OSIA

Unlocking the ID Ecosystem with OSIA: A universal interoperability framework for innovation, competition, and sustainability

OSIA
An Open Standard and a Digital Public Good

2022

www.osia.io



Principles on Identification for Sustainable Development: Toward the Digital Age

In 2019, the Secure Identity Alliance, along with other organisations committed to the development of ID systems that are inclusive, trusted, and accountable and supported the development of a set of shared 'Principles for Good Identification'.

The vision was to create a guiding framework that governments around the globe can use to ensure they build inclusive and trusted digital ID and civil registration systems that both enhance people's lives – and empower them to gain access to social and economic opportunities.

This need is embodied in Target 16.9 of the Sustainable Development Goals (SDGs):

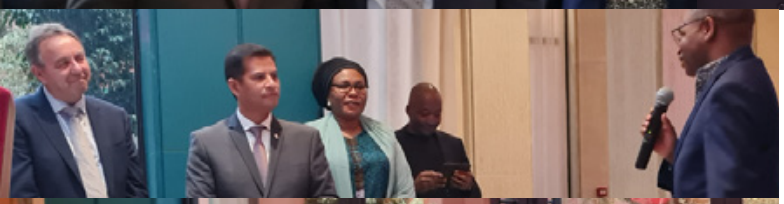
"by 2030 to provide legal identity for all, including birth registration."

From principles to practical action

Principle 5 enshrines the importance of enabling ID systems that utilize open standards to both achieve improved efficiencies and functionality and assure that ID systems can be evolved and adapted to accommodate changes over time.

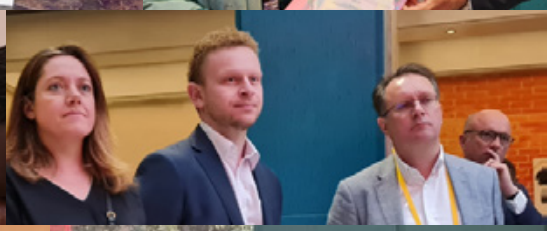
OSIA provides the open standard interfaces (APIs) that enable seamless connectivity between all building blocks of the ID management ecosystem – regardless of technology, solution, architecture, or vendor.

https://www.idprinciples.org/





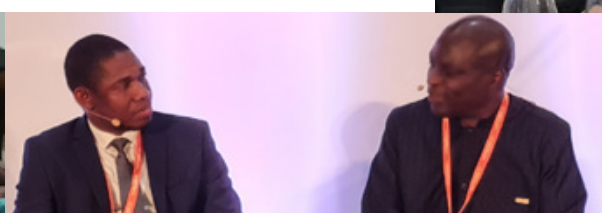
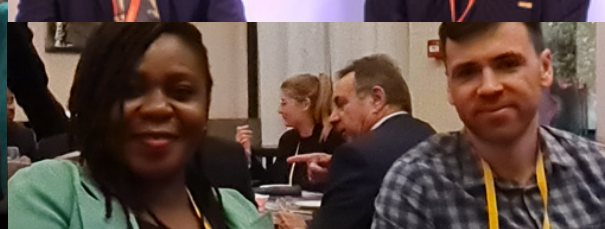


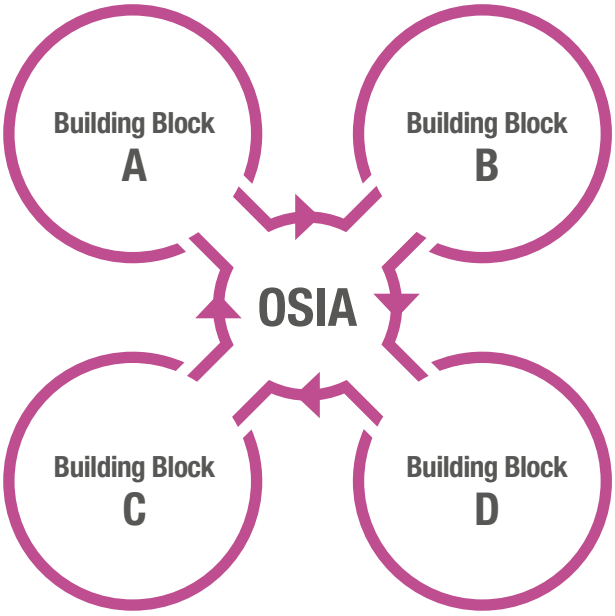






A digital public good, OSIA is an open standard set of interfaces (APIs) that enables seamless connectivity between building blocks of the identity management ecosystem – independent of technology, solution architecture or vendor.



Interoperability benefits innovation and competition and can only be achieved with the contribution and engagement of the whole community!

Get involved in OSIA!

www.osia.io


VISO

1. Introducing the OSIA Initiative

What's at stake

Around the globe, trusted legal identity is the foundation of national security, social protection, and economic growth strategies.

As the identity market matures, technologies like digital ID, biometrics and cloud platforms are transforming the ID landscape. Making it possible to:

- enable national identity schemes that are truly inclusive and serve the needs of all stakeholders
- initiate the delivery of innovative digital public and private services.

To capture this opportunity without undue cost or time-consuming integration effort, governments need to be free to evolve, adapt, modernize, and add to their systems with confidence – and without fear of future compatibility issues.

Until recently, however, the initiation of highly functional and interoperable ID systems that are easy to upgrade or change has been constrained by a siloed approach and lack of standardization that made it difficult to connect registries or exchange, consult, or update data between systems.

In 2019, the Secure Identity Alliance (SIA) launched the global OSIA initiative to address these challenges.

OSIA: Promoting open and transparent government-industry collaborations

Enabling the all-important government-industry collaborations needed to create the frameworks that make it possible to build truly open, innovative and future-proofed national ID systems, OSIA is transforming how governments leverage ID to deliver real-world impacts for their citizens and national economies.

Guiding principles

Sovereignty

The ability of governments to choose what their ID solution 'looks like' is a core principle that goes to the very heart of sovereignty. They must have the freedom to decide which building blocks of the identity ecosystem to use, and how to combine them.

Technology Neutrality

The value of deployed legacy technologies must be preserved, and governments free to use any technology they choose. Technology partners must also be free to innovate on emerging technologies to find new ways to solve problems.

Privacy by Design

To achieve regulatory compliance and to ensure an ethical and responsible approach to managing citizens' data, identity ecosystems must embed privacy by design – from repositories through to interface layers. Ecosystems must ensure data can be user controls with stringent access rights.

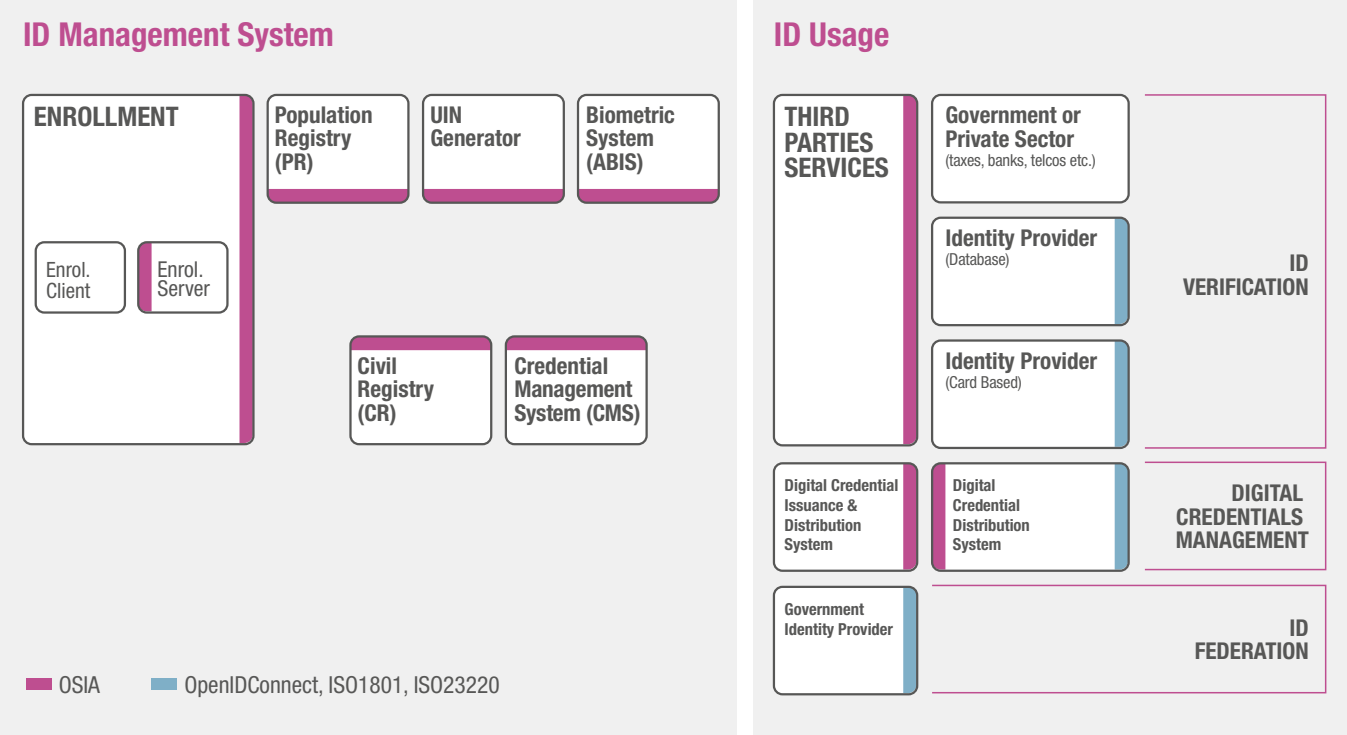

OSIA

2.
OSIA: An overview

To solve the interoperability challenges within the identity sector, the OSIA initiative is focused on a clearly defined scope of work:

1. Build a common understanding of the functional scope for identity systems building blocks

OSIA's first step has been to formalize the definitions, scope, and main functionalities of each building block within the identity management system.



2. Create a set of standardized interfaces and data dictionary

For this core piece of work, OSIA is focused on developing the set of interfaces and standardized data dictionary needed to connect the multiple identity system building blocks and ensure seamless interactions via pre-defined services.

It is then down to each government to define and implement the interaction processes between individual building blocks (which in turn determines which interfaces are associated with each building block), according to local laws and regulations.

"OSIA is an efficient and cost-effective way of leveraging industry expertise and experience while pushing continuous innovation."

3.
OSIA interfaces to date

Interfaces

- Notification
- Data Access
- UIN Management
- Enrollment Services
- Population Registry Services
- Biometrics
- Credential Services
- ID Usage

1 interface = multiple services

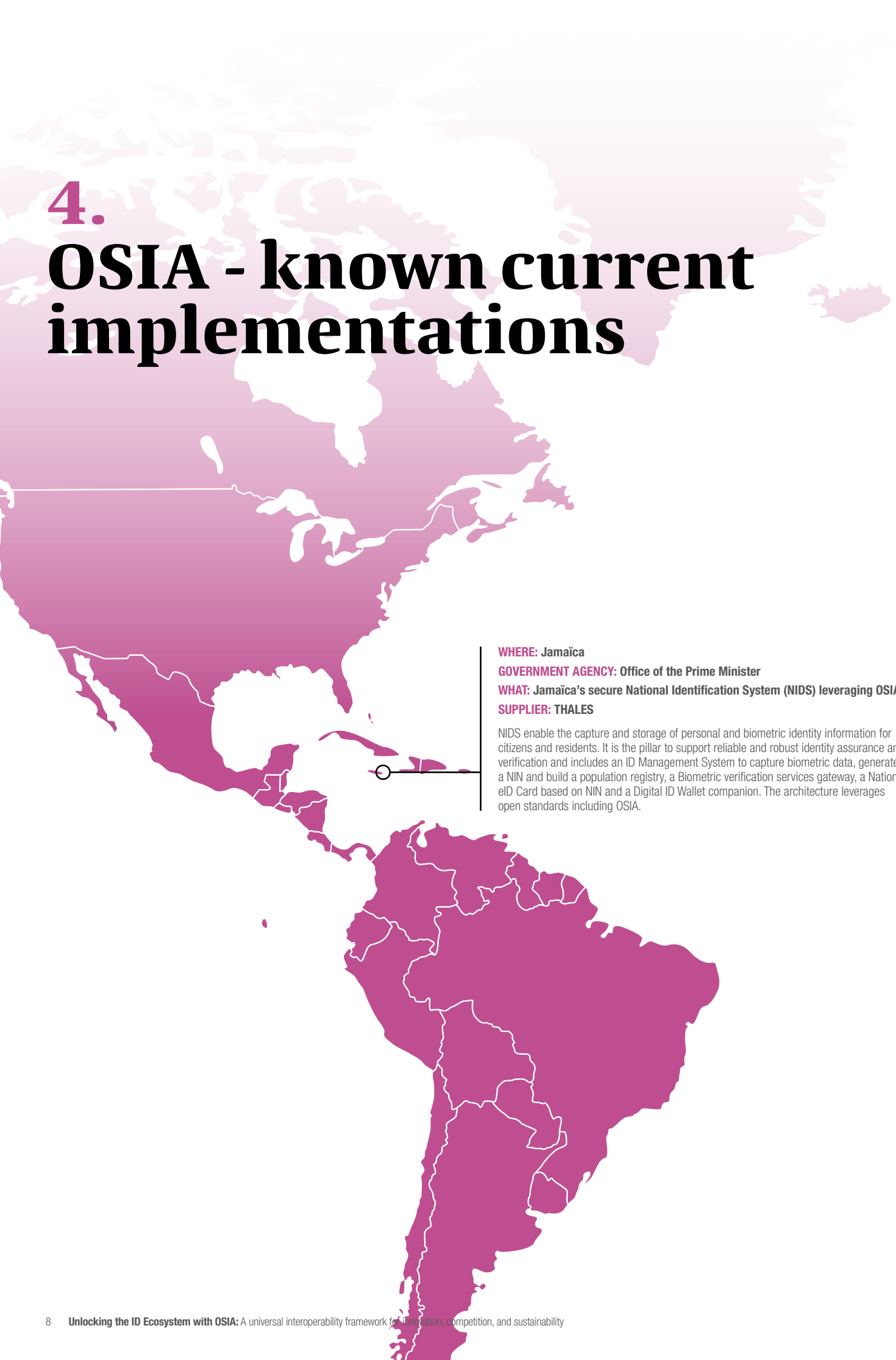
Complete list of services

Services	Description
Notification	
Subscribe	Subscribe a URL to receive notifications sent to one topic
List Subscription	Get the list of all the subscriptions registered in the server
Unsubscribe	Unsubscribe a URL from the list of receiver for one topic
Confirm	Confirm that the URL used during the subscription is valid
Create Topic	Create a new topic
List Topics	List all the existing topics
Delete Topic	Delete a topic
Publish	Publish an event to all systems that have subscribed to this topic
Notify	Callback registered during subscription and called when an event is published
Data Access	
Read Person Attributes	Read person attributes
Match Person Attributes	Check the value of attributes without exposing private data
Verify Person Attributes	Evaluate simple expressions on person's attributes without exposing private data
Query Person UIN	Query the persons by a set of attributes, used when the UIN is unknown
Query Person List	Query the persons by a list of attributes and their values
Read document	Read in a selected format (PDF, image, etc.) a document such as a marriage certificate
UIN Management	
Generate UIN	Generate a new UIN
Enrollment Services	
Create Enrollment	Insert a new enrollment
Read Enrollment	Retrieve an enrollment
Update Enrollment	Update an enrollment
Partial Update Enrollment	Update part of an enrollment
Finalize Enrollment	Finalize an enrollment (mark it as completed)
Delete Enrollment	Delete an enrollment
Find Enrollments	Retrieve a list of enrollments which match passed in search criteria
Send Buffer	Send a buffer (image, etc.)
Get Buffer	Get a buffer
Population Registry Services	
Find Persons	Query for persons, using all the available identities
Create Person	Create a new person
Read Person	Read the attributes of a person
Update Person	Update a person
Delete Person	Delete a person and all its identities
Merge Persons	Merge two persons
Create Identity	Create a new identity in a person
Read Identity	Read one or all the identities of one person
Update Identity	Update an identity. An identity can be updated only in the status claimed
Partial Update Identity	Update part of an identity. Not all attributes are mandatory.
Delete Identity	Delete an identity
Set Identity Status	Set an identity status
Define Reference	Define the reference identity of one person
Read Reference	Read the reference identity of one person
Read Galleries	Read the ID of all the galleries
Read Gallery Content	Read the content of one gallery, i.e. the IDs of all the records linked to this gallery

Services	Description
Biometrics	
Create Encounter	Create a new encounter. No identify is performed
Read Encounter	Read the data of an encounter
Update Encounter	Update an encounter
Delete Encounter	Delete an encounter
Merge Encounter	Merge two sets of encounters
Set Encounter Status	Set an encounter status
Read Template	Read the generated template
Read Galleries	Read the ID of all the galleries
Read Gallery content	Read the content of one gallery, i.e. the IDs of all the records linked to this gallery
Identify	Identify a person using biometrics data and filters on biographic or contextual data
Verify	Verify an identity using biometrics data
Credential Services	
Create Credential Request	Request issuance of a secure credential
Read Credential Request	Retrieve the data/status of a credential request
Update Credential Request	Update the requested issuance of a secure credential
Delete Credential Request	Delete/cancel the requested issuance of a secure document / credential
Find Credentials	Retrieve a list of credentials that match the passed in search criteria
Read Credential	Retrieve the attributes/status of an issued credential (smart card, mobile, passport, etc.)
Suspend Credential	Suspend an issued credential. For electronic credentials this will suspend any PKI certificates that are present
Unsuspend Credential	Unsuspend an issued credential. For electronic credentials this will unsuspend any PKI certificates that are present
Revoke Credential	Revoke an issued credential. For electronic credentials this will revoke any PKI certificates that are present
Set Credential Status	Change the credential status
Find Credential Profiles	Retrieve a list of credential profils that match the passed in search criteria
ID Usage	
Verify ID	Verify Identity based on UIN and set of attributes (biometric data, demographics, credential)
Identify	Identify a person based on a set of attributes (biometric data, demographics, credential)
Read Attributes	Read person attributes
Read Attributes set	Read person attributes corresponding to a predefined set name

For more information and detail on these services, visit:
https://github.com/SecureIdentityAlliance/osia

4.
OSIA - known current implementations



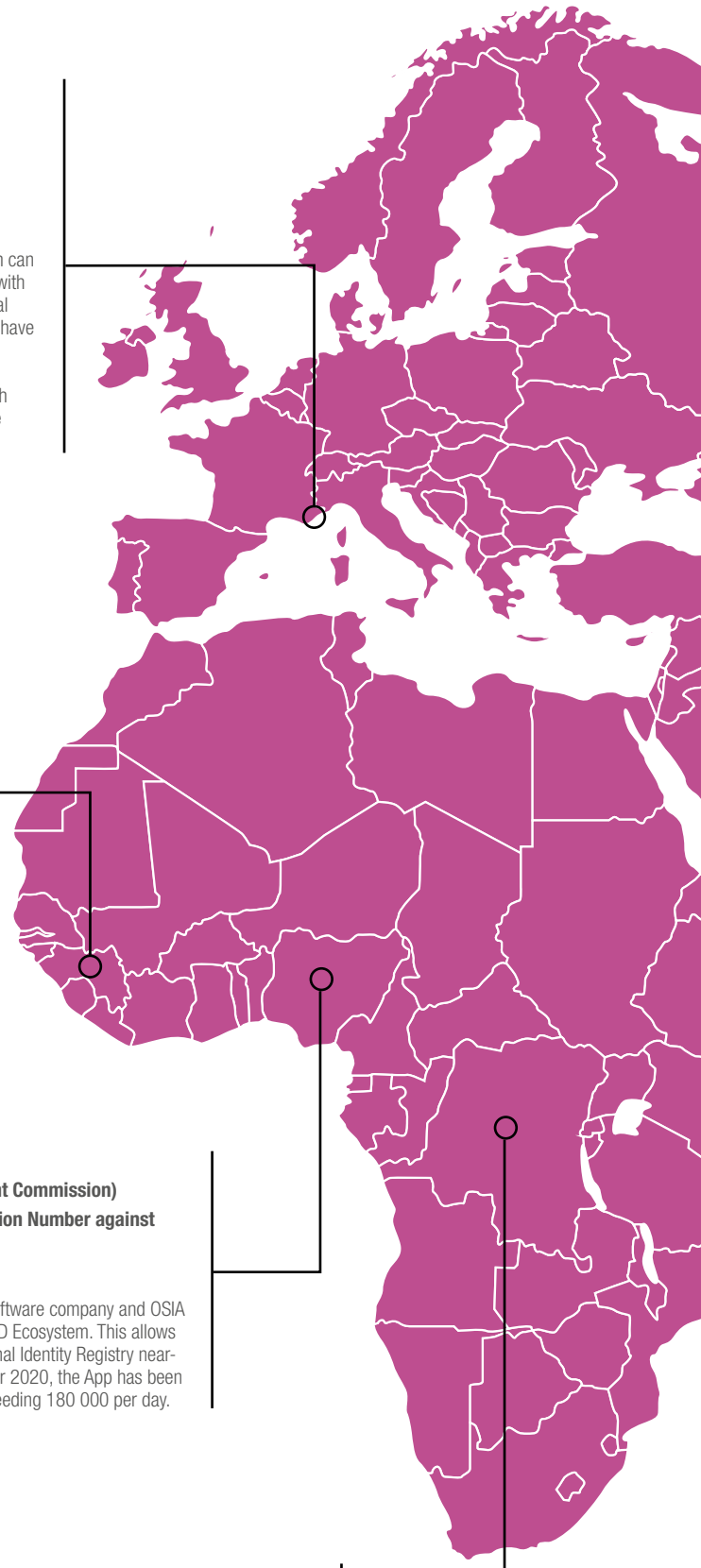
WHERE: Jamaïca

GOVERNMENT AGENCY: Office of the Prime Minister

WHAT: Jamaïca's secure National Identification System (NIDS) leveraging OSIA

SUPPLIER: THALES

NIDS enable the capture and storage of personal and biometric identity information for citizens and residents. It is the pillar to support reliable and robust identity assurance and verification and includes an ID Management System to capture biometric data, generate a NIN and build a population registry, a Biometric verification services gateway, a National eID Card based on NIN and a Digital ID Wallet companion. The architecture leverages open standards including OSIA.



WHERE: Monaco

GOVERNMENT AGENCY: Monaco Principality Digital Transformation Interministerial Delegation

WHAT: 'Extended Monaco', a comprehensive, integrated ID system (physical and digital)

SUPPLIER: INGroupe

The digital ID in Monaco, built into the new electronic ID card which can be used on a smartphone or PC, is based on a process that starts with physical enrolment and ends with the delivery of physical and digital identification, allowing Monaco citizens and residents the option to have their own digital identity when they want, or to renew their national identity. Designed to straddle the physical and digital worlds, the Monaco digital (mobile) ID enables high level authentication with qualified signatures and is based on a modular service architecture making extensive use of open standards such as OSIA and OIDC.

WHERE: Guinea

GOVERNMENT AGENCY: ANIES (National Agency for Economic and Social Inclusion)

WHAT: OSIA-based identity management system to drive major economic and social inclusion programs across the country

SUPPLIER: IDEMIA

Approximately 40% of the population of Guinea are undocumented, lacking any formal identity. This group is therefore unable to access government support. As part of a wide-ranging National Economic and Social Development Plan (PNDES), Guinea plans to introduce a 'beneficiary card' to provide previously undocumented citizens with access to a range of financial services and social rights. Led by Guinea's National Agency for Economic and Social Inclusion (ANIES), and following a census and biometric enrolment program, an OSIA-based population registry will form the basis of an open and interoperable identity system able to interface with government departments and service providers across the country.

WHERE: Nigeria

GOVERNMENT AGENCY: NIMC (National Identity Management Commission)

WHAT: ID verification services using the National Identification Number against the Population Registry leveraging OSIA

SUPPLIER: COMMON IDENTITY

Facilitating access to Nigeria's national identity program, African software company and OSIA member CommonIdentity has developed the Nigeria NIMC Mobile ID Ecosystem. This allows citizens to have their Unique ID verified against the country's National Identity Registry near-instantly and securely via an OSIA interface. Launched in December 2020, the App has been downloaded 3.3 million times in 90 days, with download rates exceeding 180 000 per day.

WHERE: Democratic Republic of Congo (DRC)

GOVERNMENT AGENCY: ONIP (National Office for the Identification of the Population)

WHAT: Connecting Civil Registry and Population Registry leveraging OSIA

SUPPLIERS: DIGITECH, IDEMIA, CIVIPOL(the technical cooperation operator of the French Ministry of the Interior), UNFPA (United Nations Population Fund) and CARITAS (confederation of 165 Catholic relief, development and social service organizations)

With 60% of DRC's children unregistered at birth, this World Bank funded, multi-agency program aims to register 2.4 million children and produce 600,000 birth certificates. The program has two streams: digitalization of the current Civil Registry and allow children enrolled in nursery and primary schools to register for free should they belong to the undocumented group. The data collection process was launched in April 2019 in the schools of Kinshasa, and is now entering its second phase with the integration of the registration data from the Civil Registry system into the Population Registry using the OSIA interface.


OSIA


OSIA

5.
OSIA Benefits

Unleash market innovation

OSIA establishes the conditions that support an equal marketplace and makes it possible for the wider identity community to collaborate in new ways.

- **Create a marketplace where all vendors can compete equally**

  OSIA operates at the interface layer and does not define – or therefore favor - any technology at the component layer (which is typically where the differentiation among vendors takes place).

- **Support the emergence of new local market models featuring local suppliers and SMEs**

  Like the Open Banking revolution, OSIA exposes high performing standardized interfaces that enable new use cases and market offers – from the simple to the complex.

- **Ensure product(s) compatibility after Mergers & Acquisitions**

  Market consolidation can often lead to major products being put into maintenance – leaving governments with little choice but to replace these. With OSIA, whatever the status of a product, it will continue to be interoperable with new offers.

Address integrator/vendor lock-in

OSIA enables governments to exert full control over their sovereign identity systems. So, they can pursue their national development agendas - without any fear of integrator/ vendor lock-in. Governments are no longer forced to implement a wall-to-wall solution from a single vendor and will not encounter compatibility difficulties when evolving their existing legacy solutions. They can:

- **Implement multi-vendor programs** by mixing selected building blocks from different suppliers.
- **Extend legacy solutions or replace legacy building blocks(s)** with a new building block(s) from a different supplier(s).

Enable identity as a service

OSIA empowers governments to build new inclusive eGovernment solutions that give citizens ease of access to public services or trusted digital ID schemes that extend the use of citizen ID into other online areas - such as banking and payments.

- **Driving digital ID market growth**

  OSIA facilitates the link between sovereign identity management solutions and digital identity solutions, like mobile ID, by standardizing the ad hoc interfaces that decouple providers of the ID management solution and the digital ID solution.

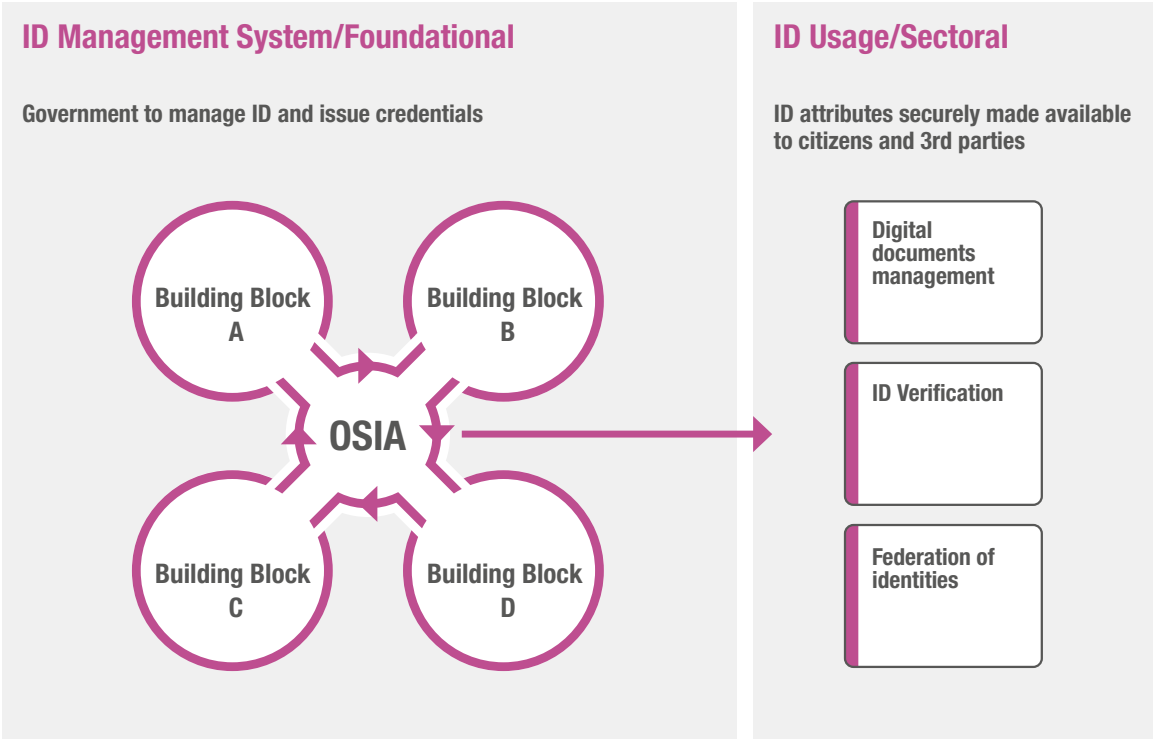
- **Reducing fraud within siloed databases/multiple ID systems**

  OSIA enables the secure and controlled flow of data and services, like ID deduplication and authentication, across multiple foundational and functional registries – even where these registries are run by separate ministries and government agencies. Governments are able to reduce public sector payroll fraud, leakage in social benefits, fraud associated with tax filing and ensure the integrity of the electoral process.

6.
OSIA and digital ID

Identity verification and document authentication

ID Usage consists of a set of services implemented on top of identity systems to favour third parties consumption of identity data. The services can be classified in three sets. The first, the Relaying Party (RP) API is provided within the OSIA framework, with the second and third – Digital Credential Management and Federation Services – delivered within an extended framework of ISO and Open ID Connect standards.



"Weather the headwinds. The tailwinds to propel you forward are over the horizon."

Engr. Aliyu Abubakar Aziz, Chair of the OSIA Advisory Committee

OSIA Relying Party API: submitting citizen ID attributes for validation

The purpose of the OSIA Relying Party (RP) API is to extend the use of government-issued identity to registered third party services. The individual will submit their ID attributes to the relying party in order to enroll for, or access, a particular service. The relying party will leverage the RP API to access the identity management system and verify the individual's identity. In this way, external relying parties can quickly and easily verify individuals based on their government issued ID attributes.

Example use case application: telco enrolment

The RP API enables a telco operator to check an individual's identity when applying for a service contract. The telco relies on the government to confirm that the attributes submitted by the individual match against the data held in the database therefore being able to confidently identify the new subscriber. This scenario can be replicated across multiple sectors including banking and finance, airlines, hospitality, aid agencies and many more.

ISO Digital Credential Management: delegating digital issuance to third parties

The purpose of the Digital Credential Management is to enable external wallet providers to manage government issued digital credentials distribution, storage and usage. The OSIA specification points to the ISO ISO22230 standard.

Example use case application: digital driver license

The DCM enables individuals to request a digital driver license as a digital credential in their selected wallet to use for online and offline identification.

Open ID Connect Federation: user-initiated attributes sharing

The purpose of federation is to enable the user to share their attributes with a chosen relying party using well-known internet protocol: OpenID Connect. The relying party benefits from the government's verified attributes.

Example use case application: on-line registration to gambling website

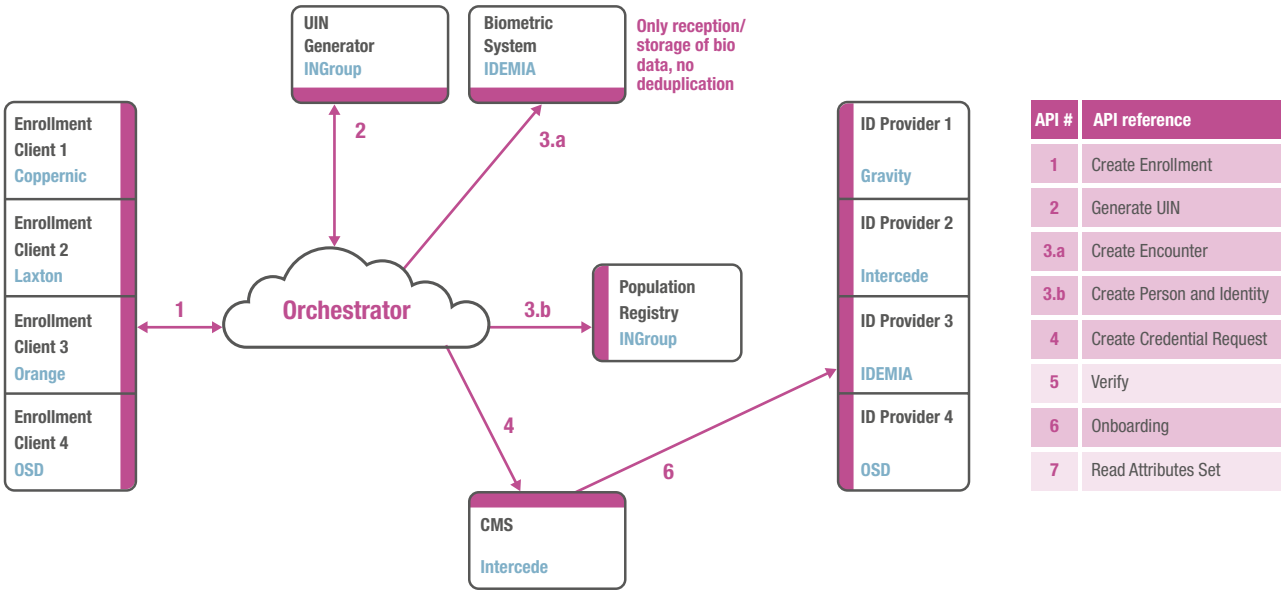
Here, the Federation service enables individuals to log-in with their government credential (log-in/password) and share verified attributes ex. age (above 18) with the relying part.

Interoperability Demo:

Use Case 1 – ID Credential Issuance

In this demo, a Government issues an Identity Card (physical and digital) to a Citizen.

Watch video at https://secureidentityalliance.org/osia-ressources/osia-videos/entry/osia-use-case-1-id-credential-issuance



API #	API reference
1	Create Enrollment
2	Generate UIN
3.a	Create Encounter
3.b	Create Person and Identity
4	Create Credential Request
5	Verify
6	Onboarding
7	Read Attributes Set

Enroll → Establish → Issue → Use Digital ID

7.
OSIA is not a new concept

Harnessing open APIs to unlock value, fast track transformation, increase the agility of service development, and build deep and integrated identity systems isn't a new notion.

Other industries have already seized on the transformational power of APIs to:

- easily share information across applications, services and systems – even legacy systems
- rapidly scale and evolve their systems and services to meet new requirements
- bring new products and services to market

Let's take a look at just two sectors that are using APIs to unlock new value, and to build and connect modern applications to one another – and to the data and services that power them.

Telecom

The telecommunications sector is deploying open APIs to enable rapid, repeatable, and flexible integration among operations and management systems that make it easier to create, build and operate complex innovative services.

Collaboratively developed by stakeholders from across the industry, the TM Forum's Open API suite of 50+ APIs are propelling innovative new digital services in a number of key areas – including IoT applications, smart cities, mobile banking and more.

Open Banking

Powered by APIs that facilitate the flow of data and make it possible for banks to securely share customer information with verified third-party service providers, the Open Banking revolution is enabling banks to build new digital ecosystems and adapt fast to business and consumer demands for innovative services that save them time and money.

Whether that's seeing all of their accounts, savings and credit cards in one place – regardless of who they bank with. Or tracking their payments to gain insights on spending patterns. Or determining their creditworthiness and demonstrating their eligibility for a range of financial services.

The evolution of the Open API Economy

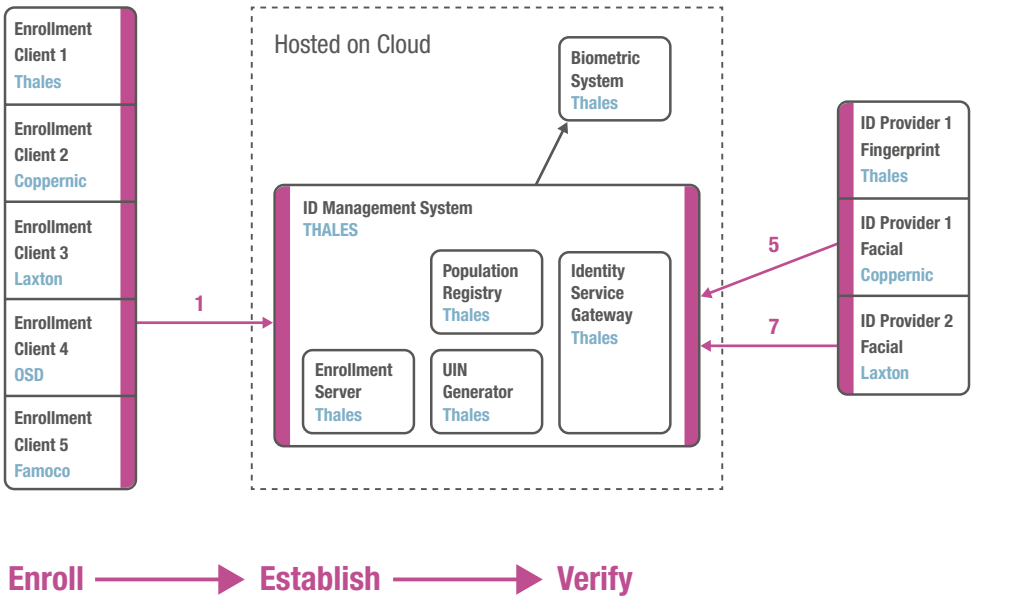
Open APIs are now major enablers of full scale digital transformation across both public and private sectors. Beginning in the early 2000s as internal initiatives within technology companies, Open APIs evolved rapidly as online eCommerce giants like Amazon recognized the opportunities of levering this approach to open up systems and data to their merchant base. Today, we see a wealth of exciting new initiatives – not least open banking – being driven by a ever-evolving Open API ecosystems. Now, as adoption of OSIA grows across the world, we are witnessing the rapid growth of an Open API ecosystem coaleccing around Identity Management – and though this, the ability to create truly inclusive and more efficient public services.

Interoperability Demo:

Use Case 2 – Unique Identity Registration & Verification

In this demo, a Government establishes a Unique Identity for a Citizen and opens services for Third Parties (Banks, Telcos etc.). to verify the identity of their Customers using Biometrics.

Watch video at https://secureidentityalliance.org/osia-ressources/osia-videos/entry/osia-use-case-2-unique-identity-registration-verification



API #	API reference
1	Create Enrollment
2	Generate UIN
3.a	Create Encounter
3.b	Create Person and Identity
4	Create Credential Request
5	Verify
6	Onboarding
7	Read Attributes Set

Enroll → Establish → Verify

8.
Qualification program

From Q4 2022, SIA is launching the OSIA global qualification program*, adjudicated by an independent body, GlobalPlatform who will maintain a list of all vendors and products that have been qualified as OSIA compliant.

The qualification scheme will support the growing number of government bodies that want to introduce OSIA qualification as a solution pre-requisite as part of their tendering process.

As part of this program, OSIA has developed a test plan** that will enable vendors to assess the performance of their products/solutions against OSIA specifications and confirm their solution is OSIA qualified.

* It is called a 'qualification program' and not a 'certification program' because in order to have a certification program as per ISO definition you need to have external labs acting as accreditation body (ie running the compliancy tests). In this case, there is no external accreditation body and the compliancy tests are run by each vendor with its preferred tool (self-evaluation) following the testing procedures as prescribed by GlobalPlatform.

** The test plan is freely available to SIA Members and Affiliated Members. Non-Members can purchase the test plan at www.osia.io.


Contact
Jean-Claude Perrin at:
Stephanie de Labrolle at:
More information at:
Follow us at:
Secure Identity Alliance

9.
OSIA Governance

GitHub community and license

OSIA is based on an open copyright and software license.

OSIA specifications are published on GitHub supervised by an external and independent consultant.

Any country, technology provider or individual is free to download the functional and technical specifications to implement in their foundational and sectoral ID systems.

Governments can also reference OSIA as Open Standards in tenders.

OSIA Working Group

Consists of public and private Members and Affiliated Members of the SIA.

The Working Group meets once a month to manage the evolution of all OSIA functional and technical specifications. It also solicits feedback from the GitHub Open Community and has the power to accept or reject code contributions proposed by members and third parties and to control releases.

OSIA Advisory Committee

Consists of government and academic Affiliated Members of the SIA.

The Advisory Committee meets twice a year to review the progress of OSIA and provide strategic guidance for the initiative.

OSIA: Promoting open and transparent government-industry collaborations

Enabling the all-important government-industry collaborations needed to create the frameworks that make it possible to build truly open, innovative and future-proofed national ID systems, OSIA is transforming how governments leverage ID to deliver real-world impacts for their citizens and national economies.

Where to find OSIA specifications

OSIA GITHUB PAGE
https://github.com/SecureIdentityAlliance/osia

OSIA DOCUMENT
https://osia.readthedocs.io/en/latest/

www.osia.io