intercede

PIV derived credentials

Chris Edwards
CTO, Intercede

DIGITAL TRUST
from Silicon to Services

Contents

1 Overview

The use of mobile devices has accelerated rapidly over the past four years, with many organizations implementing ‘Bring Your Own Device’ or ‘Choose Your Own Device’ strategies to improve the efficiency of an increasingly mobile workforce.

To some degree however, this has risked compromising the high levels of security necessary for remote access. This is especially true within government agencies, where the PIV program for smart card strong authentication has been the cornerstone of secure physical and logical access to resources for several years now.

To meet this requirement, NIST have defined the use of a ‘derived credential’ for use on mobile devices. This can be used to provide secure access to agency systems, services and data from the smartphones, tablets and laptops that are now the preferred routes to business information systems.

This white paper describes the background to PIV derived credentials, explains the technology behind them and offers practical solutions to the problems of implementing an effective and compliant solution for your agency.

It makes reference to the Intercede MyID suite of credential management services and products to illustrate how to deliver a complete derived credential ecosystem using currently available components and services.

The technologies employed in these solutions are by no means restricted to Federal Government environments of course. Commercial organizations are equally able to take advantage of the techniques and products described here to help with the secure mobilization of their employees, contractors and customers.

2 Background

2.1 The PIV program

The US Federal Government personal identity verification (PIV) program was implemented in response to a presidential directive (HSPD-12) in order to improve the security of government resources and facilities. Core to this activity was the FIPS 201 standard for smart cards to be used for physical and logical access control. This standard and its related special publications defined hardware, systems and processes for the secure issuance and maintenance of high assurance trusted identity credentials.

The PIV program has been successfully rolled out over the entire Federal Government, with a technically identical credential being deployed to government contractors ('PIV-I') and non-government organizations ('CIV'). PIV cards are now being used to manage access to facilities, authentication to networks and online services and to secure communications through signing and encryption.

When PIV was instigated, a similar program was already underway in the defense department, using a differently specified 'Common Access Card' (CAC). Over the intervening years, these two standards have slowly converged to the extent that CAC and PIV cards now share a significant number of content containers and provide a largely interoperable 'card edge' programming interface. As of 2014 there are approximately 1.4 million PIV cards and 3 million CACs in circulation. Once related deployments (such as the Transportation Worker Identification Credential, with over 2 million cards) and numerous enterprise solutions (especially in the aerospace and defense contractor markets) are taken into consideration, it is evident that there are well in excess of 10 million technically compatible smart cards in current use.

2.2 Smart cards

The smart card form factor is very convenient in many respects. It fits neatly into your wallet, can operate in contact or contactless modes, is highly standardized and hence offers very good levels of interoperability. Enterprise grade laptops typically include smart card readers. External readers for desktop computers are widely available and cheap.

The ubiquity of the PIV standard in particular has meant that operating system vendors have been able to provide native support for the cards, largely removing the need to source third party drivers and middleware.

The contactless technology chosen for PIV cards is compatible with the widely implemented ISO-14443 standard, as used in numerous ticketing and physical access security systems (PACS) in addition to the mobile NFC standard. The vendors of these systems have therefore been able to provide PIV-enabled variants with relative ease.

Put simply, the cards 'just work'.

2.3 Mobility

A major change has taken place over the past five years in the way that we all work and communicate. Around 60% of internet access is now from mobile devices1. Remote access to corporate networks and cloud services is needed from locations other than your desk. However, the security requirements of such access have not changed; a high level of confidence in the identity of an individual connecting to these data services is still necessary. If anything, with the dissolution of geographical boundaries, such strong authentication becomes even more important.

With the move towards mobile devices however, using a smart card is no longer an easy option. Phones and tablets do not have integrated card readers. It is evident then that we need to provide trusted credentials that can be used conveniently by mobile devices.

Initial attempts to provide strong mobile authentication relied on externally connected card readers for mobile phones and tablets. Wired card readers were not especially practical, but Bluetooth coupled card readers were adopted by some sectors to address the problem. These too had their issues though. Battery life was a problem (they require independent power) and of course it meant carrying yet another device, similar in size to the phone itself.

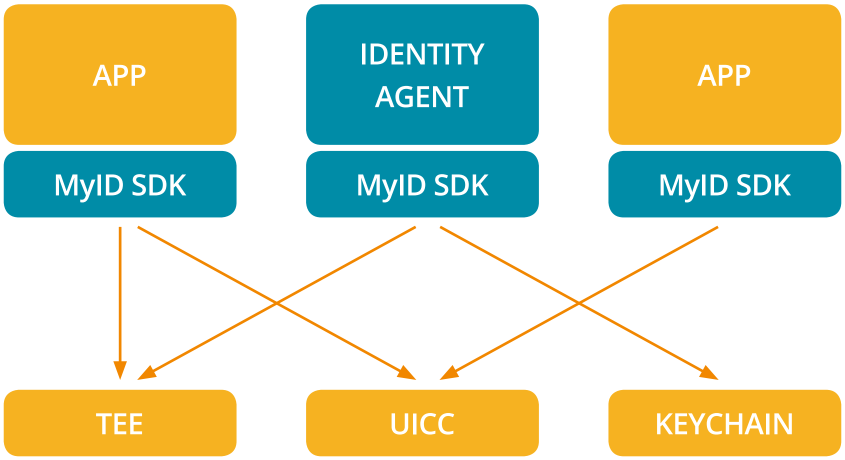
What was needed was a way to put the credential directly into the phone or tablet, while being able to achieve an acceptable level of security for the private cryptographic keys that are relied upon for authentication, signing and encryption. As it was clear that mobile credentials would not be able to fully replace smart cards for some time, a solution based on 'derived credentials' (PIV-D) was proposed in the revised FIPS 201-22 standard, with detailed guidance to be provided in the NIST special publication 800-1573.

2.4 Mobile use cases

The primary application considered for mobile use was, historically, secure email. The ability to sign emails with a trusted credential is important, but so too is being able to read encrypted emails when away from your desk. This remains a very important application for every user.

Increasingly however, secure access to corporate resources and cloud services is emerging as the most important requirement. This allows strongly authenticated connections to data repositories such as SharePoint. For this you need a secure browser capable of client TLS authentication, and probably VPN access too. Virtual desktops are also popular, so these too will need to be PIV-D enabled.

Agencies are also expanding their use of dedicated mobile apps to perform specific business activities. These apps are either 'home grown', contracted out or adapted from existing public apps to suit their particular needs. This will often include identity and authentication related functions. It is imperative therefore that an API and software libraries are available to allow these apps to consume the PIV-D credentials in a consistent manner.

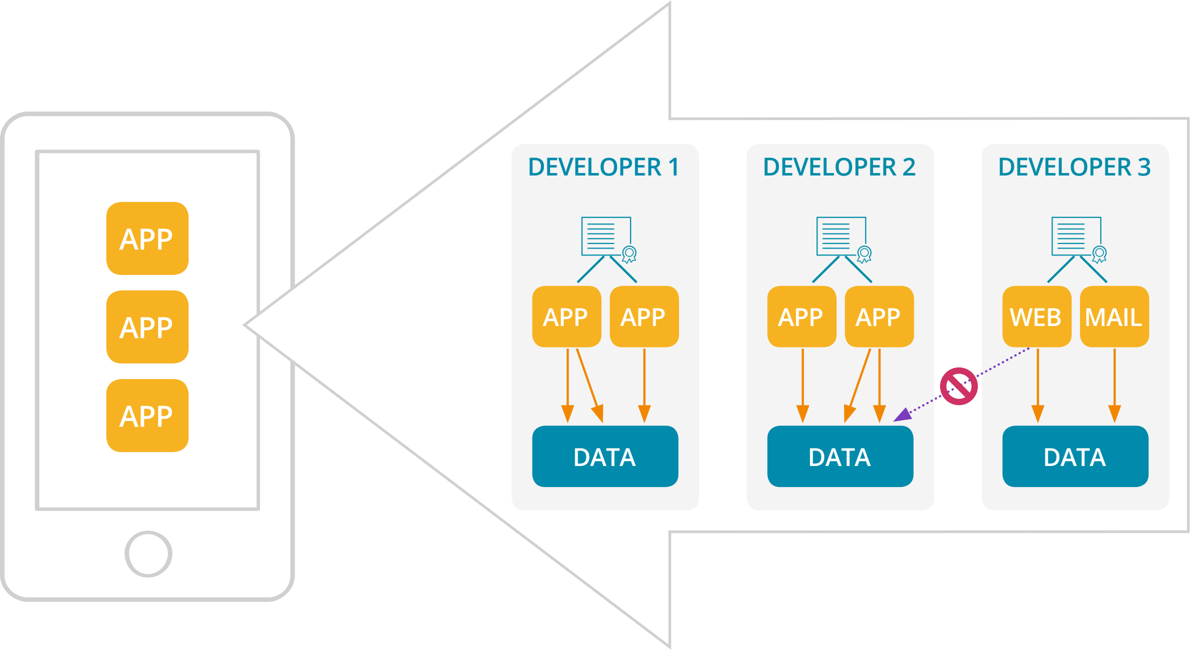


3 Mobile credentials

3.1 Software keystores

Smartphones and tablets present special challenges when it comes to delivering high-integrity PKI credentials. Operating systems such as BlackBerry OS7 and Windows include a shared 'cryptographic service layer' – a standardized programing interface through which any app can access credentials delivered to the device. This means that provided you can deliver keys and certificates to the phone, the operating system will take care of the 'plumbing' to manage their usage.

Apple iOS and Android however adopted a far more 'siloed' approach to their operating systems and do not provide a device-wide, comprehensive cryptographic layer for apps to consume. For example, certificates and keys installed using Safari on an iPhone cannot be used by your own apps – only by the 'native' apps such as Safari itself and the default mail app. Similarly, if your app directly imports credentials to its keychain, then Safari and Mail cannot use them.



Another challenge with iOS and Android is that there is no secondary authentication to the keychain. Once you have unlocked your phone, apps can use the credentials without needing further user authentication. Given the problems that have been encountered historically with lock-screen security on a number of phones, it is evident that this is not a reliable basis for a higher security credential.

3.2 Hardware keystores

For enhanced security we need to protect private keys by storing them in 'secure elements' (SE). These are hardware devices, technically similar to smart cards but with different form-factors. An SE provides an environment where keys can be held in a non-exportable form, with cryptographic functions such as signing and encryption being performed within the SE. Access to functions that need to use the keys may be protected by a user PIN, with a 'lockout' after a fixed number of failed user authentication attempts.

In phones and tablets, secure elements may be present as:

- UICCs (aka 'SIMs')
- embedded within the device (to support NFC functions for example)
- removable 'secure microSD' memory cards
- externally attached elements in sleeves or dongles
- wirelessly connected devices using Bluetooth or NFC

In addition, many devices support a Trusted Execution Environment (TEE), which can also provide key storage with a 'trusted user interface' for PIN entry.

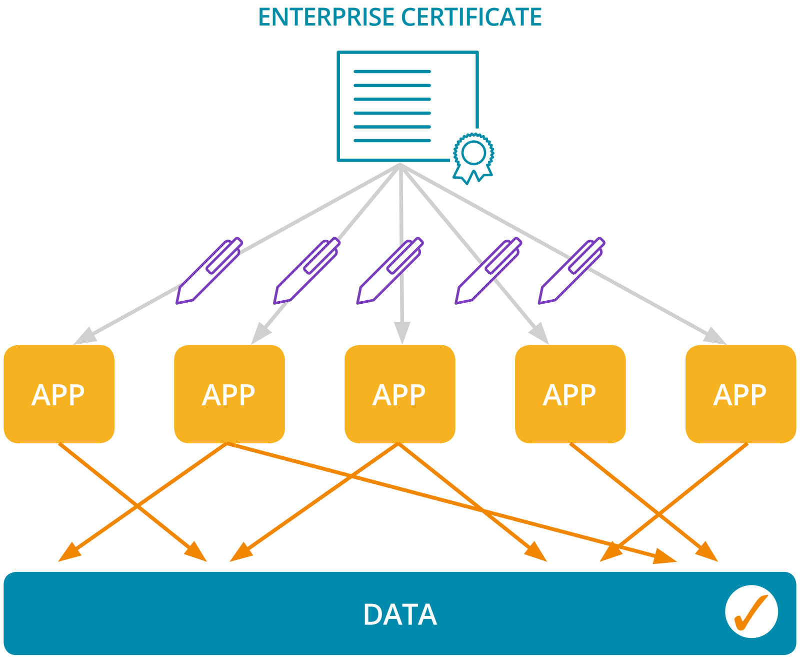
Secure elements offer features that would enable a higher Level of Assurance than software key stores. Typically this would allow LOA-4 rather than LOA-3 credential compliance. However, to be acceptable to US Government, any cryptographic component must have passed a FIPS 140 assessment. At present, this effectively prevents the use of almost all hardware secure elements in mobile devices.

3.3 Mobile device architectures

Most mobile devices available today are based on operating system architectures that have some fundamental differences from traditional desktop computers. The main difference is in the degree of isolation provided between applications. On iOS and Android, each mobile app is signed with a developer or enterprise certificate, which lets the O/S create what is effectively an execution and data 'silo' for each set of apps signed by the same issuer. This means that data objects created by one set of apps cannot be read or modified directly by another app.

Importantly, these platforms lack a secure, shared cryptographic key storage and access mechanism. This means that although the strict separation performs an excellent role in preventing a high proportion of malware attack methods, the ability to deliver strong authentication that can be used by any app on the device is somewhat limited.

This limitation can be turned to our advantage however, in that it provides the means to isolate sets of apps into discrete working environments so that for example, work data can be kept separately from personal information. The only downside to this is then the inability to share provisioned credentials with the 'native' apps provided by the platforms.



3.4 Key storage on mobile devices

The most important aspect of using strong credentials on a device is the underlying security of private and secret key storage. The 'gold standard' for key storage is probably represented by smart cards, where a dedicated hardware device is used to store and process cryptographic material without the protected keys ever being exposed outside of the card itself. Access to the functions of the card can be protected by a user PIN or on-board biometric match, with enforced lock-out after a defined number of invalid authentication attempts.

At the opposite end of the security scale, we have the default software 'keychain' methods available on iOS and Android, which rely largely on the device screen-lock for their protection and have limited protection against key export and no 'lock out' facilities.

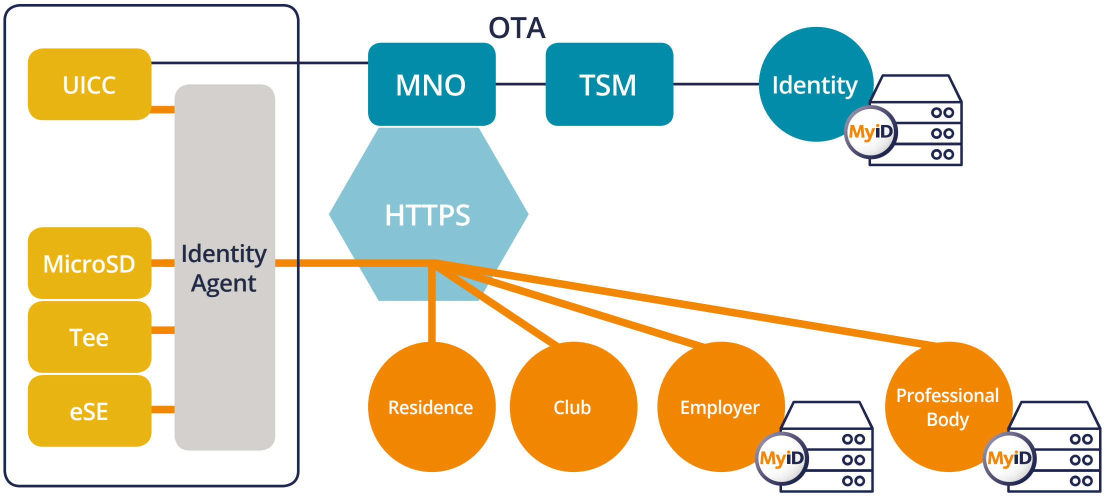
Between these two extremes there are many mechanisms for providing cryptographic storage and programming interfaces, all of which rely to some degree on the use of third party software, devices and apps.

3.4.1 UICC

The highest security is probably afforded by the use of the UICC (aka 'new generation SIM'). This is a removable device having essentially the same technology as a traditional smart card. UICCs typically run a Global Platform environment that allows multiple 'applets' to run on them, including for example a PIV applet. This 'ideal' solution does however have two serious drawbacks.

First, programmatic access to the UICC from mobile apps is limited or non-existent. iOS does not allow apps to communicate directly with the UICC at all. On Android, the FSeek library (from the SIM Alliance) is present on an increasing number of devices, although the completeness of the driver implementation is somewhat patchy (for example, support for extended APDU command sequences is absent in some cases).

The second issue is more commercial in nature, but no less important. UICCs are configured and issued by each Mobile Network Operator (MNO). UICCs have limited capacity and there are competing demands for applets on the chip, which will differ for each service provider. In a BYOD environment, multiple MNOs may need to provide a common solution, which could vary for each of their corporate customers. The resulting conflicts make deployments extremely difficult to achieve in practice at an economical price. The proposed solution to this problem involves a third party 'Trusted Service Manager' (TSM) to install identity applets onto each UICC. MNO-independent TSMs are emerging, but it is unclear how successful they will be in negotiating the commercial and technical agreements needed to make this option universally tenable.



For US Federal applications, any cryptographic module must have a FIPS 140-2 accreditation. Due to the security targets, the nature of UICCs, the co-resident GSM applets and other architectural considerations, achieving FIPS 140 compliance has proved difficult.

3.4.2 Embedded secure element

Many mobile devices include a secure element on the mainboard itself, often in support of an NFC chip for example. Although potentially more exposed to physical tampering than the UICC, they typically present a similar level of security, with most running a Global Platform environment capable of running PKI applets. FIPS 140 validation may again present some challenges, and API support for app programmers may be limited or heavily constrained depending on the platform.

3.4.3 Secure microSD card

The MicroSD storage card is supported by a significant number of phones and tablets, especially many Android devices. Specialist cards are available that combine storage with a secure element that behaves like a smart card.

These devices may interface to the phone through a recognized file-based command system (such as ASSD) or use a proprietary communication channel. It is also possible to personalize these devices through a reader directly connected to a workstation.

There are secure microSD cards available that have FIPS 140 level 3 certification.
[e.g. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1191.pdf]

3.4.4 External security devices

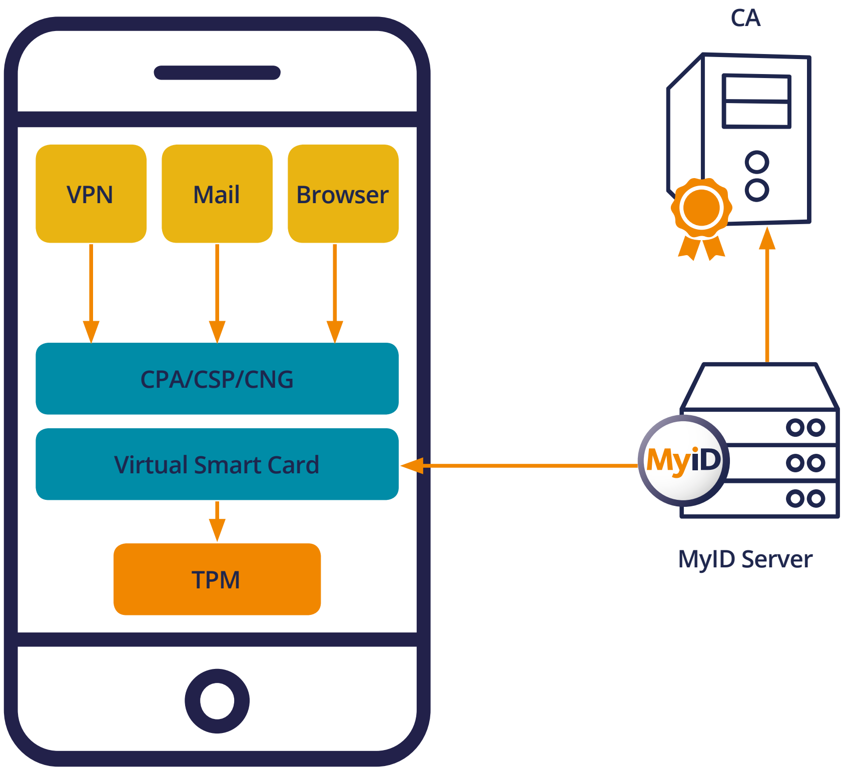
Numerous after-market peripherals present opportunities for secure element key storage on mobile devices. Physically connected smart card / SIM readers, NFC sleeves and microSD connectors fall into this category. Wireless connected peripherals are also available – these may have an embedded secure element directly, or rely on a physically cut-down smart card to provide cryptographic storage and functions.

Peripherals that accept an existing cut-down smart card have the advantage of being able to use existing FIPS 140 compliant devices. However, there are some concerns over the communications channel security (forced re-pairing of Bluetooth devices for example), and the need to carry an additional device, however small, is often disliked by consumers.

3.4.5 Trusted Platform Modules

Every Windows 8 device includes a 'Trusted Platform Module'; that is, a secure element built onto the mainboard. This provides secure key storage and protected cryptographic processing to support identity, authentication and system integrity checking capabilities.

When combined with the Windows 8 'virtual smart card' feature and a credential management system, this presents an attractive option for derived credentials, as virtual smart cards are tightly integrated with apps on phones, tablets and desktops, thanks to the universal cryptographic services layer present on all Windows devices.



The Windows 8 cryptography layer has been certified to FIPS 140 Level 1, as have some TPMs.

3.4.6 Trusted Execution Environments

The overwhelming majority of phones and tablets on the market today have a 'Trustzone®' available within their ARM® System-On-A-Chip processors. An increasing number of devices now also include the necessary Trusted Execution Environment implementations for apps to take advantage of the higher integrity, data segregation, privileged access and trusted user interface afforded by these environments.

The level of protection afforded to cryptographic keys in a TEE is typically lower than that offered by a dedicated secure element, but the trusted UI and memory protection do have significant benefits for keystore operations.

3.4.7 Software keystores

The baseline for key storage and cryptographic operations is the software keystore present in some form on most devices. They have the big advantage of being relatively easy to implement and use, but offer limited protection for the private keys. PIN protection and control over key export is not always enforced, and the absence of PIN lockout in many cases leaves them susceptible to brute forcing.

Application data silos can help to protect unsanctioned access to credentials (as each keystore is encrypted using a key derived from the developer certificate) and the concept of 'hardware backed' keystores means that the encryption root is well protected.

Individual providers can of course implement their own security enhancements within a software keystore, which can add PIN lockout for example.

By taking full advantage of these features, it is reasonable to consider a software keystore as being suitable for LOA 3 credentials, which are adequate for a high proportion of Federal Government applications.

4 Using derived credentials

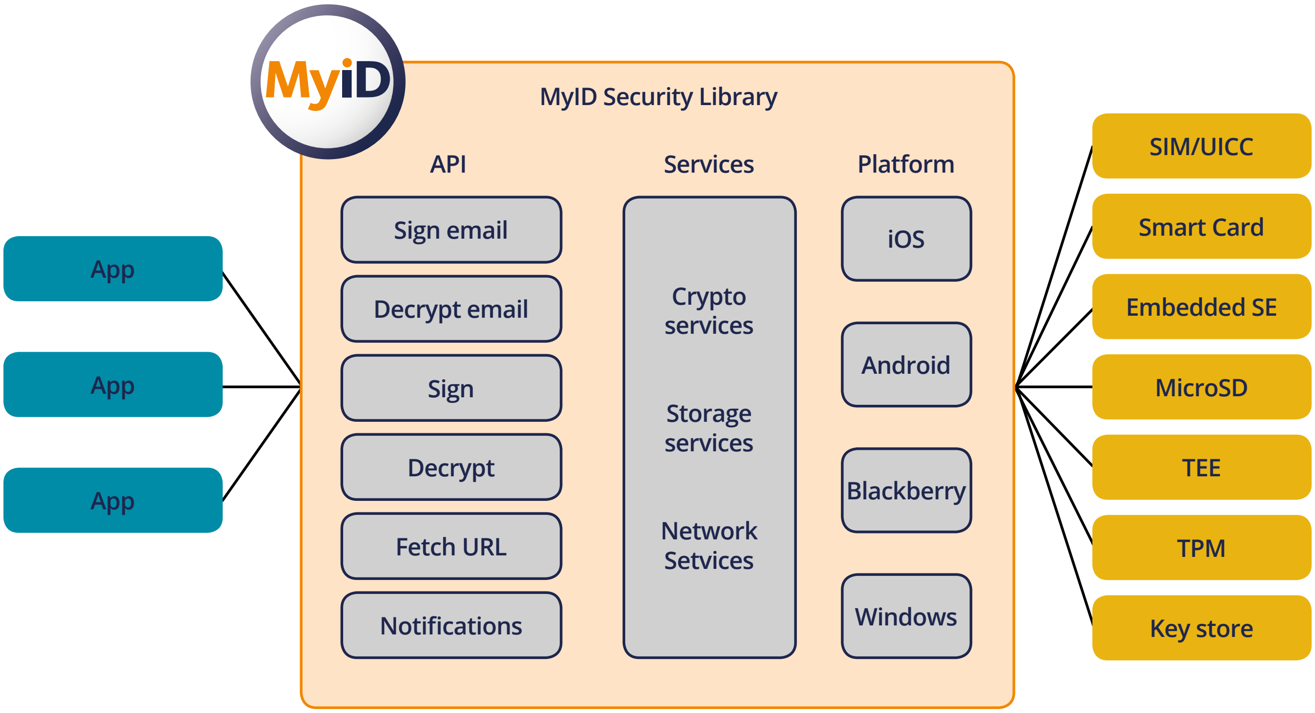
For derived credentials to be of any use they must clearly be made available to apps on your mobile device. The 'formal' definition of a derived credential is purely an authentication certificate. This must be able to be used for securing connections to services, systems and data. Typically this is through the use of 2-way TLS authentication to websites and services, VPN access to systems or authenticating to virtual desktop environments. Other services may implement their own PKI authentication schemes in which the derived authentication certificate may be used.

With the wide range of cryptographic key storage devices available, most of which support different programming interfaces, it is clear that we need a readily consumed library for apps to operate with a range of devices as transparently as possible. Once you add the (widely requested) additional features such as signing, encryption, physical access, verifiable flash badges and other use cases, the consumption of mobile credentials becomes even more challenging for app vendors.

Traditionally, cryptographic interfaces on other platforms have provided APIs that let application authors navigate the content of keystores and devices at a relatively low level. Public API standards such as the 20 year old PKCS#11, or vendor-specific layers such as Microsoft's CSP / CNG have provided the syntax for communicating with these devices. The onus is still very much on the application writer to understand the meaning and intended use of each credential within each carrier. This is time-consuming and requires a lot of code to enumerate devices, recognize them, enumerate the content, examine certificate usage, understand the specific user authentication schemes and then potentially handle proprietary extensions for secure device management.

What is really needed however, is a higher level abstraction of functions, at an application level. For example, 'sign email', 'get URL with 2-way TLS', 'decrypt data'. One method call of this nature can replace hundreds of lines of application code and provide a highly consistent policy and user preference enforcement without specialist knowledge on the part of the programmer.

One such library is provided as part of Intercede's 'MyID Mobile SDK'. This abstracts cryptographic functional support to the level of single method calls for the most commonly used operations. It supports a wide range of hardware and software keystores and devices, and may also be coupled to the MyID credential management system to provide credential generation and full lifecycle management (see next page).



Intercede provide some commonly used apps (MyID Mail, MyID Browser) and also license the SDK for use by third party app developers. This enables software vendors and in-house teams to enhance their apps to take immediate advantage of PIV derived credentials with minimal cost and very short lead times.

5 Credential delivery and management

With any credentialing environment, a secure, policy-enforcing lifecycle management system is vital. In the case of PIV-D, the standard describes specific business processes for the two supported levels of assurance, which must be followed by any compliant solution. Such a solution will need to have strong authentication for operators and full audit capabilities to allow rapid, secure access to administrative functions.

The process for delivering a PIV derived credential demands a number of stages to establish the identity, entitlement and suitability of the applicant and the mobile device that will hold the PIV-D.

These stages are:

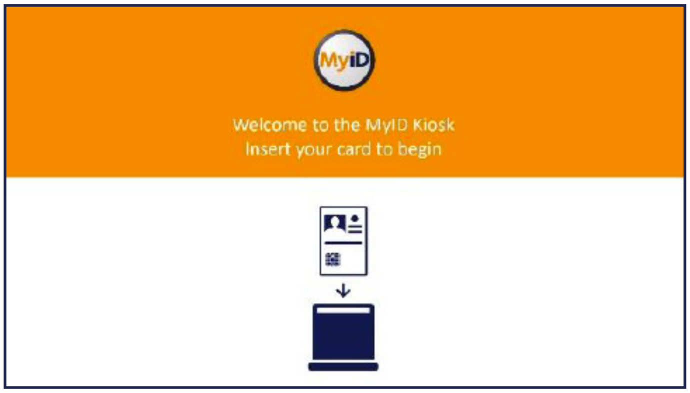
- Read and validate the applicant's existing PIV card
- Perform a user authentication with the card to verify the owner's presence
- Identify the device that is to hold the credential and associate it with the applicant
- Establish a secure connection between the device and the PIV-D CMS
- Create and install the PIV-D credentials

To minimize cost and inconvenience, a self-service process is allowed for derived credentials. This may be unattended (for LOA3) or attended (for LOA4). The higher assurance variant also requires a biometric verification of the cardholder before PIV-D issuance is permitted.

5.1 PIV-D issuance to a phone

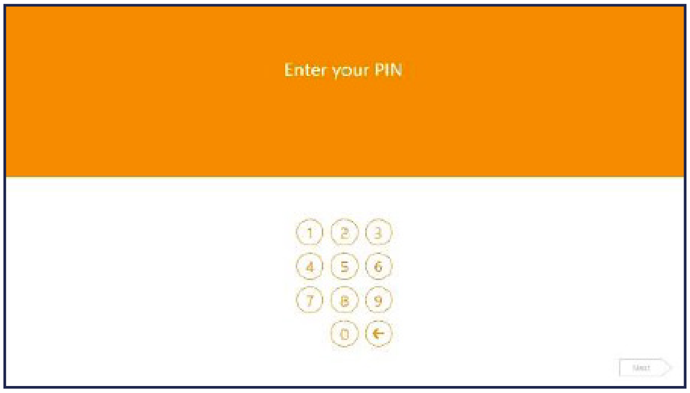
A typical PIV-D issuing environment would therefore be a ‘self-service kiosk’ such as Intercede’s MyID product, that looks and behaves in a manner similar to a banking ATM. The sequence of screens is shown below:

1. A PIV cardholder approaches the kiosk and inserts their PIV card to begin the process.



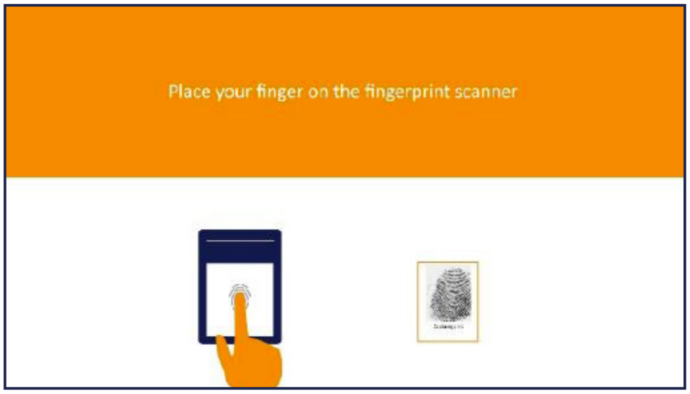
Welcome to the MyID Kiosk
Insert your card to begin

2. The kiosk reads their card and validates it against the list of issuers and agencies that it has been configured to support. It then prompts the applicant to enter their PIN.



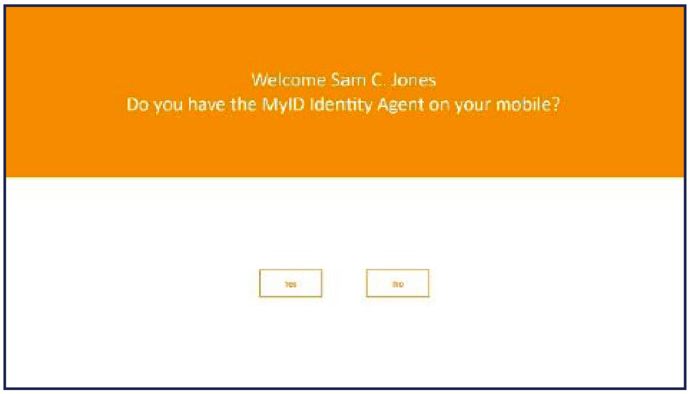
Enter your PIN

3. If LOA4 credentials are to be issued, the applicant is asked to authenticate biometrically by giving a fingerprint sample.



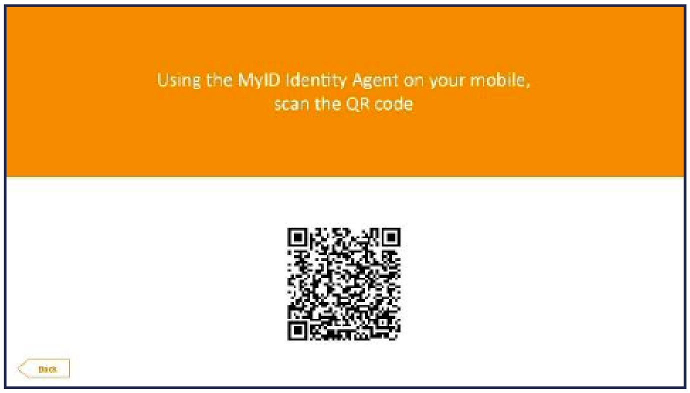
Place your finger on the fingerprint scanner

4. The kiosk checks that the applicant has the necessary Identity Agent app on their phone (and provides a QR link to download it from the app store if necessary).



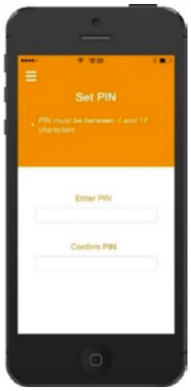
Welcome Sam C. Jones
Do you have the MyID Identity Agent on your mobile?

5. The applicant is now asked to scan the QR code using the Identity Agent app on their phone. This contains a unique, single-use reference to a derived credential request, which confirms the physical presence of the phone and associates it with the applicant's PIV-D account.



Using the MyID Identity Agent on your mobile, scan the QR code

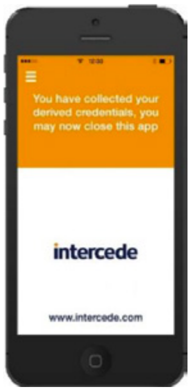
1. The PIV-D CMS now communicates directly with the phone app (using WiFi or another internet connection) to create containers, generate keys and install the credentials. As part of this process, the applicant must choose and confirm a PIN for their credential store.



Set PIN

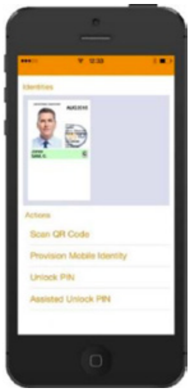
PIN must be between 4 and 12 characters

2. The PIV-D, plus any additional credential data (such as signing keys and virtual badges) are transmitted to the phone and stored securely within the container that is managed by the Identity Agent.



You have collected your derived credentials, you may now close this app

3. A visual representation of the credential may be included if desired as a 'virtual badge'.



This simple process can of course be augmented where necessary to meet specific agency requirements for business process – for example, by requiring an administrator to explicitly authorize the PIV-D request. The principle of a low-impact solution remains though.

5.2 PIV-D lifecycle management

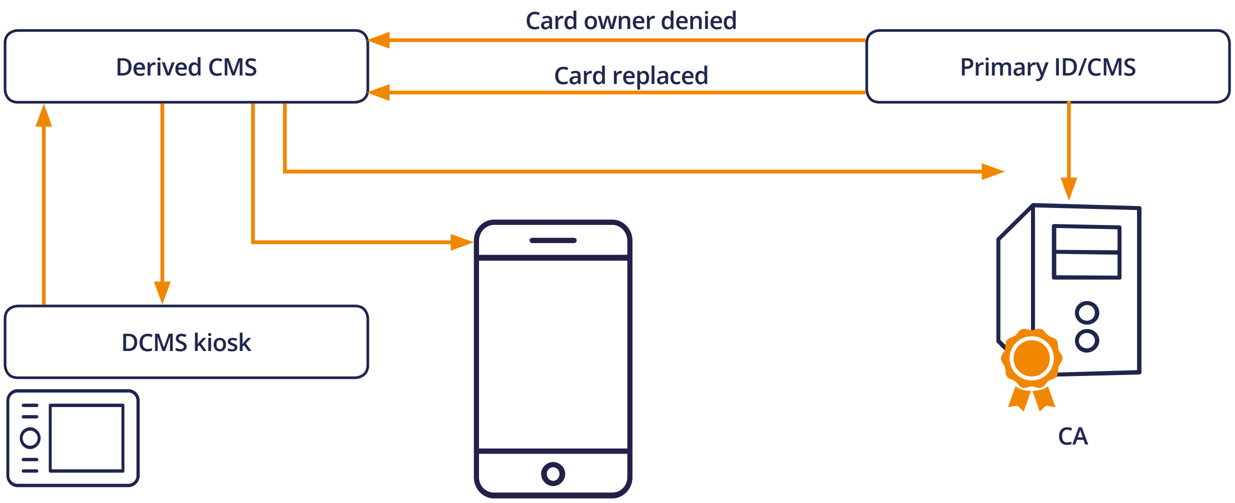
Delivering the PIV-D credential to the phone is in many respects the simple part of the problem. Once a credential has been issued, you must be able to manage it throughout its lifecycle. Planned events such as expiration and renewals must be accommodated, but so too must exceptions such as theft, loss or damage to the phone or PIV card, locking the PIN on the PIV-D container, selling and replacing the phone, change of employment status and so on.

Within the US Federal Government's definition of derived credentials, the link between the original PIV card and the PIV-D is akin to that of the i9 'breeder' proof-of-identity documents that are required when applying for the original PIV card. It is used to establish the applicant's identity and (in principle) their right to a PIV-D credential. Once enrolled for PIV-D, the status of the original PIV card is of no more interest than the status of a PIV cardholder's passport after the card has been collected.

This means for example that the PIV-D can have a lifetime that extends beyond the expiration date of the card and that if the card is lost and revoked, there is no need to revoke the PIV-D. In fact, this is one of the primary benefits of PIV-D; it provides continuity of service while a replacement card is procured.

However, there are some circumstances under which the PIV-D credential *must* be revoked. Loss or theft of the phone is one such event, but so too is the situation where the cardholder is considered to be no longer eligible for a credential – PIV or PIV-D. This would happen in the event of termination of employment for example.

For these reasons, a derived credential management system (DCMS) needs to have a link back to the PIV card issuing system (CMS or IDMS). This link could be purely a defined manual business process (just as removing a terminated employee's accounts and permissions may be), but it is more efficient and reliable to establish a data connection between the CMS and the DCMS, so that revocation under prescribed circumstances can be automated.



There are two main options for links between the card and PIV-D management systems. One is based on an enquiry model, where the PIV-D system interrogates the CMS to discover the status of cards and cardholders. A method based on the 'backend attribute exchange' is a strong candidate for this architecture, although one or two additional attributes may need to be provided (such as the 'cardholder PIV-D eligibility' and the 'superseded FASC-N'). Although this would work with minimal changes to existing CMS installations, it does have the drawback of needing regular 'polling' to detect changes in the status of cards and people. As a result, the long-term scalability of such a system may be called into question.

A more efficient alternative is an event notification architecture, where the CMS sends messages to a web service on the DCMS. Only two message types are needed here; one to notify the DCMS that a cardholder's PIV-D credentials must be revoked, and another to inform the DCMS that a PIV card has been superseded by a replacement card (in order that a consistent, verifiable chain of trust to the cardholder can be maintained).

5.3 Live credential updates and resets

One major advantage of mobile credential carriers is that they are effectively an 'always on' connected device. This means that certificate renewals and updates can be performed without needing to attend a specific location; an internet connection to a trusted system is all that is required.

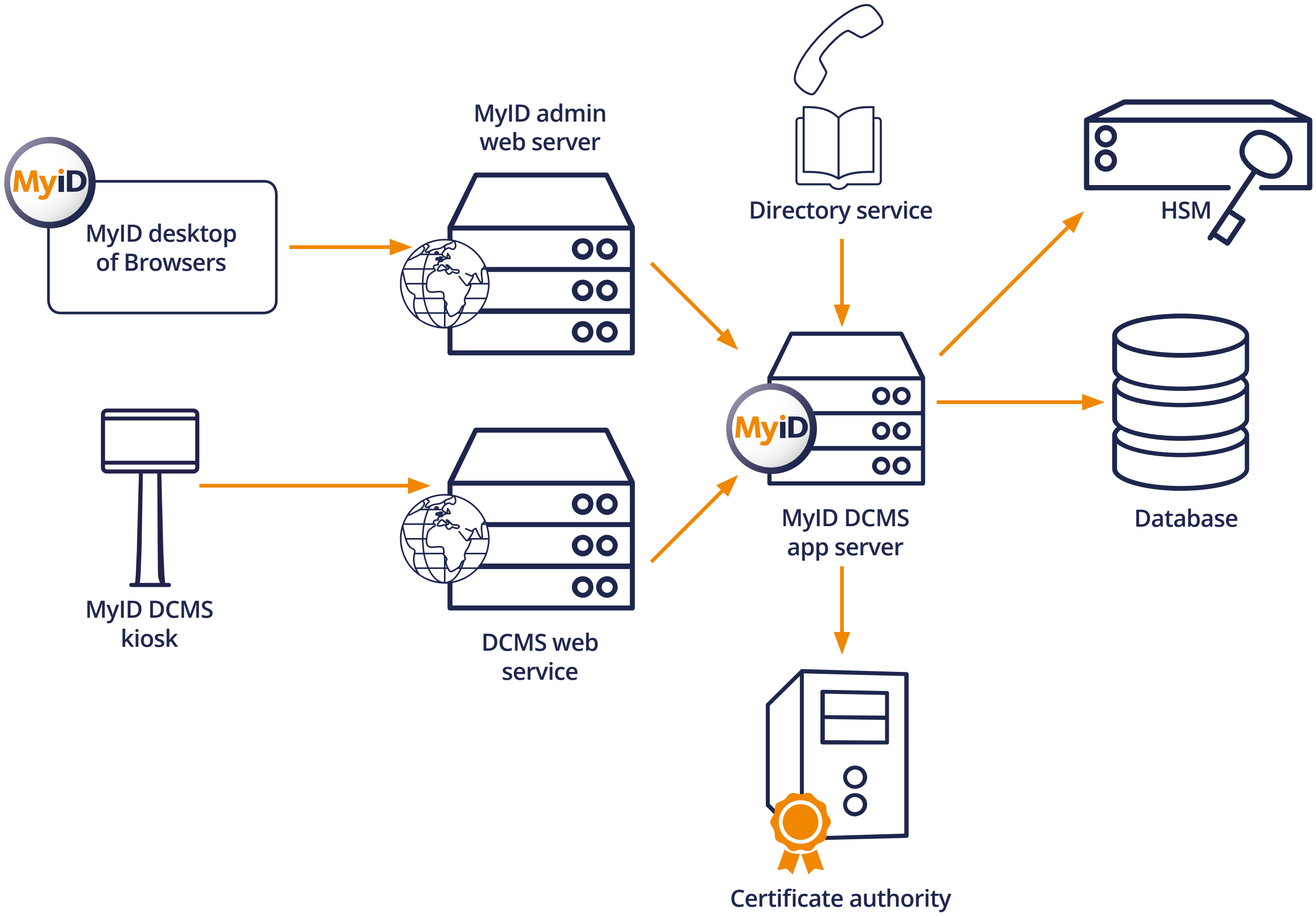
For situations such as PIV-D PIN lockouts, a self-service kiosk solution can also help; a user could authenticate to the PIV-D kiosk using their previously enrolled PIV card and use this as the necessary authority to deliver the PIN reset instruction to their phone via the Identity Agent app.

5.4 Governance and audit

Any system that delivers high integrity services must be capable of meeting high standards of audit and governance. A PIV-D credential management system is no exception, so features such as signed, tamper-evident audit trails, strong operator authentication and strict role separation are vital considerations. There is little merit in issuing high security credentials if the system responsible for issuing them is only protected by a username and password for its administrators.

This level of protection extends beyond the immediate scope of the CMS and impacts the supporting infrastructure – databases, web services, network connectivity etc. all require high levels of security. Achieving this in a consistent manner may be more readily achieved through the use of pre-configured cloud services, although individual deployment models are clearly at the discretion of the agency.

Intercede's MyID DCMS uses the same platform as its GSA Approved Product Listed card personalization software and includes smart card operator authentication, card-signed transactions, sever signed audit trails and role-based authorization. It can be deployed on-premise or as a cloud service through FedRAMP certified providers.



6 DCMS deployment options

A derived credential management system should be deployed into an environment where it has direct connections to the CMS (or BAE broker), a connection to a certification authority capable of issuing trusted PIV-D certificates, and wired and/or wireless LAN or WAN access from mobile devices, issuance kiosks and administration consoles. Agencies may of course choose to limit access to certain features to be from within their own private networks, but in principle public internet access is a realistic option for certain use cases.

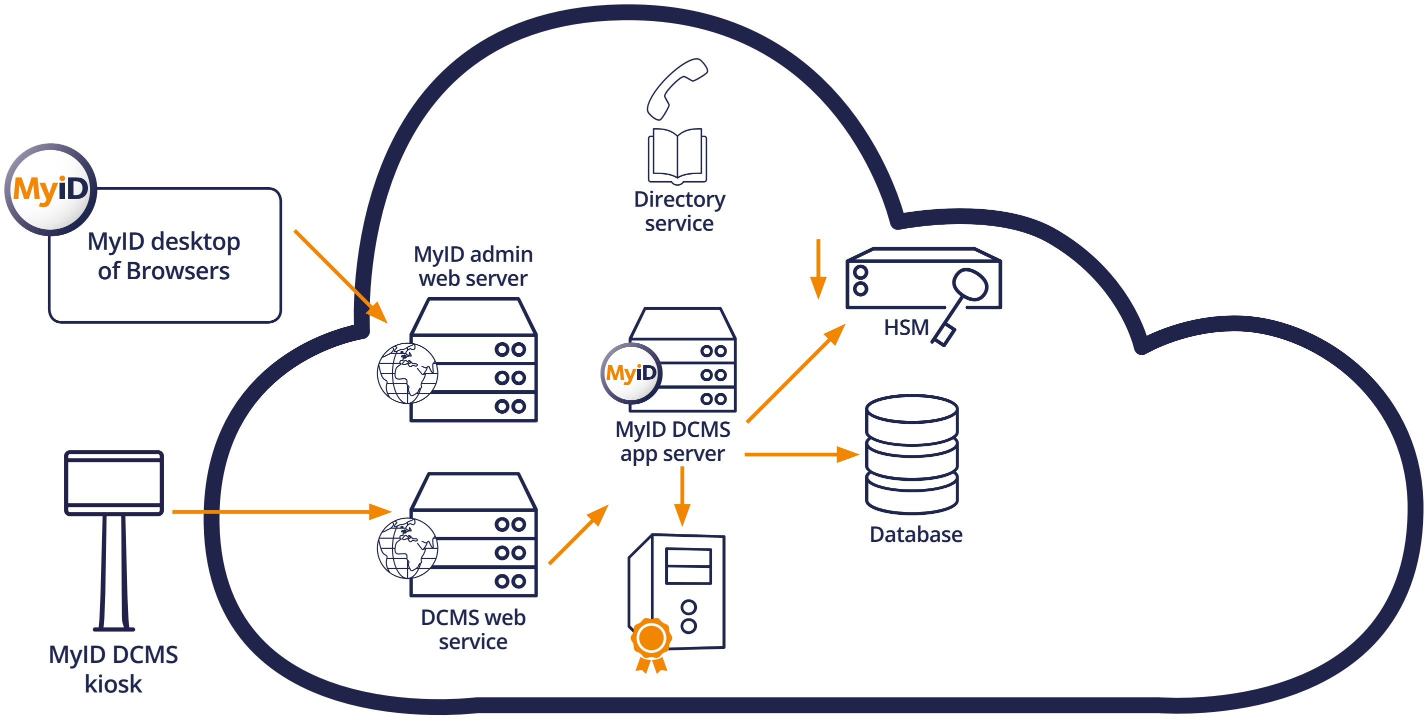
DCMS may be purchased as a fully managed service, administered directly by the agency, or installed as a product on premise. The best option will vary by agency according to cost, security, connectivity and resilience needs. It is expected that most DCMS products will offer a full range of deployment architectures.

6.1 DCMS as a cloud service

Subscribing to a cloud DCMS service offers the fastest way to deploy a derived credential solution. Using a FedRAMP accredited service provider (such as Azure or AWS), an agency-specific instance of the service can be created from standard templates in a very short period of time. These cloud instances can be highly scalable, with the ability to dynamically add and remove processors to an existing service according to the demand.

Secure VPN connections back to the agency's network ensure high levels of integrity, which is enhanced still further by the PIV card operator authentication offered by products such as MyID.

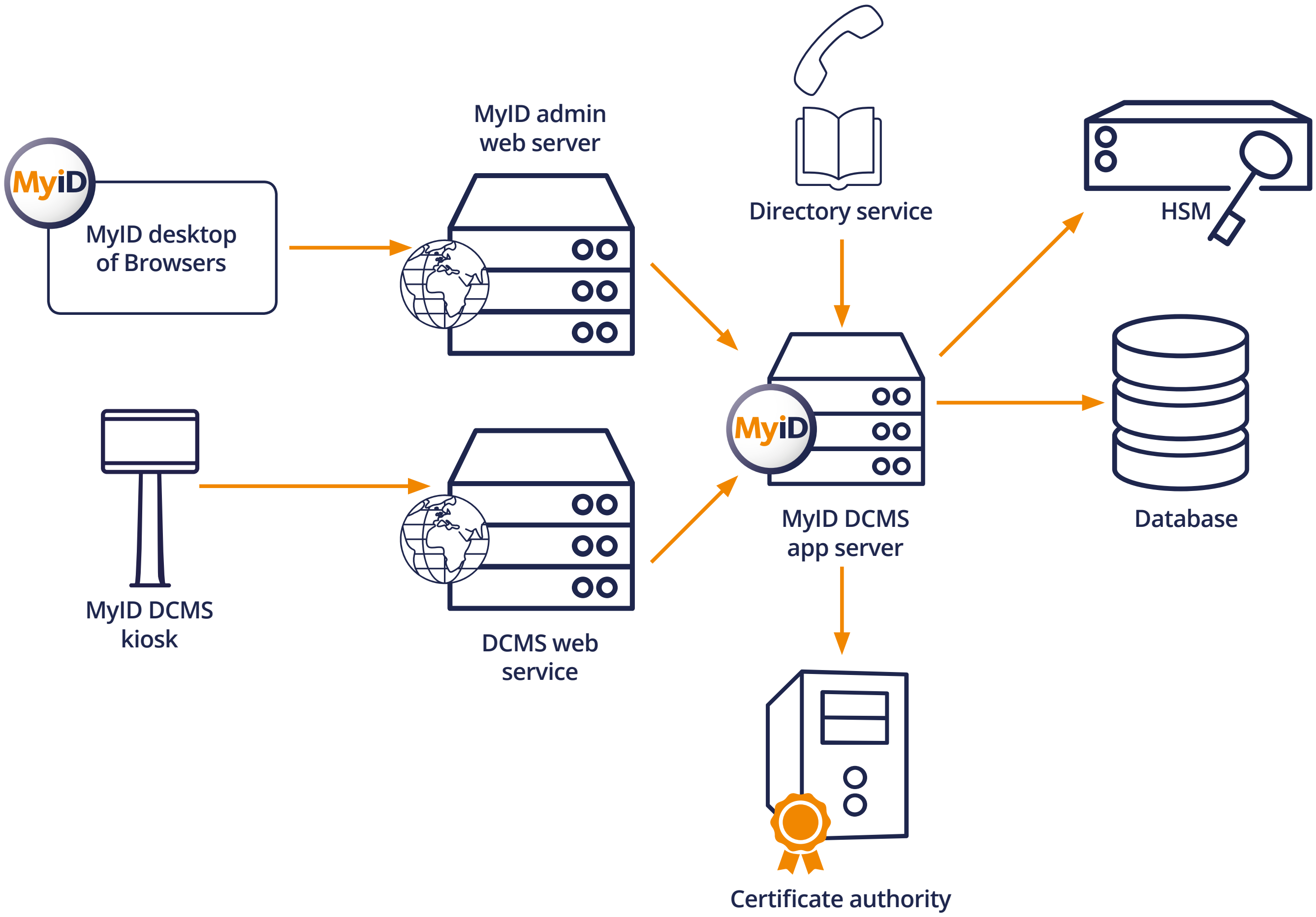
Similarly, secure connections to the connected services (CA, CMS/BAE, HSM) are readily configured as part of the on-boarding process for the service.



6.2 DCMS on-premise

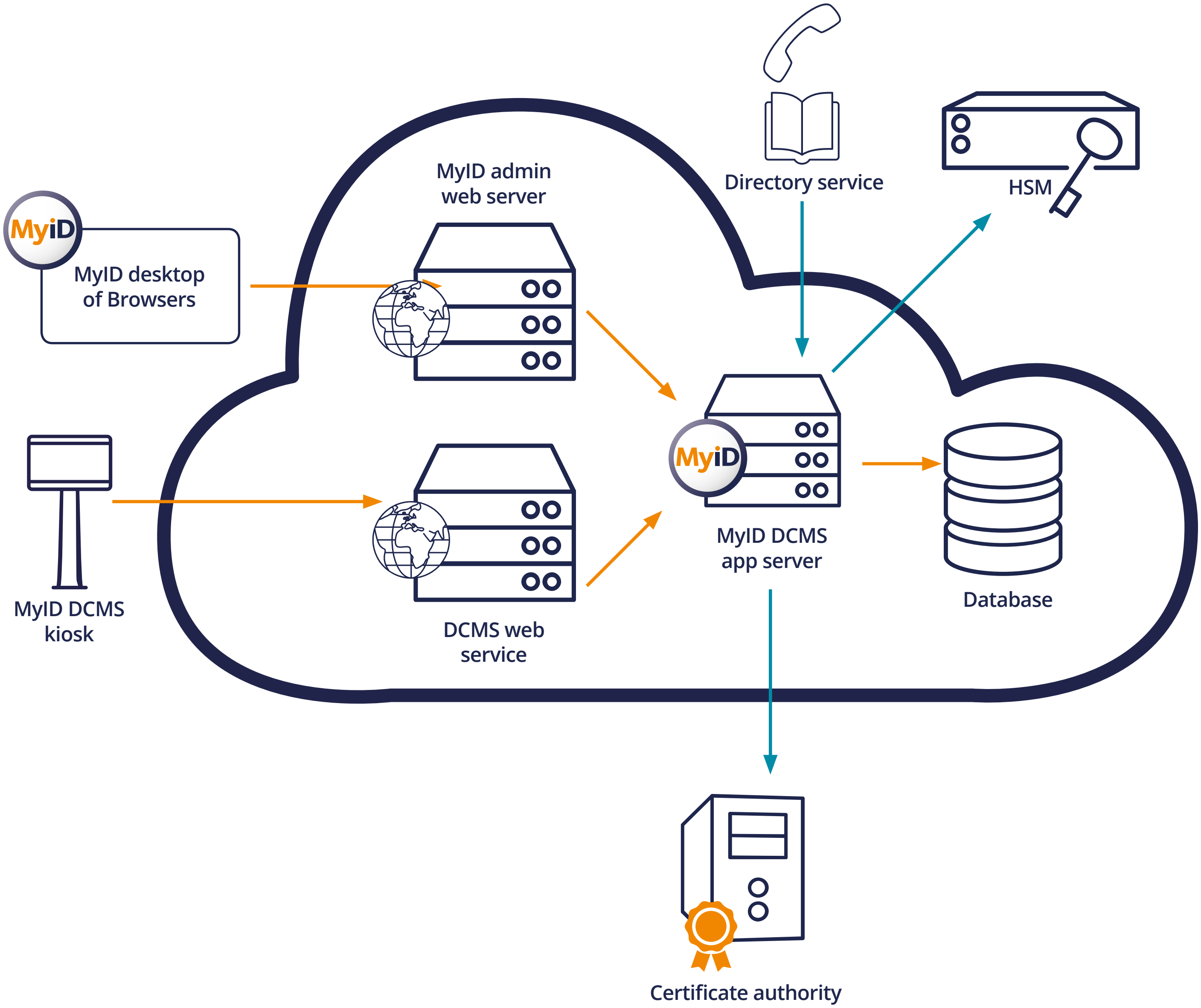
For situations where cloud services are not considered appropriate (due to specific policy exclusions for example), the same product can of course be installed within the agency's own datacenter. This has the benefit of retaining all of the components within a physical security perimeter, but risks needing more time to install and being more demanding to maintain at the infrastructure level.

It is however a very good option where co-residence with an in-house PIV CMS is needed and the security of communication channels between connected systems is generally simpler to enforce. Physical co-location of hardware security modules (HSMs) is also of benefit.



6.3 Hybrid DCMS

In many cases a hybrid solution may be chosen for production systems. For example, hosting the main DCMS server in the cloud, but retaining the HSM and database on premise. The security and performance implications of such hybrid architectures must be evaluated carefully though before deciding on a particular configuration.



7 Mobile device management

It is important that mobile apps used for delivering and consuming derived credentials are able to be managed via the MDM / EMM products that an agency uses to control its phones and tablets. This means that the apps for delivering the credentials (such as the MyID Identity Agent) and those needed to access them (such as email clients or browsers) need to be part of your organization's 'trusted application ecosystem'.

At its simplest, this may require you to sign the apps with your own enterprise certificate, so that they can safely exchange the data held in the keychain on your phones. In other cases though, this might entail building the MDM vendor's 'wrapper' around each app to redirect specific system calls to their own secure data silo.

Intercede's apps have been successfully integrated with a number of the leading MDM vendor's wrapping SDKs, including MobileIron, Good Technology and Citrix.

MDM integration might also extend to being able to deploy apps from a local enterprise app store, and automating the configuration of those apps. For example, the MyID Mail app can be provisioned directly by Airwatch so that the end user does not need to manually configure the connection to your Exchange server.

8 Enhanced derived credentials

The standard PIV-D credential is simply a user authentication certificate. While this is extremely useful, it does not address a number of other critical services that many agencies will expect to be able to use from their mobile devices.

8.1 Signing certificates

The ability to sign emails, documents and transactions is one such set of use cases. Although it is technically possible to use the authentication certificate for this purpose, it typically exceeds the scope of the certificate usage policy for this credential. In addition, a signing credential will usually enforce a 'PIN every time' user authentication.

Delivering a signing certificate is a relatively simple process for the Identity Agent. To be able to assert a high level of non-repudiation, it is important that the keypair is generated on the mobile device itself (which MyID for example will do anyway), but aside from that, the operation is essentially identical to issuing an authentication certificate.

8.2 Encryption certificates

Closely related to the signing certificate is an encryption certificate (or more commonly, a set of current and historical encryption certificates). The situation here is complicated, as encryption certificates and keys need to be capable of escrow and recovery over a secure channel. In order to be able to work flexibly between desktop and mobile environments, the ability to recover keys previously used on the PIV card is important, not just using keys created specifically for the mobile device.

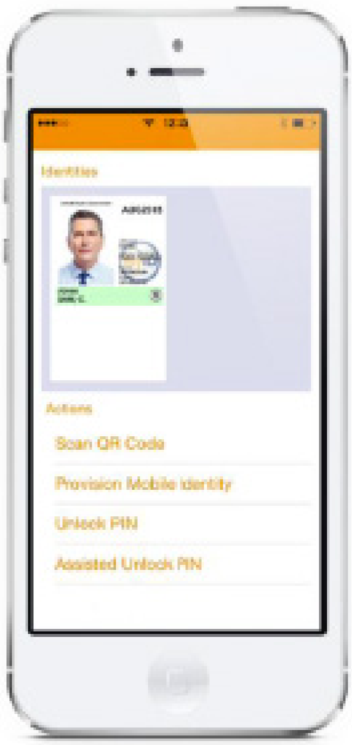
This has two important consequences. Many existing encryption certificates have been issued under a policy that requires their keys to be held exclusively in hardware stores. This means that a mobile solution would have to support a FIPS 140 accredited hardware secure element. Secondly, the DCMS will need to have privileged access to the key escrow service of the PIV CMS or certification authority, so that it can recover existing keys to the phone.

One pragmatic solution to this problem is for the agency to change its certificate policy to allow the encryption keys to be stored in software. Although this would not help with pre-existing certificates, once a credential refresh is applied to their PIV cards, users would be able to read subsequent encrypted email from either environment. For this to work however, the issuing CMS must be able to readily upgrade issued cards to renew their encryption certificates with ones from the less rigorous policy.

8.3 Virtual badges

The ability to show a visual representation of a derived credential is very useful, but not an especially strong security feature. Virtual badges can be used to provide additional information such as medical data (blood group, allergies and physician), qualifications and rights (such as emergency responder roles) and other images such as 2D barcodes.

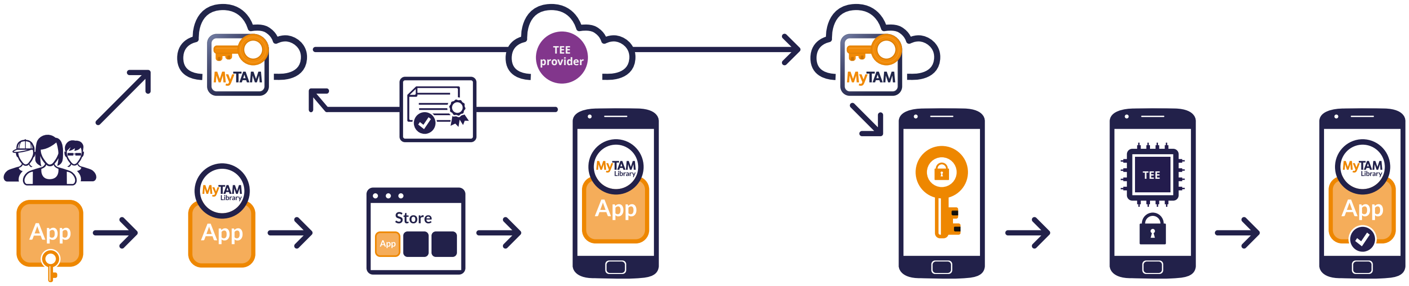
It is also possible to build in higher levels of security for these credentials though, such as a QR code link to a verification service or the ability to read the information as a signed block of data whose integrity and trusted authenticity can be verified via NFC for example.



8.4 Trusted Execution Environments

An increasing number of phones and tablets are being enabled with Trusted Execution Environments. These offer potentially stronger protection of data, verifiable access to peripherals and, perhaps most importantly for this discussion, a trusted user interface for PIN entry or biometric user authentication.

To use these features within a PIV-D container service on your phone, it is necessary to deploy a 'trusted app' to the TEE. This requires special privileges that can only be granted by the owner of the TEE (for example Trustonic) or one of their partners via a Trusted App Management service.



The MyTAM cloud service communicates with the TEE provider's directory to access the cryptographic keys needed to use the TEE. Secure containers are then created in the TEE, cryptographic keys are regenerated and the encrypted trusted application is delivered to the device. MyTAM also installs a key that can be used by the app to carry out additional personalization if required, for example to update an account balance.

The operation of this is transparent to the end user, but does reduce the risk of PIN 'phishing' to provide a higher level of trust in the credential.

9 Conclusions

The use of derived credential for PIV presents the opportunity for greatly enhanced access and usability of protected resources from mobile devices. The NIST special publication SP800-157 in conjunction with the FIPS 201-2 standard provides the framework for highly practical solutions to the issues that employees and contractors encounter on a regular basis.

The mobile market continues to evolve extremely rapidly, with an increasing number of options for the storage and processing of cryptographic data. Using a vendor-neutral library to access these credentials that is capable of working equally well with card readers, hardware secure elements, trusted execution environments and numerous flavors of software credential stores is therefore a worthwhile investment.

The choice of DCMS is important too. It must be able to integrate with multiple certification authorities and your existing card management or identity management systems. It should have a strong track record of successful deployments in the complex and demanding Federal marketplace. It needs to be supported by knowledgeable, experienced engineers who are capable of adapting it precisely to meet your particular business objectives.

As a respected, existing PIV card personalization provider, Intercede has the tools, products and services that are needed to deliver PIV-D solutions today. They can be consumed as cloud services or implemented on-premise or via IT service providers as part of your existing datacenter environment. Intercede's continued investment in PIV credential management solutions is evidenced by its market-leading MyID product line and its innovative solutions to real-world problems. With one of the largest global teams dedicated to identity and credential management software and services, it is ideally positioned to play a leading role in your strategic solutions for the secure management of PIV derived credentials.

9 Conclusions

The use of derived credential for PIV presents the opportunity for greatly enhanced access and usability of protected resources from mobile devices. The NIST special publication SP800-157 in conjunction with the FIPS 201-2 standard provides the framework for highly practical solutions to the issues that employees and contractors encounter on a regular basis.

The mobile market continues to evolve extremely rapidly, with an increasing number of options for the storage and processing of cryptographic data. Using a vendor-neutral library to access these credentials that is capable of working equally well with card readers, hardware secure elements, trusted execution environments and numerous flavors of software credential stores is therefore a worthwhile investment.

The choice of DCMS is important too. It must be able to integrate with multiple certification authorities and your existing card management or identity management systems. It should have a strong track record of successful deployments in the complex and demanding Federal marketplace. It needs to be supported by knowledgeable, experienced engineers who are capable of adapting it precisely to meet your particular business objectives.

As a respected, existing PIV card personalization provider, Intercede has the tools, products and services that are needed to deliver PIV-D solutions today. They can be consumed as cloud services or implemented on-premise or via IT service providers as part of your existing datacenter environment. Intercede's continued investment in PIV credential management solutions is evidenced by its market-leading MyID product line and its innovative solutions to real-world problems. With one of the largest global teams dedicated to identity and credential management software and services, it is ideally positioned to play a leading role in your strategic solutions for the secure management of PIV derived credentials.

10 References

1. Comscore report: http://www.comscore.com/Insights/Blog/Major-Mobile-Milestones-in-May-Apps-Now-Drive-Half-of-All-Time-Spent-on-Digital
2. NIST FIPS 201-2 - Personal Identity Verification (PIV) of Federal Employees and Contractors (August 2013)
3. NIST SP800-157 – Guidelines for Derived Personal Identity Verification (PIV) Credentials