SECURE
IDENTITY
ALLIANCE

Putting government back in control

Solving vendor lock-in with open standards

Executive Summary

Target 16.9 of the UN Sustainable Development Goals is to “provide legal identity for all, including birth registration” by the year 2030. But there’s a major barrier: the lack of vendor/provider and technology neutrality – commonly known as “lock-in”.

In the search of an answer, two approaches have evolved to help governments gain the freedom they desire. One approach – open standards – offers a pragmatic solution to solving the problem today. The other – open source – does not. Instead, this latter approach adds unnecessary levels of complexity, potentially higher costs of ownership and significant deployment delays by taking development down to the atomic level.

The Secure Identity Alliance and its members are convinced that if all stakeholders come together around the open standards table, the identity community can chart a simple way forward that strengthens identification systems, supports development and empowers individuals.

Uncovering dependency in ID systems

Trusted, legal identity is the lynchpin of today's national security, social protection and economic growth strategies. It is a matter of sovereignty, and the role of a resilient, flexible and sustainable identity ecosystem cannot be underestimated. Therefore, governments must be able to evolve, adapt, and add to their systems. And be free to choose the most appropriate solutions and partners to meet their needs.

All too often, however, rapid market evolution and a lack of standards and regulations mean national ID ecosystems have developed in silos, on proprietary technologies from multiple technology partners. Incompatible registries struggle to "talk" to one another and cannot easily be replaced with those from other vendors. This all creates a challenging operating environment in which the threat of partner dependency is very real.

At the 2018 Annual Meeting of the ID4Africa Movement, a poll of the delegates identified the lack of provider and technology neutrality as the biggest concern among those tasked with implementing national identification systems. Respondents said they felt handcuffed by their solution provider. In short, members feel "locked in" to existing providers and unable to take advantage of innovation or choose the most appropriate solution because the costs and risks of doing so are prohibitive.

The World Bank agrees. One of a number of global organizations that lists lock-in as an obstacle to development in the digital age, saying it can "increase costs and reduce flexibility to accommodate changes over time". Yet, although these and other international development agencies have identified the issue, it has yet to be clearly defined and examined.

The problem has many root causes, and manifests itself in many ways. In order to solve lock-in, we must first understand exactly what it means to be reliant on single or multiple partners. Which is exactly what we will explore here.

Understanding the problem of dependency

As the identity market matures, new technologies are drastically redefining the identity landscape. Digital solutions, sophisticated biometrics, cloud computing, and more has made it possible to develop integrated national ID ecosystems that are efficient, cost-effective and secure.

The lack of partner and technology neutrality and its consequences becomes apparent when a customer needs to replace one component of the ID ecosystem with one from another provider, or expand the scope of their solution by linking to new components.

For many policy makers, starting from scratch isn't an option. Systems are already in place and being utilized by agencies and citizens. To change is to invite considerable cost. Not to mention significant risk of operational failures. At the same time, to benefit from the latest technologies, governments need to update, adapt, and add to their systems. And be free to choose the most appropriate solutions to meet their needs. The identity marketplace does not currently offer this flexibility and freedom.

Considering the very real operational risks caused by inflexible infrastructures and provider dependency – both in terms of compatibility problems with upgrades, and the ability to maintain operational continuity as solutions are migrated and/or hot swapped – throwing money at the problem is neither a guarantee of success nor a practical reality. It's time to address the problem with a real-world, pragmatic open standards approach.

Root causes of dependency

As we see from Figure 1, we can largely break down the challenges into three key areas: technology, people and process. The major barriers are technical, of course – in terms of incompatible proprietary technologies and data portability, but other issues remain and need to be addressed.

TECHNOLOGY →	Interoperability	Data portability
PEOPLE →	Human resources	Decentralized government oversight
PROCESS →	Contractual Commitments	

FIGURE 1:
Root cause of dependency

Lock-in is seen as the biggest concern among those tasked with implementing national identification systems.

Barriers to change

Technology barriers to change

Interoperability

This is a challenge of two parts: architecture and interconnection. Many components of ID ecosystems (civil registry, population registry, biometric identification system etc.) are functionally incompatible with those made by a different provider because they are not designed based on a common definition/understanding of broader functionalities and scope. Furthermore, many components are unable to communicate with each other due to lack of standardized interfaces (APIs).

- **Architecture**
  The fundamental issue at the heart of interoperability is the fact that solution architectures are not interoperable by design. The lack of common definitions as to the overall scope of an ID ecosystem, as well as in the main functionalities of a system's components as described above, blurs the lines between components and leads to inconsistencies. This lack of so-called irreducibly modular architectures makes it difficult, if not impossible, to switch to a third-party component intended to provide the same function and leads to incompatibilities when adding a new component to an existing ecosystem. If providers developed these components based on standards that defined their scope and functionalities, switching to a third-party component would present no obstacle at all. It would be as simple as swapping out one module for another commercially available equivalent one.

- **Interconnection**
  The second part of the interoperability puzzle is the absence of standardized interfaces (APIs). Components are often unable to communicate with each other due to varying interfaces (APIs), making it difficult to swap out components or add new ones to the system. In order to comply with the existing interfaces and connect the new component, additional programming and other modifications may be required. In some cases, a new interface (API) must be developed, often with considerable time and effort. And there is no guarantee the two components will talk to each other.

Data portability

Data portability is key here too. Every provider defines and manages their data differently. The ability to export data from one system in a way that is useful to another system is arguably the most complex cause of dependency. It is also vitally important because in most cases it would be extremely costly to replace lost data.

Many factors must be considered, including:

- **Data availability**
  In order to be portable, data first needs to be available. Lack of access to data not only makes migration impossible, it also makes it extremely difficult to customize, modify or enlarge the scope of a particular component or the ecosystem as a whole. This would mean that only the original developer of the component or system will be able to develop the new function. For example, if the new provider has to deal with encrypted biometric templates, it would need to access the raw biometric images to re-calculate those templates. If those raw images are not available, they will be forced to re-register the entire population.

- **Data format**
  Because every provider does things differently, and due to a lack of international standards, data is often stored in formats that make portability difficult. For example, dates may be stored as dd/mm/yy or mm/dd/yy. Alternatively, one provider may use an open source automated biometric identification system (ABIS) that encodes the templates using a proprietary format. Because that format is not standardized, it will not be easy for another to use it.

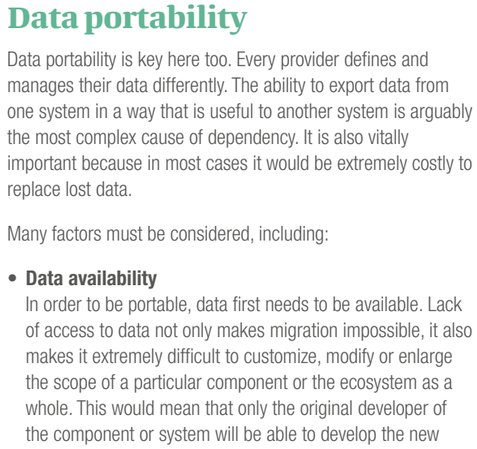


FIGURE 2:
Not all data models are equal. Migrating from B to A may work, but from A to B would present a problem. (P=person; P1=mother; P2=father; K=relationship)

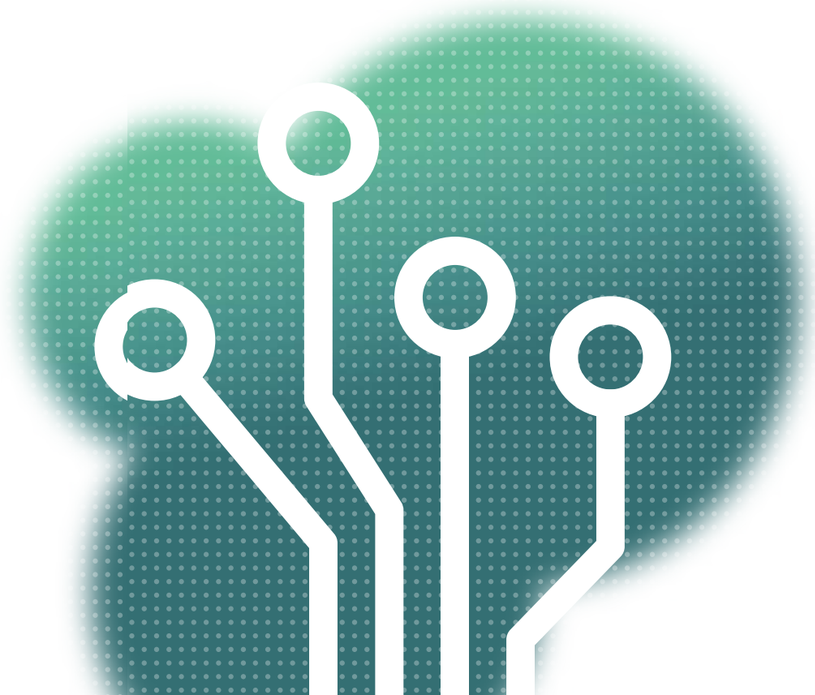
- **Data model**
  Portability between two systems that manage data differently can give programmers a real headache and lead to high costs. That's because data models define the following:

  - Data structure
  Two systems based on two different data models can also present problems. In these cases, migration in one direction may be relatively unproblematic, but the other would require additional effort (see Figure 2).

  - Entities
  If the defined entities do not exist in both models, it's difficult to map them from one model to the other.

  - Data fields
  If the fields are not the same, data might be lost in migration. For instance, one model dedicates four fields to the surname while the other only has two dedicated fields.

- **Data encryption**
  Encrypted data requires a decryption key, without which you cannot migrate the data. The key needs to be easily accessible and readily available. This is not always the case especially when a government does not hold the key and is trying to replace a solution provider who manages it.



People barriers to change

Human resources

Sometimes referred to as human resource knowledge risk, the time and effort needed to train personnel and/or add additional resources may also create dependencies and make the risk of change too high. Teams that have worked with a single system for some time have likely gained valuable expertise. Ramping up their knowledge and skills to operate and/or maintain the new system as efficiently as the old one will cost both time and money.

Decentralized government oversight

The lack of centralized management of a country's ID ecosystem creates an overwhelming bureaucratic hurdle, fueling the perception that change is impossible. Many functional registries are run by separate, sometimes competing ministries and government agencies. Because many of these ministries and agencies have had little contact, each has developed the systems documents separately. This reality has helped contribute to the highly diverse and disconnected ID ecosystems we find today, with multiple functional systems provided by multiple providers.

Process barriers to change

Contractual commitments

Governments can find themselves unable to make changes to their systems without incurring additional costs due a range to contractual constraints as changes may be outside the scope of the original contract. Similarly, contractual terms and conditions may also preclude integrating third-party systems or stipulate access rights to only certain parts of the system.

Finding the solution to lock-in

In defining a new approach, it's also important to think about what policy makers and implementers actually want. Here, the discussion is less about technology and integrations, but rather one of value.

Governments want to be free to choose the best approaches and partners that suit their use case and commercial model. They want to be able to deploy systems, upgrades and add-ons as cost effectively as possible, and with the minimum levels of operational risk. And they want to embed agility and flexibility from the core to the edge to ensure the ability to evolve their ID systems to adapt to changing needs.

Just as importantly, policy makers and project leaders within government need to get their new or evolved systems and/or components online and in use as quickly as possible.

Ultimately, the value for customers is not in the technology approach, the registries or the data but in what they actually enable – be that secure borders, fair and democratic voting, social inclusion, ability to achieve the UN's 2030 birth registration targets and so on. If being dependent on technology providers, integration partners or other third parties prevents these outcomes then things must change. And indeed they are.

Today, we see two competing approaches that rethink the lock-in issue. One is based on open standards, the other on open source technology. It is the belief of the Secure Identity Alliance and its members that only one approach, that based on open standards, can deliver in the real-world against the success criteria above. And do so today.

Indeed, it is precisely because of the potential to directly and swiftly address technology and partner dependency that the world's biggest ID providers have taken the unprecedented move of coming together to drive an open standards approach through the Secure Identity Alliance's Open API initiative.

Lego building Blocks. An analogy.

At its most basic level, an open, extensible and flexible ID infrastructure is built on a series of components that seamlessly interconnect and interact to create the whole. As they evolve, more components are added. Just as a child would craft a Lego model.

Because of the uniformity of the connecting elements of the Lego brick, other bricks from other Lego sets can be added and complex structures built. All the while remaining connected and stable. This is the Open Standards approach. The 'bricks' are already available in the form of market-proven modules – including civil registry, population registry and a host of functional registries for managing vehicle registration, passports, voter rolls and so on. All that's needed is the standardized Open API and commitment of the industry (already gained from the market leaders) to ensure its modules adhere to it.

It is not required, for example, for each Lego user to craft their own individual bricks. This would take time, raw materials, design plans and a manufacturing process. Even then, they couldn't be certain of the accuracy of the connections and the corresponding viability of the final structure. Plus, their bespoke bricks may not be able to connect with those made by other enthusiasts.

This is essentially the challenge of the open source approach. To combat lock-in governments don't need to go to an atomic level and build the bricks. This isn't where the problem lies. Governments simply want the freedom to swap in and out, and connect, the modules (or bricks) they want, from the partners they choose. And they should have it.

Why rebuild the bricks, when the bricks aren't the problem?

Contrasting the different approaches

Let's begin with this stark contrast highlighted in the Lego analogy. An open standards approach utilizes existing modules and components from existing ID technology providers, and uses an Open API to enable the information interchange. Quite apart from the fact that these field-proven modules encapsulate decades of expertise from trusted partners, there is nothing to build. The modules are available on the market today.

In contrast, the open source approach requires customers to go down to the source code (of non-standardized components), only to build them up again. The result is a set of proprietary components that still won't interact without creating standardized interfaces. While customers may arrive at an effective solution, the design, planning, development and testing, and integration could take years.

Better surely to short-cut the process and focus on developing the interface to existing, proven components and modules.

Added to which, in the open source model the customer carries the risk – in design and deployment, through compatibility and interoperability with existing ID infrastructures, to compliance with security and data protection regulations and more.
In the open standards approach, all the necessary due diligence to bring components to market has been completed (as modules exist) so the risks (such as they are) are carried by the technology provider.

That is not to say there is no value in open source. Quite the reverse, many of today's ID modules and components include open source code. The issue is whether an open source approach is an appropriate platform on which to build and manage an entire identity infrastructure. While public access to the code may encourage open collaboration, it also asks difficult security questions about whether access opens up sovereign ID resource to cyberterrorism and state-sponsored cyberattack.

In a connected point, the size and enthusiasm of any open source community directly impacts its success. To date, the ID open source community and surrounding ecosystem appears limited. It is also impossible to gauge its likely longevity at this stage of its infancy. In contrast, today's ID technology providers are multi-billion-dollar organizations whose business models, R&D investments, product road maps and customer base are built for longevity and future success.

Indeed, perhaps ironically, should the open source community fail to gather momentum, customers are at risk from being locked-in to a small number of systems integrators.

Then, of course, there is the issue of cost. Typically, open source licenses are free – although this depends on the licensing model. However, while the upfront cost may be zero, it will be important for potential customers to thoroughly examine cost of ownership. Certainly, there will be significant resource costs associated with taking code through to production environments and to support this complex code, and in terms of overall systems maintenance. Again, because of the immaturity of the community, it is difficult to get a clear view.

Ultimately, if we assume the purpose of open source is to deliver the kind of flexibility, extensibility and agility customers require, it seems a little strange that they also risk being locked-in to the technology upon which their 'open' solution will be built. Of course, as the market evolves there may be many open source solutions on the market. But gambling your sovereign identity infrastructure on what is today an immature community of localized contributors is a major risk to take.

The open standards approach, on the other hand, simply allows customers to choose any of the components already on the market, from any technology provider. So long as it suits their needs. It is, without a doubt, the lowest risk solution.

A deeper dive into open standards

Overall, open standards create a framework for developers by defining the components of a system and how they interact with each other. That can also help customers define their requirements and ensure providers deliver what they need. Furthermore, open standards don't have to involve core technology, meaning technology providers can protect their intellectual property and differentiate themselves from the competition, which drives innovation.

For example, they could standardize an interface layer, such as the Open API, that allows communication between components. And they could define data formats and attributes, in order to enable access to raw data and portability while maintaining trade secrets (e.g. biometric algorithms) and thus competitive edge. This is important for competition and innovation. Technology providers will continue to push the technological envelope in order to gain market share.

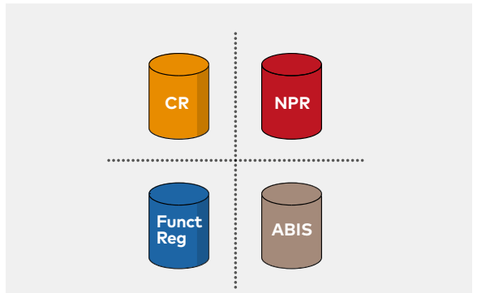


FIGURE 3:
Current ID landscape with fragmented silos.

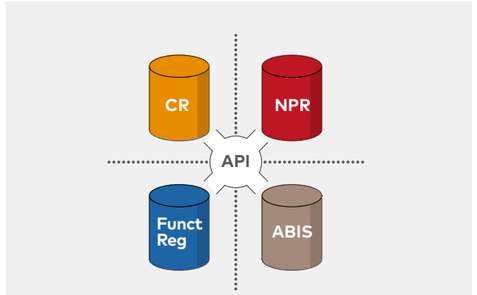


FIGURE 4:
An integrated ID landscape based on open standards and APIs.

Standards also reduce the complexity of updating older systems in the future. By standardizing what components make up a system and how they communicate, systems become more agile and agnostic. This leads to provider and technology neutrality and provides the flexibility to plug in the best solutions to meet specific needs.

In this approach governments will be at a lower risk of contractual lock-in because patents and other proprietary issues no longer stand in the way. Training human resources and replacing hardware will be less complex or costly. The politics of integrating national ID ecosystems will no longer be frustrated by technical road blocks. And the risk of making the wrong decision based on misunderstandings or misperceptions becomes less of an issue because open standards make systems more agile and adaptable.

One of the challenges will be ensuring that the defined set of components covers the entire ID ecosystem. Otherwise we run the risk of making only parts of the ecosystem interoperable while leaving entire blocks of components susceptible to dependency.

Ultimately, an open standards approach allows governments to strategically plan and evolve their systems without fear of future compatibility issues – providing a guarantee of consistency and harmonization across government identity ecosystems. They can invest with confidence – accelerating the development of robust identification platforms for citizens, while preserving the value of existing investments.

The Open API Initiative

By injecting new levels of flexibility and openness, the Open API initiative enables governments to exert full control over their sovereign identity systems. It has been developed based on three core principles:

1. 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 components of the identity ecosystem to use, and how to combine them.

2. Technology Neutrality

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

3. Privacy by Design

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

Launched in mid 2018, the project is already well advanced. Secure Identity Alliance members are implementing the Open API across their component portfolios. Work is continuing through an open, collaborative and consensus-driven process.

An elegant solution to a complex problem, the Open API initiative provides a simple, open standards-based connectivity layer between all key components and systems within the identity ecosystem. So everything works together seamlessly.

The first step has been to formalize definitions, scope and main functionalities of each component to within the identity ecosystem, as we see below in Figure 5.

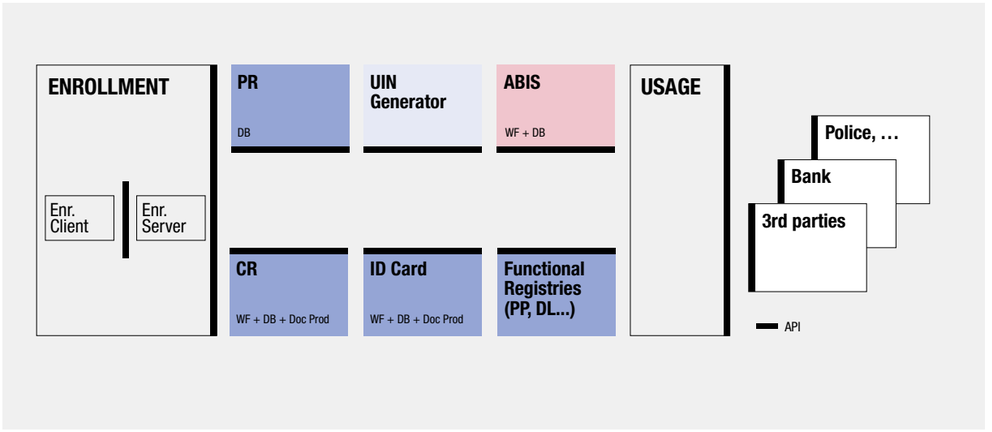


FIGURE 5:
Components forming an identity ecosystem

The Open API Initiative Continued

The second step has been to create a standardized open interface. This core piece of work develops the standardized data formats and open interface to connect the multiple ecosystem components to ensure seamless interaction of services in figure 6.

	ID ECOSYSTEM COMPONENTS							
SERVICES	Enroll	PR	UIN gen.	ABIS	CR	ID Card	Funct. Reg	Usage
Notification								
Notify event		U			U			
Subscribe		U		U	U	U	U	
Unsubscribe		U		U	U	U	U	
Event callback		I		I	I	I	I	
UIN Management								
Generate UIN		U	I		U	U		
Data Access								
Get Person Attributes	U	IU		U	IU	U	U	U
Match Person Attributes		IU			IU	U	U	U
Verify Person Attributes		IU			IU	U	U	U
Get Person UIN	U	IU			IU	U	U	
Get document		IU			IU			
Biometrics								
Verify	U			I		U	U	U
Identify	U			I		U	U	U
Insert		U		I		U		
Read		U		I		U	U	U
Update		U		I		U		
Delete		U		I		U		
Get Gallery		U		I		U	U	
Get Gallery content		U		I		U	U	
3rd parties services								
Verify ID								I
Identify ID								I
Get Attributes								I
Get Attributes set								I

FIGURE 6:
List of services the Open API will interface with. (I) indicates the components implementing the services defined and (U) indicates the components using the services

The Open API initiative is vendor and technology neutral. It protects investments today and tomorrow, and forever eliminates issues of supplier dependency. With Open API governments are free to select the components they need, from the suppliers they choose – without fear of lock in.

And because the Open API operates at the interface layer, interoperability is assured without the need to rearchitect environments or rebuild solutions from the ground up. Components are simply swapped in and out as the use case demands – from best-of-breed options already available on the market.

This real-world approach dramatically reduces operational and financial risk, increases the effectiveness of existing identity ecosystems, and rapidly moves government initiatives from proof of concept to live environments.

Governance Overview

The Open API initiative is developed by the not-for-profit Secure Identity Alliance (SIA) with the full support of its membership. It is governed under a formal structure including an independent Open API Advisory Board, with work carried out by the Open API GitHub Community and Open API Workgroup. These bodies have transparent and publicly available terms of reference to guide intra and inter committee relations.

Any country, technology partner or individual is free to download the functional and technical specifications to implement it in their customized foundational and sectoral ID systems or components. Governments can also reference the API as Open Standards in tenders.

More information, and guidance on how to contribute to the Open API initiative, can be found at the GitHub landing page, https://secureidentityalliance.github.io/opensourceapi.html.

All contributions from the wider identity community are warmly welcomed.

INITIATIVE LAUNCH:

June 2018

TECHNICAL TIMELINE:

- **Build Start**
  Sept 2018
- **API v1.0 (CR/PR/ID Card reg.)**
  Dec 2018
- **API v.1.1 (functional registries)**
  April 2019
- **API v2.0 (ABIS)**
  June 2019
- **API v3.0 (enrollment and KYC)**
  Sept 2019

GOVERNANCE TIMELINE:

- **Invitation for contributions from the worldwide ID community**
  Sept 2018
- **Stakeholder engagement**
  from Oct 2018 to Sept 2019

- **Information meeting at ID4Africa**
  Thursday 20th June 2019 from 11.00 to 12.00

- **First meeting of Open API Initiative Advisory Board**
  Nov 2019

SECURE IDENTITY ALLIANCE

About the Secure Identity Alliance

An expert and globally recognized not-for-profit global body, the Secure Identity Alliance brings together public, private and non-government organizations to foster international collaboration, shape policy and provide guidance on the key issues of legal identity.

With 85% of the world's population covered by identity-based applications from members, the Secure Identity Alliance is a trusted partner to work with governments, private organizations and third-party stakeholder to support the global adoption of the Open API initiative.

The Secure Identity Alliance Members include DeLaRue, Gemalto, IDEMIA, INGroupe, Veridos, Keesing Technologies (Group Surys), Entrust Datacard and Vision Box. To see the list of companies who have joined the Secure Identity Alliance Open API Initiative, go to: www.secureidentityalliance.org.

The Secure Identity Alliance Member heritage

- Experience in over 190 countries
- Over 25000 scientists, experts and professionals
- Developed the key ID related technologies in use today
- Participated in the development of the over 1000 ID related standards in use

Policies and bodies supported

- UN's 2030 Agenda for Sustainable Development
- World Bank Group Identification for Development (ID4D) Program's "Principles on Identification for Sustainable Development: Toward the Digital Age"
- Charter of Fundamental Rights of the European Union
- ID4Africa and its Identity Council