

End-to-end national ID card solution

Connecting physical documents
to digital identity services





1. Introduction

A trusted legal identity is the cornerstone of access to essential services and full civic participation. More than a simple ID card, it is a gateway to education, healthcare, financial services, and the exercise of fundamental rights. A secure identity allows individuals to prove who they are in both the physical and digital worlds, enabling governments and institutions to deliver services efficiently and fairly. To do so, they must provide a legal identity that is valid from birth and throughout each citizen's life. Despite major social and technological advances, 800 million people worldwide still lack an identity according to UNO in 2025.

At the same time, identity fraud remains a constant threat, making it crucial to provide solutions that are increasingly robust and secure.

At IN Groupe, it is our mission is to close this gap. By delivering reliable and secure identity solutions, we empower individuals to access their rights, support governments in strengthening their identity ecosystems, and help build the trust that underpins modern societies while combating fraud.

IN Groupe...

is front runner in developing tailor-made ID solutions. We provide expertise in the most advanced security features and applications on the market.

This guarantees citizens receive reliable documents that protect their personal and biometric data.

2. IN Groupe vision for a modern and trusted National Identity & Resident Permit program

At IN Groupe, we understand that the objective of governments is to implement a solution which is cost-effective and sustainable over time, but also tailored to the local needs and existing infrastructure. For that reason, we offer a modular and interoperable end-to-end ecosystem of software solutions, compliant with Open Standards Identity APIs (OSIA), biometric devices and robust ID cards, to securely set up, manage and materialise your population's identity.

THIS ECOSYSTEM IS BUILT ON EIGHT PILLARS

Biometric-based

Biometrics are unique, universal and verifiable, making them the most secure and convenient way to identify and authenticate individuals. They are captured through our enrolment solution, processed by our biometric recognition system, and securely stored in both the national database and the electronic component embedded in the ID card.

Available from birth

A national ID system should provide a secure and unique legal ID from birth that lasts throughout the citizen's life, enabling both physical and digital credentials.

Always up to date

Functional registries must be updated whenever a person's attributes change, with information automatically shared across all registries linked to the foundational ID. For ID cards, our JPatch solution enables secure remote updates of the operating system embedded into the OS, even after issuance, without recalling or replacing cards. This allows patches to address new vulnerabilities or regulatory changes.

Modular

The system's components should be selected based on the needs of your country and existing infrastructures. It should allow upgrades or change of specific components without having to replace the entire system.

Secure

A national ID system must be secured to protect citizens' personal data, prevent identity theft, maintain trust in public services, block counterfeiting or fraud for cards and cyberattacks for system, and ensure that sensitive information is neither manipulated, stolen, nor misused for malicious or illegal purposes.

Easy to use

A modern national ID system must be convenient for citizens (pre-enrolment, appointment booking, VIP services, etc.) and efficient for government operators (investigation and administration, credential management, post issuance, etc.).

Open standards-based

Open standards ensure interoperability, enabling governments to plan and evolve their ID systems while maintaining consistency across the ecosystem. Initiatives such as OSIA promote standardised interfaces to simplify integration, accelerate deployment and increase choice.

Digital-native

Trust is key for the adoption of digital identity by citizens and service providers. Only governments can provide the highest level of confidence when creating digital identities—based on a pre-existing national database and/or state-issued ID documents.

3. National identity end-to-end solution

We provide secure documents, systems and services covering the entire identity value chain. Whether customers require specific components or a complete end-to-end solution, we deliver a seamless, efficient, and secure identity ecosystem. As a trusted partner, we manage technological complexities and financial considerations, ensuring smooth operations and peace of mind.

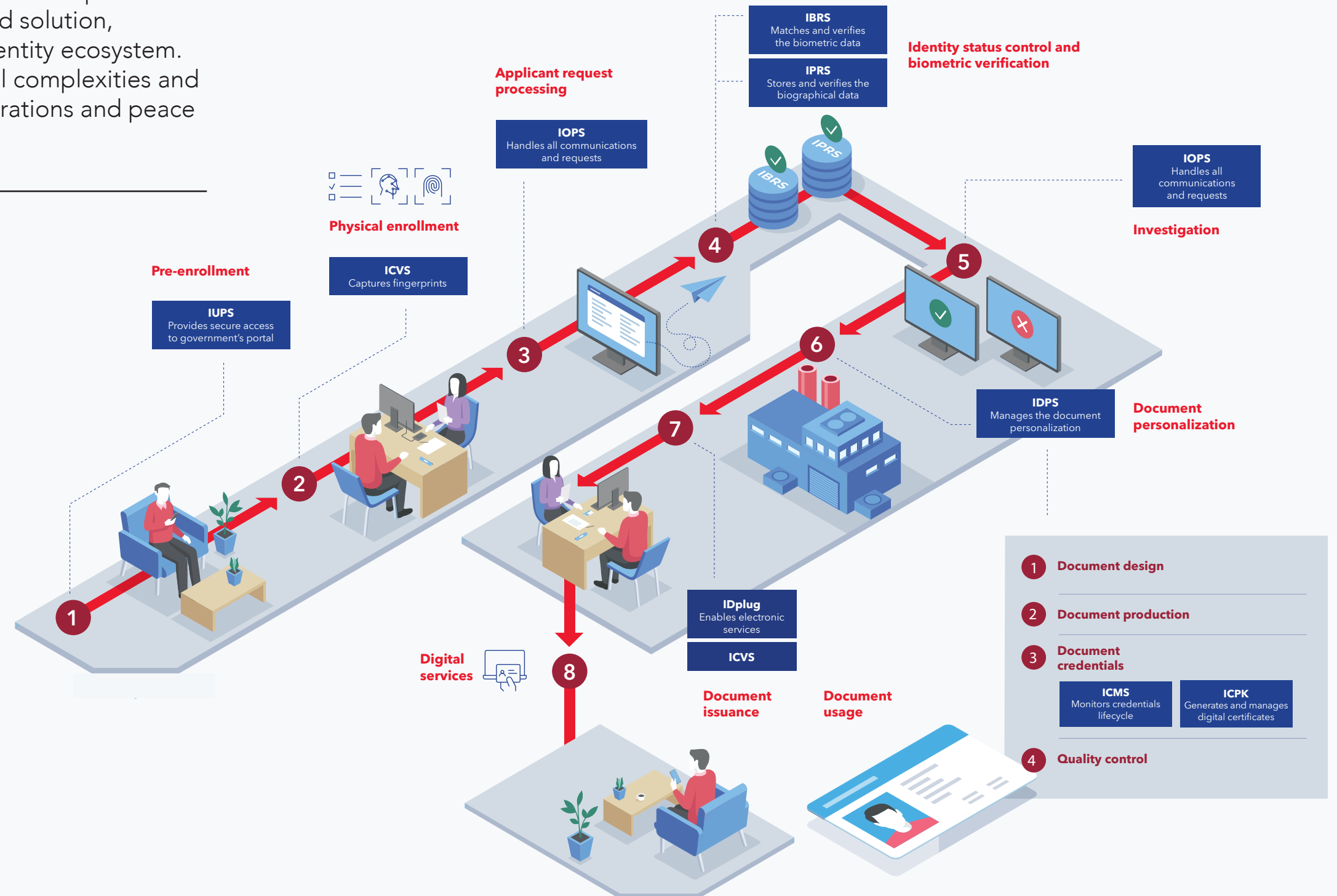
From home, the citizen connects to the **Universal Portal** to complete pre-enrolment: entering personal data, uploading documents and making payments online. They choose an appointment and receive a QR code for in-person enrolment.

At the city hall, the QR code retrieves the citizen's data instantly. An operator (or kiosk) captures biometric data (portrait, fingerprints and iris) using the **Capture and Verification System**. The citizen signs to validate the application and receives an enrolment receipt.

The integrated platform securely processes all attributes. After **Biometric Recognition**, the **Population Registry** is updated. The **Credential Management System** authorises production of the eID card, and the **Personalization System** performs graphical and electronic personalisation.

Once validated, the card is sent to the city hall. At pick-up, the operator verifies the citizen's identity via fingerprint.

With the card in hand, access to **Digital Services** is enabled through **IDplug**, which allows secure authentication, digital signatures and encryption on desktop or mobile (PIN + card reader or NFC smartphone).



4. Pre-enrolment and enrolment

The key to successful implementation of a national biometric identity register is the accurate enrolment of citizens. Since biometric data ensures the uniqueness of each identity, it is the most reliable way to authenticate and identify individuals. As part of this process, capturing high-quality biometrics is essential.



ONLINE PRE-ENROLMENT

The **IN Groupe Universal Portal System (IUPS)** hosts all eGovernment services on a single platform enabling secure digital onboarding and service access through fully digitised interactions. It supports pre-enrolment from home, booking appointments, and integrates seamlessly with authentication services for enhanced convenience and security.

IUPS saves time by reducing queues and offers strong authentication methods (based on ID cards, etc.) to



BIOMETRIC ENROLMENT

The **IN Groupe Capture and Verification System (ICVS)** is built to enrol and identify individuals anytime, anywhere. ICVS also verifies electronic ID documents and guarantees a high level of security thanks to its multibiometric system (fingerprints, face and iris). ICVS can be deployed on desktops, mobile devices and kiosks, offering a fully customisable experience—parameters, languages and interfaces can all be tailored to your needs. ICVS operates both online and offline and meets global standards such as GDPR.

Biometric capture devices are often stand-alone devices. To enhance efficiency and user experience, IN Groupe has developed the **IDstudio Desktop Station**, an integrated and compact solution for high-quality identity photo capture that meets ICAO and LASINK™ colour portrait requirements. It also embeds a powerful tenprint scanner, as well as a signature pad. With its compact size and lightweight structure, IDstudio Desktop Station has a minimal footprint.

To further streamline the user experience, we also provide **self-enrolment kiosks**, allowing citizens to complete the data capture process independently while remaining under the supervision of an operator or a central system. This kiosk is modular and can integrate keyboard, barcode reader, camera, tenprint scanner and signature pad.

Finally, to accommodate field enrolment, IN Groupe offers a range of mobile enrolment solutions based on

5. ID Management

Secure identity management is the foundation of any trusted system. By ensuring the uniqueness and integrity of each identity from the moment of enrolment, it becomes possible to accurately assign rights, services and permissions to the rightful individual. Without this reliable foundation, no access-control or credential-issuance mechanism can function properly.



ORCHESTRATION

The **IN Groupe Open Platform System (IOPS)** identity management solution is built on secure, standardised communications, ensuring reliable data exchange between external and internal systems, while providing an OSIA-compliant interface for interacting with devices and enrolment systems. It also relies on a secure identity management process orchestrated by the Open platform's BPM engine, ensuring consistent procedures across all deployment contexts, while allowing workflow customisation to meet specific customer needs. The solution also incorporates advanced investigation and administration capabilities through a dedicated interface that enables experts to analyse requests using multiple criteria: biometric data, demographics, request type, watchlist status, and an administration interface that provides complete visibility into the tracking and management of all requests submitted to the platform.



POPULATION REGISTRY

The **IN Groupe Population Registry System (IPRS)** solution ensures secure identity storage, reliably maintaining all information related to an individual as well as their associated history. With its UIN Generator, it assigns a unique primary number, guaranteeing the uniqueness and traceability of each identity. IPRS also handles the complete management of the identity lifecycle, providing biographical management and verification services throughout the user's journey. Identity lookups are facilitated by the Operator Portal, which provides simple and efficient access to data recorded in the population registry.



BIOMETRIC RECOGNITION

The **IN Groupe Biometric Recognition System (IBRS)** solution leverages advanced biometric capabilities, including fingerprint, facial, and iris recognition, to ensure reliable and highly secure identification. It incorporates standardised biometric workflows and automated decision-making mechanisms based on algorithms that have won multiple awards in NIST evaluations, guaranteeing performance and accuracy. For complex or disputed cases, a manual adjudication tool is available: its side-by-side interface allows experts to replace automatic verification with in-depth human analysis, thereby enhancing the quality and robustness of the identification process.



CREDENTIAL MANAGEMENT

The **IN Groupe Credential Management System (ICMS)** solution provides comprehensive management of the credential lifecycle, serving as a central registry and management platform for all types of credentials: ID cards, passports, driver's licenses, and digital IDs. It supports every stage of the lifecycle, ensuring continuous traceability in line with established processes. ICMS also includes advanced tracking capabilities for credentials and packaging, including management of dual-level packaging (envelope and box). A dedicated interface enables operators to manage credential requests, administer credentials or boxes, resubmit failed requests and effectively monitor all active applications.



6. Physical document

An ID card is more than just a piece of identification; it represents a country's identity and its commitment to trusted and reliable citizen services. IN Groupe excels in designing secure and visually appealing identity solutions. Our ID cards are crafted with advanced features that resist evolving fraud tactics.

With a range of hard-to-reproduce yet easy-to-inspect security elements, the IN Groupe ID card offers unmatched protection. Tailored to meet each country's specific needs, it provides a robust, durable identity solution that strongly resists fraud and data manipulation, ensuring trust and reliability in everyday use.



DESIGN

All visual elements must work together to create a coherent and secure document. As a national identity card is often an object of pride, the graphics must be carefully selected to truly reflect a country's identity. Co-design workshops are the best way to collaborate with the manufacturer to create aesthetically pleasing documents, incorporating the security features selected and national symbols. Renewing the design of documents every five to ten years is also recommended to stay one step ahead of fraud.



POLYCARBONATE

Today, two out of three countries use polycarbonate for their identity cards. Identity documents must meet two main requirements: durability (resistance to time and use), and security (resistance to attack). Polycarbonate meets both these needs perfectly. It offers high mechanical and thermal resistance and can be used to personalise the data at the heart of the card, as well as incorporating security features to combat counterfeiting and falsification.



SECURITY FEATURES

IN Groupe offers a broad portfolio of security features designed using the latest technological advancements, compliant with the most stringent international standards and fully interoperable. Thanks to our technological expertise and security-driven approach, we provide state-of-the-art security features that ensure authenticity, durability, and fraud resistance.

- **Bright Color UV** synthesises the three RGB colours: red, green, and blue, which are superimposed to create a realistic image. This unique technology combines a very high level of security with unrivalled aesthetics and far surpasses all other types of UV fluorescent inks. Millions of combinations are possible. It is compatible with laser engraving and embossing elements. The registration between the visible and the surface represented by the BCU makes it possible to secure a large part of the document's data. Beyond security, Bright Color UV enhances the document's aestheticism and modernity.

- **DOVID** (Diffractive Optically Variable Identification Device) can be integrated into polycarbonate. Positioned over the portrait area, it provides strong protection against photo substitution and alteration. The latest-generation DOVIDs feature several holographic elements of different shapes scattered over the portrait area, rather than a single patch. This protects both biographical data and the portrait area while offering new design possibilities.
- **Window technology** creates a fully transparent area within the card, linking both sides through a single optical space. A window can be laser-customised with the holder's data (such as an additional portrait), providing strong protection against counterfeiting and delamination. Since 2020, nearly one-third of identity cards now include a transparent window, a trend that continues to grow. To increase resistance to imitation, its structure should be asymmetrical, with two complex shapes of different sizes. The window should also feature visible and UV-fluorescent security backgrounds, allowing the design to remain perfectly aligned and continuous across the card, even through the transparent area.



DOVID



Creative window

To address this challenge, IN Groupe has developed advanced portrait security features.



Electronic interface

The IN Groupe’s secure operating system (OS) offers the highest levels of interoperability, security and reliability. Built on the latest Java Card and GlobalPlatform versions and certified under Common Criteria, it ensures compliance with industry standards while delivering unparalleled cryptographic capabilities.

IN Groupe has developed a strategy to achieve the best implementation of services, together with the highest possible level of security, leveraging its internal expertise. Our team consists of experts in all key domains, including secure code development, Common Criteria certification, logical and physical attacks on components, regulatory compliance and standardisation.

To reinforce security, IN Groupe relies on Java Card technology for the national ID card market. Our Java Card OS are Common Criteria certified with the highest vulnerability-assessment levels (chipset EAL6+, OS EAL5+ and applets EAL5+ certified for qualified signatures and travel applications). This technology is regularly updated with state-of-the-art cryptography and security mechanisms, including secure messaging and PACE. Our products support RSA up to 4096 bits and ECC up to 521 bits. Additionally, the implementation of postquantum cryptography in our OS is already underway.

To counteract natural security erosion, our embedded software can be updated using the JPatch mechanism, allowing upgrades to either the OS or the applets.

Our portfolio of in-house applets for eID includes specialised multi-service applications that implement a wide range of authentication, digital signature, and biometric data-matching mechanisms based on the latest standards:

- CombICA0: an all-in-one applet
- ID-A: designed to meet market needs for eID digital service access
- TnD: tailored to ICAO-compliant products with additional services
- Tailor made applets to meets specific customer requirements

Why embed a chip in an ID card?

A chip:

- cannot be replicated, making it the strongest guarantor of a citizen’s identity.
- enables controlled access to citizen information base on service requirements.
- supports strong authentication and qualified electronic signatures.

This is why the number of ID cards with a chipset increases significantly every year.



Middleware

To enable the use of the smartcard once it is in the hand of a citizen, IN Groupe IDplug Middleware provides the technological bridge that leverages the smartcard data to securely access eGovernment and private services from their computer or smartphone.

This solution offers integration capabilities for desktop and mobile applications, enabling the use of digital certificates securely stored in IN Groupe chips and applets to perform the three main cryptographic operations: **authentication, electronic signature and encryption.**

The IDplug software benefits from over 15 years of development, making it one of the most reliable and stable solution on the market to cover all types of application requirements. Three options are available to

meet different device specifications:

- **IDplug Classic**, compliant with standard specifications from Microsoft, Apple and Linux native applications (PKCS#11, MiniDrivers, CryptoTokenKit)
- **IDplug WebConnector**, designed for browser-based applications on Windows
- **IDplug Mobile**, enables secure access to applications or networks on mobile devices (iOS and Android)



8. Document issuance

PUBLIC KEY INFRASTRUCTURE

The use of a PKI (Public Key Infrastructure) is essential to issue and manage digital certificates which are a mandatory component of the process. A digital certificate is an electronic document used to prove ownership of a public key and, indirectly, to confirm that an individual is who they claim to be. It enables governments to establish a full chain of trust.

IN Groupe's PKI offers flexibility, either as part of a full document personalisation system or as a standalone module, with tailored PKI components compliant with ICAO Doc 9303 and ETSI eIDAS trust service standards for citizen digital identity and trust services.

After ensuring the citizen's uniqueness, based on both biometric and biographical data, the request is approved. In a highly secure environment, a personalisation machine performs the electrical and graphical personalisation of a blank document to produce a

PERSONALISATION

The IN Groupe Document Personalization System (IDPS) is deployed at personalisation sites. The system supports the entire personalisation process, controlling every stage of the lifecycle, from receipt of blank documents to the dispatch of the personalised document.

During production, IDPS optimises workflows by parallelising machine operations, preventing downtime, and ensuring consistent quality and integrity. It prepares personalisation data, generates elements such as 2D codes, PINs or PUKs, and performs inline or offline quality checks. Full traceability is maintained throughout the entire cycle, from stock management to final distribution.

IDPS architecture is flexible, supporting both centralised and decentralised deployments. Each site has its own independently managed inventory, with the ability to transfer blank document between sites while maintaining full traceability.

The system is compatible with both large and small volume due to a wide range of integrated and tested personalisation machines, from desktop to personalisation equipment.

9. Driving digital transformation with secure Digital ID solution

Digital identity is at the heart of modern governance, enabling faster processing times, cost savings and centralised identity management. By digitalising identity verification and service access, governments can enhance data security, improve transparency, and streamline interactions with citizens and private corporations. A secure, government-backed digital identity—derived from official national documents—ensures trust, efficiency, and seamless access to eServices.

As a global leader in identity solutions, IN Groupe empowers governments with secure, compliant, and future-ready eID solutions. Our eID cards and digital identity ecosystems provide citizens with a reliable, government-backed digital identity, ensuring access to essential services while upholding the highest security standards.

Thanks to the certificates stored in the chip, digital ID creation is both simple and secure. Citizens can use dedicated kiosks or their smartphones as an NFC reader and enter the card's PIN code to digitally store data on the device.

Once this is done, the user can access their digital companion (a digital copy of the ID card) to prove their identity offline. Most importantly, the eID can be used as an authentication method to access online governmental services.

10.

IN Groupe's references

Key references

	Albania		Kenya		Peru
	Armenia		Kosovo		Seychelles
	Benin		Latvia		Switzerland
	Chile		Mauritania		
	Colombia		Monaco		
	Djibouti		Morocco		
	France		Nepal		
	Gabon		Netherland		
	Greece		Netherland – Aruba		
	Haiti		Netherland – St Marteen		
	Hong Kong		Nicaragua		



11.

IN Groupe's expertise: case studies

France

The French electronic identity card: an innovative and highly secure document



Introduced in 2021, the French electronic identity card embodies a new generation of security and design. It integrates advanced innovations such as a next generation holographic device with colour shifting effects protecting the holder's portrait, secure transparent borders with optical effects, a complex shaped lens revealing a changing image, and an engraved module containing a highly secure chip.

The project was the result of close collaboration between multiple entities of the Ministry of the Interior — including ANTS, DLPAJ, document fraud experts from IRCGN and DCPAF — and industrial partners who jointly ensured a smooth and successful nationwide deployment.

The card's design reflects the symbols of the French Republic, visible throughout the document: in the secure printing, in the holographic device, on the engraved module, and on the card's surface through tactile and optically variable effects.

Deployment began progressively in March 2021, enabling full nationwide rollout by August of the same year. The new French ID card now provides citizens with a modern, secure and aesthetically distinctive identity document that meets the highest international security standards.



Latvia

Latvia renews commitment to secure electronic identity with IN Groupe's Cosmo OS.



In 2023, Latvia reinforced its trust in IN Groupe by extending its national eID contract. This new phase of collaboration introduces ID-One Cosmo OS, IN Groupe's latest modular Java Card operating system, into the national eID program. Cosmo OS enables the secure storage and dynamic update of multiple applications on the card and is certified to the highest security level of the Common Criteria certification – ensuring trusted digital services for years to come.

Latvia's current eID card, launched in 2019, was designed from the outset to be future-proof. It significantly enhances the security and functionality of its predecessor, combining advanced visual security features – such as LASINK™ Origin colour portrait and 3D lenticular image – with a powerful dual-interface chip for secure digital identity.

Built to evolve, the card supports contactless use, biometric authentication, and post-issuance updates. It was recognised with the Best New National eID Card award at HSP EMEA 2020. Since the start of the partnership, almost 2.5 million eID cards have been delivered.



Morocco

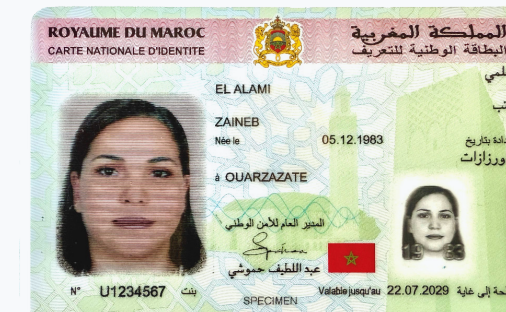
IN Groupe delivers the new national eID card and a full authentication platform for secure online services.

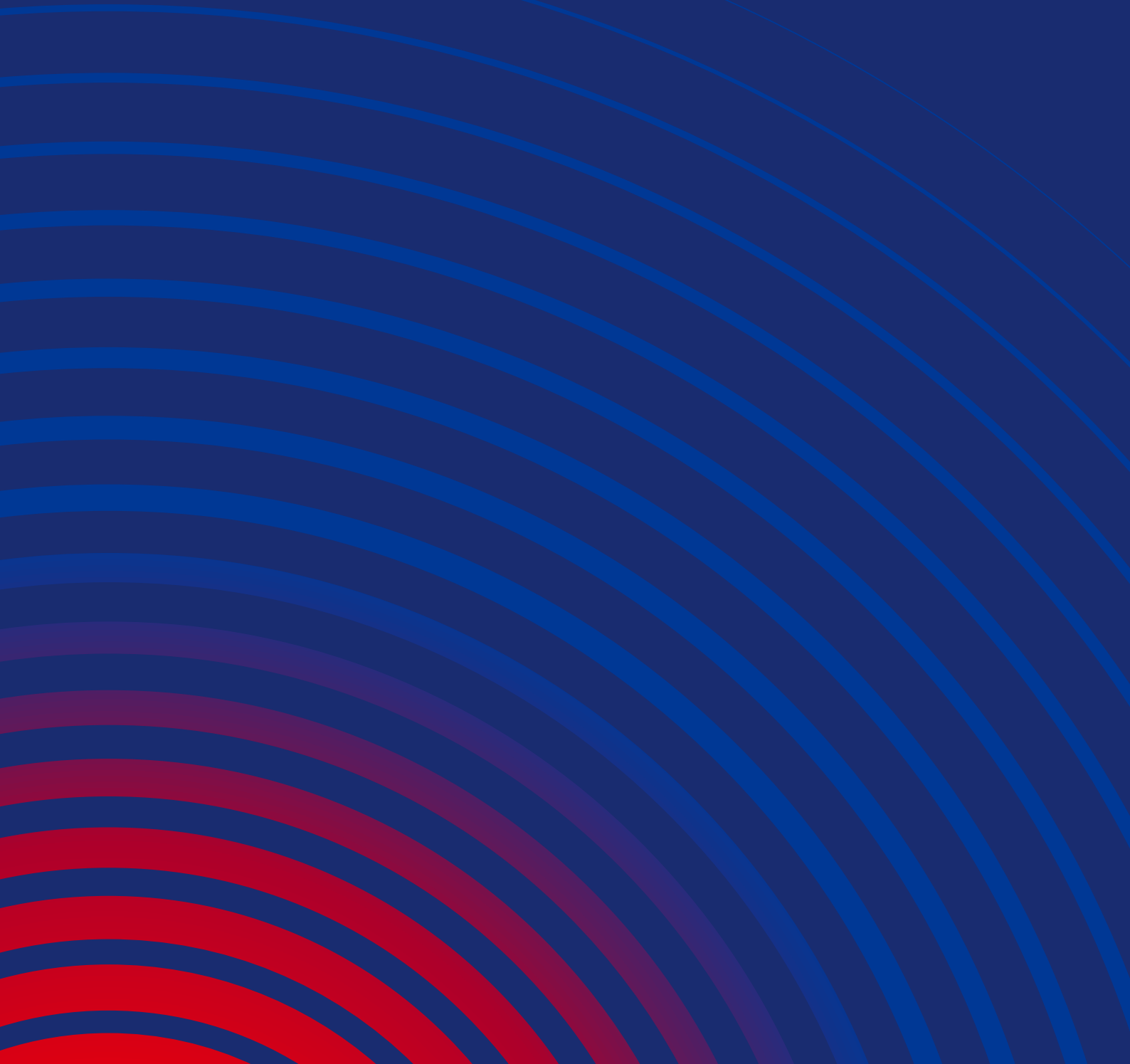


In 2022, Morocco launched an authentication platform for digital services, based on the new national eID card introduced in 2020. The national eID card features a contactless chip, embedded certificates for remote authentication, LASINK™ Origin colour photo, and SLI® secondary portrait, and serves as the primary authentication factor for citizens accessing services remotely.

The platform allows public and private online service providers to verify users' identities when accessing digital services, and enables citizens to securely share personal data from their eID cards and subscribe to new remote services. It also supports multifactor authentication (MFA), a robust security process that requires at least two validation factors to confirm the holder's identity.

Since the beginning of this partnership, more than 23 million eID cards have been issued, enhancing both security and convenience for Moroccan citizens.





Thank you

All rights reserved. Specifications and information subject to change without notice. The products described in this document are subject to continuous development and improvement. All trademarks and service marks referred to herein, whether registered or not in specific countries, are the property of their respective owners.

ingroupe.com

