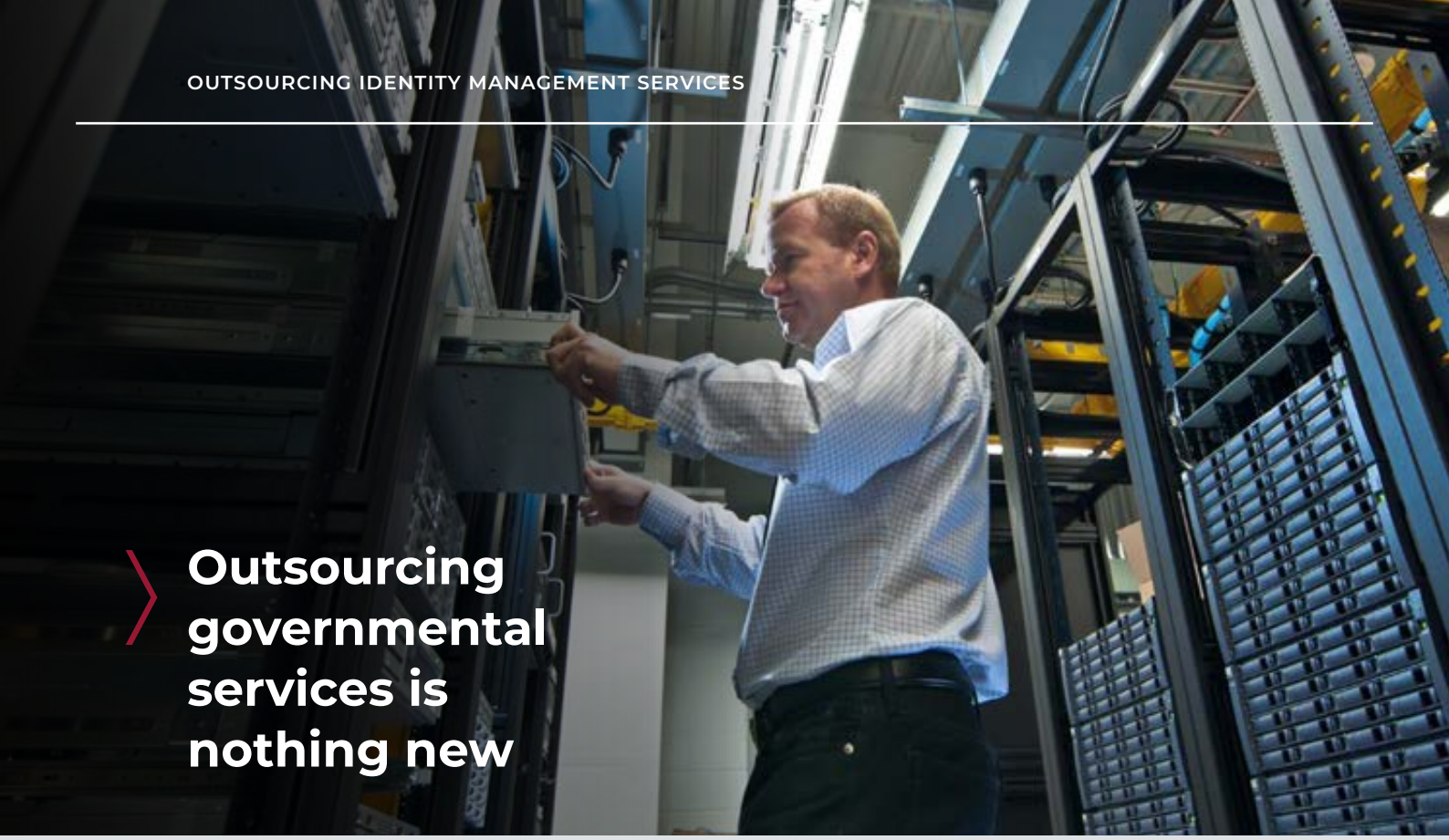
WHITE PAPER

IDEMIA
SMART
IDENTITY

Outsourcing identity management services

Benefits and key success factors



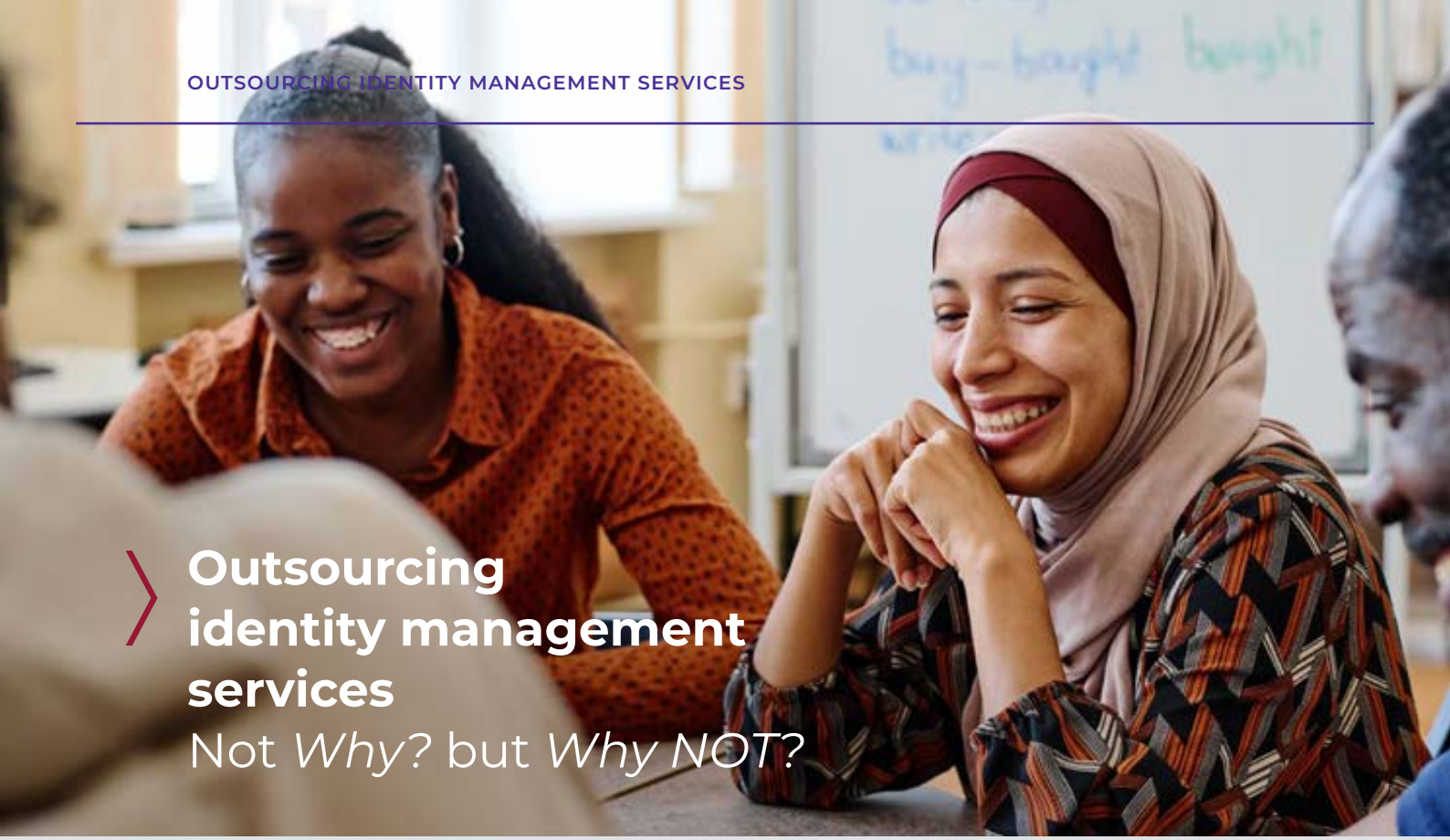
Outsourcing governmental services is nothing new

Governments around the world have increasingly turned to outsourcing various services to the private sector as a strategic approach to enhance efficiency, reduce operational costs, and leverage specialized expertise.

By partnering with private companies, public institutions can focus on their core responsibilities while benefiting from innovation and cutting-edge technology. This trend is evident across multiple sectors, where governments have sought private sector support to improve service delivery, achieve higher productivity, and meet the evolving needs of citizens.

A notable example is the UK's National Health Service (NHS), which has outsourced non-clinical services, such as IT infrastructure, facilities management, and even medical equipment procurement, to streamline operations and reduce administrative burdens. In Australia, the government has outsourced large-scale infrastructure projects, such as toll road construction and public transportation systems, to private sector companies to ensure timely completion and advanced engineering solutions. Meanwhile, in India, the government has partnered with private firms for digital transformation initiatives, such as the Aadhaar project, a massive biometric identification system aimed at delivering efficient public services to millions of citizens.

These examples demonstrate that governments outsource not only to achieve cost savings but also to access private sector expertise that drives innovation and improves public service delivery. Whether it is large-scale infrastructure projects, IT services, or even identity management, the private sector's ability to bring specialized skills and resources to the table has proven essential in enabling governments to meet the growing demands of modern governance.



Outsourcing identity management services

Not *Why?* but *Why NOT?*

In light of the benefits of outsourcing government services to the private sector, it is almost surprising not to see more governments going down this path. Services provided by the government and agencies hinge on the capacity to reliably prove everyone's identity. Therefore, building and sustaining an efficient national identity framework is a fundamental mission of the state. It contributes to state security, economic development, and social cohesion.

Poor identity systems lead to a number of major issues: individuals missing or being denied social benefits or access to the most primary private services, such as opening a bank account. Such flawed identity systems also provide fraudsters with ways to exploit and abuse citizens' rights, generating extra expenditure for the state or extra costs and losses for a private entity. Moreover, mediocre identity documents, and the lack of tools to verify identities, facilitate the creation of false identities and identity theft that most often underpin financial fraud, as well as, in the worst case, terrorism and other serious forms of criminal activity; this also undermines border and citizenship controls and is highly detrimental to the protection of privacy.

WHEN IT COMES TO IDENTITY MANAGEMENT SYSTEMS, THE QUESTION TO ASK IS NOT "WHY?" BUT "WHY NOT?" OUTSOURCE.

Benefits of outsourcing identity management services

The benefits of outsourcing identity management services are as plenty as the initial motivational factors for considering this option. Often, the drive to outsource is embedded in the culture of the nation.

Benefiting from specialized skills and cutting-edge technology

Setting up and running an efficient identity framework requires multiple skills in the fields of large project management and IT integration. An identity management infrastructure encompasses so much more than "just" the production of secure physical credentials. The accompanying systems need to be interoperable and modular to seamlessly integrate with already existing systems, if they are used. Compliance with international standards for both physical and digital credentials, as well as the systems, especially when it comes to biometrics, is a must and requires an in-depth understanding of the local and international legal and regulatory framework.

Using the right private partner ensures the expertise and the technical solutions are the most up to date for the optimum outcome for both the government and its citizens.

Sharing risks

If a public entity wanted to meet the challenge of setting up a modern identity system on its own, it would face a number of risks (technical, operational, and financial). Depending on the exact contractual setup (see section on public-private partnerships), the public entity still has to meet the challenge; however, it has the advantage of transferring part of the risk to its private partner – in particular, the financial and operating risks.

The table below presents generic risk ownership between public and private partners in the framework of identity programs.

Risk type	Public entity	Private entity	Risk description
Design and implementation		●	Inadequate design, obsolete or inappropriate technology, cost overrun, program delay, inadequate quality control
Operation and maintenance		●	Cost-efficiency, workload fluctuation, inadequacy and high turnover of human resources, increase in energy and material prices, deterioration or depreciation of assets, process failure, material defects or site security
Transfer	●		Risks based on the transfer of assets, inventory, human resources, and know-how for running operations
Market		●	Securing the source of revenue, setting up the right pricing; ensuring that actual demand will reach demand expectations set in the business plan
Financial		●	Cost of capital, interest rates, and cash flow management
Compliance	●	●	Compliance with certain standards, like security-related ISO 27001 or other international standards
Legal and regulatory	●		Legal and regulatory risks
Political	●		Long-term stable political environment for the PPP task force to operate in

Enhancing citizen service and transferring knowledge

For several reasons, including budgetary constraints, public organizations often lack adequate resources and are already overwhelmed by the existing workload and administrative burden. With new processes, procedures, and citizens' demands as part of a modern identity system, the existing staff might struggle to offer the service the citizens expect. A private entity offering the necessary services on behalf of the government would not only lead to improved citizen service in terms of quality and speed of delivery but also, to some extent, ensure knowledge transfer and direct or indirect training of governmental staff.

Gaining funding

An identity management system is a long-term and large-scale project that requires substantial upfront investment, as well as continuous expenditure in maintenance and upgrades over time. Partnering with a private provider means launching such a project with minimal impact on the public budget.

Furthermore, in the case of public-private partnerships (PPP), the public entity would only have to cover the expenses related to the PPP task force and the partner selection process.

FOCUS REMAINS ON THE GOVERNMENT'S CORE MISSION

Whatever the setup or the extent of the outsourcing of identity management services, what should remain in the hands of the government is the “custodian mission” of identity management: the final confirmation of the identity of a person by a government official. The private entity always only operates on behalf of the government and must be in compliance with the applicable legislation and regulation in place. It is the public entity who owns the project and remains closely involved in its setup and achievement of milestones.

A special formula
Public-private partnerships

There are several options available to a government for financing nationwide projects such as an identity management framework, one option being the PPP. In fact, for over 40 years now, PPPs have emerged in all kinds of public sector activities, enabling the private sector to invest in transportation and telecommunication infrastructures, the utilities sector, education, and health projects, as well as in identity management programs.

By definition, a public-private partnership is a contractual relationship between a public sector organization and a private entity. The most common model of PPP in identity management is the concession.

In such cases, the government would grant a private company a contract to invest on its own to build the necessary infrastructure and then operate it for a certain period to recover the initial expense. It is thus an alternative to a more conventional approach where the public authority would procure, own the infrastructure, and then operate it on its own. The government should adopt a PPP approach when it is convinced that this type of model can deliver better value for money than the alternatives.

The benefits of a PPP are very similar to outsourcing identity management services under a different contractual agreement. However, when choosing a concession model, the additional gain is time. There are sometimes political deadlines, such as elections, that require projects to launch very quickly and to achieve results in a very short timeframe. In this case, PPPs accelerate project implementation and speed up the delivery of results.

A SPECIAL FORMULA: PUBLIC-PRIVATE PARTNERSHIPS

The concession model consists of three main phases in which the private partner focuses on the following aspects of the project:

1 Build

- Fund the project
- Specify, design, develop, and implement the identity management system and business processes
- Prepare facilities and infrastructure
- Deploy and validate the system
- Recruit and train resources to operate, administrate, and maintain

2 Operate

- Enrollment of citizens
- Identity database and service management
- Identity document production and personalization
- Delivery of documents
- Management of the entire lifecycle
- Maintenance of the overall system

3 Transfer

- Hand the system back to the public entity
- Train public operators and administrators

Key success factors

A combination of several different factors is required for the outsourcing of identity management services to be successful and deliver the appropriate outcomes.

First, the government should fully support the project and its stability in the long term, creating a legal framework that enables the private company to operate.

Second, there should be long-term demand for the service to ensure financial viability, sufficient profitability to attract investors to the project, and clear understanding and agreement on the program timeline.

In order to meet these conditions and ensure the technical and operational success of the project, choosing the right partner is crucial. Not only must the partner be able to demonstrate experience and skills, along with the ability to adapt them to specific local contexts, but also that it has the financial capability to support investments sustainably.

The role of the private entity

Experience and skills

A private company should be asked to provide strong references for similar projects. These are a good starting point for assessing a company's level of expertise and experience in conducting and operating an identity management project. Indeed, field experience and proven expertise in key identity technologies and business processes are good signs of the reliability of a company.

For example, implementing an identity management business process requires familiarity with privacy issues. Hence, the partner must demonstrate its ability to guarantee the protection of sensitive data. Best-in-class companies have a proven track record, with international quality standards and accreditations. Moreover, the private partner needs to ensure that the processing of identity data is strictly in line with the laws of the country.

Having qualified staff with a wealth of experience also makes a difference. An identity management project involves many different products and technologies that need to be adequately integrated to form the basis of a cohesive and efficient identity service. Integrating this variety of technological elements is a key challenge and could be the source of unforeseen costs generated by the need to interface heterogeneous systems from different vendors. Delays could also compromise the on-time delivery of a service if integration proves more difficult than planned.

A qualified workforce is not only conducive to efficient implementation and operation of the identity management system, taking in-the-field reality into account, but will also ensure that the transfer period of the contract runs smoothly, which is crucial to keeping the system operational and continuing service delivery.

Ultimately, it is important to build trust in the private partner, ensuring that it will meet the challenges involved in implementation, production, compliance, and quality of service.

KEY SUCCESS FACTORS

Financial capability

Depending on the contractual agreement, the private partner might be expected to come up with its own financial resources or a financial package to cover the project in whole (or in part), as it will be required to procure new assets, or renovate or upgrade existing ones.

The private partner must be able to prove the viability of the project. In order to do this, it is important to ensure that the partner's financial capability is sustainable, along with its ability to access funds and manage cash flows. The project's financial viability assessment should consider several elements, such as construction phase costs, repayment of debt, interest calculations, operating revenue and costs, tax, working capital, cash flow (source and use of funds), lenders' coverage ratios, and investors' returns.

The assessment should cover the whole period, from the initial development costs of the project right to the end of the contract, to ensure financial efficiency throughout the overall contract period.

KEY SUCCESS FACTORS

Understanding the specific local context and building up local partnerships

There is a third key element that needs to be taken into consideration. It is the partner's ability to deploy global practices that take pre-existing local conditions into account; that is, its ability to appreciate the uniqueness of local context and to adapt its way of running the business, its operations, and the proposed solution accordingly.

Some of these characteristics are:

Organizational

Being capable of building up a local structure and partnerships with local suppliers.

Recruiting local key talents to manage the concession and its partners.

Recruiting local people that speak the country's language to develop the local economy and ensure better customer service.

Providing a close support structure that will be reactive and ensure the best level of service.

Operational

Adapting to the local topography of the country, the level of urbanization/ rurality, and its network infrastructure to set up the right means to deliver the service to all citizens.

Adapting to the culture of the country—for example, modifying the enrollment procedure to specific laws or common cultural habits.

Taking into account seasonal effects—for example, a peak in the demand for passports in the run-up to summer.

Learning from new local situations and continuously improving the process to make it more efficient, user-convenient, and secure.

Strategic

Planning mid-term developments and suggesting improvements based on the country's identity management strategy and citizens' feedback at the service level.

Supporting the government's strategy to deploy new services or expanding the scope (e.g., delivery of other types of identity documents).

The role of the public authority

While the selection of the right partner is important, the public sector also has an essential role to play afterward in order to create the right conditions for the private partner to invest and operate in the country. Below are five conditions falling within the role of the public entity that are conducive to the success of outsourcing identity management services.

Creating a contract focused on outputs

The public authority is in charge of setting the objectives and the outputs of the project. It has to keep in mind that the contract is for services and not for the procurement of assets or goods and, as such, should trust its partner to implement what is needed to deliver the service. Therefore, the contract must focus on outputs in terms of results and levels of service expected (e.g., production capacity, system availability, document delivery).

If the objectives are poorly defined, they will compromise the ability of the private partner to provide a quality service or may undermine the financial analysis of the project.

Setting the legal framework

A trusted identity requires a solid ecosystem and widespread infrastructure, and, given the risks inherent in not having trusted identities, the responsibility of providing a trusted identity can only lie with the state. The legal framework that grants and limits the roles and responsibilities of each party needs to be clearly defined in law.

Setting the appropriate legislative framework that will regulate the service is necessary to acknowledge the responsibility of the parties involved in the project and ensure usage of the service and its operating conditions. Such a framework is also important to provide sufficient protection to both parties concerning the evolution of economic conditions (inflation, exchange rate, etc.) in the long term.

KEY SUCCESS FACTORS

Sharing information of a country's specific context

Since the private partner must be able to anticipate its revenue to maintain its financial stability, the public party shall provide a reference framework, enabling the private party to forecast key metrics, such as the volume and usage of the civilian identity system. Also, it should provide information on local processes, regulations, and customs, so that the company may operate the system efficiently.

Facilitating the building of infrastructure

Building or furnishing the infrastructure is an important part of system implementation in the concession model. This is, in fact, a major cause of delay in identity projects, mainly because of logistical or administrative processes (e.g., construction permits). If necessary, the government should provide the means to facilitate setting up the infrastructure.

Furthermore, identifying and advising the private partner on potential threats (e.g., floods, earthquakes, political or criminal risks) is essential to the success of the project.

Communicating on the project

The citizen-oriented communication on the program, and the benefits provided by the program, must be carefully handled by the public entity. Indeed, the success of the project hinges on it being supported and adopted by citizens.

IDEMIA Smart Identity's expertise at your disposal

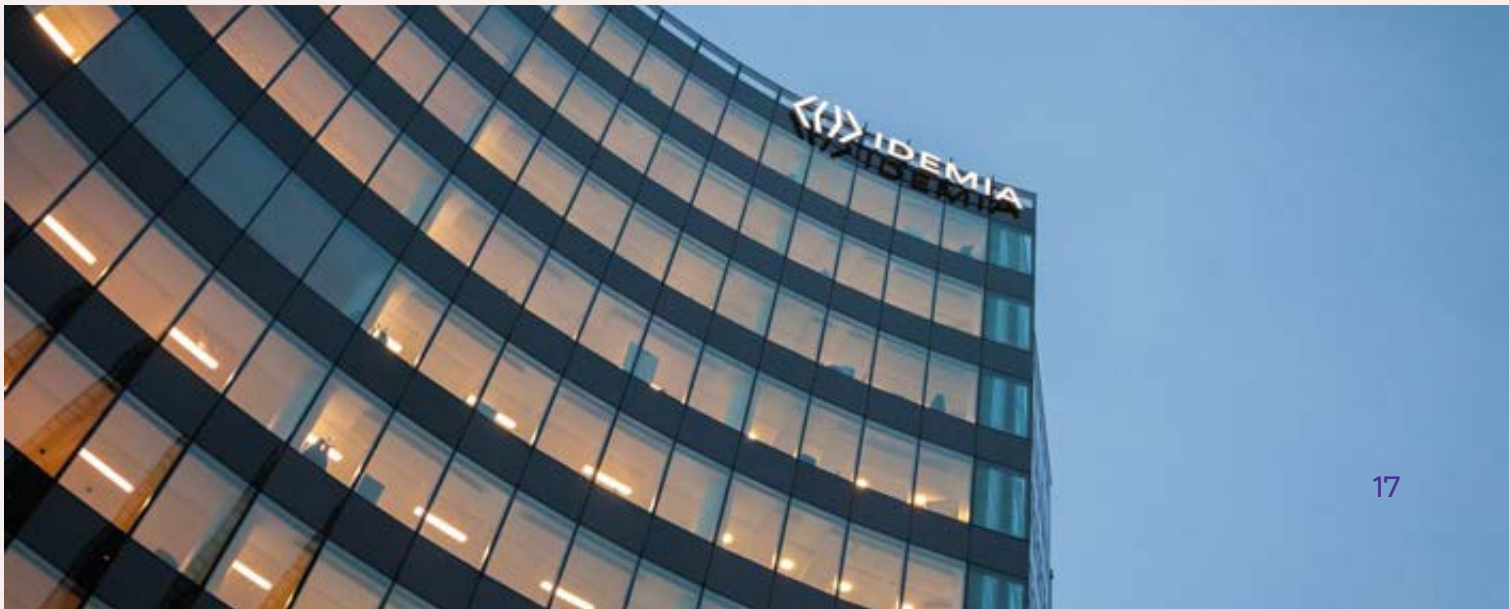
When partnering with a private entity on such a critical project like identity management, you want to be 100% sure of selecting the right partner. IDEMIA Smart Identity will convince you with:

Experienced staff that take in-the-field reality into account

Understanding local context, cultural differences, and strong local partnerships is not only critical to get the setup of the program right from the beginning but also essential for resourcing and training local staff and maintaining a high level of support throughout the lifetime of the contract. IDEMIA Smart Identity delivers global best practice in your local environment.

Proven project management skills

IDEMIA Smart Identity has a proven track record in dealing with complex project deployments to guarantee the work is done on time. With high-profile projects, you want to be sure that your partner delivers on time and within budget, and IDEMIA Smart Identity has been a successful partner of many governments globally.

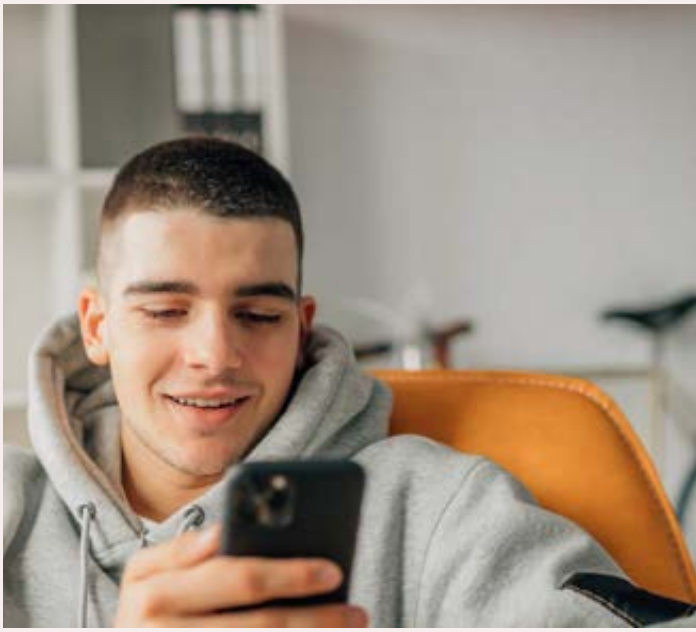


Privacy by Design at every level of our work

Data protection and privacy issues are the most sensitive topics when managing citizens' identities. IDEMIA Smart Identity delivers best-in-class technology that ensures your citizens' data is safe and international and country regulations are taken into account.

Data privacy has been integrated into our development process and IDEMIA Smart Identity's Global Security Policy. Security and Privacy by Design are implemented at both product and program level. Our technology is compliant with all relevant international quality standards and accreditations, specifically with the General Data Protection Regulation (GDPR) imposed by the EU.

GDPR compliance is demonstrated through a Data Privacy Impact Assessment (DPIA). When IDEMIA Smart Identity acts as a data processor or sub-processor, we work closely with our customers to ensure that GDPR obligations are included in the contractual commitments. At the beginning of each program, a GDPR assessment is performed. A data privacy risk assessment is undertaken and a DPIA is implemented. IDEMIA Smart Identity includes the purpose limitation and the principle of data minimization in the solution design. The data retention period is limited to the necessary minimum. The security measures defined in the DPIA are integrated into the program security plan, and the security test plan checks that the measures are effective. The DPIA will be regularly updated during the system's lifetime.



Proven financial capability

IDEMIA Smart Identity is a leading provider in identity management, with an annual revenue of over €400 million. IDEMIA Smart Identity's end-to-end offer ensures long-term growth and, with that, the financial stability needed for your project.

Strategic advice in the long term

With our longstanding expertise and global footprint, we will be able to assist you with forecasting needs for mid-term developments and suggest improvements based on your identity management strategy and citizens' feedback at the service level. If needed, we will advise you on deploying new services or expanding the scope (e.g., delivery of other types of identity documents).

CASE STUDY:

Modernizing Chile's identity management and document production system

THE CHALLENGE

In the early 2000s, the Republic of Chile made the very important decision to initiate modernization of its identification system. This included the digitization of its fingerprint records.

In 2009, Chile launched a new tender to modernize its identification system, incorporating a biometric engine of fingerprints and facial biometrics, as well as electronic identity and travel documents. The identity credentials were required to be made of polycarbonate material—modern, secure, and adhering to international standards.

The goals were straightforward:

1.
Modernize the procedures for capturing and managing data that identifies individuals.

2.
Provide citizens with new identity cards and passports with contactless chips.

3.
Implement a new Automated Fingerprint Identification System.

IDEMIA SMART IDENTITY'S SOLUTION

IDEMIA Smart Identity entered into a contract on the basis of a Build – Operate – Own model. IDEMIA Smart Identity created a local branch and then proceeded to implement two central sites, each one equipped with a datacenter and a document personalization center. In the datacenter, all citizens' biometrics (face and fingerprint) and biographical information are stored and processed. The personalization center deals with adding citizens' data onto their passports' data page or ID cards.

STRATEGIC ADVICE IN THE LONG TERM

Thanks to this program, the Chilean government could ensure that the solution was deployed in the shortest amount of time and with low impact on its budget. The main production site has a personalization infrastructure for a total throughput of 2,000 ID cards and 280 passports per hour. The central database can store more than 24 million identities and support up to 1,000,000 transactions a day. Enrollment times in Chile have been dramatically reduced. This significant time decrease was made possible thanks to the connectivity of the registration process and the optimization of the civil servant tasks.

According to the Henley Passport Index, the Chilean passport now ranks as the most powerful passport in Latin America. The biometric ePassport, along with Chile's remarkable economy, also enabled the country to be included in the US Visa Waiver Program.

CASE STUDY:

A modernized passport system for Mali

THE CHALLENGE

Before the end of the civil war and the reestablishment of the constitution in 2015, Mali's existing machine-readable passport did not comply with international standards. The document had little international credibility due to its low quality. Malians were vulnerable to identity fraud as tampering with passports was commonplace. Furthermore, Malians had to wait several months to receive their document. The Republic needed to modernize its setup and provide a secure high-tech solution.
Yet, financial means were hindering Mali's development.

IDEMIA SMART IDENTITY'S SOLUTION

The Build – Operate – Transfer agreement between IDEMIA Smart Identity and the Malian government led to the establishment of a subsidiary in Bamako. On behalf of the government, the subsidiary handled the creation of the central database and the setup of necessary infrastructure. Further local operations include back-end operations, personalization services, and additional support functions.

From the collection of citizens' payments to the registration and validation of applicants, IDEMIA Smart Identity offers an end-to-end solution.

THE OUTCOME

Over the course of the ten-year contract, the Malian government and its citizens benefited from:

approx. 180,000 passports produced and delivered to Malian citizens annually.

about 60 enrollment stations set up.

express passport delivery service in only 24 hours.

a standard delivery time of one to two weeks.

IDEMIA Smart Identity's solution also includes practical payment methods and passport delivery notifications via SMS.

CASE STUDY:

State-of-the-art ID document infrastructure at the cornerstone of the Republic of Albania's ambition

THE CHALLENGE

The Republic of Albania was looking for the most secure and modern ID system that would also serve as an additional argument for demonstrating the image of a modern democracy and supporting the country's strategic aspiration to strengthen relationships with both the EU and the USA. Being an EU member would facilitate its economic and cultural exchanges.

In 2008, the Albanian government signed a concession contract with IDEMIA Smart Identity for an end-to-end identity management solution, from the design and personalization to the management of citizen enrollment and identity document distribution.

STATE-OF-THE-ART ID DOCUMENT INFRASTRUCTURE AT THE CORNERSTONE OF THE REPUBLIC OF ALBANIA'S AMBITION

IDEMIA SMART IDENTITY'S SOLUTION

IDEMIA Smart Identity established a concession company, Aleat, in the record time of only five months, enabling citizens to vote in the June 2009 parliamentary elections with their ID documents in hand for the first time since 1991, recording one of the highest voter turnouts in the country's history. In the first half of 2009, 1.4 million ID cards were produced and delivered, with over 25,000 cards created daily at the height of the enrollment process. The partnership was such a tremendous success that the contract was renewed through to 2023. IDEMIA Smart Identity also delivered online identity services as part of its digital service initiative. This resulted in the creation of a secure platform that leverages eID cards, allowing citizens to access secure eServices.

THE OUTCOME

Thanks to the very high standard of the secure documents introduced, as well as the demonstrated integrity of the ID document issuance process implemented, the EU decided, in 2010 and only months after the Go-Live, to grant Albanian citizens holding a biometric passport the right to travel throughout the Schengen Area without a visa.

In 2011, for the same reasons, the USA decided to extend the validity of US-entry visas for Albanian citizens holding the new biometric passports to ten years.

Moreover, in 2011, Aleat, the concession company, was awarded ISO 27001 certification, proof of its dedication to maintaining the highest security standards with regard to handling the identity management business process and citizens' data.

During the course of the concession, additional services were implemented, such as registration at the embassies and delivery of refugee cards.

By 2024, IDEMIA Smart Identity handed over the whole infrastructure, the operational procedures, and the know-how to the Albanian government in the shortest amount of time, enabling the Albanian government to now run the project autonomously.

IDEMIA SMART IDENTITY

Unlock the world

Contact us to learn more:
smart.identity@idemia.com

IDEMIA GROUP

www. idemia.com