

A grayscale background image of the US Capitol building's dome and columns.

# SIMPLIFIED IDENTITY AND CREDENTIAL MANAGEMENT FOR US GOVERNMENT

**A major US government federal agency had already deployed an identity and credential management system to comply with the FIPS 201 standard but wanted to replace the system with a more open and easier to support solution.**

## THE CHALLENGE

The agency specified a number of strategic goals for a replacement solution:

- **Compliant** - the solution must be fully compliant with FIPS 201 and associated special publications and FICAM standards
- **Open** - the system must enable the agency to easily access their own data and integrate with existing in-house solutions
- **Scalable** - the solution must scale to managing identities and credentials for hundreds of thousands of globally dispersed employees and contractors
- **Flexible** - the solution should allow the agency to define their own security processes and workflows
- **Low cost** – the solution should minimise costs by being able to work with existing data, systems and hardware

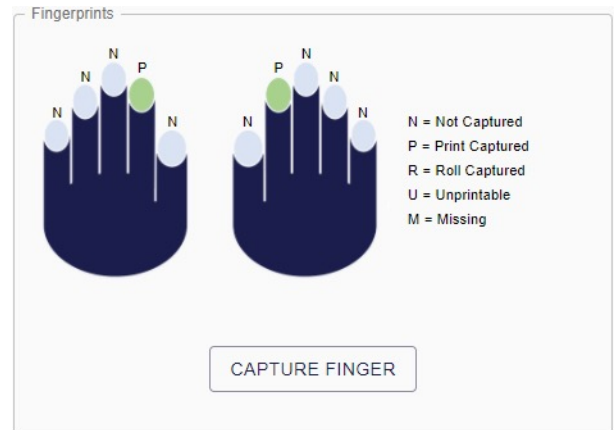
## THE SOLUTION

MyID was used as a combined Identity and Credential management solution, meeting each of the stated project goals:

- **Compliant** - MyID has helped many US government agencies achieve an Authority To Operate (ATO) for their identity and credential solutions and with MyID PIV provides a pre-configured for FIPS 201
- **Open** - MyID's extensive range of pre-built connectors, APIs and SDKs enabled it to be easily integrated with existing systems including PKI, HSM and an in-house user on-boarding database. The built-in enquiries and reports combined with the ability to access data by API or database enquiry tools enabled the agency to gather management information previously unavailable to them
- **Scalable** - MyID has been used for solutions from tens of thousands up to national programmes with millions of users, proving its ability to manage large volumes of identities and credentials at scale
- **Flexible** - In addition to the APIs and SDKs provided with MyID, the solution itself can be configured to hold customer specific data and implement particular business processes with a zero-code mechanism, simplifying ongoing support and placing the customer in control of their own system configuration.
- **Low cost** - MyID's technology independence and open nature allowed it to work with in-house systems in addition to supporting the existing deployed hardware such as fingerprint readers and cameras.

## The Solution in Use

1. Data is passed to MyID from an in-house user onboarding solution via the MyID REST APIs
2. MyID is used to capture a full PIV enrolment data set for each applicant, including 10-slap fingerprints, scanned ID documents and facial biometric capture
3. Biometric data is passed to an Automated Biometric Identification System (ABIS) to provide deduplication and protection against fraudulent enrolment
4. Once verified MyID is used to request and issue credentials for individuals via integration with HSMs, PKI and smart card printers
5. MyID provides ongoing management of the identity and credential lifecycle including, renewal, updates, unlock and revocation.



## Future Proofing

In addition to meeting all of the agency's goals, MyID provides additional capabilities over and above the basic requirements including derived PIV credential issuance, PKI-based strong authentication and FIDO for the enterprise. These demonstrate Intercede's ongoing investment in MyID and commitment to the FIPS 201 standard, ensuring the agency can gain maximum ongoing value from their choice of MyID.



## CONTACT US TO FIND OUT MORE

Contact us now to discover what MyID has to offer your organisation:

[info@intercede.com](mailto:info@intercede.com)

+44 (0)1455 558 111

+1 888 646 6943