Kantara Identity & Privacy Incubator

Architecture

Mobile Device Attribute Validation

Version 0.4

Stephen Wilson, Lockstep Technologies

October 2016

COMMERCIAL IN CONFIDENCE

Architecture
Mobile Device Attribute Validation
Version 0.4
[Lockstep Technologies MDAV Architecture (0.4)]

Stephen Wilson

COMMERCIAL IN CONFIDENCE

Lockstep Technoloigies (est. 2006) develops unique new smart ID solutions that enhance privacy and prevent identity theft.

http://lockstep.com.au/technologies

Table of Contents

1. Executive Summary 4
2. Glossary 5
3. Architectural principles 6
4. Background 8
5. Archetypal use case: First Responder IDAM 9
6. MDAV High Level Design 10
7. References 19

Table of Figures

Figure 1: Certificates as “capsules”

Figure 2: Stepwise capsule schematic

Figure 3: Stepwise capsule presentation schematic

Figure 4: MDAV PKI Communities of Interest

Figure 5: MDAV PKI Block Diagram

Figure 6: MDAV Mobile Applications Stack

Figure 7: MDAV certificate installation and use

Figure 8: MDAV Wallet-Reader actor diagram

1. Executive Summary

The Mobile Device and Attributes Validation (MDAV) project is implementing a new method to present personal attributes in a secure manner with minimum disclosure of ancillary personal information of an attribute holder. The method is especially well suited to use cases where a Relying Party aims only to verify a specific thing about a Subject – in the MDAV use case, a First Responder's emergency work qualification – and the issuer of that qualification. Lockstep Technologies has researched and developed a way to use anonymous or pseudonymous digital certificates to hold an attribute each, devoid of extraneous PII, and arrange for the certificate to be signed by or on behalf of the attribute issuer or credentialing authority.

The MDAV solution is aligned with a shift in focus in the identity management industry, from *personal identity* to *concrete attributes*. There tends to be more interest now in *what* someone is rather than *who* they are. The MDAV architecture is based on using public key certificates to hold such attributes, rather than identifying information per se, and to use digital signatures to bind those attributes to transactions, as a way of presenting the certificate holder's credentials. Certificates will be managed in a digital wallet app on a mobile phone.

This detailed architecture paper is a deliverable of the first "viability" phase of the MDAV project, and forms the basis of a second "execution" phase.

Acknowledgement

The Mobile Device and Attributes Validation project is funded by a Department of Homeland Security Science & Technology grant. The work is conducted by Lockstep Technologies under the auspices of the Kantara Identity and Privacy Incubator (KIPI) and the Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA) at Rutgers University.

2. Glossary

ABAC	Attribute Based Access Control
AP	Attribute Provider
BLE	Bluetooth Low Energy
CA	Certification Authority
CAPI	Cryptographic API
CCICADA	Command, Control and Interoperability Center for Advanced Data Analysis
COI	Community of Interest
CP	Certificate Policy
CPS	Certification Practice Statement
CSP	Certificate Service Provider (outsourced PKI provider)
ICA	Intermediate Certification Authority
IDAM	Identity and Access Management
IdP	Identity Provider
KIPI	Kantara Identity and Privacy Incubator
KYC	Know Your Customer
LAC	Logical Access Control
LEA	Law Enforcement Agency
MDAV	Mobile Device and Attribute Validation
MITM	Man-in-the-Middle
NFC	Near Field Communication
PAC	Physical Access Control
PACS	Physical Access Control System
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RA	Registration Authority
RBAC	Role Based Access Control
RP	Relying Party
RCA	Root Certification Authority
S&T	Science & Technology (department of DHS)
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
2FA	Two Factor Authentication

3. Architectural principles

The MDAV (Mobile Device and Attribute Validation) architecture is premised on a new approach to directly presenting select personal information and attribute values of users to Relying Parties, such that the data cannot be stolen and replayed. The aim is for transaction systems to obtain verified information about individuals in context, in use cases where authentication decisions may be made on the basis of that information.

3.1 Relationship Certificates

MDAV makes use of a novel configuration of otherwise standard Public Key Infrastructure, and digital signature capabilities in modern mobile phones to encapsulate personal details in anonymous or pseudonymous digital certificates.

Conventional PKI certificates act to bind an identity to a public key (and hence a key carrier like a smartcard or mobile device) for "authentication" purposes. Additional "authorization" of an individual under Attributes Based Access Control requires that attribute information be additionally bound to transactions or challenge-response handshakes. At one point in the early stages of PKI practice, special purpose X.509 "Attribute Certificates" were used for this purpose, and we bound to messages before being digitally signed using an "general purpose identity certificate, being a public key certificate. The original "Attribute Certificates"[1] did not hold public keys and could not be used directly for digital signatures. They proved difficult to implement in practice, largely because there was no standard way to include them in the payloads to be digitally signed.

Circa 2006, Lockstep Consulting and the Australian Government developed the concept of "Relationship Certificates" for conveying context-specific information about users, instead of general identity [1][2]. Relationship Certificates express a relationship between a Registration Authority (RA) and a certificate subject, such as membership of a, community of interest. Where such membership is subject to formal rules and represented by a membership number or similar, unique on the domain of the community, then a Relationship Certificate can be used as strong proof of membership, and by extension, of authorization to act according to those rules.

Relationship Certificates are not intended to *identify* their holders per se but to *authorize* them in the context set by the issuer. Relationship Certificates have been successfully implemented by Medicare Australia [3] and have become dominant in Australian healthcare PKI.

[1] To distinguish original "Attribute Certificates" from MDAV public key certificates, we will use shudder quotes.

MDAV certificates are a form of Relationship Certificate, issued to support AttribuTE Based Access Control and authorization. *The meaning of an MDAV certificate is nothing more and nothing less than the fact that the holder of the matching private key has the named attribute, according to the issuer which signed the certificate*. It is expressly assumed in the architecture assumed that that a Relying Party is able to reasonably determine the authorization of an MDAV certificate holder to perform duties in a specific context based on little nothing more than the holder's ownership of an attribute value.

3.2 Vision

MDAV represents a prototype of a new type of infrastructure for identity and access management (IDAM), one that provides for authentication of context-independent attributes with widely understood meaning, instead of abstract identities that are only ever understood locally. MDAV enables wallets of personal details to be managed through a mature PKI-based system of vouchsafing precise attributes and conveying their provenance in digital certificates.

Such wallets will be able to:

- present important identifiers like health IDs, Social Security Numbers, customer reference numbers, and account numbers
- anonymously assert personal attributes like proof of age, location, residency, health conditions, and insurance status
- demonstrate verified facts about the wallet owner such as date of birth, residential address, passport number and so on, to meet Know Your Customer rules in banking
- interoperate with a free marketplace of Attribute Authorities which can compete to provide notarised details about individuals
- show the authority that issued or vouched for the attribute, allowing RPs to distinguish "secondary" sources from "primary" or authoritative sources of information
- self-assert attributes such as social network handles
- verify the originality and integrity of attributes in offline and occasionally connected environments
- be strongly auditable
- be processed quickly with de-centralized, lightweight and standards-based software modules.
- leverage the native cryptography in modern smart phones, smartcards, and future IoT devices.

4. Background

Lockstep Technologies has previously researched and developed a way to use anonymous or pseudonymous digital certificates to hold an attribute each (with little or no other identifying information) and arrange for the certificate to be signed by or on behalf of the attribute issuer or credentialing authority. The technique is marketed as "Stepwise".

Stepwise certificates are issued against a private key held within the secure key store of an approved mobile device.

4.1 Terminology

We sometimes represent Stepwise certificates schematically as "capsules" to indicate that they primarily contain *or encapsulate* a specific piece of information about the holder (namely the attribute). Additionally, the capsule symbol indicates two types of "branding": the name of the attribute authority and the type of device carrying the certificate are both borne by the capsule.

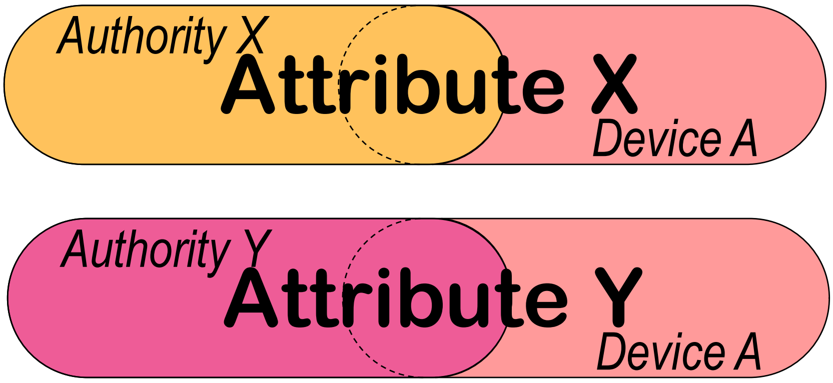


Figure 1: Certificates as "capsules"

5. Archetypal use case: First Responder IDAM

An archetypal use case for Lockstep's Stepwise and attribute management is identity and access management for First Responders.

A first responder in a remote field location must often prove their credentials to a local field officer before being cleared to undertake safety-critical tasks, for example relocating a group of school children. With the MDAV solution, the first responder can carry credentials in Stepwise digital certificates (referred to as "capsules"), each signed by the originating agency. The manager can receive and cryptographically verify the relevant capsule on their own mobile device, with minimal network connectivity and no exposure of extraneous information.

Field officers on the ground face a major challenge in rapidly verifying the bona fides of visitors. The veracity of paper or plastic identity credentials is rarely self-evident. Yet centrally managed electronic credentials are not an easy alternative, for they can be hard to authenticate in disaster-affected locales with low network availability. Furthermore, traditional central solutions generally compromise privacy by over-identifying individuals, collecting excessive PII in the first place, and then disclosing too much of it in routine transactions.

First Responder IDAM takes several forms, including:

- field officers often need to verify in-person a visiting worker, in order to admit them to a physical site, or approve them to work on certain hazardous tasks
- visitors may need to log on to local computer systems under temporary access arrangements, and
- visitors may need to electronically sign off on their activities (such as medical assessments or engineering certifications) using their relevant credentials.

5.1 High level Design Requirements

- convey precise entitlements via digitally signed attributes
- leverage embedded cryptographic capabilities of mobile devices
- minimize collection and disclosure of extraneous personal information (especially circumstantial details and shared secrets used for indirect or "knowledge-based" authentication)
- provide metadata about the issuer of the credentials or attributes, to allow local authorities to determine whether the attributes are reliable in context
- provide metadata to help qualify the intended use of the credential.

6. MDAV High Level Design

The MDAV solution takes Lockstep Technologies' original R&D into anonymous and pseudonymous certificates for safeguarding identifiers, and combines the techniques with mobile technology and native cryptography to securely convey specific attributes and authorizations. The initial MDAV application is to enable First Responders to convey to others the provenance of their professional attributes, of their attributes' sources, and of the digital wallet device, while disclosing less PII.

6.1 PKI configuration

The core innovation in MDAV is a re-configuration of standard PKI digital certificates. Stepwise capsules embody a new way of thinking about authentication and PKI certificates. Instead of loading a certificate with personal identity, we store one specific attribute in a special purpose certificate or capsule, issued to a device under the attribute holder's control. A strong logical triangle is formed, joining the person, their device and the attribute, baking in the provenance of the device and the attribute issuer.

When such a certificate is used to verify a digital signature, the Relying Party is assured of the attribute and its provenance, without disclosing excessive information about the attribute holder. A signature verified by an MDAV certificate evinces that the signer was in control of a device carrying the associated key, and is therefore authorized to present the attribute concerned.

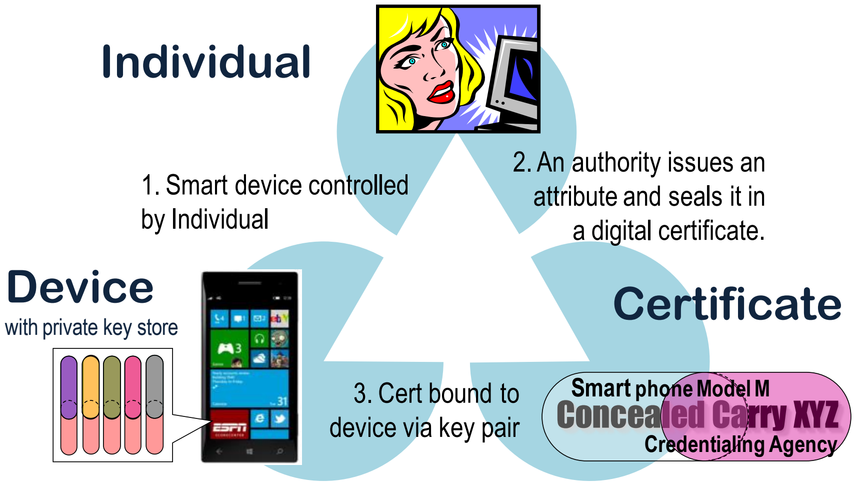
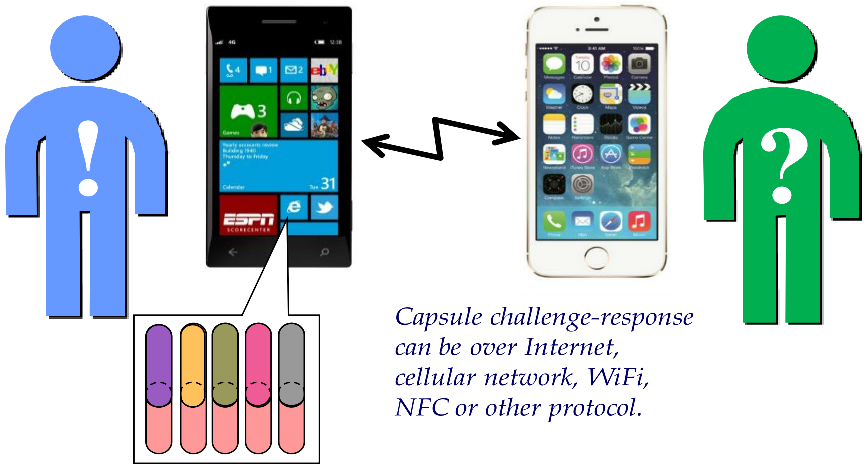

Individual
1. Smart device controlled by Individual
2. An authority issues an attribute and seals it in a digital certificate.
Device
with private key store
Certificate
3. Cert bound to device via key pair
Smart phone Model M
Concealed Carry XYZ
Credentialing Agency

Figure 2: Stepwise capsule schematic



Capsule challenge-response can be over Internet, cellular network, WiFi, NFC or other protocol.

Figure 3: Stepwise capsule presentation schematic

6.1.1 MDAV Certificates

Each MDAV certificate is to be issued against a private key held within the secure key store of an approved mobile device. The MDAV Policy Authority will maintain a list of approved devices.

Because the private key is assumed to be secure within an approved device controlled only by the attribute Subject, the meaning of any digital signature that can be verified against the MDAV certificate is that the purported holder of the attribute was willingly involved in the creation of the signed data. An MDAV certificate may therefore be used to:

- digitally sign electronic transactions in one's capacity as a qualified First Responder, or

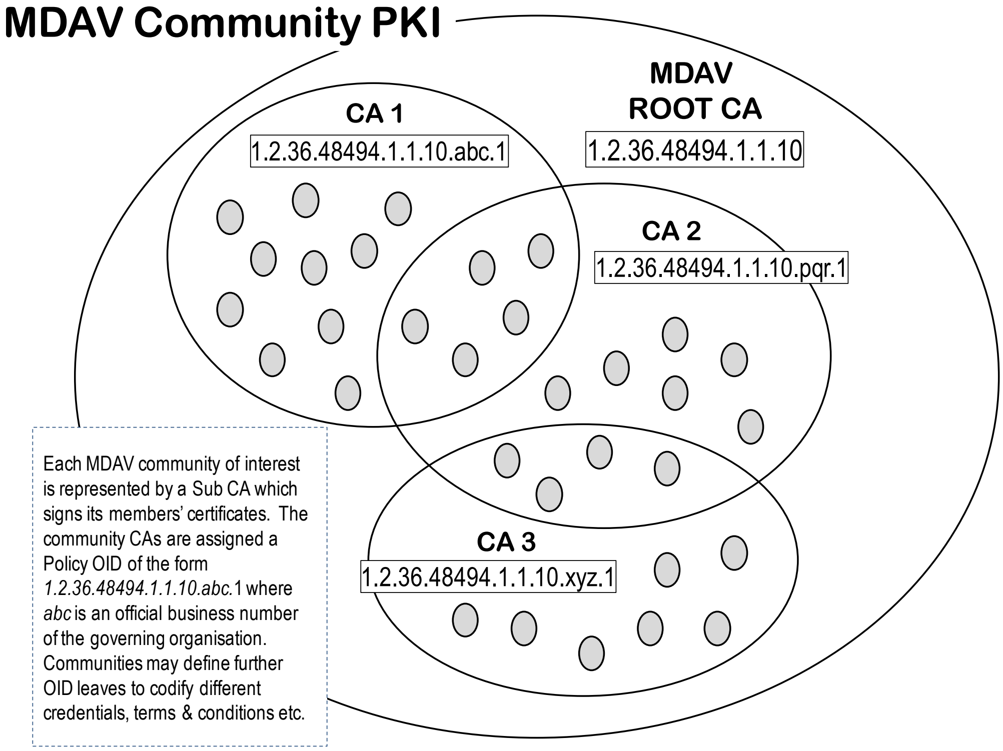
- sign a challenge-response from a reader app, in order to prove one's credentials to another officer, face to face, in real time.

6.1.2 Policy OIDs

The way in which certificates and CAs chain together to the Root CA in this PKI is different from conventional PKI, and should be noted carefully. MDAV certificates will be signed by CAs operated by (or on behalf of) attribute authorities. It is envisaged that a full scale MDAV scheme would oversee participating attribute authorities and their CAs, ensuring that fit and proper systems are in place at each CA to meet the quality control needs of the scheme. A Root CA will be operated by the MDAV scheme, and will sign participating CAs' certificates. The meaning of a CA certificate in the MDAV hierarchy is nothing more and nothing less than the fact that the CA is approved to operate, to issue MDAV certificates to individuals. The precise process for vetting individuals and credentialing them will always be determined by the attribute authorities and not by MDAV.

The MDAV PKI represents a set of nested communities of interest, rather than a hierarchical tree, which helps to emphasis the autonomy of each community CA to set its own registration rules, and terms & conditions for using an MDAV certificate.

Thus there is a separation of powers in the scheme. The MDAV Policy authority plays no role in the credentialing process. The identification and authentication elements of the CP of each attribute authority are set by that authority, in keeping with its normal autonomous business rules, without any dependencies on the higher or peer CAs in the system.


MDAV Community PKI
MDAV
ROOT CA
1.2.36.48494.1.1.10
CA 1
1.2.36.48494.1.1.10.abc.1
CA 2
1.2.36.48494.1.1.10.pqr.1
CA 3
1.2.36.48494.1.1.10.xyz.1

Each MDAV community of interest is represented by a Sub CA which signs its members' certificates. The community CAs are assigned a Policy OID of the form *1.2.36.48494.1.1.10.abc.*1 where *abc* is an official business number of the governing organisation. Communities may define further OID leaves to codify different credentials, terms & conditions etc.

Figure 4: MDAV PKI Communities of Interest

Therefore, unlike conventional PKI, there is no direct relationship between the CP of the MDAV Root CA and the CP's of any participating attribute authority CA. This means that the CP OIDs of MDAV certificates may not have the conventional parent-child form of typical PKIs.

The following block diagram illustrates the major PKI building blocks to implement the above schema.

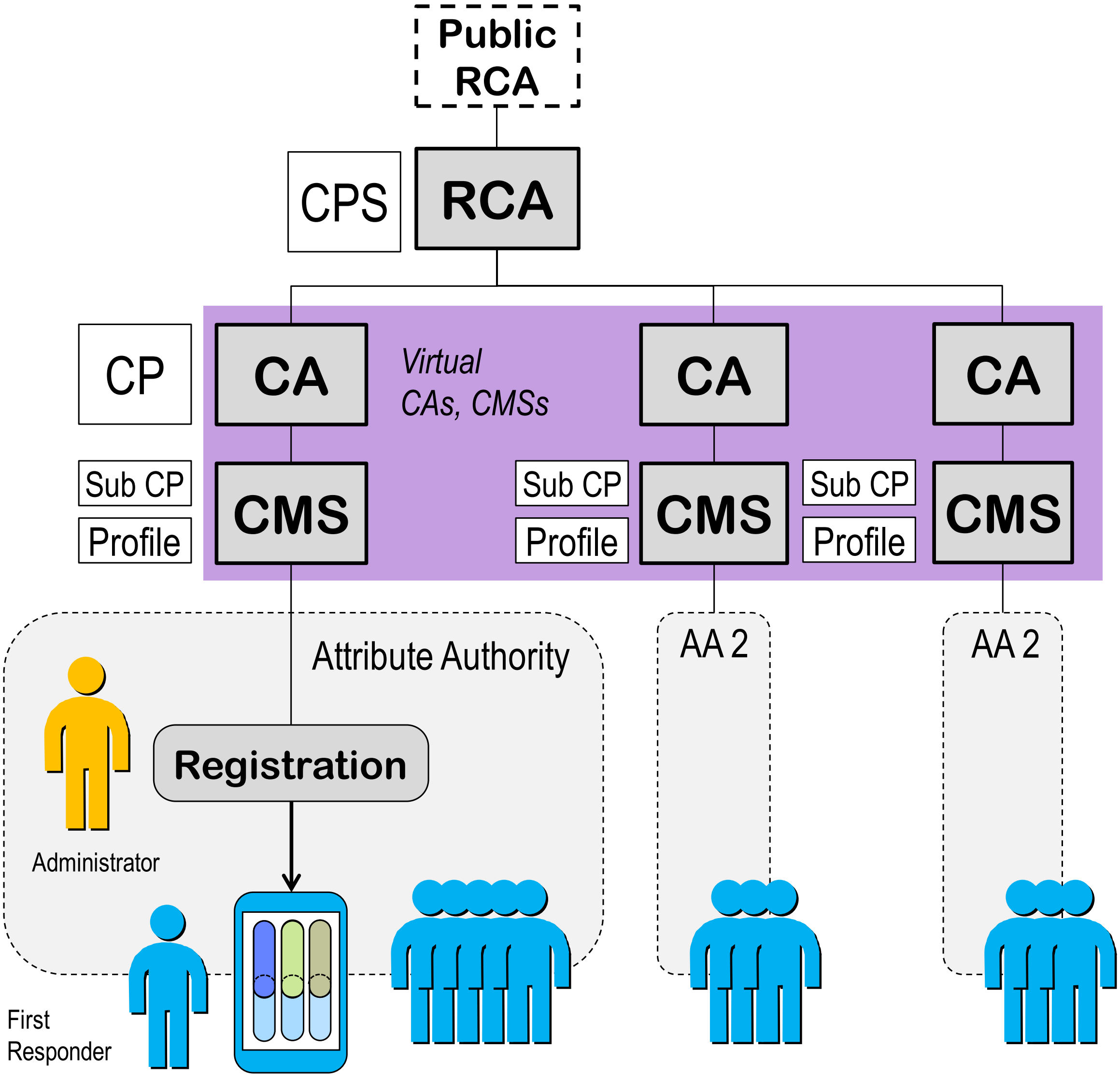


Figure 5: MDAV PKI Block Diagram

6.1.3 Interpreting MDAV certificates

The meaning (semantics) of an MDAV certificate is determined by the context in which it is issued, and rules set by the Attribute Authority.

The existence of a chain of MDAV certificates from the Subject back to the private MDAV Root can be taken by the RP to mean that the Subject is the legitimate bearer of the certified attribute, and that the issuing CA has been authorized by the MDAV administrator to participate in the go on, because each intermediate CA is performing a different type of check.

It is envisaged[2] that the MDAV administrator will publish guides (and Policy OIDs) that define sub-communities of interest within the MDAV community. There will be CAs responsible for different regions, and emergency work disciplines. And there will be CAs that simply accredit the ability of sub CAs to do their job as issuing attributes. See also section 4.4 [2].

An intact certificate chain extending from the Subject all the way to the Root in MDAV will mean that the end user's certificate is valid, but to interpret the meaning of the attribute within the certificate will require the RP software to also know about the Policy OIDs. Simply, the MDAV administrator will ultimately publish Policy OIDs that represent details of Attribute Authorities. The unbroken certificate chain means that each CA is performing as expected by the MDAV scheme.

Note that private keys corresponding to MDAV certificates must be carried in approved mobile devices. An MDAV participating CA will not issue an MDAV certificate to a person unless they present an approved phone. Scheme rules will specify devices with secure key media resistant to cloning, so there will not be uncontrolled propagation of MDAV certificates.

6.2 Mobile applications

MDAV in full scale production will establish a reasonably light weight administration that draws on existing credentialing organisations and DHS's processes for recognising them, and will treat each as an "Attribute Authority" to use the IDAM idiom. MDAV will operate a PKI that serves to encapsulate attributes in secure memory in approved mobile devices. And MDAV as a scheme will provide support for developers writing apps that serve up selected attribute capsules from a First Responder's device to another device or to backend servers, in order for the user to prove something important about themselves.

The principle use case for MDAV will be implemented with two mobile apps (operating with the customised PKI backend described above). A secondary use case involves accessing a backend service with one of the apps.

[2] In time, MDAV will spawn an ecosystem of developers and spin-off applications leveraging attribute capsules. The MDAV administrator will serve as a peak design authority, providing guidance, design patterns, and dictionaries or approved attributes and device types. Third party auditors (not shown) are expected to come into the fold as MDAV grows, to provide quality assurance. The longer term vision for MDAV administration is beyond the scope of the planned MDAV Phase 2 which is confined to a proof of concept and will not include the MDAV administrative component.

6.2.1 Device to device (Wallet & Verification)

Two client applications, a *Wallet* and a *Reader*, communicate with each other by one of a range of channels:

- Internet over 3/4G network or enterprise network,
- Bluetooth (or equivalently Bluetooth Low Energy), or
- NFC.

The choice of app-to-app channel is left open to the developer.

The Reader is used by a field officer to check that a visiting First Responder has a required credential or attribute, pertinent to the local context.

The Wallet presents the attributes in a meaningful graphical way (to be determined in detail by the developer), as is common now with smart phones' organization of tickets, boarding passes and the like. There will always be clear context to assist the user to select the right attribute – such as a first aid certificate, a security clearance, or an authorization – from their Wallet to be presented to a field officer.

The Reader's interaction with a Wallet opens with a handshake, such as a bar code scan, that will logically bind the two devices for the duration of a session, so that the two users may be sure they are interacting with each other and not an unseen Man-in-the-Middle.

Once an attribute selected by the First Responder, the Wallet software will, under the covers, send a tamper-resistant digital signature plus a copy of the capsule across to the Reader. PKI techniques allow the Reader software to check the integrity and originality of the capsule, thus confirming that the First Responder does indeed have the attributes they claim.

6.2.2 Client to backend service

The Wallet app may alternatively be used by the First Responder to authorise themselves to a backend server for role-based or attribute-based access control. A handshake will be needed between the server and the client, through which a message or object is signed using the private key for the MDAV certificate.

6.2.3 Mobile app stack

The Wallet and Reader apps are built on top of industry standard Cryptographic APIs providing access to services in cryptographic co-processors of approved devices including:

- root public key installation[3]
- key pair generation (within the confined of the processor)
- public key export (for certificate creation)
- public key certificate import (or load)
- selection of designated private as parameters for digital signature
- creation of digital signature on a given data object
- verification of a given digital certificate against a Root Public Key
- verification of a given digital signature and signed data object.

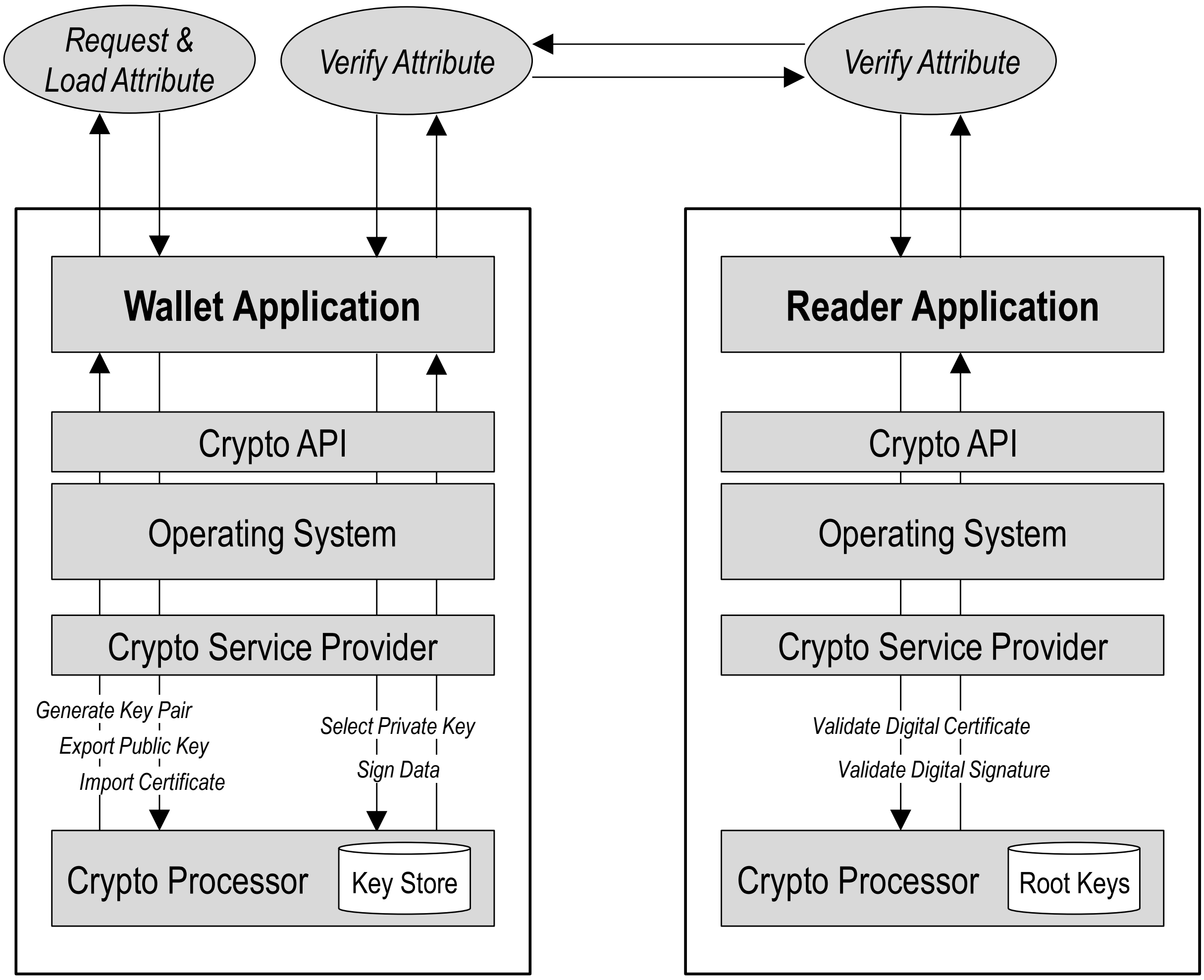


Figure 6: MDAV Mobile Applications Stack

[3] The MDAV scheme private Root CA will have its public key installed in reader devices when the reader app is loaded.

6.2.4 MDAV certificate install and use

The installation and use of MDAV certificates, plus the interaction between wallet and reader apps, are shown in more detail in the following block diagram and actor diagram.

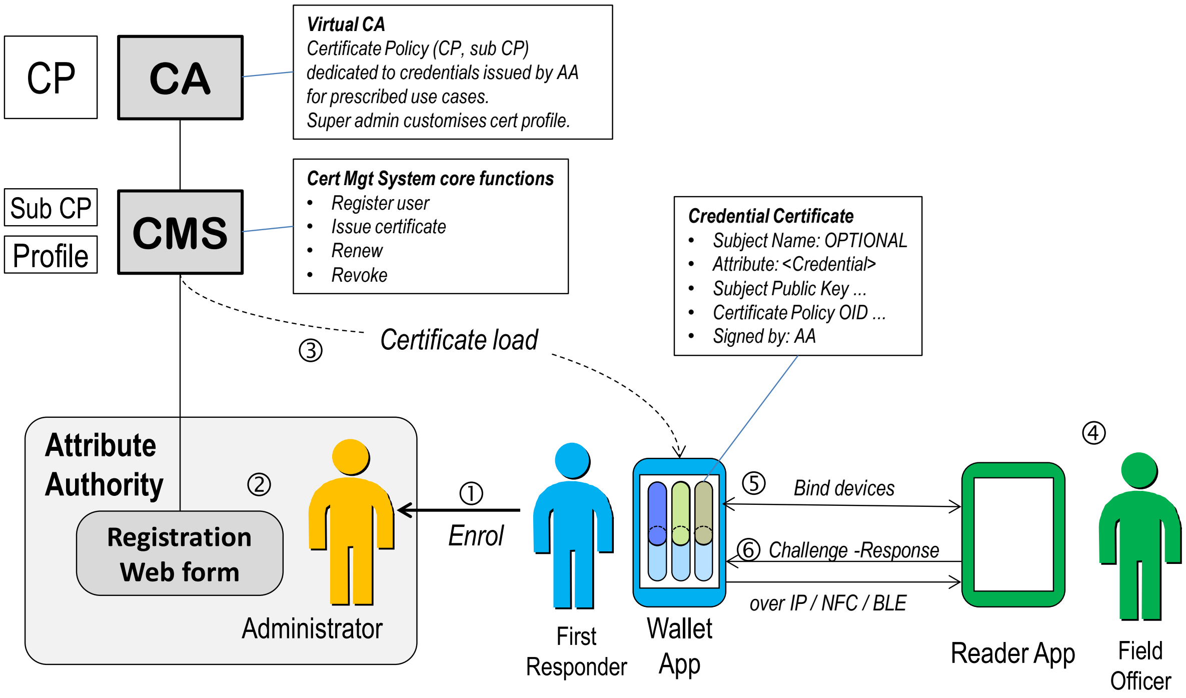


Figure 7: MDAV certificate installation and use

1. A First Responder enrols for an MDAV certificate by presenting to a credential administrator (in person or remotely, depending on the administrator's rules) which acts as an AA in the MDAV scheme.
2. Typically the administrator will have secure access to a registration web form interfacing to the Certificate Management System. Most AAs will use a virtual CA hosted by the MDAV backend CSP.
3. The hosted CMS enables the administrator to register a First Responder for a certificate, issue the certificate to a mobile device, renew and revoke. The web form may be a standalone form with data entered manually (acceptable for the initial proof of concept). In time, it is expected that the form will be integrated with the AA's local CRM so that certificates may be ordered automatically.
4. In use, the First Responder will meet a Field Officer (RP) and together they will negotiate the expected credential needed to operate in the given context.

5. Once the desired credential is agreed, it will be selected via the reader UI. Before the attribute maybe reliably transmitted, the Reader and Wallet devices must first bind themselves for a session, to avoid Man in the Middle attack. The architecture allows for a variety of binding mechanisms; the simplest may be to generate a random session ID and display that ID in the form of a QR code on the reader, scanned by the wallet app.

6. Once logically bound, the reader will issue a challenge to the wallet app, which returns a digital signature created using the private key of the MDAV certificate in question. Verification by the reader app of the response signature against the MDAV certificate proves possession by the First Responder of the attribute.

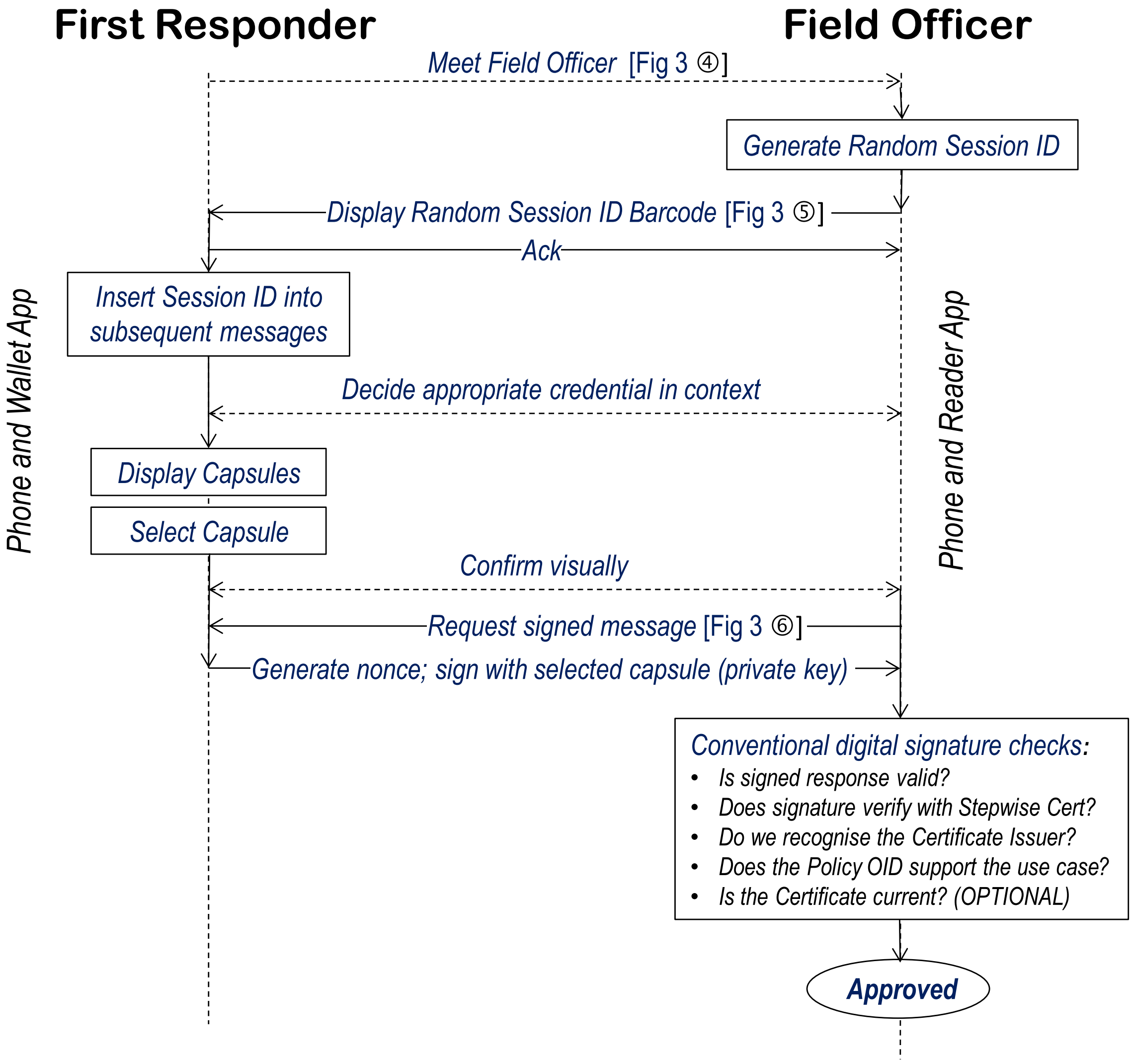

First Responder
Field Officer
Meet Field Officer [Fig 3 ④]
Generate Random Session ID
Display Random Session ID Barcode [Fig 3 ⑤]
Ack
Insert Session ID into subsequent messages
Decide appropriate credential in context
Display Capsules
Select Capsule
Confirm visually
Request signed message [Fig 3 ⑥]
Generate nonce; sign with selected capsule (private key)
Conventional digital signature checks:
• Is signed response valid?
• Does signature verify with Stepwise Cert?
• Do we recognise the Certificate Issuer?
• Does the Policy OID support the use case?
• Is the Certificate current? (OPTIONAL)
Approved
Phone and Wallet App
Phone and Reader App

Figure 8: MDAV Wallet-Reader actor diagram

7. References

[1]. *Gatekeeper PKI Framework – Relationship Certificate Guidebook*, Australian Government Information Management Office, February 2009, http://www.finance.gov.au/sites/default/files/Relationship_Certificate_Guidebook.pdf

[2]. *Public Key Superstructure – It's PKI Jim but not as we know it*, Stephen Wilson, NIST IDTrust'08 Workshop, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2548224

[3]. *Medicare Australia Organisation Certification Authority Certification Practice Statement* V2.4, Stephen Wilson et al, Medicare Australia, 2006 https://www.humanservices.gov.au/sites/default/files/documents/organisation-certification-authority-certification-practice-statement.docx

[4]. *Anonymously indexing electronic record systems* US Patent 8,347,101.