intercede

NIST: Providing a best practice framework for derived personal identity verification (PIV) credentials

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MyID | PIV

The National Institute of Standards and Technology (NIST), together with the National Cybersecurity Center of Excellence (NCCoE) are the United States' leading bodies in providing real world, best practice architectures for federal agencies and companies to overcome specific cybersecurity challenges.

In this use case we look at why NIST and NCCoE included MyID PIV credential management as part of their solution. How the overall solution works and the functionality MyID PIV credential management adds.

THE CHALLENGE

With the introduction of a new Federal Information Processing Standard (FIPS), specifically FIPS 201-2; Personal Identity Verification (PIV) of Federal Employees and Contractors, federal government had a new opportunity to take advantage of new technologies for the secure authentication of their employees and contractors.

The original standard (FIPS 201) was published in 2005 and as such was focused on setting multi-factor authentication standards, using public key infrastructure (PKI), for technology in use at that time; largely desktop and laptop computers.

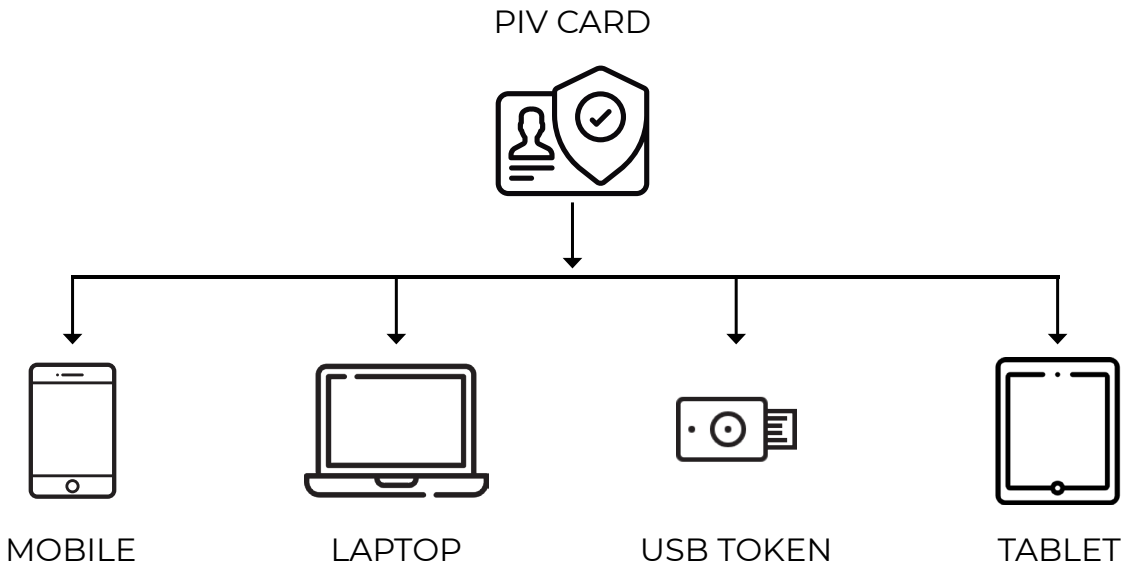
FIPS 201 therefore was focused on users being issued with a PIV smart card to provide common multi-factor authentication via their desktop computers and laptops using in-built or auxiliary smart card readers.

Fast forward to today and the technology landscape has changed significantly – the computing power of mobile phones has changed exponentially while tablets and hybrid computers are all now prevalent alongside new identity form factors like the USB token.

The limitations of PIV smart cards to work with the technology that federal employees of 2020 want to use day-to-day as part of their jobs was plain to see.

To extend the use of PIV systems into mobile devices, tablets, and laptops (without in-built smart card readers), NIST developed technical guidelines on the implementation and life cycle of identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV Card.

NIST published guidelines to indicate how derived PIV credentials would enable the federal sector to leverage proofing and vetting results of current and valid PIV credentials and derive those credentials to other secure technologies for multi-factor authentication, such as mobile devices.



The guidelines are also relevant to many companies, particularly key government suppliers who look to meet federal standards.

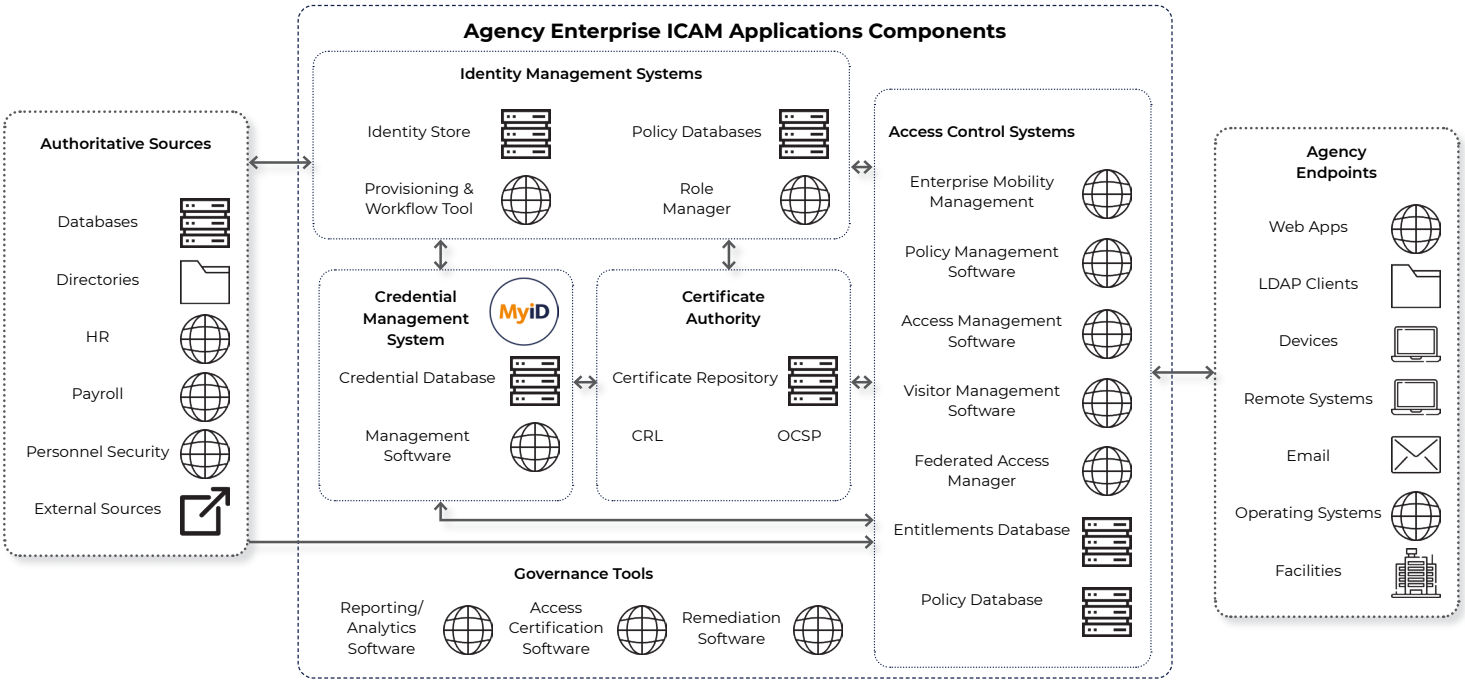
THE SOLUTION

To demonstrate how the federal sector and companies could take advantage of derived PIV credentials, NCCoE built two security architectures using commercial technology that enable the issuance of a derived PIV credential to mobile devices that use Federal Identity Credentialing and Access Management shared services.

One option uses a software-only solution, while the second option uses hardware built into many computing devices used today. Both options utilise MyID credential management software.

- **The environment**: Both options resemble a typical enterprise network using commonplace components found in federal agencies and companies across the US; identity repositories, supporting certificate authorities, and web servers.
- **Product and capabilities**: Where possible SaaS or shared service providers (SSPs) that operate under federal policy were leveraged, such as certificate authorities operating in accordance with Federal PKI Policy Authority policy. The advantage of such providers being that federal agencies can avoid the costs associated with ongoing maintenance of such systems.

As the diagram below illustrates, there are multiple components identified in the working solution. At a critical part of the working solution sits MyID PIV credential management.



Here, MyID PIV credential management is central to executing the life-cycle operations; sponsorship, registration, issuance, maintenance, and termination of authentication credentials.

The MyID server platform comprises an application server, a database, and a web server. It provides connectors to infrastructure components such as hardware security modules (HSMs) and PKI, and application programming interfaces (APIs) to enable integration with the organisation's identity and access management system.

For mobile devices, the MyID Identity Agent runs as an app or an SDK embedded into an MDM and interfaces with the MyID server to support iOS and Android mobile devices and credential stores, including the device's native key store, software key store, and microSD storage.

THE BENEFITS

The overall benefit of the NCCoE solution is that it provides a real world, working example of how organisations can issue derived PIV credentials to its workforce across a variety of form factors, including smartphones, and meet FIPS 201 / SP800-157 requirements.

The central benefit being that an organisation can evolve its multi-factor authentication solution from the PIV card to a suitable method that fits today's workforce requirements.

A secure, strong multi-factor authentication that enables employees to access the information they need, both in the office and from remote locations, using anything from a smartphone or tablet to USB token.

From a credential management perspective, the benefit of MyID PIV is that it provides a highly interoperable, compliant credential management system that enables IT teams to manage credentials centrally with all the policy controls necessary for compliance to FIPS 201.

Operating as an on-premise, hybrid cloud or fully cloud managed solution, MyID PIV software:

BENEFITS OF MyID PIV

OPTIMUM SECURITY Configure certificate and device issuance policies, ensuring the right people receive the right digital identities	**PROCESS-DRIVEN** Features simple, process-driven workflows for helpdesk to issue replacement devices when lost or re-enable locked devices
EASY TO MANAGE Provides a single integrated solution to sponsor, enrol, approve, issue and lifecycle manage users and PIV credentials	**FREES UP IT** Frees up IT support by enabling employees to collect new certificates to their own devices through a simple self-service application
FULL AUDITABILITY AS STANDARD Maintains full auditability and reporting capabilities – allowing visibility of who issued which digital identities, to which users, and on what device; helping with audits and proof of compliance with federal policy	**ULTIMATE INTEGRATION FLEXIBILITY** MyID PIV is developed to work with the IT architecture you already have, minimising impact on your existing environment and speeding up deployment

You can find the full NIST Special Publication 1800-12B; Derived Personal Identity Verification (PIV) Credentials here: https://www.nccoe.nist.gov/publication/1800-12/VolB/index.html

CONTACT US NOW TO FIND OUT MORE

MyID PIV is a proven credential management system that is widely deployed across US federal government and companies. From deployments of 500 running up into the millions, MyID PIV is an integral part of FIPS 201 compliant identity and access management solutions.

Contact us now to find out more or to arrange a demo of MyID PIV in action.

info@intercede.com **+44 (0)1455 558 111** **+1 888 646 6943**