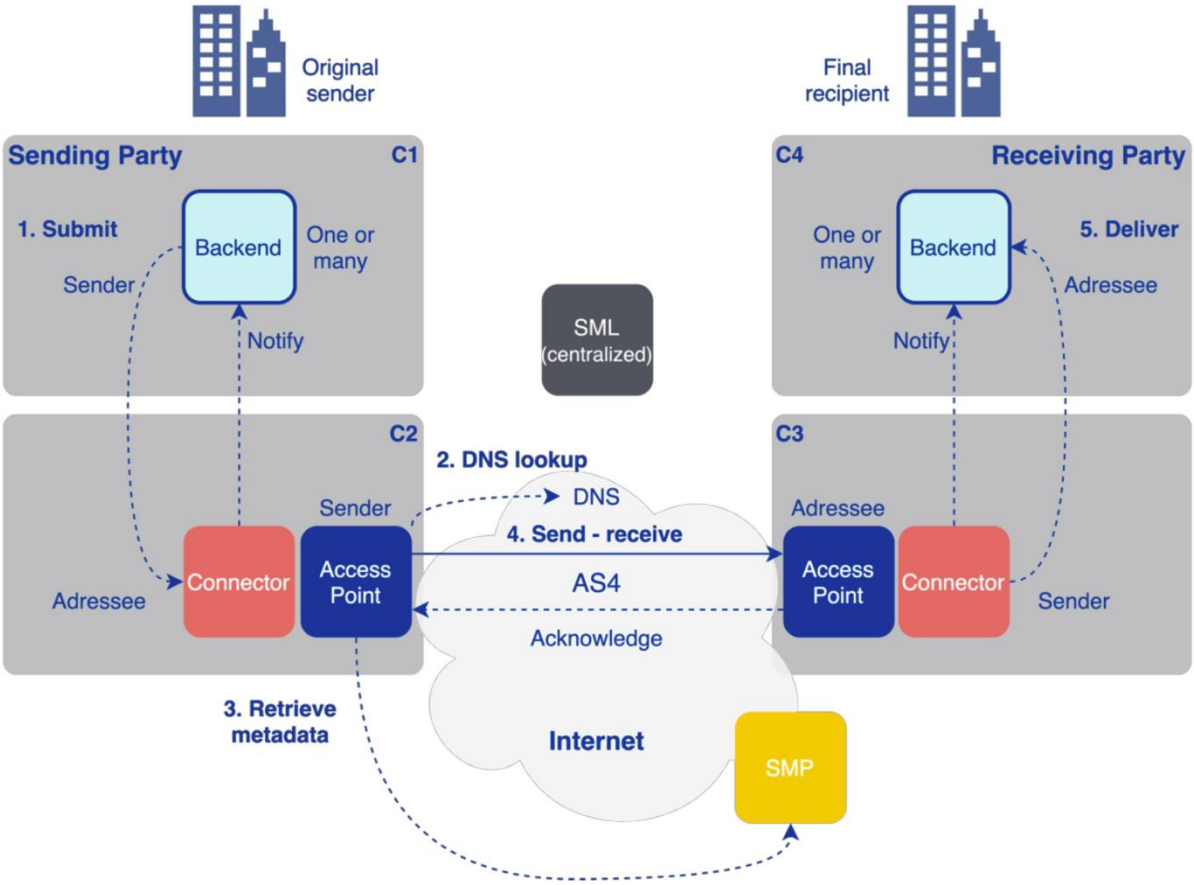

Figure 1. SATA-DIP Planned Architecture – e-Delivery case. Source: www.niis.org

Components

The SATA-DIP consists of several systems with specific roles.

Component	Role
PKI (not depicted)	A single installation of EJBCA to provide all services related to certificate management (creation, suspension) and certificate validity checks (OCSP).
SML	Service Metadata Locator, in conjunction with a DNS server, provides a dynamic service locator service on SATA-DIP-specific domain name.
SMP	Service Metadata Publisher is the registry of services available in the environment.
Access Point	Each member has an access point that operates as the gateway for sending and receiving e-Delivery messages. Access control is also configured in the Access Point.
Connector	Optional component to add service-specific functionality to the Access Point and/or provide protocol conversion for the backend.

Cryptography

Asymmetric crypto: RSA2048
Digests: SHA256

Performance Considerations

The infrastructure is initially forecasted for up to 10 Customers, where each service provider Customer will provide one service. The forecast on request volumes is low or medium for the Pilot.

Remote Access

A VPN server provides secure remote access to the administrative UIs and terminal interfaces. The VPN technology must have free clients for Windows, Mac, and Linux computers. For instance, OpenVPN is a suitable solution. Through VPN, access to servers uses internal addresses.

Support and Operations

The Provider should ensure the Pilot Project production environment uptime of 90% or higher. Optionally, high-availability architecture could be offered.

The Provider should offer 24/7 support services with 8h reaction time.
The Provider should offer 2nd and 3rd-level support included.

APPENDIX 3

TECHNICAL REQUIREMENTS FOR X-Road TECHNOLOGY

The components described here are installed as one cloud environment for the SATA Pilot Project.
This approach minimizes the maintenance effort and resource requirements.

The architecture and technical requirements described in this Appendix 3 are considered mandatory to qualify for the evaluation.

X-Road
Data interoperability solution (X-Road) made available by Nordic Institute for Interoperability Solutions (NIIS).

Infrastructure Overview

The SATA-DIP environment uses the X-Road technology, with trust services provided by EJBCA Community Edition software. The environment consists of a central component managed by Smart Africa Secretariat (SAS), acting as both Governing Authority and Trust Services Provider and components used by each party connected to the environment, the Customers' Security Servers).

The whole system is depicted in the diagram below (Figure 1).

All components including security servers (except the Customer Information Systems), are installed in a single dedicated cloud environment with VPN access to the web and terminal interfaces.

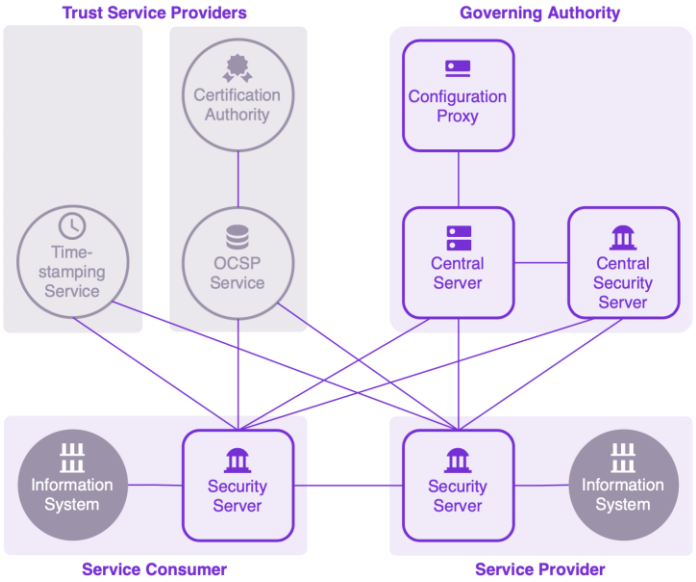

Figure 2. SATA-DIP Platform Planned Architecture – X-Road Case Source: www.niis.org

Components

The SATA-DIP consists of several systems with specific roles.

Component	Role
Trust Service Providers	A single installation of EJBCA to provide all services related to certificate management (creation, suspension), certificate validity checks (OCSP), and

	signed timestamps (TSA). The certificates are issued to members (signing certificates) and security servers (authentication certificates).
Configuration Proxy	Not used
Central Server	Infrastructure-wide configuration and member list management. The Central Server distributes a system-wide list of members, trust service providers, and essential parameters to all security servers, thus creating a distributed configuration that is resilient to communication disruptions.
Metrics Server (not depicted)	X-Road Metrics software for central collecting and reporting on service usage.
Central Security Server	Security Server for member activation requests and operational monitoring data collection.
Security Server	Communication gateway for SATA-DIP customers. All data transmitted between Service Consumers and Service Providers are passed directly between their respective Security Servers, without involving the Governing Authority. The Security Server takes care of communication encryption, digital signatures, and secure timestamps. Counterparties of the communication are validated. Security Servers keep a signed and timestamped message log of all requests and responses. All Security Servers must have central operational monitoring enabled. Each member will have a separate Security Server with remote UI access (see 0 below).

Member Addresses

SATA-DIP members are addressed in a hierarchical format: INSTANCE/CLASS/ID, where:

- INSTANCE is the X-Road environment code – SATA-DIP -;
- CLASS denotes country (e.g., SN for Senegal) and if the member is private (COM) or public (GOV);
- ID is a well-known identifier in the class, e.g., a business registry code.

For instance, Customer 1 with business registry code 12345 would be addressed as SATA-DIP/C1-COM/12345.

Each member registers one or more subsystems that usually denote separate services or information systems.

Cryptography

It is allowed to use software tokens for key storage, in the interests of simplicity.
Token PIN entry must be manual.

Asymmetric crypto: RSA2048
Digests: SHA256

Performance Considerations

The infrastructure is initially forecasted for up to 10 Customers, where each service provider Customer will provide one service. The forecast on request volumes is low or medium for the Pilot.

Technical Resources

Each component is installed in a separate Ubuntu Linux virtual machine (VM).
The minimal VM specification is as follows:

- Ubuntu 20.04 LTS (x86-64);
- 5 GB RAM;
- 10 GB disk space (depends on message log/monitoring database volume) with disk encryption;
- 64-bit dual-core Intel, AMD, or compatible CPU;
- 100 Mbps network interface with an Internet connection;
- Software HSM (software token) where one is required.

All servers are installed in one dedicated internal subnet, with an atypical subnet address to avoid conflicts with users' networks (e.g., 10.170.7/24). Each server has an external as well as an internal IP address. The SATA DIP global configuration uses external IP addresses to enable the installation of on-premise security servers. From the internet, only documented external inbound ports should be open.

Customer Accounts

The pilot environment Customer personnel will have personal user accounts at all SATA-DIP components. The SAS team will have personal user accounts at Trust Services and Central Server user interfaces:

- Trust Services access to approve certificate creation and revocation.
- Central Server access to approve registration requests.

Customers will not have access to any systems except for operational reports.

Remote Access

A VPN server provides secure remote access to the administrative UIs and terminal interfaces. The VPN technology must have free clients for Windows, Mac, and Linux computers, for instance, OpenVPN is a suitable solution. Through VPN, access to servers uses internal addresses.

SATA-DIP Parameters

Parameter	**Value**
The instance identifier	SATA-DIP
Customer classes (to be confirmed)	C1 - COM C1 - GOV C2 - COM C2 - GOV

Support and Operations

The Provider should ensure the Pilot Project production environment uptime of 90% or higher. Optionally, high-availability architecture could be offered.

The Provider should offer 24/7 support services with 8h reaction time.
The Provider should offer 2nd and 3rd-level support included.

APPENDIX 4

TECHNOLOGY COMPLIANCE

HIGH-LEVEL TECHNICAL REQUIREMENTS

Criteria	Comply / Not comply	A short explanation of how the requirement will be met by the solution
MANDATORY REQUIREMENTS		
Single common data exchange environment		
Data Sovereignty		
Open Standards		
Privacy by Design		
Non-domain-specific		
Secure communication		
Secure systems		
Suitable for public Internet use		
High Availability		
Open Source Licence		
Centralised Governance Model		
Decentralised Data Exchange		
Fine-grained access control		
Centralised Monitoring		
Digitally signed, logged and timestamped data exchanges		
Real-time request-response		
Fast scalability		
ADDITIONAL REQUIREMENTS		
Fast Scalability		
Real-time request-response		