intercede

UNIFIED CREDENTIAL MANAGEMENT IN FEDERAL GOVERNMENT

WHITE PAPER

Chris Edwards
Chief Technical Officer, Intercede

About the Author

Chris has over 35 years' experience within the IT industry, 18 of them at senior level within the security sector. He was responsible for the initial design of Intercede's MyID product and retains overall responsibility for the architecture and technology within it.

Chris was instrumental in making MyID the first electronic personalization system to achieve FIPS 201 accreditation as part of the FIPS201 (PIV) Approved Products List and has substantial experience of working on both US and UK government and commercial security projects.

Chris is directly responsible for Intercede's R&D team, with a special interest in mobile identities, IoT and credential convergence.

About Intercede

Intercede® is a cybersecurity company specialising in digital identities, derived credentials and access control, enabling digital trust in a mobile world.

Headquartered in the UK, with offices in the US, we believe in a connected world in which people and technology are free to exchange information securely, and complex insecure passwords become a thing of the past.

We have been delivering trusted solutions to high profile customers for over 20 years. Our team of experts has deployed millions of identities to governments, most of the largest aerospace and defence corporations, and major financial services and healthcare organizations, as well as leading telecommunications, cloud services and information technology firms, providing industry-leading employee and customer credential management systems.

For more information visit: intercede.com

Contents

2 **Introduction**

3 **Historical Perspective**

3 HSPD-12 & FIPS201
3 Expansion
4 Mobile
4 Alternatives

6 **Challenges**

6 Trust frameworks
6 Technical vs Human Factors
7 Smartphones - PKI
7 Smartphones - FIDO
8 USB Tokens
8 Consistent processes
10 Privacy vs Convenience
10 Managing policy changes
10 Credentialing non-person entities
11 Relying party and client technologies
11 Mobile device management

11 **Necessary solutions**

12 Multi-device Credentials
12 FIDO Credential Binding
14 FIDO Credential Replacement
14 Federation
14 IoT

15 **Conclusions**

16 **Additional Information**

16 Glossary of Acronyms
17 References

Introduction

This is the first in a series of white papers that explore the issues around secure authentication in a number of market sectors. In this paper, we focus on the US Federal Government, with emphasis on their PIV program and the impending expansion to embrace new form factors and protocols. Subsequent papers are planned to address other markets including healthcare, finance, critical national infrastructure, telecommunications and manufacturing.

The use of strong authentication to protect IT assets and services is becoming increasingly important. Legacy means of authentication such as passwords have been widely discredited and should no longer be considered as a viable means of securing business environments.

Although the US Federal Government have had a smart card solution in place for over 12 years now, this form factor has not always proved to be the most convenient for many common use cases.

The recent OMB memorandum (OMB-19-17) emphasized the need to generate and consume cryptographically-backed credentials held on different devices, including mobile and USB-keys. Although x509 certificate-based Public Key Infrastructure (PKI) is still regarded as the 'gold standard', protocols such as FIDO have enabled the use of asymmetric cryptography for some limited cases without the operational overhead of a certification authority.

This paper describes the historical context and explains what new problems we need to solve. It assesses the competing and complementary technologies that are available now (or in the near future) to address these challenges.

It outlines the human factors and extended business processes that will be needed to manage an expanded set of authentication devices and then proposes solution components to achieve this.

Finally, this discourse concludes with a call to action, to bring federal credentials under strong management at the earliest opportunity, before agencies lose effective control over their expanding credential real-estate.

Historical Perspective

HSPD-12 & FIPS201

In the wake of 9/11, the risk posed by insecure government ID badges was highlighted to such an extent that in 2004 a presidential directive (HSPD-12) was issued, directing agencies to implement smart card security for all federal employees and contractors. This led to the fast-track development of a set of standards and implementation guidelines to ensure that the solution would be secure from a both a technical and a procedural standpoint. The core FIPS201 standard for Personal Identity Verification (PIV) has been at the heart of this initiative for the past 15 years.

The original goal was to address the security of physical access, identity verification and then logical access to federal facilities, systems and communication. Despite the short timescale over which the standards were developed, they proved to be an effective means of authentication for millions of personnel.

In contrast to other standards at the time, a key aspect of FIPS201 is the specification of the processes that must be followed to enroll cardholders, issue cards and manage those devices throughout their lifetime. This included aspects of sponsorship, enrolment of biographic and biometric data, adjudication (with background checks as necessary), secondary approval, card personalization, delivery, activation, and subsequent 'lifecycle' events.

Expansion

Around 5 years into the program, every agency had virtually all of their staff credentialed, along with millions of Defense workers who had a broadly equivalent 'CAC' card. The scope was extended to allow for 'PIV-I' and 'PIV-C' credential for non-federal employees, leading to the largest card roll-out by the TSA for their Transport Workers Identity card (TWIC – now called TIM).

Work also commenced on converging the card technologies for PIV and CAC devices, so that higher levels of interoperability could be achieved. This was important too for the evolving physical access applications, when door reader and controller technologies had to evolve to accommodate the use of 'PKI at the door'. This was necessary to replace the easily spoofed proximity cards that were (and still are!) commonly in use.

Mobile

By 2013, it was apparent that mobile devices were going to become a crucial part of the business IT infrastructure, so an additional special publication (SP800-157) was instigated to define the technology and processes needed for mobile 'derived' credentials. Following its publication in 2014, the industry stepped up to deliver demonstrable solutions to this requirement in conjunction with NIST and the NCCoE.

What emerged from that exercise again emphasized the crucial role of credential management in such ecosystems. When the status of an individual changes, automated rule-based systems are necessary to ensure the continued security and integrity of the organization by immediately revoking or enabling correct levels of access to resources and services.

With no strong mandate or specific funding for this initiative however, adoption of derived credentials has been very slow. To a large extent, this had also been held back by a paucity of usable service authentication mechanisms that are able to consume mobile PKI credentials.

Alternatives

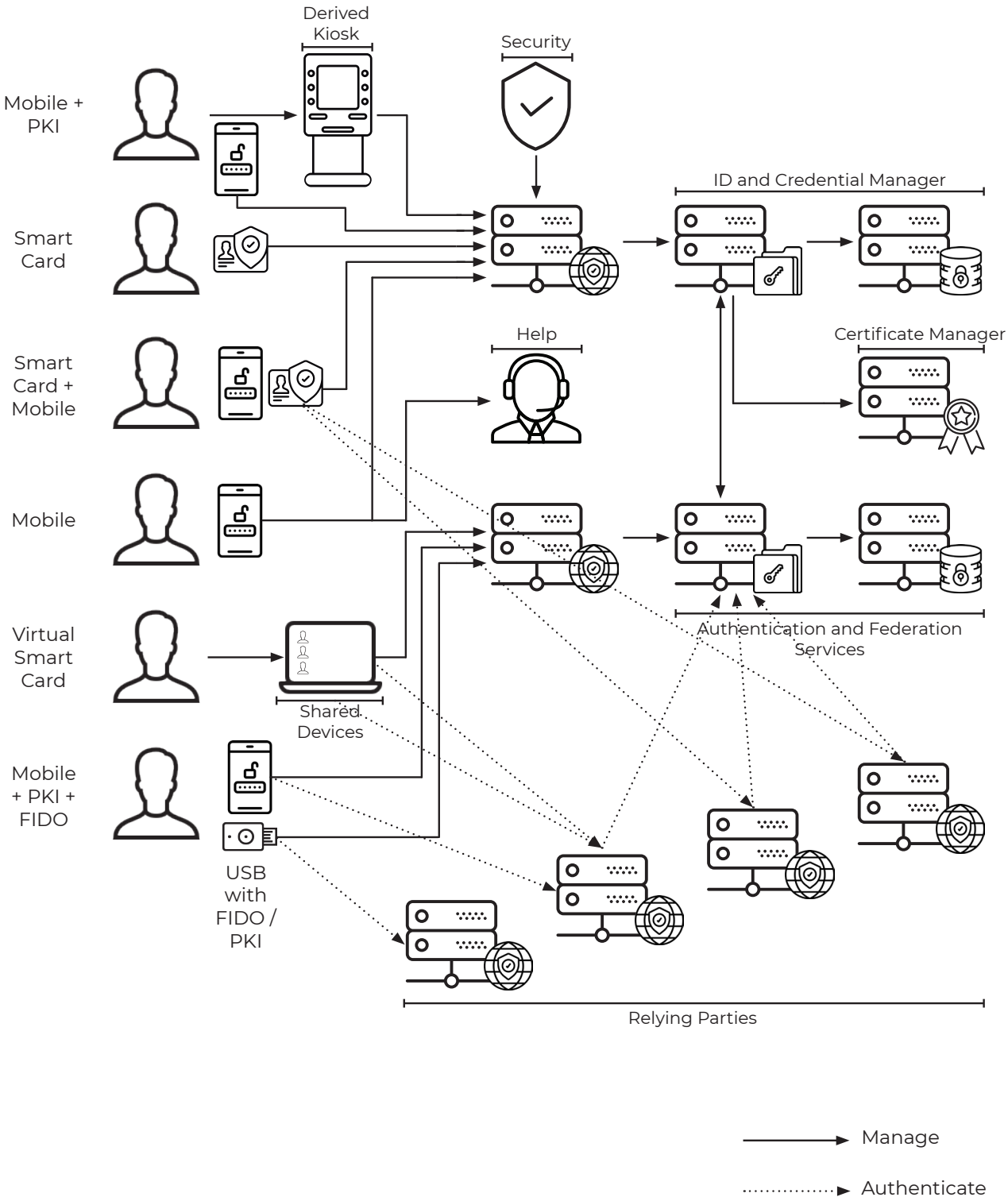
Meanwhile, alternative strong credential form factors (such as USB tokens and FIDO authenticators) have been gaining in popularity, and the use of one-time-passwords delivered via SMS has been shown to have serious security flaws.

Implementing PKI-based authentication within all services is not always practical (and in some cases has been applied incorrectly – for example, using the wrong PIV certificate for website authentication). The user experience presented via many browsers for mutual authentication is also less than intuitive in many situations.

In addition, the growing use of federated authorization services has to be recognized and accommodated where it is appropriate, with due consideration given to privacy and resilience.

This is where OMB-19-17 enters the arena, with a call to arms for agencies to enable their systems and services to alternative authentication schemes so that business processes can be significantly enhanced without jeopardizing the security and integrity of the IT environment.

Credential lifecycle management is complicated



So, as we look at the overall direction of travel, what challenges are evident and what sort of solutions will we need to address the extremely complex ownership and lifecycle issues?

Challenges

Trust frameworks

The challenges of maintaining trust within such expanding environments cannot be understated. We are seeing multiple authenticator technologies using different combinations of activation factors (PINs, fingerprints, facial etc.), each of which then has to map through to an assessed 'level of assurance' (LOA) in the credential.

Recent updates to special publication SP800-63 extended the basic LOA guidance to embrace three different measurements of the trust we can associate with an assertion of identity. The first of these relates to the validity of the 'real world' identity of an individual. How robust was the identity proofing process used during enrolment? How many forms of trusted ID 'breeder' documents were presented and were any background checks performed to verify these? This gives you a measurement known as the Identity Assurance Level (IAL).

Secondly, you need to know how must trust to place in the authentication process. For this, you need to consider the hardware and technology being used to perform an authentication, and also the management processes employed for credential issuance, binding to the individual and subsequent lifecycle management.

These factors combine to give you an Authenticator Assurance Level (AAL).

Finally, if a federated identity service is used to deliver authorization tokens for consumption by relying services, the integrity and policies that control that service and the token construction itself contribute to a third factor – the Federation Assurance Level (FAL).

It is worth noting that SP800-63-3 advises that the use of a federated service can bring benefits in aligning varying IAL and AAL scores through a consistent policy. This has to be balanced against the risk of having a single point of failure in the system, and the security weaknesses associated with some forms of authorization token (unbound 'bearer tokens' for example).

Technical vs Human Factors

There are innumerable technical solutions to the problems facing us. Each has positive and negative aspects relating to security, ease of use, ease of maintenance, ubiquity and interoperability. In practice however, the overriding concern of end-users has been shown to be convenience. If a chosen technology is perceived to be obstructive or complex, it will either be bypassed or simply fall into disuse.

Until the arrival of the smartphone, the physical constraints of a smart card were a significant constraint on the wider adoption of this technology. Having a card in your wallet from each financial institution, employee and loyalty scheme was ok until you exceeded about 8 of them, at which point it became unwieldy. Although the technology is designed with multiple containers, allowing different credential providers to share a physical card, this potential has never really been realized.

A smart card also requires readers which, although straightforward to deploy in public locations and enterprises, have never really attracted domestic adoption. The cost and clumsiness of add-on readers is also a barrier to adoption. Contactless cards have given a new lease of life in retail and transport for example, but the limited capacity of the devices, privacy concerns and conflicting ownership models still limit their use.

Smartphones - PKI

By contrast, a smartphone has almost limitless capacity for storing credentials, albeit with varying levels of security associated with cryptographic key storage. This should pave the way for 'identity wallet' apps, but that initiative has, until recently, been heavily constrained by the internal architecture of smartphones – especially the 'siloed' segregation of app data.

Smartphones regularly have inbuilt biometric sensors – fingerprint and facial recognition being the most common. This gives a highly convenient way of authorizing the use of a securely held private key for a signing or authentication operation for example. The fact that the reference samples are held on the phone too (typically in a secure enclave or element built into the fingerprint sensor) adds to their attraction, as there is then no need for sensitive biometric data to leave the direct control of the owner.

There are however some negative aspects to using phones of course. They have batteries that run down. There are prone to theft, damage and technical failure. Perhaps most importantly however, they are likely to be replaced on a regular basis. This means that credential lifecycle management is especially important, as the recovery and re-provisioning of dozens of credentials from different issuers is otherwise a thankless time-consuming chore.

Smartphones - FIDO

The emergence of FIDO authenticators began with USB tokens and extended to provide a solution for smart phones. However, the model used for FIDO deliberately places strong constraints on the visibility of credentials that

have been issued by different relying parties. Although a single relying party may allow the presentation of the same credential via different 'Facets' (e.g. website for browser, web service for apps), client agents belonging to different relying parties cannot enumerate or check the existence of another party's credentials.

This means that managing your credentials from a 3rd party app on your phone is not possible, so a solution must be implemented at the authentication service or at the point where the relying party maps the FIDO credential to a 'real' account.

With no current standards to define how binding / unbinding should work, each relying party must implement their own proprietary solution.

A secondary impact of this design decision is that there is no generic credential recovery / replacement protocol, which means that users have to manually re-enroll with every relying party in the event of a phone being lost, damaged or replaced.

USB Tokens

Although USB form-factor smart chips have been available for about 20 years, there has been a resurgence of interest in them recently, largely in response to the efforts of the FIDO Alliance in promoting them as a portable solution for 2-factor authentication to browsers. The addition of a 'touch to activate' sensor has also helped, as it addresses the strong desire to provide positive consent to the use of a credential.

The latest devices from Yubico for example now combine FIDO credentials with full FIPS-140 compliant cryptographic operations and PIV functionality in the same device. This is driving significant levels of adoption within agencies as a secondary means of authentication where a card reader is not available. Variants having USB-C connectivity are also opening up access from Apple MACs and Android phones.

This explosion of devices may be acceptable in a public / consumer environment, but within an enterprise or government, far more control is of crucial importance. Multiple credentials need to be able to be revoked from an authoritative source as part of a single, simple administrative process.

From the user's perspective, having discrete credentials to connect to hundreds of relying parties is transparent – until you lose or replace your phone, at which point the absence of any agreed standard for registration or recovery condemns you to a laborious exercise regenerating all of your credentials.

Consistent processes

With so many credentials and authenticators in circulation, the delivery of trust is heavily reliant on the strict, verifiable compliance to agree credentialing and maintenance policies. For some one-to-one trust models this is simple to enforce at the relying party's service entry point. For example, by enabling mutual TLS, where trusted issuers can be verified, and accounts

and policies can be mapped from the contents of the certificate being presented.

For credential types that do not explicitly carry policy information within the authentication response, the situation is much harder. In closed communities, this is unlikely to be a problem, as you would typically have a single authority responsible for ensuring consistent, appropriate policies throughout.

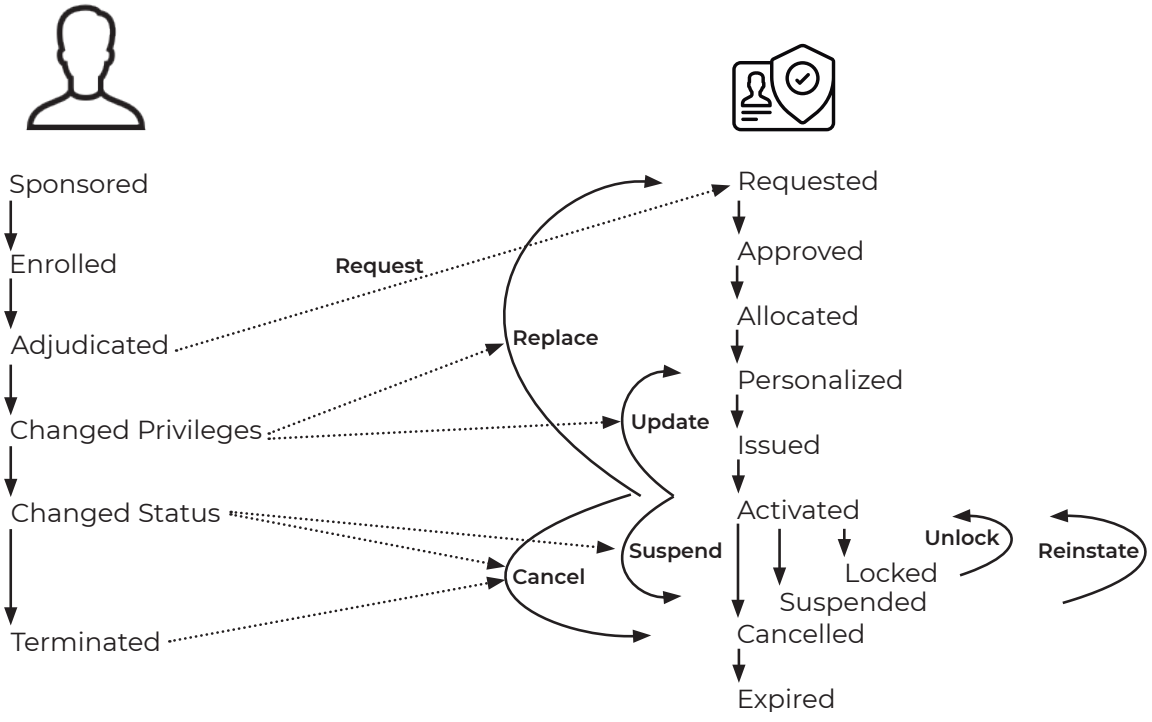
However, in an environment where individuals can effectively 'bring their own identity', this is much harder to enforce.

With many systems, the initial enrolment and protection of credentials is rarely the weak point that bad actors would exploit. Softer targets are the renewal / replacement / reset operations, where some form of back-up user verification is used, often involving live communications with support personnel who may be prone to social engineering deceptions.

For this reason, understanding and enforcing the entire user and credential lifecycle process is vitally important. Relying on manual processes to achieve this is dangerous.

The need to enforce lifecycle policy applies equally at the user level too. Any change to an employee's status may necessitate a flow-down of status changes to some or all of their managed devices and credentials.

Typical person and credential status lifecycles



Privacy vs Convenience

One of the drawbacks of PKI-based authentication schemes is the traceability of credentials, which allows relying parties to correlate user activity. This is rarely a problem in enterprise or government environments but can present risks in a 'bring your own' environment. In hybrid situations, we have to address the competing demands of one-to-one credentials (such as FIDO) and widely trusted ones (such as public PKI issuers).
FIDO credentials offer a very high level of privacy, as every relying party only sees their own FIDO authentication response. However, this isolation also applies to apps on the phone itself, making it impossible (by design) for an app to enumerate FIDO credentials that it (or another Facet of the same relying party) owns.

This means that on-device management of your entire FIDO credential list is not achievable with compliant authenticators. The solution must therefore reside on the authentication servers and potentially 3rd party trusted proxy credential issuers to deliver the lifecycle features that make FIDO credentials truly usable over time.

Managing policy changes

As cyber-attack tools steadily become more adept, it is necessary to be able to respond by upgrading your security policies. This might for example include migrating algorithms and key sizes for existing credentials and forcing renewals and reissuance processes to use the new policies. An exercise of this nature was performed a few years ago to migrate PIV cards from RSA1024/SHA-1 to RSA2048/SHA-256 keys.
With the ever-growing threat of quantum computers becoming available, cyber-agility will certainly be needed within the next 5-10 years.
This challenge clearly becomes much more complex when managing tens or hundreds of credentials for each employee. Again, some form of multi-party re-provisioning service would be needed to let agencies handle FIDO credentials with the necessary level of automation.

Credentialing non-person entities

Although the growth in credentials for authenticating people is considerable, it seems highly probable that delivering and managing credentials to non-person entities will present a substantially larger problem. As the Internet of Things (IoT) expands, the need to provide strong authentication bound to specific known devices is vital if we are trust these devices to connect to our networks. Being able to confirm identity and ownership is equally important if we are to trust the data from these devices, especially if we grant them permission to act with any degree of autonomy.

Relying party and client technologies

With so many assets, data and services residing on different systems and with varying levels of protection, finding a single solution to controlling access to resources is impractical. Over time, migrating to using authorization tokens (SAML, OAuth etc.) will help, but this is unlikely to be a quick fix given the huge list of legacy platform solutions currently in use.
It is clear that different solutions are needed for different purposes. Internal resources are generally simpler to manage but controlling access to shared services from a broad range of clients will need a high degree of flexibility. Until recently, the focus has been on using web browsers as the client of choice. While this offers a common baseline for many services, it is not the preferred option for desktop applications (e.g. word processing, spreadsheets, presentations, project management), nor is it the natural route for mobile users, where dedicated apps are far more convenient and generally more secure.
This means that different solutions are needed to handle these cases, resulting in specific authenticators according to the demands of the services being used.

Mobile device management

Most agencies and other organizations have one or more Mobile Device Management solutions in place to control their mobile population. Some CMS products support tight integration with one or more MDM vendors. This means that the management of the device is tightly bound to the management of credentials on that device.
MDM solutions alone cannot address the problems of unified management though. Certificate management, unblocking, renewals and numerous other issues demand a closely coupled solution to enforce policy and to ensure the integrity of the devices and their credentials.

Necessary solutions

It is obvious from the above that the expansion of credentials will require additional management capabilities, and that these should be unified under a common framework to ensure that the ‘flow down’ of status changes and events is handled consistently.
There is however a conflict regarding the type of credentials now being proposed. Historically, authentication within enterprises or other closed communities has used credentials capable of being centrally managed

Multi-device Credentials

Existing CMS solutions (e.g. Intercede's MyID) already have extensive capabilities in this area, being able to manage a very broad range of devices having complex ownership models and variable lifecycles. The following are crucial capabilities for anyone needing to manage such an ecosystem:

- Role-based permissions for all actors
- Strong authentication for CMS administration
- Secure audit to verify compliance
- Groups / scoping models to determine which people and devices can be managed
- Multiple credential profiles to accommodate changing form factors and content
- Credential profile versioning to support cyber agility and policy migration
- Concurrent interoperation with multiple certification authorities
- Good self-service capabilities to minimize administrative overheads

All of the above are fine for 'traditional' devices and credentials, but with the 'bring your own ID' model used by FIDO, this becomes more problematic. There are three primary components for a solution here.

- Binding a FIDO credential to a person
- Revocation of a FIDO credential if compromised, lost or the user's status changes
- Semi-automated recovery or replacement of lost credentials

FIDO Credential Binding

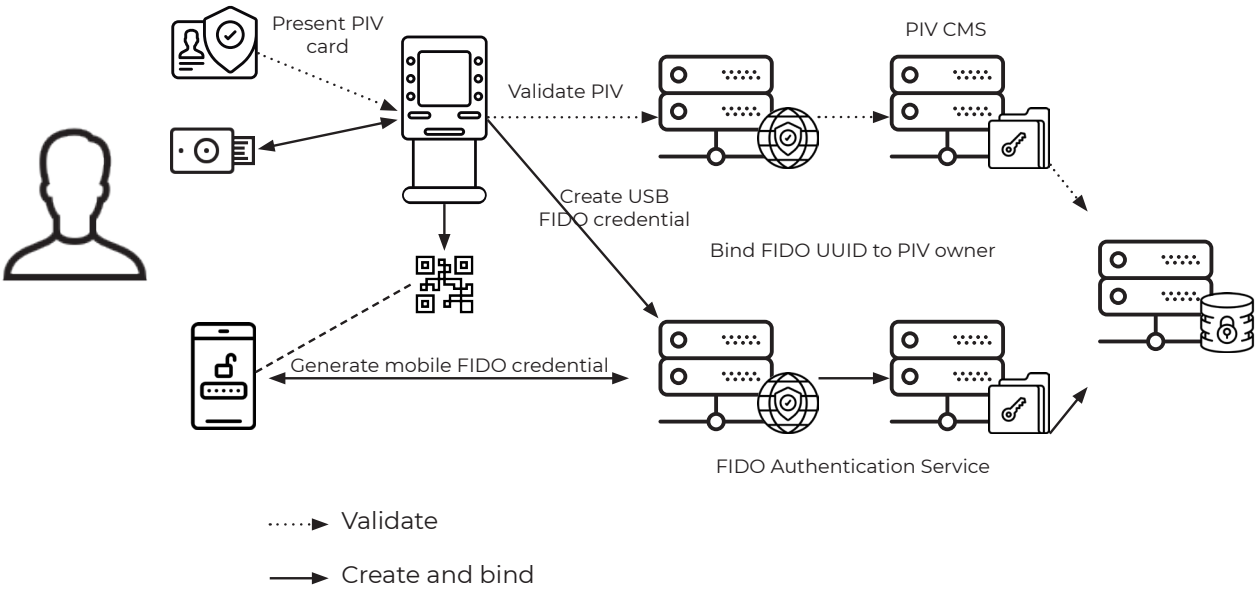
A significant challenge with using FIDO credentials for federal employees is that FIDO is designed as an essentially anonymous authenticator. The association with a 'real person' is purely down to the relying party. This means that the relying party needs to be able to validate the identity of the individual during the enrolment process – essentially the same as a derived PIV credential enrolment.

The good news then is that an adaptation to existing derived credential self-service 'kiosk' software, with an updated mobile SDK or app might allow a common framework to be deployed to meet this requirement.

There is however one other component needed – a service to selectively bind a FIDO public key to a federal identity. This would be provided as an attribute or assertion service, having the ability to selectively return data about the person who has presented the credential.

In order for this to function as a centralized lookup service, it would of course have to reflect the current status of the bound user account. This effectively builds in a revocation check for the entire user or a specific credential.

PIV Derived FIDO Credentials



All of this is achievable of course, but it does beg the question 'why?'

What we have done is taken an anonymous authenticator that is designed to be able to be checked 1:1 by a single relying party, and then added the necessary infrastructure to allow multiple relying parties and bind it to a centrally managed identity. Is there actually any benefit in using this convoluted solution to replace PKI - an existing well-proven standard?

Additionally, the strictly siloed nature of FIDO credentials means that every app on the phone would need to have its own credentials, or rely on an OpenID Connect-style token-based authorization mechanism, which is quite clumsy to operate from a user perspective (the authentication step typically has to redirect via the browser, even if you are logging into an app)
The main benefit in this case would be the ability to use authenticator keystores on phones that may be more secure than the hardware-backed software stores typically used for PKI solutions. In particular, the standardization of biometric activation and the ability to have cryptographically attested FIDO authenticators does provide a higher level of confidence in the integrity of what could be a large range of otherwise proprietary clients.

FIDO Credential Replacement

Once FIDO credentials have been deployed, they will need to be managed throughout the lifecycle of the device they are on. With cell phones typically being changed every 2 to 3 years, due to failures, obsolescence, theft, damage etc., users have to be able to remember every one of the relying parties with whom they have a relationship and return to each of those providers' registration or recovery portals to follow a manual recovery process. This is clearly undesirable when compared with the relatively painless process of getting a replacement smart card. What is needed therefore is some form of semi-automatic credential recovery broker, capable of securely recording the list of public keys and relying parties for each user, that is trusted by consenting relying parties to perform re-credentialing on their behalf, subject to an agreed protocol.

Federation

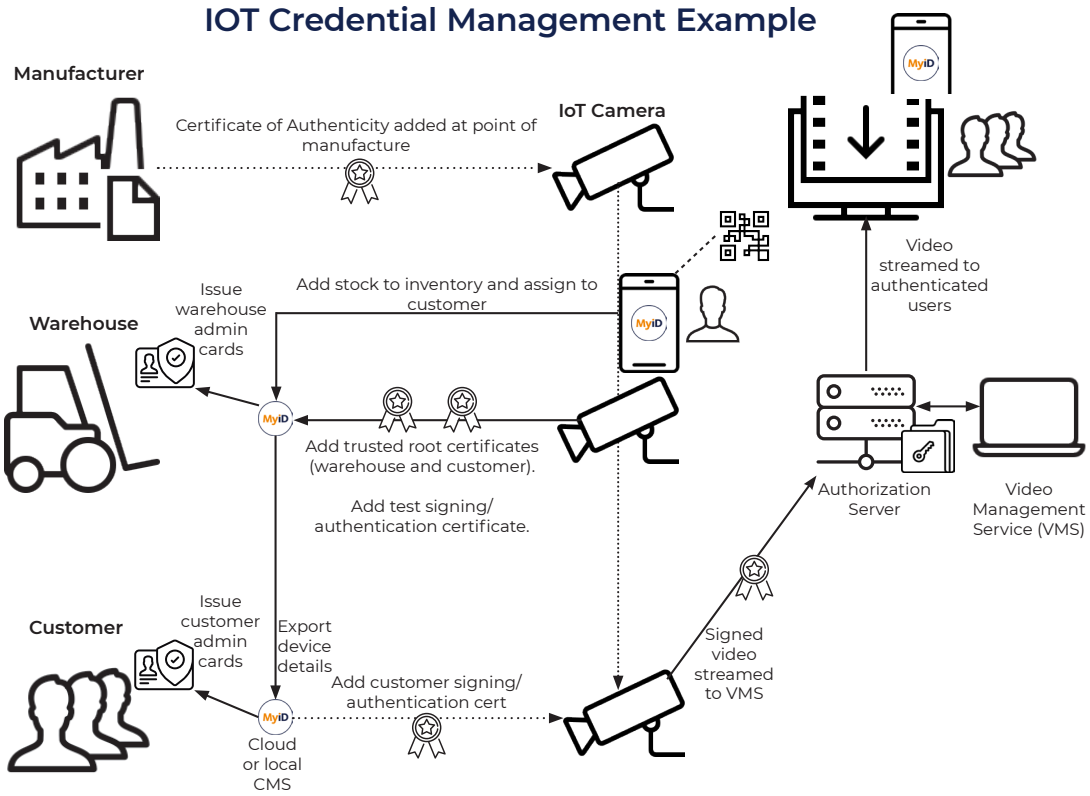
A lot of the issues above can be side-stepped by opting for a federated authorization service. This would allow relying parties to trust tokens issued by the service. In theory this avoids many of the pitfalls associated with FIDO – users would only need to manage a few FIDO credentials on their phone, making manual recovery less onerous. The server could also act as an attribute broker, being able to include specific attributes in the generated tokens, in addition to validating the current user account status. It does however only address some of the use cases we need and represents a potential single point of failure in the system (something that FIDO was also trying to avoid by devolving the authentication the relying parties themselves).

IoT

Managing the identity of things requires solutions to address some or all of the following:

- Establish a chain of trust back to the original device manufacturer
- Install a trusted client certificate to enable local network access and permissions
- Install a server SSL certificate to allow your users and services to trust the device and communicate over TLS
- Lock down the device to only permit mutual TLS administrative access

A provisioning service will in most cases also assign an 'owner' for each device, so that a chain of responsibility can be maintained. Whenever an owner is changed, it may be necessary to re-provision some or all of the post-factory credentials.
Some cases may be even more complex than this, with a further tier of credential to represent some form of equipment test and approval status (for example, registering commercial drones with the FAA before assigning owners/operators). The schematic overleaf illustrates an existing commercial solution for managing high security surveillance cameras.



Conclusions

Extending the number and types of authenticator that can be used in federal government and related sectors, is an important and necessary step towards achieving ubiquitous secure access to resources and services. It is evident however that achieving this will require significant investment to upgrade existing CMS solutions for the new device types and processes.

A lot of the necessary functionality is in place within existing CMS products, but there are still known gaps to be filled, and more that will emerge as the market matures.

What has to be avoided though is the risk of discrete, ad hoc solutions to parts of the problem without a plan for eventual unified management. Agencies and contractors should already be considering the architecture and tools they will need to control the expected explosion of devices and credentials, before the problem reaches critical proportions.

The choice of an appropriate, adaptive platform for credential management is the core of any such solution architecture. It should be one of the first components to be considered as the new wave of devices, form factors and credentials begin flowing out around federal agencies and associated industries.

Additional Information

Glossary of Acronyms

AAL	Authentication Assurance Level
CMS	Credential Management System
FAL	Federation Assurance Level
FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standards
HSPD	Homeland Security Presidential Directive
IAL	Identity Assurance level
IIoT	Industrial Internet of Things
IoT	Internet of Things
LOA	Level of Assurance
MDM	Mobile Device Management
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OAuth	Open Authorization (an authorization token standard)
OMB	Office of Management and Budget
OpenID	An authentication protocol standard
PIN	Personal Identification Number
PIV	Personal Identity Verification (the Federal ID card standard)
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language (an authorization token standard)
SDK	Software Development Kit
SP	Special Publication
SSL	Secure Sockets Layer (superseded by TLS)
TIM	TSA – TTAC Infrastructure Modernization Program
TLS	Transport layer security
TWIC	Transport Workers Identity Card
USB	Universal Serial Bus

References

HSPD-12	https://www.dhs.gov/homeland-security-presidential-directive-12
FIPS 201-2	https://csrc.nist.gov/publications/detail/fips/201/2/final
OMB-M-19-17	https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
SP800-63-3	https://pages.nist.gov/800-63-3/
SP800-157	https://csrc.nist.gov/publications/detail/sp/800-157/final

intercede

@ intercedeMyID

e info@intercede.com

w intercede.com

UK

Lutterworth Hall, St. Mary's Road,
Lutterworth, Leicestershire
LE17 4PS UK

t +44 (0)1455 558 111

US

Suite 920, 1875 Explorer Street,
Reston, VA 20190 USA

t +1 888 646 6943