Homeland Security S&T

MDAV Certificate Policy

Version 1.0 DRAFT

Lockstep Technologies

July 2016

COMMERCIAL IN CONFIDENCE

Project report
MDAV Certificate Policy

Version 1.0 DRAFT
For Homeland Security S&T

[Lockstep Technologies MDAV Stage 1 Certificate Policy (1.0.1)]

COMMERCIAL IN CONFIDENCE

http://lockstep.com.au/technologies

Table of Contents

1. Introduction

This is a master Certificate Policy for the Mobile Device and Attribute Validation (MDAV) PKI, setting out baseline policy requirements for all MDAV certificate issuers, and indicating where detailed policy variations are to be made for different communities of interest and Attribute Authorities.

1.1 Overview

The MDAV system deploys anonymous and pseudonymous X.509 certificates to users of approved mobile devices. Certificates are issued from a hierarchy of Certification Authorities and virtual CAs representing Attribute Authorities. All CAs chain to a Root CA dedicated to the MDAV community.

EDITORS NOTE: It remains to be decided whether the MDAV Root could be a sub-root under a public CA root key. Or the MDAV certificates might terminate at the MDAV root, in which case trusted copies of the MDAV root public key will need to be loaded in mobile devices at the time an MDAV app is installed.

1.2 Document name and identification

Certificates issued under this CP shall bear the Policy OID:

1.2.36.109313411.1.10.1.X

where:

- **1.2.36.109313411.1.10** is the MDAV Root CA at top of the MDAV PKI hierarchy. The RCA has its own CP.
- **1.2.36.109313411.1.10.1** is this master Certificate Policy.

Further leaves will be uniquely allocated to different organisations acting as Attribute Authorities recognised within the MDAV community.

MDAV Certificate Policies and Certificate Practice Statement will be published at http://lockstep.com.au/technologies.

1.3 MDAV PKI Participants

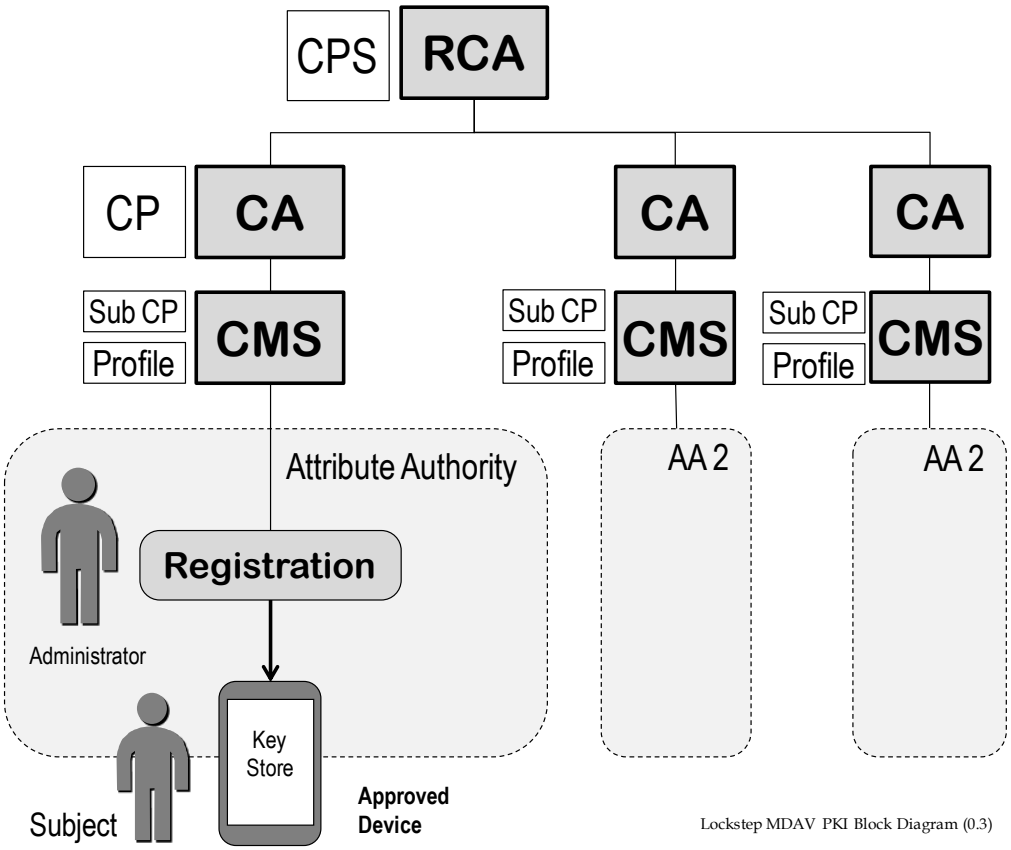
In overview, MDAV certificates carry copies of particular attributes issued to individuals by Attribute Authorities (such as credentialing bodies for First Responders). A registration process provisions an MDAV certificate to a particular Subject and a key store on a mobile device controlled by the Subject. Only MDAV-approved mobile devices may carry MDAV certificates; this rule is enforced by the registration process.

Participating Attribute Authorities use a Certificate Management System (CMS) to interface the registration process to a CA in the MDAV hierarchy. Certificates are issued by each AA's CA under a Certificate Policy specific to that AA, and carry a unique Policy OID. Each MDAV Certificate Policy will in particular specify the meaning of the attribute, the rules for a Subject to qualify for the attribute, any terms and conditions governing how the Subject should act in the context of the attribute, the normal lifetime of the attribute, conditions for renewing or cancelling the attribute, and details of the approved device(s) that the certificate may be issued to.

Each certificate issued within MDAV uniquely specifies (through the Policy OID):

- an attribute value assigned to the certificate Subject
- the identity of the Attribute Authority, and
- the type of device to which the certificate has been issued.

This set of facts may be securely conferred to any Relying Party by a certificate holder by digitally signing a message with the private key associated with the certificate.



1.3.1 Certification Authorities

All CAs in the MDAV PKI are *virtual CAs* run by the MDAV Operator on behalf of participating Attribute Authorities. Each CA Certificate Policy is assigned a unique Policy OID.

1.3.2 Registration Authorities

All registration of MDAV certificate Subjects is done via a CMS accessed by authorized administrators of participating Attribute Authorities. Such administrators and their registration systems may be regarded as "RAs". There are no separate RAs in MDAV.

1.3.3 Subscribers

All Subscribers (Subjects) of MDAV certificates are bona fide members of communities of interest represented by respective Attribute Authorities. Each Subject is known by an AA according to rules of that AA sufficient for an attribute value to be assigned to that Subject. The MDAV scheme plays no part in setting the membership or registration rules of Attribute Authorities.

Subjects may be issued multiple MDAV certificates by multiple AAs, to one or more approved devices.

1.3.4 Relying Parties

Relying Parties in the MDAV scheme are any individual or organisation choosing to interact with a Subject on the basis of the attribute and associated Attribute Authority. Relying Parties generally recognise the authority of an AA in a certain context.

Relying Party applications are to be written in order to transact with certificate Subjects in that context. Relying Party applications will need to each have a reliable copy of the MDAV Root Public Key and will need to recognise particular Policy OID values in order to validate a given Subject and their presented certificate.

1.3.5 Other Participants

Developers writing software that processes MDAV certificates will generally need to obtain information about Policy OIDs from the MDAV Operator.

EDITORS NOTE: Some sort of developers support help desk is envisaged in the medium term, plus a directory, out of scope for the Execution Phase.

1.4 Certificate Usage

1.4.1 Appropriate Certificates Uses

Each MDAV certificate is expected to be used to convey the fact that the Subject has been issued a given attribute value by the Attribute Authority named in the certificate (issuer field). Technically, MDAV certificates will typically be used to sign messages or digital objects originating from the Subject which are authorized in some context by way of the attribute value.

An MDAV certificate means nothing more and nothing less than the fact that the certificate Subject has been issued with a particular attribute value by the Attribute Authority named in the certificate.

Appropriate certificate uses will be precisely specified in a sub-policy specific to the Attribute Authority.

1.4.2 Prohibited Certificate Uses

Prohibited certificate uses will be specified in a sub-policy specific to the Attribute Authority.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The MDAV Root CA CP is administered by the MDAV Operator. MDAV Certificate sub policies are administrated by Attribute Authorities, as named in the certificates.

1.5.2 Contact Person

Stephen Wilson, Lockstep Technologies

swilson@lockstep.com.au.

1.5.3 Persons Determining CPS Suitability for the Policy

Stephen Wilson, Lockstep Technologies

Acting MDAV PKI Manager

swilson@lockstep.com.au.

1.5.4 CPS approval procedures

To be developed.

1.6 Definitions and Acronyms

MDAV Wallet app	A client application in an approved mobile device which manages a set of MDAV certificates. The Wallet displays the loaded certificates, allows a user to select and present certificates to a Verification app, and allows the Subject to load certificates.
MDAV Verification app	A client application in an approved mobile device, operated by an officer in the field, to request a particular attribute from a First Responder via an MDAV certificate, and which validates a received certificate in respect of its Policy OID, expiry date and if applicable the CRL.
Capsule	Lockstep Technologies marketing term for *certificate*, which holds an attribute value and indicates who issued the attribute and what sort of device holds the private key.

AA	Attribute Authority
CCICADA	Command, Control and Interoperability Center for Advanced Data Analysis
DHS	Department of Homeland Security
FIDO	Fast Identity Online
FIPS	Federal Information Processing Standard
FIPPs	Fair Information Practice Principles
ICA	Intermediate Certification Authority
IdP	Identity Provider
KIPI	Kantara Identity and Privacy Incubator
MDAV	Mobile Device and Attributes Validation
OTA	Over The Air
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PoC	Proof of Concept
RCA	Root Certification Authority
TRA	Threat & Risk Assessment
UI	User Interface
UX	User Experience
WPKI	Wireless PKI

2. Publication and Repository Responsibilities

2.1 Repositories

A repository of Certificate Policies, Certificate Profiles, Certificate Revocation Lists, and developer support materials will be maintained by the MDAV Operator.

2.2 Publication of Certificate Information

To be completed.

2.3 Frequency of Publication

To be decided.

2.4 Access Controls on Repositories

To be decided.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of names

MDAV Certificate Subjects are generally not named in the certificate, but instead are identified (if at all) by their attribute value (see 3.1.5 below).

The baseline MDAV certificate profile set out in this master CP uses the Subject Distinguished Name field to hold the attribute value, this rendering the certificate pseudonymous or anonymous. Variations to this naming schema are permitted under this policy, and must be documented in a Certificate sub-Policy.

3.1.2 Need for names to be meaningful

There is no need for attributes to be meaningful outside the context of the Attribute Authority community of interest. It is expected that Relying Parties will recognise the meaning of attribute values in context, and that the context will be completely codified by the Subject certificate Policy OID.

3.1.3 Anonymity or pseudonymity of subscribers

MDAV certificate Subscribers (ie Subjects) are generally anonymous or pseudonymous, being identified only by the attribute value.

3.1.4 Rules for interpreting various name forms

No stipulation. Attribute values are interpreted by Relying Parties in the context of the AA community of interest according to rules made by the AA and codified by the Policy OID. Information about these rules is expected to be made available to RPs and application developers outside this CP.

3.1.5 Uniqueness of names

Attribute values may or may not be unique within the associated community of interest

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

Control of the Subject's private key will be determined by the Certificate Management System and registration process at the Attribute Authority at the time the MDAV certificate is issued with the approved mobile device.

3.2.2 Authentication of organization identity

MDAV authenticates participating Attribute Authorities and equips them with authenticated CMS access.

EDITORS NOTE: More details to follow through preliminary proof of concept design later in Phase 1.

3.2.3 Authentication of individual identity

No stipulation. Attribute Authorities will authenticate Subject identity according to business rules for attribute issuance.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

No stipulation.

3.2.6 Criteria for interoperation

No stipulation. There is no expectation that MDAV certificates will be used or recognisable outside the AA community of interest.

MDAV certificates may have a Critical extension set.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication for routine re-key

No stipulation. MDAV certificates may be re-keyed [or renewed] in keeping with the AA's member or credential management process.

3.3.2 Identification and authentication for re-key after revocation

No stipulation. The AA is responsible for detailed protocols for re-key [or renewal] after revocation and must document these in a Certificate sub-Policy.

3.4 Identification and Authentication for Revocation Requests

No stipulation. The AA is responsible for detailed protocols for revocation and must document these in a Certificate sub-Policy.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate applications may only be submitted by an administrator at an AA registered with MDAV via an approved Certificate Management System.

4.1.2 Enrolment process and responsibilities

No stipulation. MDAV certificate enrolment processes are entirely a matter for the Attribute Authority.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

No stipulation. MDAV certificate Subject identification and authentication are entirely a matter for the Attribute Authority.

4.2.2 Approval or rejection of certificate applications

MDAV certificate applications are normally processed straight through. Except for system failures or planned outages, it is not expected that any certificate application from a registered CMS will ever be rejected.

4.2.3 Time to process certificate applications

To be decided.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

MDAV certificate applications are normally processed straight through. The MDAV CAs are connected only to MDAV CMSes in participating Attribute Authorities. MDAV CAs are essentially automatic.

Under this policy, certificate installation at the Wallet app may be performed over-the-air or in-person (or by other means), depending on the AA security policy and as documented in a sub Certificate Policy.

4.3.2 Notification to subscriber by the CA of issuance of certificate

MDAV certificate Subjects will be notified of issuance through the MDAV Wallet client application in which the certificate is embedded and provisioned via the CMS. The user experience of certificate issuance will be of a new attribute being loaded to the MDAV Wallet client app.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Certificate acceptance will be embedded in the Terms & Conditions of the MDAV Wallet client app, which will need to be unambiguously accepted when the app is installed and when attributes are loaded.

4.4.2 Publication of the certificate by the CA

MDAV certificates will be published by the issuing CA on a directory. The directory will not necessarily be public but may be access controlled according to rules set by the associated Attribute Authority.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation. It is not generally necessary for certificate issuance to be notified because an MDAV certificate merely reflects the fact that a Subject has a given attribute, a fact that should be known or otherwise accessible by others in the AA's community of interest.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The private key associated with an MDAV certificate must only be used for conveying the attribute value. More particularly, the private key may only be used by an approved MDAV client application running on an approved mobile device.

Note that an MDAV certificate may, at the discretion of the Attribute Authority, have an X.509 Critical Extension asserted, so as to mitigate against the certificate being used in non MDAV applications.

4.5.2 Relying party public key and certificate usage

Relying Parties should only use MDAV certificates to validate the association of a Subject with a given attribute value. RPs are reminded that an MDAV certificate means nothing more and nothing less than the fact that a Subject has been issued with an attribute of a certain value by the AA named in the certificate.

A Sub Certificate Policy for the MDAV certificate may describe in more detail the associated approved mobile device (including how it is expected to be activated by the Subject) and the detailed process by which the AA Administrator loads the MDAV certificate. These details may help RPs and MDAV Validation app developers understand the strength of the association between an MDAV certificate value and the expected operator of the device.

EDITORS NOTE: More tutorial-style detail on these points is to be developed as the project develops. We will discuss ways for locking the user's device, and the level of verification done when the certificate is provisioned, and how the MDAV Certificate Policy OID represents these

details, so that RPs can interpret and risk-manage their engagement with Subjects.

4.6 Certificate renewal

MDAV certificates are never "renewed" in the X.509 sense of the term; that is, re-issued with the same profile information and the same public key. All replacement and refreshed MDAV certificates are *re-keyed*. See section 4.7.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

Note that MDAV certificates are always re-keyed when an attribute is renewed and a new certificate issued. MDAV certificates are never renewed without creating a new public-private key pair.

4.7.1 Circumstance for certificate re-keying

An MDAV certificate may be automatically re-keyed as and when the attribute it asserts is renewed. A membership or customer relationship management system (CRM) operated by the Attribute Authority may trigger a certificate re-key request at the CMS.

Under this policy, installation of a re-keyed certificate at the Wallet app may be performed over-the-air or in-person (or by other means), depending on the AA security policy and as documented in a sub Certificate Policy.

4.7.2 Who may request re-key

In general, re-key of MDAV certificates is automatic and follows renewal of the corresponding attributes, or recovery after revocation. Re-key as such need not be specially requested by any party.

4.7.3 Processing certificate re-key requests

Certificate re-key requests received by an MDAV CA from an authorized AA CMS are processed automatically by the CA.

4.7.4 Notification of new certificate issuance to subscriber

MDAV certificate Subjects will be notified of issuance through the MDAV Wallet client application in which the certificate is embedded and provisioned via the CMS. The user experience of new certificate issuance will be of a new attribute being loaded to the MDAV Wallet client app.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Certificate acceptance will be embedded in the Terms & Conditions of the MDAV Wallet client app, which will need to be unambiguously accepted when the app is installed and again when attributes are loaded.

4.7.6 Publication of the re-keyed certificate by the CA

MDAV certificates will be published by the issuing CA on a directory. The directory will not necessarily be public but may be access controlled according to rules set by the associated Attribute Authority.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation. It is not generally necessary for certificate issuance to be notified because an MDAV certificate merely reflects the fact that a Subject has a given attribute, a fact that should be known or otherwise accessible by others in the AA's community of interest.

4.8 Certificate modification

MDAV certificates are never "modified". All updated MDAV certificates are *re-keyed*. See section 4.7.

4.8.1 Circumstance for certificate modification

Not applicable.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

MDAV certificates should be revoked when any of the following occurs:

— the association between Subject and Attribute Authority has ended

— the Subject's standing with the AA has changed such that the attribute value is no long valid or meaningful

— the Subject's private key has been compromised

— the Subject's mobile device has been replaced and the MDAV Wallet app recovered or re-installed, or

— there are grounds to suspect that the Subject's private key may have been compromised.

4.9.2 Who can request revocation

— An Attribute Authority

— A Subject (by contacting the Attribute Authority).

— The MDAV Operator (if for example an MDAV CA is itself revoked).

4.9.3 Procedure for revocation request

Revocation requests are normally submitted via a CMS y an authorized Administrator at an AA.

CAs will generally allow revocation requests to be submitted directly by CA administrators.

4.9.4 Revocation request grace period

There is no revocation grace period.

4.9.5 Time within which CA must process the revocation request

The CA will normally revoke certificates within one hours of a revocation request unless a maintenance period is in operation.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

4.9.7 CRL issuance frequency (if applicable)

Twenty four hours.

4.9.8 Maximum latency for CRLs (if applicable)

Twenty four hours.

4.9.9 Online revocation/status checking availability

To be decided.

4.9.10 Online revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

Subjects will be required to report promptly any known or suspected private key compromise, with detailed obligations to be set out in the terms & conditions for the MDAV Wallet app.

4.9.13 Circumstances for suspension

MDAV certificates may not be suspended.

The MDAV certificate subject is responsible for protecting their MDAV app and private key(s) against misuse at all times.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

To be decided.

4.10.2 Service availability

The Certificate Revocation List should be available on a substantially 24x7 basis in the MDAV directory.

An OCSP Service is intended to be available on a substantially 24x7 basis over HTTP.

4.10.3 Optional features

To be decided.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

No keys are escrowed or backed by the MDAV PKI.

Subject private keys may be backed up by a CMS or as part of a mobile device management process, at the discretion of the Subject. This policy takes no position on device management except to stipulate that in the event that a device holding MDAV keys is lost or compromised such that the device and MDAV app are restored on a new device, then the previous MDAV certificates must all be revoked.

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. Management and Operational Controls

See Certification Practice Statement.

EDITORS NOTE: The MDAV PKI follows the "Security Printer CA" model[1] where the role of the backend certificate issuance server is produce certificates on command of an authorised RA or CMS. Broadly speaking, the physical, operational and technical security of the MDAV CAs will be in line with that of US Federal PKI standards. We will engage the services of a CA service that meets the FPKI physical and operational security benchmarks.

The CPS for the MDAV CA may yet need to be written as a standalone document, given that the MDAV CA may need to be specified separately because of its "Security Printer" model.

5.1 Physical Security Controls

TBD.

5.2 Procedural Controls

TBD.

5.3 Personnel Controls

TBD.

5.4 Audit Logging Procedures

TBD.

5.5 Records Archival

5.5.1 Types of Event Recorded

TBD.

5.5.2 Retention Period for Archive

TBD.

5.5.3 Protection of Archive

TBD.

[1] See *Public Key Superstructure: It's PKI Jim But Not As We Know It*, Stephen Wilson, 7th Symposium on Identity and Trust on the Internet, NIST, Gaithersburg, MD, USA 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2548224.

5.5.4 Archive Backup Procedures

TBD.

5.5.5 Requirements for Time-stamping of Records

TBD.

5.5.6 Archive Collection System (Internal or External)

TBD.

5.5.7 Procedures to Obtain and Verify Archive Information

TBD.

5.6 Key Changeover

TBD.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

TBD.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

TBD.

5.7.3 Entity Private Key Compromise Procedures

TBD.

5.7.4 Business Continuity Capabilities after a Disaster

TBD.

5.8 CA or RA Termination

TBD.

6. Technical Security Controls

See Certification Practice Statement.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

TBD.

6.1.2 Private Key Delivery to Subscriber

TBD.

6.1.3 Public Key Delivery to Certificate issuer

TBD.

6.1.4 CA Public Key Delivery to Relying Parties

TBD.

6.1.5 Key Sizes

TBD.

6.1.6 Public Key Parameters Generation

TBD.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

TBD.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

TBD.

6.2.2 Private Key (m of n) Multi-person Control

TBD.

6.2.3 Private Key Escrow

TBD.

6.2.4 Private Key Backup

TBD.

6.2.5 Private Key Archival

TBD.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

When a Cryptographic module is used, the Private Key of the Medicare TBD.

6.2.7 Private Key Storage on a Cryptographic Module

TBD.

6.2.8 Method of Activating Private Key

TBD.

6.2.9 Method of Deactivating Private Key

TBD.

6.2.10 Method of Destroying Private Key

TBD.

6.2.11 Cryptographic Module Rating

TBD.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

TBD.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

TBD.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

TBD.

6.4.2 Activation Data Protection

TBD.

6.4.3 Other Aspects of Activation Data

TBD.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

TBD.

6.5.2 Computer Security Rating

TBD.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

TBD.

6.6.2 Security Management Controls

TBD.

6.6.3 Life-cycle Security Ratings

TBD.

6.7 Network Security Controls

TBD.

6.8 Time-stamping

TBD.

7. Certificate and CRL Profiles

7.1 Certificate Profiles

7.1.1 Version Number(s)

All MDAV certificates are X.509 version 3 certificates.

7.1.2 Certificate extensions

EDITORS NOTE: To be decided in collaboration with the Proof of Concept CA partner.

We will consider making an extension Critical in order to restrain unexpected use of the MDAV certificate.

7.1.3 Algorithm Object Identifiers

To be decided.

7.1.4 Name Forms

Subject

Field	Usage	Count	Contents
CN	Required	1	Attribute value as issued to Subject, e,g, "CN=1234567890"
	Required	1…N	Minimal additional naming attributes for uniquely identifying the subject *if required*, including individual name, serial number etc.

MDAV CA

Field	Usage	Count	Contents
CN	Required	1	Descriptive name for Attribute Authority, e.g., "CN=Credential XYZ Issuer"
OU	Required	0…1	"Administrator XYZ" or similar text
O	Required	1	Issuer name, e.g., "O=Credential XYZ Issuer"
C	Required	1	Country name, "C=US"

MDAV Root CA

Field	Usage	Count	Contents
CN	Required	1	"CN=MDAV Proof of Concept Root CA"

O	Required	1	Issuer name, "O= MDAV Proof of Concept Root CA"
C	Required	1	Country name, "C=US"

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

EDITORS NOTE: To be decided with the Proof of Concept CA partner.

7.1.7 Usage of Policy Constraints Extension

EDITORS NOTE: To be decided with the Proof of Concept CA partner.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

All MDAV CRLs are X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

7.3.1 Version Numbers (s)

EDITORS NOTE: To be decided with the Proof of Concept CA partner.

7.3.2 OCSP Extensions

EDITORS NOTE: To be decided with the Proof of Concept CA partner.

8. Compliance Audit and Other Assessment

EDITORS NOTE: To be decided with the Proof of Concept CA partner, in line with FPKI benchmarks and existing compliance arrangements.

8.1 Frequency of Entity Compliance Assessment

TBD.

8.2 Identity / Qualifications of Assessor

TBD.

8.3 Auditor's Relationship to Assessed Entity

TBD.

8.4 Topics Covered by Assessment

TBD.

8.5 Actions Taken as a Result of Deficiency

TBD.

8.6 Communication of Results

TBD.

9. Other Business and Legal Matters

EDITORS NOTE: To be decided with the Proof of Concept CA partner, in line with FPKI benchmarks and existing legal matters.

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

TBD.

9.1.2 Certificate Access Fees

TBD.

9.1.3 Revocation or Status Information Access Fees

TBD.

9.1.4 Fees for Other Services

TBD.

9.1.5 Refund Policy

TBD.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

TBD.

9.2.2 Other Assets

TBD.

9.2.3 Warranty Coverage

TBD.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

TBD.

9.3.2 Information not within the scope of confidential information

TBD.

9.3.3 Responsibility to protect confidential information

TBD.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

TBD.

9.4.2 Information treated as private

TBD.

9.4.3 Information not deemed private

TBD.

9.4.4 Responsibility to protect private information

TBD.

9.4.5 Notice and consent to use private information

TBD.

9.4.6 Disclosure pursuant to judicial or administrative process

TBD.

9.4.7 Other information disclosure circumstances

TBD.

9.5 Intellectual Property Rights

9.6 Representations and Warranties

9.6.1 CA representations and warranties

TBD.

9.6.2 RA representations and warranties

TBD.

9.6.3 Subscriber representations and warranties

TBD.

9.6.4 Relying party representations and warranties

TBD.

9.6.5 Representations and warranties of other participants

TBD.

9.7 Disclaimers of Warranties

TBD.

9.8 Limitations of Liability

TBD.

9.9 Indemnities

TBD.

9.10 Term and Termination

9.10.1 Term

TBD.

9.10.2 Termination

TBD.

9.10.3 Effect of termination and survival

TBD.

9.11 Individual Notices and Communications with Participants

TBD.

9.12 Amendments

TBD.

9.12.1 Procedure for Amendment

TBD.

9.12.2 Notification Mechanism and Period

TBD.

9.12.3 Circumstances Under Which OID Must be Changed

TBD.

9.13 Dispute Resolution Procedures

TBD.

9.14 Governing Law

TBD.

9.15 Compliance with Applicable Law

For further information, refer to Section 9.15 of the Medicare Australia RCA CP.

9.16 Miscellaneous Provisions

TBD.

9.16.1 Entire agreement

TBD.

9.16.2 Assignment

TBD.

9.16.3 Severability

TBD.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

TBD.

9.16.5 Force Majeure

TBD.

9.17 Other provisions

TBD.