# Intercede MyID for
# national identity schemes

## The challenge

National identity schemes are inherently large scale complex projects to deliver. They often consist of multiple component parts such as fingerprint capture, photo capture, document scanning, background checks, electronic document personalization and citizen-facing kiosks, all of which need to be integrated to form a complete solution.

Governments need to be able to trust identities and credentials that are presented to them, and to do that they need to be confident that the system that issued them is trustworthy. Identities need to be produced in a secure environment by responsible, verified operators using a defined process that can be proven via audit and traceability.

Large scale integration projects are risky (the component parts may not interoperate easily), costly (the integration work itself takes effort) and time consuming (any new solution needs to be tested). It is also unlikely that the requirements can be defined to the extent that change is not required during the project lifecycle. The inability to accommodate change (e.g. changes to the law or to protect against a new technical threat) is one of the key reasons that national identity programs are often late, suffer from costly overruns or even fail completely.

National identity schemes also face the dual challenges of security and usability; citizen data must be kept secured, but the system must be easy to use for operators and citizens alike. For a solution to combine the two it must provide simple and efficient workflows built on a secure platform.

## The MyID solution

MyID® from Intercede® is a national identity solution delivered as commercial off-the-shelf (COTS) software. It is designed to simplify the deployment of national identity schemes by providing citizen registration, identity verification, electronic ID issuance and lifecycle management in one single easy-to-use integrated product.

Although it provides an end-to-end solution in its own right, MyID is modular by design and its connector-based architecture and APIs allow it to be easily integrated with existing systems. Examples include importing data from enrollment or citizen databases and pushing card status changes to external systems.

## Key features

- Proven complete solution for national ID programs
- Reduces costs, risk and time to deployment
- Scalable from thousands to millions of citizens
- Highly flexible modular COTS solution
- Citizen self-service kiosk interface
- Easy-to-use guided workflows for operators
- Secure card management

Built on a secure platform, MyID utilizes cryptographic devices (such as hardware security modules), secure firewall-friendly three-tier server deployment, data separation (e.g. biographic and biometric), strong role-based access control, signed operations and a tamper event audit trail to ensure citizen data is protected and only accessible to trusted and strongly authenticated operators.

Avoiding the tendency of some secure solutions to be difficult to operate, MyID presents simple workflows to operators, allowing them to perform the functions they need with minimal training. Citizens are presented with an 'ATM-like' experience at a self-service kiosk, allowing them to perform simple operations such as collecting updates to a device or reporting one lost and ordering a replacement.

MyID can work with devices (such as smart cards, fingerprint readers and printers), applications (such as PKI and AFIS) and services (such as card personalization) from multiple vendors. This technology independence allows governments to choose third party components that best fit their needs and swap out providers as requirements change.

MyID is a highly flexible solution, designed to adapt to country-specific requirements; language, data capture screens, workflows and user interfaces can all be configured to meet project needs, minimizing the need for bespoke development.

MyID has been used to successfully deploy millions of smart cards and electronic passports worldwide, including multi-applet national ID cards for Kuwait, Transport Worker Identification Credentials (TWIC) in the US and cards for secure data access in the healthcare sector in both the UK and Australia.

## Security and scalability


MyID provides a secure platform on which to build a national identity solution, providing HSM and smart card encryption of sensitive data, separate storage of biographics and biometrics and strong authentication of all system operators via signed logon and operations. MyID records each event in a central signed audit trail. This acts as a chain of trust, binding operators to the actions they performed, providing full non-repudiation of actions via built-in enquiries and customizable reports.

Secure three-tier server deployment means that MyID is deployed with separate web, application and database servers, which gives a high degree of security in terms of firewall protection between the server components. Each of the tiers of MyID can be replicated for failover purposes, so that one server can take the place of another should a failure occur. Multiple servers can also be deployed for performance and throughput purposes, with load balancing managing the processing across multiple machines that can easily deal with national ID schemes involving millions of citizens.

## Registration

MyID has the capability to capture registration data pertaining to individual citizens and store that data for use in future identity management processes. This information includes: fingerprints (single finger and ten-slap), photos (ICAO/FIPS 201 standard), facial biometrics, document scanning, electronic document verification (e.g. passport or driving license), physical signature, biographic data (e.g. date of birth, height, eye color) and personal attributes (e.g. medical alert data). Data can be input manually or retrieved from one or more connected citizen databases. During registration, MyID makes sure that a defined data capture process is enforced, which can be anything from simply adding a photo and signature to full FIPS 201 compliant multi-stage sponsorship and enrollment.

## Identity verification


MyID connects to background checking services (e.g. Equifax or OPM), which validate data against multiple trusted data sources (e.g. electoral rolls). These confirm that the claimed identity is genuine and has a 'social footprint'. In addition, MyID can also check whether someone is on a known risk register (e.g. police or immigration) or a trusted register (e.g. driving license).

MyID has the ability to pass fingerprints to a central automated fingerprint identification system (AFIS) so that the applicant's fingerprints can be matched against all the records in the system, which can provide positive identification of an individual against a previous identity. MyID also compares fingerprints against a local biometric store, which can help protect against fraudulent re-enrollment attempts.

## Issuance

MyID provides a technology independent platform to issue a wide range of credentials onto a variety of devices such as smart cards and ePassports. The MyID software communicates with these secure devices to generate the encrypted key pairs required for PKI certificates and provides Global Platform compliant applet management as well as standards-based personalization (e.g. ICAO, IAS-ECC or FIPS 201).

Issuance methods control how a device is personalized and securely delivered to the end user. Options include: face-to-face; centrally in batches with local activation; at a citizen kiosk; and integrated with third-party personalization bureaus (including data preparation and formatting). Security controls include who can issue a device, who can receive it, key management and PIN policy. MyID supports multiple applets on multiple security domains for data separation; this allows different government departments to share a single card, but only be able to access the data that is contained on their area of the card.

## Post-issuance lifecycle management

MyID allows for the intelligent management of issued devices and credentials by letting government agencies control who can carry out which card operations, renew certificates, replace lost and forgotten cards and suspend or revoke credentials. Some functions, such as unlocking a card, can be carried out by citizens using a self-service kiosk. It also allows person data to be updated and notifies users when credentials are about to expire, walking them through a self-service collection of the replacement credential. Data and applets can be updated to match the latest content without having to reissue the card.

MyID can also demonstrate that security policies are being enforced (e.g. FIPS 201) or prove that access to citizen data is being managed (e.g. Sarbanes-Oxley). The built-in configurable reports and web-service enquiries make reporting and analysis of all identity and credential management activity simple.



**+1 888 646 6943 • info@intercede.com • www.intercede.com • @intercedeMyID**