Request For Proposal (RFP)

FY22-25809

Mobile Driver License Digital Trust Service (Minimally Viable Product)

November 3, 2021

AAMVA - Official Use Only

The American Association of Motor Vehicle Administrators (AAMVA) is a non-profit organization, representing the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws.

American Association of
Motor Vehicle Administrators

Address 🖃: AAMVA
4401 Wilson Boulevard
Suite 700
Arlington, VA 22203

Telephone ☎: 1-888-226-8280
1-703-522-4200

Fax 🖷: 1-703-522-1553

E-mail ✉: AAMVA Help Desk (helpdesk@aamva.org)

Help Desk Hours 🕓: 7:00 a.m. - 10:00 p.m. (Eastern Time)
Monday - Friday
8:00 a.m. - 4:30 p.m. (Eastern Time)
Saturday

Website 💻: http://www.aamva.org/

Contents

List of Tables

1 GLOSSARY

ISO/IEC 18013-5	Personal identification—ISO compliant driving license—Part 5: Mobile driving license (mDL) application.
Awardee	The organization selected by AAMVA as the winning response to this RFP.
Certificate Authority (CA)	Is an authority that creates certificates. Issuing Authorities would need one to create mDLs.
Intellectual Property	Documents, products, know-how, trade secrets or other material each entity brings to the engagement or creates during the engagement.
Issuing Authority (IA)	Issuing Authorities are the government entities responsible for issuing driver licenses and state issued identity credentials to people across North America. Depending on the state, province or territory, the Issuing Authority may be a Department of Motor Vehicles, Registry of Motor Vehicles, Secretary of State's Office, State Law Enforcement, Department of Transportation, or similar entity.
Issuing Authority Certificate Authority (IACA)	Issuing Authorities issuing mDLs will operate a root Issuing Authority Certificate Authority.
Jurisdictions	State, provincial, and territorial governments are referred to as jurisdictions or jurisdiction membership within the AAMVA community. Each state, province and territory in North America may participate within AAMVA as a jurisdiction.
Mobile Driver License (mDL)	Mobile Driver Licenses are the digital, next generation technology of the physical driver licenses. mDLs convey trust that they were issued by a recognized Issuing Authority and can share encrypted data with Relying Parties through reader devices and online digital services. There are many vendors competing to offer mDL solutions.
mDL Digital Trust Service (DTS)	The mDL Digital Trust Service is the basis for this RFP and is the term used to describe the system/solution AAMVA seeks input on. The vision is to provide a means through which AAMVA's Member Jurisdictions (driver license issuing agencies across North America) may easily offer Relying Parties a means of trusting an mDL based on the collection and distribution of Public Keys.
mDL reader device	A device that Relying Parties use to receive encrypted data from the mDL holder's device. Potential devices include (but are not limited to) point of sale devices (e.g., contactless payment style interfaces), mobile phones, tablets, laptops, and smart watches. Mobile apps and online services are installed/downloaded to the device and used to securely request and receive information.
Minimally Viable Product (MVP)	A product management approach that prioritizes the development and delivery of the minimal set of technical/business requirements to achieve a working/functional solution. It allows product teams to learn from real-life use of the system, constituents, customer, etc. Learnings inform next steps in the lifecycle and limit wasted effort/resources.
Private Key	The private half of a public and private cryptographic key pair that is used by an Issuing Authority to sign an mDL digital certificate. The Private Key is held securely by the Issuing Authority. The Private Key MUST never be shared. If it were to leak out a malicious actor could create mDL digital certificates that are perfectly valid even though they are fake.

Public Key	The public half of a public and private cryptographic key pair that is used by an Issuing Authority to sign an mDL digital certificate. The Public Key is used by a Relying Party to verify the signature of an mDL digital certificate. The Relying Party must have knowledge of the Public Key. They either obtained the Public Key directly from the Issuing Authority or from some sort of registry like the mDL Digital Trust Service.
Relying Party (RP)	An entity that has a need to obtain information for, or verification of an individual as a part of its business process (typically performed using credentials issued by jurisdictions). Some examples of these needs (or transactions) include (but are not limited to) age-based purchases, access to facilities, access to web-based content, online retail and eGovernment services. Relying Parties "rely" upon the players in the ecosystem to establish trust in the identity of an individual. In the case of the AAMVA mDL Digital Trust Service, the Relying Parties will be receiving Public Keys from the mDL Digital Trust Service to facilitate their processes.
Respondent	Organizations that assemble and deliver proposals related to this RFP are referred to as "Respondents" throughout this document.
Software	Software developed in advance of engagement for delivery as a stand-alone solution or as a component of a solution on a repeatable basis
VICAL	"Verified Issuer Certificate Authority List". In earlier documentation referred to as a master list. Annex C of ISO/IEC 18013-5 describes in detail what a VICAL provider is.

2 Background & Purpose

The Mobile Driver License Digital Trust Service (mDL DTS) RFP is the culmination of years of learning, collaborating and planning AAMVA's role in the mDL ecosystem. Over the past 18 months, AAMVA invested significant resources to develop RFIs, solicit insights, and gain an understanding of the important elements that need to be accounted for. AAMVA has also been actively engaged in the formation of the ISO/IEC 18013-5 standard for an interoperable mDL in support of member jurisdictions' interests. It is through these efforts that the subject of this RFP (#FY22-25809) was formed.

With driver license Issuing Authorities (IAs) across the United States moving forward with plans to issue mDLs, the challenge to achieve ubiquitous trust and interoperability have become primary concerns. Most would agree that independent activities that are delivered in the absence of a central/galvanizing function will struggle to reach their full value. The ISO/IEC 18013-5 standard defines how mDLs should interoperate with mDL reader devices. It also details key characteristics of a VICAL through which a list of trusted IAs' public keys can be registered and shared with Relying Parties (RPs). These public keys will enable the "trust" that the mDL being presented was created by a trusted IA and that the RP can proceed with confidence. This RFP is specifically focused on the technology of the mDL DTS (AAMVA's version of a VICAL provider) to support all member jurisdictions in delivering successful mDL programs to their stakeholders.

In April of 2021, the AAMVA Board of Directors was presented with a report based on industry stakeholder responses to an RFI regarding the potential for AAMVA to stand up and operate a service like the mDL DTS. The report included affirmations from the 29 respondents that the mDL DTS is the right technological approach to drive ubiquitous trust and interoperability of mDLs issued across the United States (possibly all of North America). The report went further to affirm that AAMVA was the right organization to take on this challenge based on its legacy of delivering sensitive technology infrastructures with a high degree of trust. Finally, the report advocated that the next step forward should be an investment in a Minimally Viable Product (MVP) version of the mDL DTS to initially launch a trusted and interoperable mDL ecosystem within the United States. The Board endorsed the approach and requested that the team build out a full budget request to be presented and approved for inclusion in the 2021-2022 AAMVA budget (October 2021-September 2022).

The AAMVA team fulfilled the Board's request through a series of efforts over the summer of 2021 that included definitions of key requirement, outline/preparation of supporting actions and a budgetary RFI to assist with the budget building effort. The work products were used to make the formal presentation to AAMVA's Board of Directors at their annual meeting in August 2021 at which the budget and plan were approved. This RFP is being issued as a critical step in executing the mDL DTS vision with a MVP service that will support the testing of the approach, learning about things may need to be adjusted, and setting baseline policies/governance that will support the operation. The MVP nature of this initiative will allow AAMVA to minimize the investment required to learn and prepare for a full solution in the future.

3 Objective

AAMVA's objective is to stand up the mDL DTS primary functions with minimal cost and time to market as soon as possible following award. AAMVA has selected to pursue the MVP approach because it balances the immediate activities of many IAs (and their supporting mDL application vendors) with the need to perform initial launch activities to test, learn, and plan for a future full deployment of a mDL DTS. Respondents should be careful to deliver proposals that represent the MVP spirit of the vision.

4 Minimum Qualifications

Respondents must be able to prove they have been supporting at least 3 active clients, with largely similar services as those described in this RFP, for each of the last 5 years at minimum. Further, Respondents should be able to demonstrate their participation and/or familiarity with the ISO/IEC 18013-5 standard. Respondents also must

establish in their proposal that they fully qualify with the neutrality requirement, as explained in §5: Required Neutrality. Respondents should include proof/narrative of these minimum qualification in a qualifications appendix to their response document.

5 Required Neutrality

The Awardee selected to develop and host the mDL DTS must be a neutral party that is not engaged in providing jurisdiction-specific mDL technology products and services (except as provided below concerning Public Key Infrastructure (PKI) solutions).

Respondents must establish compliance with this principle by certifying in their proposal that, during the initial term and any possible renewal or extension of the Agreement to be entered into as the result of this RFP, neither the Respondent nor any organization that is an Affiliate of the Respondent (determined as provided below) has or will seek any commercial relationship with any Member Jurisdiction of AAMVA that includes or pertains to jurisdiction-specific mDL products or services. Examples of such products or services include, without limitation, the development, production or offering of: (i) mobile technology applications that deliver mDL functionality, (ii) digital wallet services that have the capacity to include mDLs, (iii) mDL interoperability technologies to the RP community, or (iv) other mDL delivery technology approaches.

Please take note that a potential Respondent would not be disqualified under this RFP as the result of a commercial relationship with any Member Jurisdiction of AAMVA if the only jurisdiction-specific aspect relating to mDL products and services is limited to providing a Public Key Infrastructure (PKI) solution.

For purposes of establishing compliance with this qualification requirement, an "Affiliate" of an organization includes any other organization that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, that organization. The term "control" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an organization, whether through the ownership of voting securities, by contract or otherwise.

6 Period of Performance

Respondents to this RFP should prepare for an initial period of performance of up to 19 months, commencing upon contract execution following award. AAMVA may extend this period of performance for additional periods of performance with the same terms. The period of performance currently is anticipated to include the following 3 phases, although the organizational structure of services to be performed by the Awardee is subject to change in AAMVA's discretion:

- **Phase 1: Software Development/Deployment**—This is the period of time used to agree upon designs/plans, delivery and testing of the solution prior to MVP operation. Software Specification, Signoff of Specification with AAMVA, Development of software, Testing, hardware/cloud needs, software needs, possible onboarding support of initial MVP participants, QA of software, Acceptance Testing support to AAMVA, and training of AAMVA staff to operate the software

- **Phase 2: Idle Period**—AAMVA may choose to invoke an "idle" period between Software Development/Deployment and MVP Operation phases in which the project may be paused while MVP participants (select jurisdiction mDL providers and RPs) or other mDL DTS business (governance, policies, certifications, etc.) are addressed. The goal of this phase is to minimize unnecessary effort and costs to all parties.

- **Phase 3: MVP Operation**—This phase accounts for the recurring monthly costs and effort required to support the steady state operation of the mDL DTS MVP service. It is envisioned that this would be a

recurring monthly cost to AAMVA and include actions such as monitoring uptime/health of the system and responding to the needs of AAMVA staff that will arise through their use of the system

AAMVA makes no commitment to use the technology procured through this RFP after the conclusion of the Period of Performance. AAMVA reserves the right, in its sole discretion, to negotiate an agreement with the Awardee to mature the technology of the MVP of the mDL DTS service from MVP scope to a full version 1.0 solution at its sole discretion. AAMVA makes no commitment and is under no obligation to engage in further business with the Awardee beyond the scope of the award pursuant to this RFP.

7 Intellectual Property and Work Products

The respective rights of the Awardee and AAMVA concerning rights pertaining to intellectual property incorporated in elements of the mDL DTS is described in Appendix A: Summary of Terms and Conditions.

7.1 RFP Coordinator / Coordination

The RFP Coordinator is the sole point of contact in AAMVA for this procurement. All communications between the Offeror and AAMVA upon receipt of this RFP will be with the RFP Coordinator, as follows:

Alaster Sampson
4401 Wilson Boulevard, Suite 700
Arlington, VA 22203
Email: procurement@aamva.org

Any other communications will be considered unofficial and non-binding on AAMVA. Communication directed to parties other than the RFP Coordinator may result in disqualification of the Proposal.

AAMVA reserves the right to amend or supplement the RFP at any time.

7.2 Estimated Schedule of Procurement Activities

Table 1: Estimated schedule of procurement activities

RFP Issued	November 3, 2021
Respondents Conference	November 15, 2021, 4pm – 5pm
Questions Due	No later than November 17, 2021
Questions/Responses Published	November 22, 2021
Proposals Due	December 10, 2021
Down Selection of Top Responses (discretionary)	January 14, 2022
Product Demonstrations (discretionary)	January 24-28, 2022
Notification of Award	Week of January 31, 2022
Completion/Execution of Contract	February 28, 2022

Respondents conference link: https://attendee.gotowebinar.com/register/6143430379675122447

AAMVA may, at its sole discretion, change or amend any of these activities or dates. Any changes to the process will be communicated with all known potential Respondents. Any questions regarding the timeline/deadlines should be directed to the AAMVA RFP Coordinator.

7.3 Estimated Schedule of Solution Delivery/Operation Activities

Respondents should include a proposed project schedule that includes each of the 3 phases described in §6: Period of Performance. The proposed project schedule may appear in the body of the response document or as an appendix thereof.

Note: Respondents should note that AAMVA would like the Awardee to complete the Development/Deployment phase with a sense of urgency such that AAMVA could choose to begin the MVP Operations phase by September 30, 2022.

7.4 Submission of Proposal

Responses to this RFP are to be made electronically to the RFP Coordinator's email address (procurement@aamva.org) as a PDF soft copy document attachment. The email subject line must include the RFP Number. The PDF attachments must include the RFP Number and the name of the submitting party.

Proposals must respond to all RFP Functional and Technical Requirements with completeness by stating compliance or non-compliance with each requirement, and/or including any requested details or visualizations. Do not respond by referring to material present elsewhere. The Proposal must be complete and must stand on its own merits. Failure to respond to any portion of the RFP document may result in rejection of the Proposal as non-responsive. All Proposals and any accompanying document become the property of AAMVA and will not be returned. Proposals must include the following sections at minimum:

Responses should include specific reference to the applicable evaluation criteria areas defined in § 9: Evaluation Criteria & Contract Award.

- Company/Organization Overview & Qualifications Statement
- References and evidence of performance
- Executive Summary
- Acknowledgement and Assurances regarding Required Neutrality (include appendices as necessary)
- Solution Costs (Phases 1-3)
- Functional & Technical Requirements addressed (line item by line item in table form with the exception of items such as architectural diagrams and descriptions where specified.).
- Signature of Company Officer
- Appendices as required (references, product information, methodologies, etc.)

The proposal body should not exceed 20 pages in total. Additional material should be included as attachments.

Reference and evidence of performance must include at least 3 examples where your company has provided services similar in scope. Those references should include the following information:

- Company name and at least one point of contact
- Project Scope
- Relevance to this solicitation
- Approach, including timeline and hours dedicated
- Any Challenges

Provide resumes or executive summaries of the individual(s) that would be assigned to the project.

7.5 Submission of Questions

AAMVA will only accept questions from Respondents in writing and strictly limited to the contents of the RFP or of the RFP Process. All questions must be sent to the RFP Coordinator no later than the date contained in Table 1. Questions must be presented in Word document format as an email attachment sent to the RFP Coordinator. The RFP Number must be included in the subject line of the email. The attachment file name must include the RFP Number and the name of the responding organization.

AAMVA plans to publish all questions and answers to all parties known to be responding to the RFP as per Table 1. AAMVA may choose to respond iteratively depending on the volume and subject of questions received. Potential Respondents should notify AAMVA of their intent to respond in order to receive communications.

7.6 Acceptance Period

Proposals shall remain valid for 120 calendar days from the Proposals Due date in Table 1.

7.7 Responsiveness

The RFP Coordinator will review all proposals received to determine their compliance with the administrative requirements and instructions specified within this RFP. A failure to comply with any part of the RFP may result in rejection of the Proposal as a non-compliant response. Procurement will notify the vendor in the event their proposal is deemed to be non-compliant.

AAMVA reserves the right, however, at its sole discretion to waive minor administrative irregularities.

7.8 Most Favorable Terms

AAMVA reserves the right to make an award without further discussion of the Proposal submitted. Therefore, the Proposal should be submitted with the most favorable terms the Respondent can propose. AAMVA reserves the right to contact a Respondent for clarifications of its Proposal and to request virtual and/or face-to-face meetings.

AAMVA reserves the right to incorporate all or portions of the RFP and/or the Awardees proposal in the agreement resulting from this RFP. See Appendix A: Summary of Terms and Conditions for a Summary of certain anticipated Terms and Conditions in the Agreement to be entered into with the Awardee under this RFP.

7.9 General Terms and Conditions

AAMVA will issue a Notice of Intent to Award to the apparently successful Respondent. As soon as possible following the issuance of this Notice, AAMVA will provide that Respondent with a proposed form of agreement with AAMVA. A summary description of some of the important provisions that AAMVA anticipates including in the proposed agreement appears in Appendix A: Summary of Terms and Conditions.

Final issuance of the Award will be conditioned on the successful negotiation of a definitive agreement between AAMVA and the apparently successful Respondent that has received a Notice of Intent to Award. AAMVA reserves the right to discontinue discussions with an apparently successful Respondent and proceed to issue a Notice of Intent to Award to another organization if AAMVA determines, in its sole discretion, that the negotiation process is not proceeding in a timely and productive manner.

7.10 Cost to Propose

Respondent is solely responsible for all costs incurred by the Respondent in preparing a Proposal in response to this RFP, or in performing any other activities related to responding to this RFP.

7.11 No Obligation to Contract

This RFP does not obligate AAMVA to contract for the services described in this RFP. AAMVA reserves the right, in its sole discretion, to reject any and all proposals received and not to issue a contract as a result of this RFP.

8 Solution Pricing

Compliant Responses will separately price each of the following 3 components:

- Phase 1— Costs related to the design, development, testing and deployment of the software solution
- Phase 2— Costs that AAMVA will incur per month if the project is paused between Phase 1 and Phase 3
- Phase 3— Costs per month to operate the mDL DTS solution after it has been deployed. This should be a "steady-state" monthly rate that is applied monthly for each month the MVP is operational.

Notes:

- The above-described pricing components must include all software licenses/fees that will be incurred by AAMVA.
- Pricing for each phase should demonstrate the variance related to establishing an AAMVA owned Root CA Function versus the use of an external Digital Certificate signing authority as described in §12.7.2: VICAL Generation.

9 Evaluation Criteria & Contract Award

All Proposals will be reviewed initially by the RFP Coordinator. Only proposals from Respondents that meet all required qualifications and that comply with the requirements for proposals as set forth in this RFP will be forwarded to the evaluation team for further review. Responsive proposals will be evaluated against the specifications stated in this RFP and in any addendum issued. Award, if any, will be made to the vendor that provides the best overall value to AAMVA. AAMVA will evaluate all proposals with reference to the following criteria:

Evaluation Criteria
Corporate Qualification Evaluation
Financial history, reputable and established entity
References and Evidence
Neutrality (see §5: Required Neutrality)
Technical Proposal Evaluation
Experience & knowledge delivering PKI based solutions
Strength of responses to software development and support requirements
Demonstrated understanding of the VICAL concept, responsibilities and PKI Best Practices
Cost Proposal Evaluation
Overall Price

10 Scope of the mDL DTS MVP solution

AAMVA believes there is great value to be realized through the delivery of a mature version of the mDL DTS, however, there are important learning activities to complete prior to making the decision to invest in the full deployment. At a high level, AAMVA's vision is to (with help) build and operate the core technologies of the system with the expectation that interfaces between IAs and AAMVA will be manual in nature. Specifically, AAMVA plans to collect public keys directly from IAs in a manual manner. Further, AAMVA expects to add those keys, from which the VICAL will be created, to the mDL DTS system via a provided user interface. The signing of the VICAL will be a system function that will result in the creation of a VICAL and publication to a website, for RPs to download. The guiding principle is to establish core system functions while minimizing scope, through manual administration/functions where it makes sense. Interfaces for users/operators may be basic and minimized to serve the scope of an MVP deployment only.

The MVP delivery is intended to provide AAMVA with the means to:

1. Validate the technical elements at the core of the service.

2. Exercise the system in production with a select group of IAs and RPs.
3. Implement and test policy and governance expectations with MVP participants.
4. Work with all parties to harden economic aspects of the system/value to drive the formation of potential business models.
5. Demonstrate the viability of the approach and create interest across all AAMVA community members for this important mDL ecosystem enabling service.

Out of Scope:

- In the spirit of an MVP service, automated interfaces between IAs and the mDL DTS system are out of scope. All interactions between IAs and the mDL DTS will be done either through the manual exchange of keys, or using secure email, with designated AAMVA staff.
- RPs will not be registered within the mDL DTS system. They will be manually given instructions for accessing the website containing the published VICAL where they can freely download current or archived VICALs.

AAMVA's Role

AAMVA will be the sole entity interfacing with MVP participating organizations and will be the users/operators of the user interfaces developed for adding IAs to the system, inputting the initial public key, updating (i.e. revoke and issue new) public keys obtained from the IAs and initiating VICAL generation/publication.

Awardee's Role

Awardee will be responsible for building the software, hosting the service, and providing technical support. All user interactions, and interacting with the mDL DTS system, from a users' perspective will be staffed with AAMVA personnel.

11 FUNCTIONAL REQUIREMENTS

11.1 OVERVIEW

The MVP version of the DTS system provides the following functions:

- IA administration
- IACA certificate administration
- User administration
- Audit record maintenance, and reporting
- VICAL administration

This is supported by a primary data store, replicated to a secondary data store.

The sections that follow describe these functions and data stores in more detail, and separately describe non-functional requirements and requirements, including in respect of the eventual decommissioning of the DTS.

Within the context of this RFP the following system actors are defined.

1. **Awardee.** The Awardee is responsible for two distinct deliverables:
    a. Establishing the DTS infrastructure (including all hardware, software, websites and services).

b. Hosting the service described here.

2. **AAMVA staff** will be users of the system. AAMVA will use the DTS system user interface to perform the functions listed above.
3. **IAs.** IAs do not have direct access to the DTS system. AAMVA staff will act as mediators between the DTS system and IAs. IAs generate IACA certificates.
4. **RPs.** RPs are public entities who download the VICAL through a public website/service.

11.2 IA ADMINISTRATION

The creation of an IA record in the DTS system is preceded by a manual process (completely separate from the DTS) whereby AAMVA staff collect information from an IA. AAMVA staff then create and enter the IA information into the DTS system using a manual user interface. AAMVA staff also updates this information as necessary. During the MVP, an IA will NOT have a login to the DTS system.

The DTS system provides a user interface via which any IA can be administered. The functions supported by this interface are listed in Table 2.

In addition to the guidance provided in section 7.4, the Respondent's response to this section must describe the solution to the stated requirements and how it will integrate with the rest of the DTS system.

In your response to this section, please include a description as to how you would build this component and how it interacts within the overall architecture of the system.

Table 2: IA administration requirements

#	Requirement	Description
1.	Create IA	Establish a record of an IA in the DTS system.

2.	IA data fields	Maintain the following data for each IA:
		• IA Name
		• Full Address
		• Phone Number
		• Fields used to identify the IA as an issuer of an IACA cert (see Appendix B of ISO/IEC 18013-5):
		  ○ countryName
		  ○ stateOrProvinceName
		• Optionally, Signed Application (uploaded doc)
		• Points of Contact (0 or more)

3.	Upload completed application file	Optional ability to upload a signed PDF document
4.	Upload a completed contract file	Optional ability to upload a completed contract in PDF format

#	Requirement	Description
5.	IA point of contact	Add, update, or decommission a point of contact for an IA. At least the following fields are supported for a point of contact: • Full name • Email address • Contact numbers (including type of number, e.g., Work, Mobile, Fax) Information about decommissioned points of contact remain available.
6.	IA Statuses	Optionally, the DTS system assigns a status to each IA to clarify where it is in its lifecycle. This status is visible in the IA administration user interface. Examples of conceptual lifecycle states are pending, and active.

11.3 IACA CERTIFICATE ADMINISTRATION

IACA certificates are collected outside the DTS. The DTS system provides a user interface for administering IACA certificates. The functions supported by the IACA certificate administration user interface are listed in Table 3.

In addition to the guidance provided in §8.4: Submission of Proposal, the Respondent's response to this section must provide a full description of any IACA certificate validations not listed in Table 3.

Table 3: IACA Certificate administration requirements

#	Title	Description
7.	Ability to upload IACA certificate	The DTS system supports uploading an IACA root certificate and uploading an IACA link certificate.
8.	IACA certificate acceptance prerequisites	The DTS system confirms the following before allowing an IACA certificate to be accepted into the DTS: • The IA record for the IACA certificate exists in the DTS. • At least two non-decommissioned contacts exist for the IA.
9.	IACA certificate Validation	The DTS system performs at least the following validations on an IACA certificate. If any validation fails, the IACA certificate is not accepted for further processing. 1. The stateOrProvinceName element must be present. 2. IACA Certificates must otherwise comply with 3. Table 4[1] (for root certificates) and Table B.2 of ISO/IEC 18013-5 (for link certificates). This includes, and is not limited to: a. Checking that mandatory fields are present, appropriately formatted, and contain valid values (as far as can be determined). b. Checking that optional fields present are appropriately formatted and contain valid values (as far as can be determined). c. Checking that an IACA root certificate is self-signed. 4. The validity period must fall within the acceptable duration parameters.

[1] Sourced from Table B.1 in ISO/IEC 18013-5, and amended as highlighted to reflect domestic limitations on cryptographic curves.

#	Title	Description
10.	IACA certificate chain validation	The DTS system supports the cryptographic linking of two IACA root certificates by way of an IACA link certificate.
11.	IACA certificate revocation	The DTS system allows for revoking an IACA certificate. A revoked IACA root certificate is not included in subsequent VICALs.
12.	IACA certificate revocation confirmation	The DTS system allows for optional verification that the IACA certificate being revoked is in the IA's IACA CRL. It should be revoked by the IA before being revoked in the DTS.
13.	View IACA certificate	The DTS system allows for the content of any IACA certificate to be viewed.
14.	Manually validate IACA certificate	The DTS system allows for manual validation of an IACA certificate (based on visual inspection). Certificates failing manual validation are not accepted for further processing.
15.	IACA certificate status	The DTS system assigns a status to each IACA certificate to clarify where it is in its lifecycle. This status is visible in the IACA certificate administration user interface. Examples of conceptual lifecycle states are uploaded, active (passed validation), failed validation.
16.	Usage Period	The DTS system supports configurable parameters defining the usage period for IACA Certificates.
17.	IACA certificate deletion	The DTS system does not allow the deletion of any IACA certificate.
18.	IACA certificate updating	The DTS system does not allow any updates to be applied to an IACA certificate.

Table 4: IACA root certificate profile

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Version	4.1.2.1	M		Shall be v3.
Serial number	4.1.2.2	M		Non-sequential positive, non-zero integer, shall contain at least 63 bits, should contain at least 71 bits of output from a CSPRNG, maximum 20 octets.
Signature	4.1.2.3	M		Value shall match the OID in the signature algorithm (below) .

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Issuer	4.1.2.4	M		countryName is mandatory. The value shall be in upper case and contain the ISO 3166-1 alpha-2 code of the issuing country, exactly the same value as in the issuing country data element. The countryName shall be PrintableString. stateOrProvinceName is optional. If this element is present, the element shall also be present in the end-entity certificates and hold the same value. The value shall exactly match the value of the data element "issuing_jurisdiction", if that element is present on the mDL. organizationName is optional. Its value is at the discretion of the IACA. commonName shall be present. Its value is at the discretion of the IACA. serialNumber is optional. If present, it shall be a PrintableString. Attributes that have a DirectoryString and for which the encoding is not listed above syntax shall be either PrintableString or UTF8String.
Validity	4.1.2.5	M		
Not before		M		Date on which the certificate validity period begins.
Not after		M		Maximum of 20 years after "Not before" date. NOTE The 20-year validity period results from the possibility of using the IACA root certificate for issuing an IDL according to ISO/IEC 18013-3, which allows the use of DS certificates with validity periods up to 15 years. If the IACA root certificate is only used to issue mDLs, a maximum validity period of 9 years is sufficient.
Subject	4.1.2.6	M		Same exact binary value as Issuer.
Subject public key info	4.1.2.7	M		
algorithm		M		1.2.840.10045.2.1 (Elliptic curve)
parameters		M		Implicitly specify curve parameters through an OID associated with one of the following curves specified in FIPS PUB 186-4: 1.2.840.10045.3.1.7 (Curve P-256) 1.3.132.0.34 (Curve P-384) 1.3.132.0.35 (Curve P-521) ~~Or one of the following curves specified in RFC 5639:~~ ~~1.3.36.3.3.2.8.1.1.7 (brainpoolP256r1)~~ ~~1.3.36.3.3.2.8.1.1.9 (brainpoolP320r1)~~ ~~1.3.36.3.3.2.8.1.1.11 (brainpoolP384r1)~~ ~~1.3.36.3.3.2.8.1.1.13 (brainpoolP512r1)~~
subjectPublicKey		M		Public key shall be encoded in uncompressed form.
X.509v3 extensions	4.2	M		Further extensions may be present if they are marked non-critical.
Subject key identifier	4.2.1.2	M	NC	SHA-1 hash of the subject public key BIT STRING value (excluding tag, length, and number of unused bits).
Key usage	4.2.1.3	M	C	

Certificate component	Section in RFC 5280	Presence	Criticality	Description
Digital signature				0
Non-repudiation				0
Key encipherment				0
Data encipherment				0
Key agreement				0
Key certificate signature				1
CRL signature				1
Encipher only				0
Decipher only				0
Issuer alternative name	4.2.1.7	M	NC	The issuer alternative name extension shall provide contact information for the issuer of the certificate. For that purpose, the issuer alternative name shall include at least one of • rfc822Name, or • uniformResourceIdentifier. NOTE This contact information is intended to help establish trust in the certificate and the certified key by appropriate out of band mechanisms. Note that this information is only meant for contact information and does not in itself imply any level of trust in the certificate.
Basic constraints	4.2.1.9	M	C	
CA		M		TRUE
pathLenConstraint		M		0
CRLDistributionPoints	4.2.1.13	M	NC	The 'reasons' and 'cRL Issuer' fields shall not be used.
distributionPoint		M		URI for CRL distribution point.
Signature algorithm	4.1.1.2	M		Options: 1.2.840.10045.4.3.2 (ECDSA-with SHA256) 1.2.840.10045.4.3.3 (ECDSA-with SHA384) 1.2.840.10045.4.3.4 (ECDSA with SHA512)
Signature value	4.1.1.3	M		Value according to the signature algorithm. By creating this signature, the CA certifies the binding between the public key material and the subject of the certificate, i.e. the IACA.

Key

Presence:

M mandatory

O optional

Criticality:

C critical

NC not critical

11.4 User administration (add/update/remove admins users)

The DTS system user administration user interface is only used by AAMVA staff. The DTS system user administration user interface allows AAMVA staff with Admin role to manage DTS system users.

The functions supported by the IACA certificate administration user interface are listed in Table 5.

Table 5: User administration requirements

#	Requirement	Description
19.	Roles	The DTS system supports at least the following roles: • Administrator. The administrator role allows the creation, updating, suspension and archiving of DTS system users. • Regular user. The regular user role allows access to all DTS system functionality except for the functions reserved for the administrator role.
20.	Authentication	The DTS system supports standard userid and password management. The following minimum authentication requirements apply. Password Requirements Complexity • 14 characters in length • 2 special characters • 1 uppercase character • 1 lowercase character • No dictionary word of more than 5 letters • Does not contain any part of the user's name or account Other • Valid for 90 days or less • Minimum age 1 day • Shall not match any of the 24 most recent prior passwords Multifactor Authentication • Required • Use of out-of-band authentication allowed only for cases where cryptographic tokens are not possible Session Management • Session lock out after 15 minutes • Concurrent sessions must be unallowed unless functionally required Authentication • Logon banner • Failed login attempts shall not indicate whether the issue is with the account or the password

11.5 DTS Data stores

The requirements supported by the DTS system trust stores are listed in Table 6.

Table 6: DTS Data store requirements

#	Requirement	Description
21.	Data store	The DTS system maintains a primary data store to record information on all aspects of the DTS system, including on certificates, IAs, users, VICALS, and all user and system activity.
22.	Relational DB	The DTS system preferably uses a relational database such as MySQL
23.	Redundancy	The DTS system maintains a replication of the primary DTS system data store such that no data is lost in case of a failure of the primary DTS system data store.
24.	Failover	The DTS system can fail over to the replicated DTS system data store if needed. Failover does not have to be in real time.
25.	Audit	The DTS system maintains audit records for all data actions, and does so at data store level. For example, in a relational database this can potentially be handled by a peer audit table, as shown in **Error! Reference source not found.**. In this example, the IA table has an IA-AUDIT t able that gets a new record every time anything in the IA table changes.
26.	Retention	The DTS system retains all information in the DTS system data stores for the entire length of the MVP.

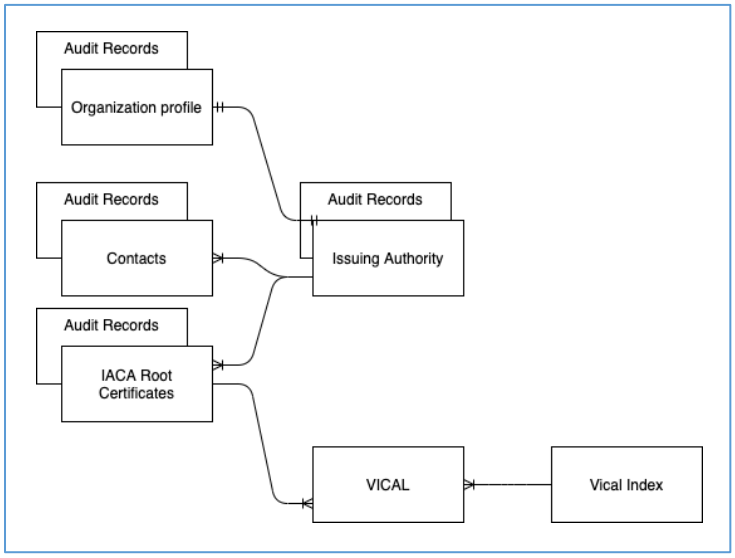

Figure 1: DTS Audit Records Relational Database Structure Example

11.6 REPORTING

The DTS system provides functionality to generate reports. At least the reports listed in Table 7 are supported.

Table 7: Reporting requirements

#	Requirement	Description
27.	IAs	A list of IAs.
28.	Certificates	A list of certificates associated with a particular IA, by certificate property (e.g., by certificate type).

#	Requirement	Description
29.	Activity	Activity reporting, including: a) Manual user activity, including log-on information. b) Automated system process execution. c) System health, errors, and warnings. d) VICAL downloads.

11.7 VICAL ADMINISTRATION

11.7.1 General

AAMVA's involvement in VICAL administration is limited to setting the policy for when a VICAL must be generated, and to initiate ad hoc VICAL generation. All other tasks related to VICAL administration are the responsibility of the Awardee.

The responsibilities of the Awardee in respect of general VICAL administration are reflected in Table 8.

Table 8: VICAL administration requirements

#	Requirement	Description
30.	Log	The generation of each VICAL is recorded.
31.	Retention	Each VICAL generated is retained.
32.	VICAL signing key	Full VICAL signing key lifecycle management is supported. This includes key generation, backup, storage, recovery, archival, and destruction and cryptographic devices for private key management.
33.	RP trust root	The trust root of a RP is either the DTS root public certificate or the VICAL signing public certificate[2].

11.7.2 VICAL generation

The responsibilities of the Awardee in respect of VICAL generation are reflected in Table 9.

Table 9: VICAL generation requirements

#	Requirement	Description
34.	Automatic generation	Automatic VICAL generation is a process that can be set up to occur automatically on a configurable frequency (e.g., once a day). When executed automatically, this process checks to see if there are any new IACA certificates or if the current VICAL is within a configurable period (e.g., 3 days) of expiring, and if either of these are true, a new VICAL is generated.
35.	Ad hoc generation	The DTS system supports the ad hoc generation of a VICAL by a DTS system user.
36.	Submission for publication	Upon generation, the VICAL is automatically passed on to the VICAL publication process.

[2] ISO/IEC 18013-5 Annex C allows either approach. Respondents must offer both, compare the options in the Respondent's proposal, price both (as noted in §8: Solution Pricing), and make a recommendation. AAMVA intends to select an option before Contract Award.

#	Requirement	Description
37.	Compliance with ISO/IEC 18013-5	The VICAL complies with the VICAL CDDL profile described in Annex C.1.7.1 of ISO/IEC 18013-5.

11.7.3 VICAL signing

The responsibilities of the Awardee in respect of VICAL signing are reflected in Table 10.

In addition to the guidance provided in section 7.4, the Respondent's response to this section must describe the manner in which VICAL generation, VICAL signing and VICAL signer key management will be implemented.

Table 10: VICAL signing requirements

#	Requirement	Description
38.	VICAL Signing	Sign the VICAL upon generation.
39.	Certificate Profile	Ensure that the keys used for signing the VICAL are in compliance with the VICAL Signer certificate profile defined in Annex C.1.7.2 of ISO/IEC 18013-5.
40.	Key management	Provide, implement and maintain a policy for managing the VICAL signer keys.

11.7.4 VICAL website

The responsibilities of the Awardee in respect of the VICAL website are reflected in **Error! Reference source not found.**.

In addition to the guidance provided in section 7.4, the Respondent's response to this section must describe the solution to establishing the VICAL website and detail how it will integrate with the rest of the DTS system.

Table 11: VICAL website requirements

#	Requirement	Description
41.	VICAL publication process	The VICAL publication process receives a VICAL from the VICAL generation process and automatically publishes it on the VICAL website.
42.	Public website	Maintain a public website, inclusive of all related administration (including hosting and monitoring), at a domain to be provided by AAMVA, with the following information: • The current VICAL • A list of all prior VICALs • The RP trust root (VICAL public signing key or DTS public root key)
43.	URL	The URL for the current VICAL remains fixed.
44.	Prior VICALs	The list of prior VICALS reflects the date and time each VICAL was generated.
45.	Prior VICAL download	Each prior VICAL can be downloaded via a unique and fixed URL.
46.	Download log	A log is maintained of all downloads. The log for each download includes the file downloaded, the timestamp of the download, and the IP address to which the file was downloaded.
47.	VICAL filenames	VICAL filenames must be human-readable and include the timestamp of VICAL generation.

11.8 DTS DECOMMISSIONING

The responsibilities of the Awardee in respect of the DTS decommissioning are reflected in Table 12.

Table 12: DTS decommissioning requirements

#	Title	Description
48.	Copy of information	Upon request from AAMVA the Awardee will provide AAMVA with a copy of information in the DTS data repository, in a non-proprietary and industry standard format, and in a manner that is commensurate with the security required for the information. This includes, and is not limited to, the following: • DTS VICAL root certificate (if applicable – see footnote 2) • DTS VICAL signing certificates • Active IA certificates • IA information
49.	Deletion of information	Upon instruction from AAMVA, the Awardee will permanently delete all the data in all the DTS data repositories, and terminate the website hosting the VICAL.
50.	Migration	If requested, Awardee will support AAMVA in the process of migrating to the successor system to the MVP.

11.9 SUPPLEMENTAL NON-FUNCTIONAL REQUIREMENTS

11.9.1 Hosting

The responsibilities of the Awardee in respect of hosting are reflected in Table 13.

Table 13: Hosting requirements

#	Title	Description
51.	Hosting	The Awardee is responsible for hosting the DTS System.
52.	Monitoring	Each system component is monitored.
53.	Restarting	Failed components are restarted either automatically or manually.
54.	Support	Contact information (email and phone) is available for AAMVA to obtain support.
55.	Hosting location	All services are hosted within the United Status or Canada.
56.	Testing	A test environment is provided for AAMVA acceptance testing.

11.9.2 System Availability

The responsibilities of the Awardee in respect of system availability are reflected in Table 14.

Table 14: System availability requirements

#	Requirement	Description
57.	Availability	The DTS system does not have to be a highly available system. Short periods of unavalibility are acceptable, so long as the DTS can be restored quickly when needed. A "hot standby" is not required.
58.	email	The DTS System does not include an email function. All email functionality are provided by AAMVA.
59.	VICAL website	The VICAL public website is available to the world and is always available. However, occasional and brief periods of unavailability is allowed.

11.9.3 Capacity

As noted elsewhere, the MVP will be limited to the minimum functions required to support the live ecosystem. The capacity expectations for the initial period of performance are as reflected in Table 15.

Table 15: Capacity expectations

#	Requirement	Description
60.	IAs	3-5 IAs are expected. The DTS system supports at least this level of participation.
61.	RPs	10-15 RPs are expected. The DTS system supports at least this level of participation.
62.	IACA Certs	It is expected that each IA will re-key their IACA certificte once. The DTS system supports at least this level of activity.

11.9.4 Documentation

The responsibilities of the Awardee in respect of documentation to be provided are reflected in Table 16.

Table 16: Documentation requirements

#	Requirement	Description
63	Custom system	If the proposed system is custom built for AAMVA then delivery includes well documented code and an architecture specification.
64	Instructions	Instructions for using the system are avialable in either online help or user manuals.
65	Policy of technical and procedural controls	A policy of technical and procedural controls, as contemplated in clause C.1.1.1 of ISO/IEC 18013-5, for areas addressed by the DTS system and for related responsibilities of the Awardee.
66	Security documentation	In addition to what is requested elsewhere, provide the following: • Awardee's company security policies • Awardee's company incident response plan

11.9.5 Security

The responsibilities of the Awardee in respect of security are reflected in Table 17. The requirements were primarily sourced from ISO/IEC 18013-5; "ISO" in the "Source column of Table 17 refers to "ISO/IEC 18013-5". Changes to ISO/IEC 1801305 are highlighted. References to "Annex C.n…" are to clauses in ISO/IEC 18013-5, as amended in Table 17.

AAMVA holds the right to conduct a security audit during the course of the engagement. AAMVA envisions to conduct this in line with ISO, SOC or other industry recognized standards.

Table 17: Security requirements

#	Security requirements	Source
67.	Data related to the DTS system must be segregated from any other customers of the vendor. It would be acceptable to share hardware.	AAMVA
68.	**Physical Controls:** ~~VICAL Provider's~~ Awardee's equipment shall be protected from unauthorized access while the cryptographic module (see Annex C.1.6.2) is installed and activated. The Awardee ~~VICAL Provider~~ shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. The DTS System ~~VICAL Provider~~ cryptographic tokens shall be protected against theft, loss, and unauthorized use. The following controls shall be fulfilled:	ISO C.1.5.1
69.	a) Physical access to components of the DTS ~~VICAL Provider's~~ system whose security is critical to the provision of its VICAL services shall be limited to authorized individuals.	ISO C.1.5.1
70.	b) Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.	ISO C.1.5.1
71.	c) Controls shall be implemented to avoid compromise or theft of information and information processing facilities.	ISO C.1.5.1
72.	d) Components that are critical for the secure operation of the VICAL service shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.	ISO C.1.5.1
73.	e) The facilities concerned with VICAL generation and management (i.e. CAs status lifecycle management) shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.	ISO C.1.5.1
74.	f) Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area.	ISO C.1.5.1
75.	g) Every entry and exit shall be logged and such access log shall be inspected periodically.	ISO C.1.5.1
76.	h) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the VICAL generation and management services.	ISO C.1.5.1
77.	i) Any parts of the premises shared with other organizations shall be outside the perimeter of the VICAL generation management services.	ISO C.1.5.1
78.	j) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.	ISO C.1.5.1
79.	k) The Awardee's ~~VICAL Provider's~~ physical and environmental security policy for systems concerned with VICAL generation and management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g., power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.	ISO C.1.5.1
80.	l) Controls shall be implemented to protect against equipment, information, media and software relating to the Awardee's ~~VICAL Provider's~~ services being taken off-site without authorization.	ISO C.1.5.1

#	Security requirements	Source
81.	m) Other functions relating to Awardee's ~~VICAL Provider's~~ operations may be supported within the same secured area provided that the access is limited to authorized personnel.	ISO C.1.5.1
82.	**Procedural Controls:** The Awardee ~~VICAL Providers~~ shall implement security measures in order to protect the authenticity, integrity and confidentiality of their data and the accurate functionality of their IT systems. The following controls shall be fulfilled:	ISO C.1.5.2
83.	a) The Awardee ~~VICAL Provider~~ shall provide AAMVA with the tools to administer user access of operators, administrators and system auditors.	ISO C.1.5.2
84.	b) ~~The administration shall include user account management and timely modification or removal of access.~~	ISO C.1.5.2
85.	c) Access to information and application system functions shall be restricted in accordance with the access control policy.	ISO C.1.5.2
86.	d) The DTS ~~VICAL Provider's~~ system shall provide sufficient computer security controls for the separation of trusted roles identified in Awardee's ~~VICAL Provider's~~ practices, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.	ISO C.1.5.2
87.	e) Awardee's ~~VICAL Provider's~~ personnel shall be identified and authenticated before accessing ~~using~~ critical applications related to the service.	ISO C.1.5.2
88.	f) Awardee's ~~VICAL Provider's~~ personnel shall be accountable for their activities.	ISO C.1.5.2
89.	g) Activation of the VICAL signing key shall be under at least dual control by authorized, trusted personnel such that one person alone cannot activate the VICAL creation system on his/her own.	ISO C.1.5.2
90.	**Personnel Controls:** The Awardee ~~VICAL Provider~~ shall ensure that employees and contractors support the trustworthiness of the DTS's ~~VICAL Provider's~~ operations. The following controls shall be fulfilled:	ISO C.1.5.3
91.	a) The Awardee ~~VICAL Provider~~ shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.	ISO C.1.5.3
92.	b) Awardee's ~~VICAL Provider's~~ personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.	ISO C.1.5.3
93.	c) This should include regular (at least every 12 months) updates on new threats and current security practices.	ISO C.1.5.3
94.	d) Appropriate disciplinary sanctions shall be applied to personnel of the Awardee violating ~~VICAL Provider's~~ policies or procedures of the Awardee or of the DTS.	ISO C.1.5.3
95.	e) Security roles and responsibilities, as specified in the DTS ~~VICAL Provider's~~ information security policy, shall be documented in job descriptions or in documents available to all concerned personnel.	ISO C.1.5.3
96.	f) Trusted roles, on which the security of the DTS ~~VICAL Provider's~~ operation is dependent and for which the Awardee is responsible, shall be clearly identified.	ISO C.1.5.3
97.	g) Trusted roles shall be named by the management.	ISO C.1.5.3

#	Security requirements	Source
98.	h) Trusted roles shall be accepted by the management and the person to fulfil the role.	ISO C.1.5.3
99.	i) Awardee's ~~VICAL Provider's~~ personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.	ISO C.1.5.3
100.	j) Where appropriate, job descriptions shall differentiate between general functions and Awardee's ~~VICAL Provider's~~ specific functions. These should include skills and experience requirements.	ISO C.1.5.3
101.	k) Personnel shall exercise administrative and management procedures and processes that are in line with the DTS ~~VICAL Provider's~~ information security management procedures.	ISO C.1.5.3
102.	l) Managerial personnel shall possess experience or training with respect to the DTS system ~~VICAL service~~ that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.	ISO C.1.5.3
103.	m) All Awardee's ~~VICAL Provider's~~ personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the DTS's ~~VICAL Provider's~~ operations.	ISO C.1.5.3
104.	n) Trusted roles shall include roles that involve the following responsibilities: 1. **Security Officers:** Overall responsibility for administering the implementation of the security practices. 2. **System Administrators:** Authorized to install, configure, maintain and recover the Awardee's ~~VICAL Provider's~~ trustworthy systems for service management. Authorized to perform system backup. 3. **System Operators:** Responsible for operating the DTS ~~VICAL Provider's trustworthy systems~~ on a day-to-day basis. ~~Authorized to perform system backup.~~ 4. **System Auditors:** Authorized to view archives and audit logs of the Awardee's ~~VICAL Provider's~~ trustworthy systems.	ISO C.1.5.3
105.	o) Awardee's ~~VICAL Provider's~~ personnel shall be formally appointed to trusted roles a, b and d by senior management responsible for security requiring the principle of "least privilege" when accessing or when configuring access privileges.	ISO C.1.5.3
106.	p) Personnel shall not have access to the trusted functions until the necessary checks are completed.	ISO C.1.5.3
107.	**Audit Logging Procedures:** The Awardee ~~VICAL Provider~~ shall record and keep accessible for an appropriate period of time, including after the activities of the Awardee ~~VICAL Provider~~ have ceased but subject to requirement #49, all relevant information concerning data issued and received by the DTS system ~~VICAL Provider~~, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. The following controls shall be fulfilled:	ISO C.1.5.4
108.	a) The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.	ISO C.1.5.4
109.	b) Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.	ISO C.1.5.4

#	Security requirements	Source
110.	c) Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.	ISO C.1.5.4
111.	d) The precise time of significant DTS system ~~VICAL Provider's~~ environmental, key management and clock synchronization events shall be recorded.	ISO C.1.5.4
112.	e) The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.	ISO C.1.5.4
113.	f) Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified by AAMVA ~~in the VICAL Provider's terms and conditions~~.	ISO C.1.5.4
114.	g) The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.	ISO C.1.5.4
115.	**Types of events recorded:** The DTS system ~~VICAL Provider~~ shall record details of the actions taken ~~to process a request and~~ to issue a VICAL, including all information generated ~~and documentation received in connection with the request~~; the time and date; and the personnel involved. The Awardee ~~VICAL Provider~~ shall make these records available to Auditors as proof of the Awardee's ~~VICAL Provider's~~ compliance with these requirements. The DTS ~~VICAL Provider~~ shall record at least the following events:	ISO C.1.5.4.1
116.	a) VICAL signing key lifecycle management events, including: 1. key generation, backup, storage, recovery, archival, and destruction; and 2. cryptographic device lifecycle management events;	ISO C.1.5.4.1
117.	b) VICAL ~~and IA~~ lifecycle management events, including: 1. CA application, re-key requests, and suspension; 2. all verification activities stipulated in these requirements; 3. date, time, phone number used, persons spoken to, and end results of verification telephone calls; 4. ~~acceptance and rejection of CA applications~~; and 5. issuance of VICALs.	ISO C.1.5.4.1
118.	c) security events, including: 1. successful and unsuccessful DTS ~~VICAL Provider's~~ system access attempts; 2. DTS ~~VICAL Provider's and~~ security system actions performed; 3. security profile changes; 4. system crashes, hardware failures, and other anomalies; 5. firewall and router activities; and 6. entries to and exits from the DTS ~~VICAL Provider~~ facility.	ISO C.1.5.4.1

#	Security requirements	Source
119.	Log entries shall include the following elements: d) date and time of entry; e) identity of the person making the journal entry; and f) description of the entry.	ISO C.1.5.4.1
120.	**Records Archival:** The Awardee ~~VICAL Provider~~ shall retain the following for at least seven years, but subject to requirement # 49, after any CA (accepted or not) based on these records ceases to be valid: a) log of all events relating to the lifecycle of keys managed by the DTS ~~VICAL Provider's~~ system; b) documentation and other evidence as referred in Annex C.1.4.2.	ISO C.1.5.5
121.	**VICAL Signing Key Changeover:** To minimize risk from compromise of the DTS ~~a VICAL Provider's~~ private signing key, that key may be changed often. From that time on, only the new key should be used to sign VICALs. If the old private key is necessary during a limited period of time to keep signing VICALs and allow the migration for Relying parties with legacy systems, the old key shall be retained and protected. Once the old private signing key is not needed anymore, it may be destroyed. The DTS ~~VICAL Provider's~~ signing key shall have a validity period as described in Annex C.1.7.2. ~~When a VICAL Provider updates its private signature key and thus generates a new public key, the VICAL Provider shall notify all subscribers that rely on its respective VICALs that it has been changed. The VICAL Provider shall provide the new public key through secure means (e.g., trusted communication channel established with subscribers/relying parties, provision of key rollover certificates – new public key is signed by the old private key, and vice versa).~~	ISO C.1.5.6
122.	**Incident and compromise handling procedures**: System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored. The following controls shall be fulfilled:	ISO C.1.5.7.1
123.	a) Monitoring activities should take account of the sensitivity of any information collected or analysed.	ISO C.1.5.7.1
124.	b) Abnormal system activities that indicate a potential security violation, including intrusion into the Awardee's ~~VICAL Provider's~~ network, shall be detected and reported as alarms.	ISO C.1.5.7.1
125.	c) The Awardee ~~VICAL Provider~~ shall monitor the following events: 1. start-up and shutdown of the logging functions; and 2. availability and utilization of needed services with the Awardee's ~~VICAL Provider's~~ network.	ISO C.1.5.7.1
126.	d) The Awardee ~~VICAL Provider~~ shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security.	ISO C.1.5.7.1
127.	e) The Awardee ~~VICAL Provider~~ shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the DTS ~~VICAL Provider's~~ procedures.	ISO C.1.5.7.1
128.	f) The Awardee ~~VICAL Provider~~ shall establish procedures to notify AAMVA ~~the appropriate parties~~ in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the VICAL service provided and on the personal data maintained therein within 24 hours of the breach being identified.	ISO C.1.5.7.1

#	Security requirements	Source
129.	g) Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the DTS has provided a service ~~VICAL service has been provided~~, the Awardee ~~VICAL Provider~~ shall ~~also~~ notify AAMVA ~~the natural or legal person of the breach of security or loss of integrity~~ without undue delay.	ISO C.1.5.7.1
130.	h) The Awardee's ~~VICAL Provider's~~ systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity. The Awardee shall implement ~~implementing~~ automatic mechanisms to process the audit logs and alert personnel of possible critical security events.	ISO C.1.5.7.1
131.	i) The Awardee ~~VICAL Provider~~ shall address any critical vulnerability not previously addressed by the Awardee ~~VICAL Provider~~, within a period of 48 hours after its discovery.	ISO C.1.5.7.1
132.	j) For any vulnerability, given the potential impact, the Awardee ~~VICAL Provider~~ may either choose to: 1. create and implement a plan to mitigate the vulnerability; or 2. document the factual basis for the Awardee's ~~VICAL Provider's~~ determination that the vulnerability does not require remediation.	ISO C.1.5.7.1
133.	k) Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.	ISO C.1.5.7.1
134.	**Computing resources, software, and/or data are corrupted:** The following controls shall be fulfilled:	ISO C.1.5.7.2
135.	a) Awardee's ~~VICAL Provider's~~ systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the Awardee ~~VICAL Provider~~ to timely go back to operations in case of incident/disasters.	ISO C.1.5.7.2
136.	b) Back-up copies of essential information and software should be taken regularly.	ISO C.1.5.7.2
137.	c) Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.	ISO C.1.5.7.2
138.	d) Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.	ISO C.1.5.7.2
139.	e) Backup and restore functions shall be performed by the relevant trusted roles specified in Annex C.1.5.3.	ISO C.1.5.7.2
140.	f) For information requiring dual control for management, for example keys, dual control shall be applied to recovery.	ISO C.1.5.7.2
141.	**~~VICAL Provider~~ DTS private key compromise procedures:** The following controls shall be fulfilled in case of a private key compromise:	ISO C.1.5.7.3
142.	a) The Awardee's ~~VICAL Provider's~~ business continuity plan (or disaster recovery plan) shall address the compromise, loss or suspected compromise of a DTS ~~VICAL Provider's~~ private key as a disaster.	ISO C.1.5.7.3
143.	b) The processes planned as per the previous requirement shall be in place.	ISO C.1.5.7.3
144.	c) Following a disaster, the Awardee ~~VICAL Provider~~ shall, where practical, take steps to avoid repetition of a disaster.	ISO C.1.5.7.3

#	Security requirements	Source
145.	d) In the case of compromise as a minimum: 1. the Awardee ~~VICAL Provider~~ shall inform AAMVA. ~~the following of the compromise: all issuing authorities point of contacts and subscribers and other entities with which the VICAL Provider has agreements or other form of direct established relations, among which relying parties and VICAL Providers; and~~ ~~2. the VICAL Provider shall indicate that VICALs issued using this private key may no longer be valid.~~ Furthermore, the following controls shall be fulfilled in case of an algorithm compromise: a) Should any of the algorithms, or associated parameters, used by the DTS ~~VICAL Provider or its issuing authorities point of contacts and/or subscribers~~ become insufficient for its remaining intended usage, then the Awardee ~~VICAL Provider~~ shall inform AAMVA ~~all of them with whom it has agreement or other form of established relations~~. b) Should any of the algorithms, or associated parameters, used by the Awardee ~~VICAL Provider~~ or its subscribers become insufficient for its remaining intended usage, then the Awardee ~~VICAL Provider~~ shall plan the transition to a new stronger algorithm and execute it the earliest possible time.	ISO C.1.5.7.3
146.	**Business continuity capabilities after a disaster**: The following controls shall be fulfilled:	ISO C.1.5.7.4
147.	a) The Awardee ~~VICAL Provider~~ shall define and maintain a continuity plan to enact in case of a disaster.	ISO C.1.5.7.4
148.	b) In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the DTS or the Awardee ~~VICAL Provider~~, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g., a security vulnerability) with appropriate remediation measures.	ISO C.1.5.7.4
149.	**VICAL Termination:** ~~Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the VICAL Provider's services and, in particular, continued maintenance of information required to verify the correctness of VICAL services shall be provided.~~ ~~Furthermore, the~~ The following controls shall be fulfilled:	ISO C.1.5.8
150.	a) ~~The VICAL Provider shall have an up-to-date termination plan.~~	ISO C.1.5.8

#	Security requirements	Source
151.	b) Before the Awardee ~~VICAL Provider~~ terminates its services, at least the following procedures apply: 1. ~~Before the VICAL Provider terminates its services, the VICAL Provider shall inform the following of the termination: all issuing authorities point of contacts and subscribers and other entities with which the VICAL Provider has agreements or other form of established relations, among which relying parties and VICAL Providers.~~ 2. Before the Awardee ~~VICAL Provider~~ terminates its services, the Awardee ~~VICAL Provider~~ shall terminate authorization of all subcontractors, if any, to act on behalf of the Awardee ~~VICAL Provider~~ in carrying out any functions relating to the processing and/or dissemination of the VICAL. 3. ~~Before the VICAL Provider terminates its services, the VICAL Provider shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the VICAL Provider for a reasonable period, unless it can be demonstrated that the VICAL Provider does not hold any such information. The minimum information set is composed of:~~ ~~i. registration information;~~ ~~ii. event log archives.~~ 4. ~~Before the VICAL Provider terminates its services, the VICAL Provider's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.~~ 5. ~~Before the VICAL Provider terminates its services, where possible VICAL Provider should make arrangements to transfer provision of VICAL services for its existing subscribers and Issuing Authorities point of contacts to another VICAL Provider.~~	ISO C.1.5.8
152.	c) The Awardee ~~VICAL Provider~~ shall have an arrangement to cover the costs to fulfil these minimum requirements in case the Awardee ~~VICAL Provider~~ becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.	ISO C.1.5.8
153.	d) The Awardee ~~VICAL Provider~~ shall state in its practices the provisions made for termination of service. This shall include: 1. notification of AAMVA ~~affected entities~~; and 2. where applicable, transferring the Awardee's ~~VICAL Provider's~~ obligations to other parties (subject to approval of AAMVA).	ISO C.1.5.8
154.	e) The Awardee ~~VICAL Provider~~ shall maintain or transfer to a reliable party approved by AAMVA its obligations to make available the DTS ~~its~~ public key or its history of VICALs to subscribers and relying parties for a reasonable period.	ISO C.1.5.8
155.	**Key pair generation and installation**: Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle. The following controls shall be fulfilled:	ISO C.1.6.1
156.	a) The VICAL signing key pair generation shall be undertaken in a physically secured environment (see Annex C.1.5.1) by the Awardee's personnel in trusted roles (see Annex C.1.5.3).	ISO C.1.6.1
157.	b) The DTS ~~VICAL Provider~~ key pair used for signing VICALs shall be created under, at least, dual control.	ISO C.1.6.1

#	Security requirements	Source
158.	c) The number of personnel authorized to carry out VICAL signing key pair generation shall be kept to a minimum and be consistent with the Awardee's ~~VICAL Provider's~~ practices.	ISO C.1.6.1
159.	d) VICAL Signing key pair generation shall be performed using an algorithm as specified in Annex C.1.7.2.	ISO C.1.6.1
160.	e) The selected key length and algorithm for VICAL signing key are specified in Annex C.1.7.2.	ISO C.1.6.1
161.	f) Before expiration of its VICAL signer certificate which is used for signing VICALs, in case of continuing with the service, the Awardee ~~VICAL Provider~~ shall generate a new key pair and obtain a corresponding VICAL signer certificate~~, and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the VICAL signer certificate~~.	ISO C.1.6.1
162.	g) Before expiration of its VICAL signer certificate, in case of continuing with the service, the new VICAL signer certificate shall also be issued and distributed in accordance with this document.	ISO C.1.6.1
163.	h) The operations described in f) and g) above should be performed with a suitable interval between certificate expiry date and the last VICAL signed to allow all parties that have relationships with the DTS ~~VICAL Provider~~ (subscribers, relying parties, Issuing Authorities, etc.) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. ~~This does not apply to a VICAL Provider which will cease its operations before its own VICAL signer certificate expiration date.~~	ISO C.1.6.1
164.	i) The Awardee ~~VICAL Provider~~ shall have a documented procedure for conducting generation of VICAL signing key pairs. Such procedure shall indicate, at least, the following: 1. roles participating in the ceremony (internal and external from the organization); 2. functions to be performed by every role and in which phases; 3. responsibilities during and after the ceremony; and 4. requirements of evidence to be collected of the ceremony.	ISO C.1.6.1
165.	j) The Awardee ~~VICAL Provider~~ shall produce a report proving that the ceremony, as in i) above, was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured.	ISO C.1.6.1
166.	k) CA signature verification (public) keys of the VICAL signing certificate shall be available to subscribers and relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.	ISO C.1.6.1
167.	**Private key protection and cryptographic module engineering controls:** The following controls shall be fulfilled:	ISO C.1.6.2
168.	a) Awardee's ~~VICAL Provider's~~ signing key pair generation shall be carried out within a secure cryptographic device which is a trustworthy system which: 1. is assured to EAL 4 or higher in accordance with [3], or equivalent national or internationally recognized evaluation criteria for IT security provided this is a security target or protection profile which meets the requirements of this document, based on a risk analysis and taking into account physical and other non-technical security measures; or 2. meets the requirements identified in [4]or FIPS PUB 140-2 level 3.	ISO C.1.6.2
169.	b) The secure cryptographic device shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.	ISO C.1.6.2

#	Security requirements	Source
170.	c) The VICAL private signing key shall be held and used within a secure cryptographic device meeting the requirements item a) and b) above.	ISO C.1.6.2
171.	d) If and when outside the secure cryptographic device, the VICAL signing private key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.	ISO C.1.6.2
172.	e) The VICAL signing private key may be backed up, stored and recovered only by personnel in trusted roles (see Annex C.1.5.3) using, at least, dual control in a physically secured environment (see Annex C.1.5.1)	ISO C.1.6.2
173.	f) The number of personnel authorized to carry out the VICAL signing private key back up, storage and recovery shall be kept to a minimum and be consistent with the Awardee's ~~VICAL Provider's~~ practices.	ISO C.1.6.2
174.	g) Copies of the VICAL private signing keys shall be subject to the same or greater level of security controls as keys currently in use.	ISO C.1.6.2
175.	h) Where the VICAL signing private keys and any copies are stored in a dedicated secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside this device.	ISO C.1.6.2
176.	i) The secure cryptographic device shall not be tampered with during shipment.	ISO C.1.6.2
177.	j) The secure cryptographic device shall not be tampered with while stored.	ISO C.1.6.2
178.	k) The secure cryptographic device shall be functioning correctly.	ISO C.1.6.2
179.	l) The CA private signing keys stored on the CA's secure cryptographic device shall be destroyed upon device retirement.	ISO C.1.6.2
180.	**Other aspects of key pair management:** The Awardee ~~VICAL Provider~~ shall use appropriately the VICAL private signing keys. The following controls shall be fulfilled:	ISO C.1.6.3
181.	a) The Awardee ~~VICAL Provider~~ shall not use the VICAL signing private keys beyond the end of their lifecycle.	ISO C.1.6.3
182.	b) VICAL signing key(s) used for generating VICALs as defined in Annex C.1.7.1 shall not be used for any other purpose.	ISO C.1.6.3
183.	c) The VICAL signing keys shall only be used within physically secure premises.	ISO C.1.6.3
184.	d) The use of the VICAL's private key shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating VICALs (defined in Annex C.1.7.2).	ISO C.1.6.3
185.	e) All copies, if any, of the VICAL signing private keys shall be destroyed at the end of their lifecycle.	ISO C.1.6.3

#	Security requirements	Source
186.	Activation data: The installation, activation and recovery of the VICAL signing key pairs in a secure cryptographic device shall require simultaneous control of at least two trusted employees, for example, using m-of-n authentication mechanisms. Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be either: — memorized; or — biometric in nature; or — recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.	ISO C.1.6.4
187.	**Computer Security Controls:** Access to the DTS system ~~The VICAL Provider's system access~~ shall be limited to authorized individuals. The following controls shall be fulfilled:	ISO C.1.6.5
188.	a) Controls (e.g., firewalls) shall protect the Awardee's ~~VICAL Provider's~~ internal network domains from unauthorized access including access by subscribers and third parties.	ISO C.1.6.5
189.	b) Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the DTS system ~~VICAL Provider~~.	ISO C.1.6.5
190.	c) Sensitive data shall be protected against being revealed through re-used storage objects (e.g., deleted files) being accessible to unauthorized users.	ISO C.1.6.5
191.	d) Local network components (e.g., routers) shall be kept in a physically and logically secure environment.	ISO C.1.6.5
192.	e) Local network components (e.g., routers) configurations shall be periodically checked for compliance with the requirements specified by the Awardee ~~VICAL Provider~~.	ISO C.1.6.5
193.	e) Local network components (e.g., routers) configurations shall be periodically checked for compliance with the requirements specified by the Awardee ~~VICAL Provider~~.	ISO C.1.6.5
194.	g) Dissemination application shall enforce access control on attempts to add or delete VICALs and modify other associated information.	ISO C.1.6.5
195.	h) Continuous monitoring and alarm facilities shall be provided to enable the Awardee ~~VICAL Provider~~ to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.	ISO C.1.6.5
196.	**Life cycle security controls:** The Awardee ~~VICAL Provider~~ shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them. The following controls shall be fulfilled:	ISO C.1.6.6
197.	a) An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the Awardee ~~VICAL Provider~~ or on behalf of the Awardee ~~VICAL Provider~~ to ensure that security is built into IT systems.	ISO C.1.6.6
198.	b) Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the Awardee's ~~VICAL Provider's~~ security policy.	ISO C.1.6.6

#	Security requirements	Source
199.	c) The procedures shall include documentation of the changes.	ISO C.1.6.6
200.	d) The integrity of Awardee's ~~VICAL Provider's~~ systems and information shall be protected against viruses, malicious and unauthorized software.	ISO C.1.6.6
201.	e) Media used within the Awardee's ~~VICAL Provider's~~ systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.	ISO C.1.6.6
202.	f) Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.	ISO C.1.6.6
203.	g) Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.	ISO C.1.6.6
204.	h) The Awardee ~~VICAL Provider~~ shall specify and apply procedures for ensuring that: 1. security patches are applied within a reasonable time after they come available; 2. security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and 3. the reasons for not applying any security patches are documented.	ISO C.1.6.6
205.	i) Capacity demands shall be monitored and projections of future capacity requirements shall be made to ensure that adequate processing power and storage are available.	ISO C.1.6.6
206.	**Network Security Controls:** The Awardee ~~VICAL Provider~~ shall protect its network and systems from attack. The following controls shall be fulfilled:	ISO C.1.6.7
207.	a) The Awardee ~~VICAL Provider~~ shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.	ISO C.1.6.7
208.	b) The Awardee ~~VICAL Provider~~ shall apply the same security controls to all systems co-located in the same zone.	ISO C.1.6.7
209.	c) The Awardee ~~VICAL Provider~~ shall restrict access and communications between zones to those necessary for the operation of the DTS system ~~VICAL Provider~~.	ISO C.1.6.7
210.	d) The Awardee ~~VICAL Provider~~ shall explicitly forbid or deactivate not needed connections and services.	ISO C.1.6.7
211.	e) The Awardee ~~VICAL Provider~~ shall review the established rule set on a regular basis.	ISO C.1.6.7
212.	f) The Awardee ~~VICAL Provider~~ shall keep all systems that are critical to the DTS system's ~~VICAL Provider's~~ operation in one or more secured zone(s).	ISO C.1.6.7
213.	g) The Awardee ~~VICAL Provider~~ shall separate dedicated network for administration of IT systems and Awardee's ~~VICAL Provider 's~~ operational network.	ISO C.1.6.7
214.	h) The Awardee ~~VICAL Provider~~ shall not use systems used for administration of the security policy implementation for other purposes.	ISO C.1.6.7
215.	i) The Awardee ~~VICAL Provider~~ shall separate the production version of the DTS system ~~systems for the VICAL Provider's services~~ from systems used in development and testing (e.g., development, test and staging systems).	ISO C.1.6.7

#	Security requirements	Source
216.	j) The Awardee ~~VICAL Provider~~ shall establish communication between distinct trustworthy systems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.	ISO C.1.6.7
217.	k) If a high level of availability of external access to the VICAL service is required, the external network connection should be redundant to ensure availability of the services in case of a single failure.	ISO C.1.6.7
218.	l) The Awardee ~~VICAL Provider~~ shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the Awardee ~~VICAL Provider~~ and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.	ISO C.1.6.7
219.	m) The Awardee ~~VICAL Provider~~ shall undergo a penetration test on the Awardee's ~~VICAL Provider's~~ systems at set up and after infrastructure or application upgrades or modifications that the Awardee ~~VICAL Provider~~ determines are significant.	ISO C.1.6.7
220.	n) The Awardee ~~VICAL Provider~~ shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.	ISO C.1.6.7
221.	o) The Awardee ~~VICAL Provider~~ shall maintain and protect all DTS system components ~~VICAL systems~~ in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones.	ISO C.1.6.7
222.	p) The Awardee ~~VICAL Provider~~ shall configure all DTS system components ~~VICAL systems~~ by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the DTS's ~~VICAL's~~ operations.	ISO C.1.6.7
223.	q) The Awardee ~~VICAL Provider~~ shall grant access to secure zones and high security zones to only trusted roles.	ISO C.1.6.7
224.	r) The VICAL issuing system shall be in a high security zone.	ISO C.1.6.7
225.	**Timestamping**: The following controls shall be fulfilled:	ISO C.1.6.8
226.	a) Asserted times shall be accurate to within three minutes.	ISO C.1.6.8
227.	b) Electronic or manual procedures may be used to maintain system time.	ISO C.1.6.8
228.	c) Clock adjustments are auditable events.	ISO C.1.6.8

#	Security requirements	Source
229.	**Compliance audit and other assessment:** The Awardee shall be able to demonstrate compliance with the security requirements in this document. ~~It is beyond the scope of this Policy to establish an auditing scheme for VICAL Providers. Nevertheless, it is understood that VICAL Providers should be able to publicly demonstrate compliance to this Policy and the security requirements.~~ ~~As a minimum, VICAL Providers shall conduct self-audits on a periodic basis (at least yearly) to assess compliance to this Policy.~~ ~~An independent third-party assessment can be achieved by an VICAL Provider based on the following principles.~~ The Awardee shall ensure that an independent third-party assessment is in place starting no later than 90 days after go-live, and shall take steps as necessary to keep it in good standing for the remainder of the contract. The Awardee shall furnish AAMVA with the results of the initial and any additional independent third-party assessments. The independent third-party assessment shall comply with the following principles: — Auditor qualification: The awardee shall select ~~VICAL Provider selects~~ an independently acting and accredited company/organisation ("Auditing Body") or certified auditors to audit the DTS system ~~VICAL Service~~ according to this Policy. The Auditing Body shall either be accredited for this purpose by its national accreditation body or authorized by a responsible government office. — Audit basis: The Audit is based on ISO/IEC 27001 and ISO/IEC 27002 (or equivalent). — Checking requirement realisation: The audit and control does not only check that procedural security controls are specified but also that they are adhered to in practice. This also includes the initial identity validation, the receipt of IACA applications and the suspension/removal procedure for IACAs. — ~~Iteration of audits and controls: Audits and controls is performed at least every three years. The Auditing Body and the VICAL Provider carry out a review at least once a year by a team of one or more auditors to ensure on going compliance with this Policy.~~ — Being not conformant: In the event that an audit indicates that the Awardee ~~VICAL Provider~~ is not conformant to the requirements in this document ~~this Policy~~, or its certification becomes invalid or expires, the Awardee notifies AAMVA immediately ~~VICAL Provider notifies its point of contacts of Issuing Authorities and subscribers~~. — ~~Availability of audit results: The certificate of conformity is made available to AAMVA can be made available to Issuing Authorities, subscribers, relying parties and other possible stakeholders.~~ Absent a completed independent third-party assessment at the time the MVP Operation phase starts, the Awardee shall present to AAMVA the results of a self-audit to assess compliance to the requirements in this document before commensing with the MVP Operation phase.	ISO C.1.8

#	Security requirements	Source
230.	The Awardee ~~A VICAL Provider~~ should implement an Information Security Management System (ISMS) for the DTS ~~its VICAL Service~~ in accordance to ISO/IEC 27001. ~~The ISMS is based on an ISMS policy of which its scope is defined by this Policy and, if applicable, the associated Practice Statement.~~ In addition, the awardee shall have the following conducted by an independent third party and share with AAMVA before commencing with the MVP Operation phase: a) Network and application penetration testing; b) Architecture security review; and c) Application source code security review. The awardee shall address any findings as follow: d) "Critical" and "high" findings/risks shall be remediated before commencing with the MVP Operation phase; e) "Medium" findings/risks shall be remediated within 60 days.	ISO C.1.8
231.	The Awardee shall conduct monthly authenticated vulnerability scans against the DTS. Results shall be shared with AAMVA on a quarterly basis. Remediation of any vulnerabilities shall be addressed as follow: a) "Critical" findings/risks shall be remediated within 2 weeks of discovery; b) "High" findings/risks shall be remediated within 30 days of discovery; and c) "Medium" findings/risks shall be remediated within 60 days of discovery.	AAMVA

11.9.6 Privacy

During the establishment and hosting of the DTS infrastructure (including all hardware, software, websites and services) and hosting the service, the Awardee shall comply with the requirements in Table 18.

Table 18: Privacy requirements

#	Requirement	Description
232.	Competence	Conduct a self-assessment of the DTS against ISO/IEC 27701 or similar and provide evidence to AAMVA of competence of the awardee's organization related to privacy at least once a year. Develop a DTS privacy policy (jointly with AAMVA).
233.	Vulnerabilities and testing	Provide details of the following from the self-assessment: (a) Privacy vulnerabilities that were identified, and remedial actions taken or reasons why action was not taken; (b) Results of the OWASP Top 10 Privacy Risks review for the website used to support the DTS.
234.	Privacy Policy	Ensure availability of the DTS privacy policy on the DTS website.
235.	PII Attestation	Attest that no PII is or will be gathered, generated, processed and disposed by the DTS System.

#	Requirement	Description
236.	Audit Authority	AAMVA shall have the authority to audit the awardee's systems related to the DTS and to the privacy requirements. AAMVA has the right to request privacy related independent third-party opinions and analysis of the DTS based on its own due-diligence and requirements.

Appendix A: SUMMARY OF TERMS AND CONDITIONS

The Notice of Intent to Award will be conditioned on the successful negotiation of a definitive agreement between AAMVA and that Respondent. As soon as possible following its issuance of a Notice of Intent to Award to a vendor AAMVA will provide that vendor with a proposed form of agreement with AAMVA. A summary description of some of the important provisions that AAMVA anticipates including in the proposed agreement appears below.

Respondents may include statements of exception to the contractual terms described below. Bidders that have not included such statements of exception will be deemed to have agreed in principle to the contractual terms as described.

The summary of contractual provisions below does not include all significant terms that may be contained in the proposed form of agreement concerning the RFP. The text that follows does not exhaustively describe anticipated contractual provisions and is subject to change as AAMVA develops the final form of proposed agreement.

In the following summary, the agreement resulting from this RFP is referred to as the "Agreement;" AAMVA is referred to as the "AAMVA;" the successful vendor is referred to as the "Awardee;" and the collective work to be carried out pursuant to the Award is referred to as the "Services."

1. **Confidentiality**. The Agreement will contain provisions to protect information treated by AAMVA as confidential (Confidential Information) including but not limited to provisions under which Awardee will agree: (i) to maintain Confidential Information in strict confidence, (ii) not use Confidential Information without the prior written consent of AAMVA, and (iii) to disclose Confidential Information only to those Awardee Personnel (defined below) who have a "need to know" for purposes of providing the Services and who are themselves bound by written agreements at least as protective as the restrictions on use and disclosure set forth in the Agreement.
2. **Most Favored Pricing**. The Agreement will require that all pricing for Services provided by Awardee is at the time of executing the Agreement and during the term of the Agreement will provide that AAMVA be charged the lowest fees, prices, and rates charged by Awardee to any of its customers for similar services. If at any time Awardee charges any fee, rate, or price for services comparable to the Services included in the Agreement that is lower than the pricing in the Agreement, Awardee shall immediately apply such lower pricing, as applicable, to the Services provided to AAMVA. Such lower pricing will apply retroactively to the date on which Awardee began charging it to the comparable customer.
3. **Performance of Services**. The Agreement will provide that Awardee will provide all Services in a timely, professional, and workmanlike manner and in accordance with the terms, conditions and specifications set forth in the Agreement. The following additional provisions are anticipated:
    a. No Subcontractors. Awardee shall not, without the prior written approval of AAMVA, engage any third party (i.e., any individual who is not an employee of Awardee, or any corporation, partnership, limited liability company or other business organization other than the Awardee) to perform any Services to be provided pursuant to the Agreement. Third parties who have been approved by AAMVA to provide Services will constitute "Permitted Subcontractors".
    b. Awardee Personnel. The Agreement will provide that Awardee's Personnel includes Awardee's employees and Permitted Subcontractors. All Services to be provided by the Awardee under the Agreement shall be provided by Awardee's Personnel in collaboration with AAMVA's Project Team. AAMVA's Project Team shall include members of AAMVA's staff and outside advisors/consultants.
    c. Awardee Personnel Matters. Prior to any Awardee Personnel performing any Services under the Agreement, Awardee must: (i) ensure that such Awardee Personnel have the legal right to work in the United States; (ii) require such Awardee Personnel to execute written agreements, in form and substance reasonably acceptable to AAMVA, that bind such Awardee Personnel to confidentiality provisions that are at least as protective of AAMVA's Confidential Information (as defined in the Agreement) as those contained in the Agreement and, upon AAMVA's request, provide AAMVA with a copy of each such executed agreement; and (iii) at its sole cost

and expense, conduct background checks on such Awardee Personnel, including, at a minimum, a review of credit history, references, and criminal record, in accordance with applicable laws.

d. Location of Performance of Services. All Services shall be provided from locations physically located within the District of Columbia or states/provinces of the United States of America and/or Canada.

e. Awardee Project Managers. For each distinct project undertaken by Awardee under the Agreement, Awardee must appoint, and thereafter maintain, an Awardee employee acceptable to AAMVA to serve as Awardee's project manager and AAMVA's primary contact (each, "Awardee Project Manager"). The Awardee shall maintain the same Awardee Project Manager throughout the work within each Awardee Project Manager's scope of responsibility unless: (i) AAMVA requests in writing the removal of the Awardee Project Manager; (ii) AAMVA consents in writing to any removal requested by Awardee in writing; or (iii) the Awardee Project Manager ceases to be employed by Awardee. Awardee shall promptly replace the affected Awardee Project Manager. Such replacement shall be subject to AAMVA's reasonable prior written approval.

4. **Intellectual Property**.

a. Rights to Work Product. Under the Agreement AAMVA will be the sole and exclusive owner of all right, title, and interest in and to all software, data, know-how, ideas, methodologies, specifications, and other technology that Awardee develops pursuant to the Agreement and that is embodied in the Mobile Driver License Digital Trust Service (Work Product).

b. Rights to Background Technology. Awardee is and will remain the sole and exclusive owner of all right, title, and interest in and to all software, data, know-how, ideas, methodologies, specifications, and other technology that were developed or otherwise acquired by Awardee prior to the effective date of the Agreement and that are embodied in the Mobile Driver License Digital Trust Service (Background Technology).

c. No Infringement. As delivered, installed, specified, or approved by Awardee and used by or on behalf of AAMVA, the mDL Digital Trust Service developed, delivered and operated by the Awardee will not infringe, misappropriate, or otherwise violate any intellectual property right or other right of any third party and will comply with all applicable laws.

5. **Termination**.

a. Termination for Cause. The Agreement will provide that either party may terminate the Agreement upon written notice to the other party if the other party materially breaches the Agreement and such breach remains uncured 30 days after the breaching party receives written notice of the material breach.

b. Termination without Cause. The Agreement will provide that AAMVA will have the right to terminate the Agreement at any time without cause and without incurring any additional obligation, liability, or penalty; provided that, as set forth in the Agreement, AAMVA will be obligated to pay required compensation for all Services and Work Product received/accepted before the effective date of the termination.

6. **Data Privacy and Security**.

a. Use and Return of Protected Data. The Agreement will include provisions concerning the use, storage, disclosure and return of information that identifies or can be used, together with other information, to identify an individual or that can be used to authenticate an individual, including, without limitation, all information included in an individual's driver's license card or government-issued identification card (collectively, "Protected Data").

b. Safeguarding Data Privacy and Security. The Agreement will include a requirement that the Awardee have and enforce written information security policies and procedures that include appropriate administrative, technical, and operational safeguards and other security measures designed to ensure the security and confidentiality of Protected Data and that protect against threats or hazards to the security and integrity of such data.

c. Security Incidents. The Agreement will include provisions concerning the prompt reporting of acts or omissions that compromise the security, confidentiality, or integrity of Protected Data or of the safeguards

established to protect such data (Security Incidents). The Agreement will include provisions concerning remediation of Security Incidents and compliance with applicable statutory notification requirements.

d. Verification of Information Security Safeguards. The Agreement will contain provisions requiring that the Awardee cooperate with periodic security questionnaires or on-site security audits to verify compliance with required security safeguards for Protected Data.

7. **Representations and Warranties of the Awardee**. Under the Agreement, the Awardee will represent and warrant to AAMVA that:

   a. Compliance with RFP Qualifications. The Agreement will a include a representation and warranty of the Awardee that as of the effective date of the Agreement and at all times during the term of the Agreement and any possible extension or renewal thereof, the Awardee will be in compliance with all qualification requirements for Respondents, including but not limited to the requirement of neutrality, described in Section 5 of the RFP. In the Agreement, the Awardee will agree to advise AAMVA in writing within seven days of the occurrence of any action or condition that would cause the Awardee to fail to be in compliance of required neutrality or any other qualification requirement.

   b. No Debarment. It is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal Government department or agency. It has not within a three-year period preceding the effective date of the Agreement been convicted of or had a civil judgment rendered against it for commission of fraud or criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes, or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property.

   c. No Contingent Fees. It has not paid or agreed to pay any company or person (other than its bona fide employees) any commission, brokerage fee, or other consideration that is contingent upon the receipt of an award for all or a portion of the project described in this RFP.

   d. No Conflict of Interest. It does not have any financial interests or business relationships or other circumstances that (i) create an actual or the appearance of a conflict of interest or (ii) would impair, or give the appearance of impairing, impartial judgment in carrying out its obligations under the Agreement in the best interests of AAMVA and of its Member Jurisdictions.

   e. Compliance with Laws. It is in compliance with and will perform all Services under the Agreement in compliance with, all applicable state or provincial, federal, and local laws of the United States and Canada.

   f. Good Title. At the conclusion of the performance of the Awardee's Services, AAMVA will receive good and valid title to all Work Product, free and clear of all encumbrances and liens of any kind.

8. **Performance Warranty**. The Agreement will include warranty provisions that all Services will be provided and that the mDL Digital Trust Service will function in conformity with the the Agreement and all applicable specifications and documentation.

9. **Service Level Agreement**. The Agreement may include service-level agreements (SLA) defining the level of service for hosting and other Services to be provided by Awardee under the Agreement. SLAs included in the Agreement will specify applicable metrics by which covered Services are measured and any applicable remedies or penalties if service levels are not achieved.

10. **Insurance**.

    a. Required Coverage. Awardee will be required to maintain insurance coverage including General Liability, Cyber Liability, and Workers' Compensation, with the following minimum limits of coverage:

       i. General Liability: minimum $1,000,000 per occurrence, and $2,000,000 in the aggregate;

       ii. Cyber Liability: $5,000,000 limit (with coverage for third party crime, including funds transfer fraud, social engineering fraud and invoice manipulation); and

       iii. Workers' Compensation: Statutory benefits of the state in which the work is going to be performed.

b. Additional Insured. Awardee will name AAMVA as an additional insured. Upon request, Awardee will provide AAMVA with a satisfactory Certificate of Insurance.

11. **Indemnification**.

a. General Indemnification. Awardee will agree to defend, indemnify and hold harmless AAMVA and AAMVA's officers, directors, employees, agents, successors and assigns (each, an "AAMVA Indemnitee") from and against all any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, fees and the cost of enforcing any right to indemnification under the Agreement and the cost of pursuing any insurance providers that are incurred by an AAMVA Indemnitee ("Losses") arising out of or resulting from any third party claim, suit, action or proceeding (each, an "Action") that arises out of or results from:

i. Awardee's breach of any representation, warranty, covenant, or obligation of Awardee under the Agreement; or

ii. Any negligence, gross negligence, or more culpable act or omission (including recklessness or willful misconduct) in connection with the performance or activity required by or conducted in connection with the Agreement by Awardee or any Permitted Subcontractor in connection with performing Services under the Agreement.

b. Intellectual Property Infringement. If any software or any component of the mDL Digital Trust Service, is found to be infringing or if any use of any software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, the Agreement will provide that Awardee shall, at its sole cost and expense:

i. Procure for AAMVA the right to continue to use such software or component thereof to the full extent contemplated by the Agreement; or

ii. Modify or replace the materials that infringe or are alleged to infringe ("Allegedly Infringing Materials") to make the software and all of its components non-infringing while providing fully equivalent features and functionality.

If neither of the foregoing is possible notwithstanding Awardee's efforts then the Agreement will provide that Awardee may direct AAMVA to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Awardee shall: (i) refund to AAMVA all amounts paid by AAMVA in respect of such Allegedly Infringing Materials; and (ii) in any case, at its sole cost and expense, secure the right for AAMVA to continue using the Allegedly Infringing Materials for a reasonable transition period to allow AAMVA to replace the affected features of the software without disruption.

12. **Miscellaneous**.

a. Time of the Essence. Awardee will acknowledge that time is of the essence with respect to Awardee's obligations under the Agreement and will agree that prompt and timely performance of all such obligations in accordance with the Agreement (including any implementation plan and all milestone dates) will be strictly required.

b. Auditing Rights and Required Records. During the term of the Agreement and for one year following its expiration, Awardee shall maintain complete and accurate books and records regarding its business operations relevant to the calculation of fees, reimbursable expenses, and any other information relevant to Awardee's representations, warranties, and covenants under this Agreement.

c. Incorporation of RFP; Entire Agreement. AAMVA may elect to incorporate the RFP or portions thereof into the Agreement. The Agreement (including the RFP, if incorporated) and those portions of the Awardee's Response that have been accepted by AAMVA shall constitute the entire agreement between the parties.

d. Governing Law; Forum. The Agreement will provide that for it to be construed under the laws of the Commonwealth of Virginia. The Agreement will provide for the consent of the parties to personal jurisdiction and venue in the federal and state courts of the Commonwealth of Virginia.