AAMVA

American Association of
Motor Vehicle Administrators

E-Odometer
Truth in Mileage Act
E-SIGNATURE
DISCLOSURE
Accuracy
Risk Management
AUTHENTICATION

E-Odometer Task Force Report

December 2014

ELECTRONIC ODOMETER TASK FORCE

Cover photo credits: © Zenstock/thinkstockphotos.com

Contents

Executive Summary 2

Section One Definitions and Acronyms 3

Section Two Background 4

Section Three Truth in Mileage Act (TIMA)Today 6

Section Four General Concepts 7

Section Five Considerations for E-Odometer Disclosures 9

Section Six Roadmap: Future Actions That Will Inhibit Odometer Fraud 14

Appendix A E-Identity Background 17

Appendix B Making the Paper Process Electronic 21

Appendix C Task Force List 22

Executive Summary

There is great interest from states to modernize the motor vehicle titling processes and implement an electronic titling (e-titling) system, which will facilitate the transfer of ownership electronically. The implementation of this process provides an opportunity for many efficiency improvements as well as inhibiting fraud, including odometer fraud. At the same time, the National Highway Traffic Safety Administration (NHTSA) will be prescribing regulations to be in compliance with the Moving Ahead for Progress in the 21st Century Act (MAP-21) and permit electronic odometer (e-odometer) disclosures.

The American Association of Motor Vehicle Administrators (AAMVA) chartered the E-Titling Working Group to develop a proof of concept for states to implement an e-titling process, but ultimately found that it would be difficult for states to implement without an e-odometer disclosure process that complied with federal regulations. In response to the outcome of the E-Title Proof of Concept and Roadmap, AAMVA approved the E-Odometer Disclosure Task Force to work toward a solution for e-odometer disclosure processes that would protect the consumers and allow enough flexibility for states to evolve from a time consuming paper process to an electronic process.

The Task Force developed multiple considerations concerning e-odometer disclosure processes that should be taken into account for all stakeholders. Flexibility was a key factor in developing the report in order to allow states an option to implement within budgetary constraints. The report also considers the specific actions within the process and the importance of authenticating the disclosure. Additionally, each state should be allowed to implement specific processes, but should not be required to do each process exactly the same. Overall, the Task Force has developed a report identifying the key components for an e-odometer disclosure program while remaining high-level as the Task Force anticipates the federal regulations.

Section One Definitions and Acronyms

For purposes of this report, the following definitions and acronyms shall be used:

AAMVA	American Association of Motor Vehicle Administrators
C.F.R.	Code of Federal Regulations
DLDV	Driver License Data Verification System
E-Odometer	Refers to the electronic processing of odometer disclosure statements
E-Title	Refers to an electronic file maintained in the state's system that replaces the traditional paper certificate of title
MCO	Manufacturer's Certificate of Origin
New vehicle	A vehicle that has not been previously titled
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NMVTIS	National Motor Vehicle Title Information System
OMB	Office of Management and Budget
POA	Power of Attorney
PKI	Public Key Infrastructure
State	The jurisdictional agency responsible for the oversight of motor vehicle titling and odometer disclosure requirements required by the Truth in Mileage Act of 1986 (49 U.S.C. § 32701)
The Rule	49 C.F.R. § 580 (2012) - Odometer Disclosure Requirements
TIMA	Truth in Mileage Act of 1986 (49 U.S.C. § 32701) is sometimes used as a shorthand reference for the statutes requiring odometer disclosure.
Certificate of Title	A document (currently secure paper) that provides proof of ownership outside of possession of a vehicle. The Rule provides guidance on the information that must appear on the certificate of title.
U.S.C.	Code of Federal Regulations
Used vehicle	A vehicle that has been previously titled
VIN	Vehicle Identification Number

Section Two Background

In 1972, Congress passed the Motor Vehicle and Cost Savings Act, frequently referred to as the Cost Savings Act. In § 408 of this Act (since recodified as 49 U.S.C. § 32705), a requirement was created for the transferor of a motor vehicle to provide a written statement of the mileage on the vehicle's odometer at the time of the transfer. In 1986, Congress passed the Truth in Mileage Act (TIMA), intending to improve the effectiveness of this requirement for odometer disclosures. Through the years, Congress has amended, repealed, and re-enacted the requirements for odometer disclosures; this report does not attempt to recount all of the details of this legislative history.

Based on this legislation, NHTSA provides guidance for odometer disclosures in 49 C.F.R. § 580 (2012) - Odometer Disclosure Requirements, referred herein as The Rule.

In 2012, Congress passed MAP-21 which contained the following provision:

> *49 U.S.C. § 32705 (g) ELECTRONIC DISCLOSURES.—Not later than 18 months after the date of enactment of the Motor Vehicle and Highway Safety Improvement Act of 2012, in carrying out this section, the Secretary shall prescribe regulations permitting any written disclosures or notices and related matters to be provided electronically. [§ 31205, 126 Stat. 761 (2012)]*

The Rule, currently in force, requires states to petition NHTSA for a waiver if they wish to electronically receive and process odometer disclosures. This process is time-consuming for both the petitioning states and NHTSA. In order to have a petition approved, a state must provide a detailed description of the proposed process. The approval of this petition requires a state to proceed with the original proposal, and does not allow the solution to adapt throughout the implementation process. At least five states (Florida, New York, Texas, Virginia, and Wisconsin) have applied and received some type of approval from NHTSA. Due in-part to the restrictive nature of these approvals, only one state (Texas) has actually implemented any e-odometer processing, which remains limited at this time. If states were not bound to the specifics of their petition, but rather were granted more flexibility to comply with an existing rule, they would be more likely to pursue e-titling systems.

In October 2013, AAMVA's E-Title Task Force, responsible for developing an E-Title Proof of Concept, closed their project and redirected efforts on solving the e-odometer challenge. The

E-Title Task Force identified the lack of an e-odometer disclosure approach that is compliant with TIMA, as the major hurdle to the development of a true e-titling environment within the

United States (US). NHTSA has oversight for compliance with TIMA.

In January of 2014, the E-Odometer Task Force, hereinafter referred to as the Task Force, was formed to identify a flexible approach to an e-odometer disclosure that the majority of states could successfully implement. NHTSA participated in meetings as a technical advisor and

Clerus Solutions, LLC, was a consultant providing project management for the kickoff meetings and report. Based on the state task force representatives' long history and experience with odometer disclosures, the Task Force identified issues, opportunities, and

challenges related to e-odometer disclosure. Consideration was also given to the overall impact on state titling programs. The Task Force believes that a flexible approach in federal regulations will allow states to move toward e-odometer disclosure, further increasing the ability to progress toward e-titling. For legal and practical purposes the Task Force has concluded that the electronic disclosure of odometer readings must be permitted in order to implement the electronic transfer of ownership.

This report is intended to provide an overview to the stakeholders of what the Task Force members believes is a flexible approach to what an e-odometer disclosure should encompass.

Section Three Truth in Mileage Act (TIMA) Today

TIMA is a federal law that requires the seller, whose name is on the title, of a motor vehicle to provide an odometer disclosure to the buyer at the time of sale or transfer of ownership. The buyer must sign the title acknowledging the mileage disclosure.

Other than instances where the title is lost, held by a lienholder, or dealer-to-dealer transactions employing reassignment documents, TIMA requires the odometer disclosure to be on the certificate of title. The title itself must incorporate security features to prevent duplication, unauthorized modifications, and forgery.

Except for instances where a power of attorney (POA) is employed to accommodate a transaction involving a seller, an intervening dealer, and a purchaser from that dealer, no one may sign an odometer disclosure statement as transferor and transferee in the same transaction.

The following information is required:

- Odometer reading at the time of transfer (not to include tenths of miles) or an alternative declaration as explained below.
- Date of transfer.
- Transferor's name and current address.
- Transferee's name and current address.
- Transferor's signature.
- Transferee's signature.
- Identity of the vehicle, including its make, model, year, body type, and VIN.

The transferor must certify whether the odometer reading reflects the vehicle's actual mileage, disclose whether the odometer reading reflects mileage in excess of the odometers mechanical limit, or if the odometer does not reflect the actual mileage, must state that the odometer reading should not be relied on. A POA may be used when the certificate of title is physically held by a lienholder, or has been lost and the transferee obtains a duplicate certificate of title on behalf of a transferor. Each new certificate of title, at the time it is issued by the state, must contain the mileage disclosed by the transferor.

States may not issue a title for a vehicle unless the applicant submits the existing title with a completed odometer disclosure statement and any accompanying POA.

Vehicles exempt from odometer disclosure requirements include:

- Vehicles 10 years old or older.
- Vehicles with a gross vehicle weight rating over 16,000 pounds.
- All-terrain vehicles.
- Trailers.
- Vehicles sold to any agency of the US government directly from the manufacturer.

If a state wishes to employ an alternative odometer disclosure scheme that deviates from the process and procedures in The Rule, a state may petition NHTSA for approval of different disclosure requirements that are consistent with the purposes of TIMA and the Motor Vehicle Information and Cost Savings Act. The regulations implementing these statutes, referred herein as The Rule, are found at 49 C.F.R. § 580 (2012)—Odometer Disclosure Requirements.

Section Four General Concepts

4.1 Distinction between Previous Titles, Current Titles and New Titles

In a paper processing environment with no e-odometer statements, The Rule establishes that when a vehicle with a current title is transferred, the odometer disclosure statement is to be executed on the certificate of title itself; thus becoming a permanent part of the title record. When a new owner applies for the new title for a vehicle, the title application will include the previous certificate of title with the odometer disclosure statement affixed. When a state issues the new title, it will include the odometer statement disclosed on the previous certificate of title (or any additional odometer disclosure statements). That state will then file and retain the previous certificate of title for the required retention period.[1] The odometer disclosure statement itself remains a part of the previous certificate of title, while the odometer reading becomes a part of the new title.

For a new vehicle, never previously titled, a paper odometer disclosure statement is submitted to the state along with other materials needed to obtain the first title. Frequently, but not always, the odometer disclosure statement is executed on the Manufacturer's Certificate of Origin (MCO). The odometer reading is shown on the new certificate of title, but the odometer disclosure statement itself is filed for the retention period.[2]

Similarly, in an environment where odometer disclosure statements are made electronically, once an e-odometer disclosure statement is executed for a previously titled vehicle, the state must ensure that disclosure becomes a permanent part of the previous e-title record. When a state issues a new title for the vehicle, TIMA only requires that the odometer reading become a part of the current e-title record. If that state archives the previous e-title record, the odometer disclosure statement must be retained as part of this previous e-title record. The important point is that TIMA requires the entire odometer disclosure statement be kept as part of the previous e-title, while it requires only the odometer reading to be part of the current e-title record.

For a new vehicle, the reported mileage must be stored as part of the newly created e-title record, but the e-odometer disclosure statement may be filed separately as long as the state retains it for the appropriate period.

4.2 The Relationship of E-Odometer to E-Titling

During its deliberations, the Task Force realized the importance of the relationship of processing e-odometer disclosure statements to the larger issue of e-titles. In effect, the handling of e-odometer disclosure statements can be seen as a subset of a complete e-titling process. The security requirements for the overall e-titling process will be, at the least, as great and probably greater, than what is required for e-odometer disclosure statements because the transfer of title involves the transfer of ownership of valuable property.

It is important to recognize that if a state allows a vehicle title transfer to occur electronically, the security established for that process will meet or exceed what is needed for odometer disclosure statements. The Task

1 Most, if not all states retain an electronic (scanned) copy of the previous title and destroy the paper copy.
2 Most, if not all states retain an electronic (scanned) copy of the odometer disclosure statement and destroy the paper.

Force expects that when states implement e-odometer processes, those implementations will be in conjunction with other electronic processing of titles.

4.3 National Solution

There was some concern within the Task Force that states pursing individual electronic odometer disclosure ("e-odometer") standards and practices may create enough variation in the process to hinder national efforts for electronic titling of motor vehicles ("e-titling"). Without a national solution, these initial individual e-odometer efforts may actually provide a barrier for adoption of a unified e-titling solution. By endorsing a national solution, this AAMVA task force could ensure that initial e-odometer efforts are consistent with future e-titling endeavors. Despite this concern, the Task Force felt that pursuit of a unified national solution would be unattainable at this time since NHTSA has yet to issue a Federal Rule. The Task Force felt that the endorsement of national standards in this document would be sufficient to prepare states to adopt a national solution at a later date, while also providing the flexibility for states to proceed at their own pace. In an effort to encourage national standards, which we hope will eventually lead to a national solution, the Task Force report does identify a number of standards to which all states must adhere when allowing electronic odometer disclosure which are summarized below.

- Each state must utilize a combination of mechanisms to assure authentications are equivalent to or greater than the controls of a Level 2 Assurance per NIST standards.
- The data captured and stored in an electronic odometer disclosure statement should be the same as required by the current paper process.
- The electronic format must include warnings about federal law.
- The e-title must be the legal controlling title.
- The state/system must retain the pertinent information that can be used to prove the validity of the signature.
- The state should verify with existing title records that the mileage declared is consistent with previous declarations.
- There is no requirement to type rather than print the name in an electronic world.
- If a paper document is scanned by a dealership and submitted electronically to the state for storage, the dealership must destroy or render the paper (previous) title non-negotiable.

The Task Force recognizes that a national solution for e-titling is desirable and will likely require more uniformity among the states in order to allow for the interstate transfers of electronic titles. This national solution is likely to include the capacity to accept and record electronic odometer disclosure statements and may replace some of the initial e-odometer efforts. The standards listed above, however, will already provide assurance that an electronic odometer disclosure statement from any state complying with these standards and meeting NHTSA requirements is valid and can be accepted even if certain state practices and standards are somewhat varied.

Section Five Considerations for E-Odometer Disclosures

The Task Force developed the following considerations that it believes will facilitate the development of e-odometer disclosures.

5.1 E- Odometer Disclosure to Contain Same Data

The Task Force believes the same data required by federal statute for a paper odometer disclosure would continue to be required for an e-odometer disclosure.

5.2 Waiver Not Required for E-Odometer

Today, states are required to follow The Rule, which does not allow electronic processing of odometer disclosure statements, and contains no guidance for electronic processing of odometer disclosure statements. If a state wants to use electronic processing, it must obtain a waiver from The Rule by petitioning NHTSA for approval of an alternate disclosure process. The alternate disclosure process must be consistent with the purpose of the Motor Vehicle Information and Cost Savings Act.

The waiver process requires a significant amount of effort for both the state to prepare and for NHTSA to review. After NHTSA publishes the petition for comment, the notice of the petition and an initial determination pending a 30-day comment period is published in the federal register. A notice of final grant or denial of a petition for approval of alternate motor vehicle disclosure requirements is also published in the federal register.

Once a new version of The Rule is published that contains guidance for electronic processing, the Task Force believes a waiver is not necessary, as long as the state operates in accordance with that guidance. If the waiver is no longer needed, stating that it is not required will save resources for both the state and NHTSA.

5.3 Tasks Performed by Non-State Entities

Federal odometer regulations impose requirements on parties other than the state. For example, consider the entire process by which a lessor can obtain an odometer from its lessee. At present, states have no role in this wholly private process. Because the state is not involved in the exchange of odometer information for the odometer disclosure statements between a lessor and lessee to date, they lack experience in administering this exchange. The Task Force believes that specific regulations may be needed for electronic processing of the practice by which a lessor can obtain an odometer disclosure from the lessee. In addition, the Task Force believes this electronic processing should be permissible to be implemented by the state, but the state should not be required to be a part of this process. There may be non-governmental entities better suited to implement the electronic exchange between the lessor and lessee, and the Task Force believes they should be permitted to do so.

When implementing an e-odometer approach, a state should ***not be required*** to provide a platform for such tasks, but should be ***permitted*** to provide such a platform if that state believes it is in its best interest to do so. The Task Force members believe that under the new regulations, states should not be required to be a part of transactions they are not part of today.

States are not currently involved in ensuring that the transferor and transferee receive copies of the odometer disclosure statements, and should not be required to do this as part of electronic processing of odometer disclosures. The electronic signatures on the disclosure statement indicate that the transferor and transferee acknowledge and accept the mileage given in the statement. An e-odometer disclosure statement process should permit the transferor and transferee to retain copies of the odometer disclosure statement, either in electronic or hard copy form. However, the Task Force believes that states cannot reasonably ensure that either party actually receives a copy of the signed statement.

Even if a state were to mail or email a copy of the odometer disclosure statement to both parties, the state has no way to reliably determine "failed delivery." Similarly, attempting to "void" the transaction at that point would not be feasible. Presumably, the seller has the money, the lien holder has the lien, and the buyer has the vehicle. Voiding the transaction could prove chaotic at best.

The Task Force felt that there are at least two other concepts that would better address this issue:

- An electronic system for odometer disclosure statements should be capable of delivering to both the transferor and transferee copies of the odometer disclosure statement, either in electronic or hard copy format.
- The state should not accept the submission of an application for a new title until both the transferor and transferee have signed the odometer disclosure statement.

5.4 Consider an Incremental Approach to E-Odometer Adoption

States should consider taking an incremental approach to facilitate the development of e-odometer disclosures. For example, it may be easier to implement electronic reporting for new vehicle sales than it is for used vehicles, or to implement intrastate transactions than to implement interstate transactions. There may be types of transactions for which it will not be possible to implement electronic processing in the foreseeable future. This will require states to provide a mixture of paper and electronic processes, but each state should decide which transactions will be paper and which will be electronic.

Until a national e-titling solution is available to exchange e-odometer disclosure and title information, each state should also be allowed to electronically exchange data for interstate title transactions.

5.5 Acknowledgement of Warnings about Federal Law

Currently, a paper document used for an odometer disclosure statement or associated POA must contain a warning that refers to the federal law and advises that failure to complete a required odometer disclosure statement or providing false information may result in fines and/or imprisonment; the person's signature indicates an acknowledgement of the warning. E-odometer disclosures must ensure that the parties signing the disclosure continue to receive and acknowledge an appropriate warning. One way to meet this requirement would be to have the person check off on the statement (similar to the way that is widely used in establishing on-line accounts) before the electronic signature can be accepted.

5.6 Conversion Between E-Title and Paper Certificate of Title

If a state operates in an e-title environment where the e-title is considered the legal, controlling record, the state should consider the necessity to be able to convert the e-title into a paper certificate of title that meets all of the provisions for content and security required for a paper certificate of title, including the most recently reported odometer reading contained in the e-title.

To facilitate the ability of states to implement e-odometer disclosures incrementally, each state should contemplate an environment with a blend of electronic and paper processes, particularly when vehicle transactions take place across state boarders.

5.7 E-Title as the Legal, Controlling Record

In a state using e-titles, if the state accepts e-odometer disclosure statements for previously titled vehicles, then the state should designate the e-title stored in its system as the legal, controlling title. The e-odometer disclosure statements must become a "permanent" part of the legal, controlling title in existence when the odometer disclosure statement is made. The state can accomplish this by adding the e-odometer disclosure statement to the e-title record in its system, but only if that e-title record is the legal, controlling title.

If a state does not use e-titles and relies solely on paper certificates of title, the paper certificate of title is the legal, controlling title. When a vehicle with a paper certificate of title is transferred, at least the initial odometer disclosure statement should be made on the paper certificate of title itself, and thus that odometer disclosure becomes a permanent part of the title. The certificate of title with the permanently affixed odometer disclosure statement remains the legal, controlling title until a new title is issued.

5.8 Electronic Signing of an E-Odometer Disclosure

The primary purpose of the odometer disclosure program is to protect the financial interests of customers purchasing vehicles. False odometer disclosures can cause significant economic loss to purchasers, so the assurance level of the identity of the party submitting the odometer disclosure statement should match the strength of the credential used in signing the statement.

To provide assurances that persons electronically signing odometer disclosure statements are who they say they are, jurisdictions should require personal information be provided that would allow for them to be uniquely identified through the use of automated and/or manual processes. Based on the validated information, electronic credentials should be issued that would uniquely identify customers while performing online transactions. The resulting credentials can consist of a username and password, a personal identification number (PIN), an electronic token, or other methods that allow the jurisdiction to ensure that the person electronically signing the disclosure has been verified.

In the absence of a method of verification by the jurisdiction, a digital certificate or other credential that has comparable assurance of the holders identity, or the use of a commercial electronic signing solution along with a documented business process that verifies a government issued identification (ID) card/Driver License (DL) against an authoritative source (e.g., the state, DLDV) would meet the requirement.

This process provides the equivalent assurance of identity of a Level 2 credential based on the NIST 800-63 Electronic Authentication Guidelines. In addition, those jurisdictions DLs and ID cards that are issued through the use of Social Security Online Verification, passport and/or birth certificate authentication, and address verification would be sufficient, and would exceed the recommendation since the personal information is not just verified through a single authority as in Level 2, but verified through multiple authorities, and provides for in-person identity proofing. Additionally, commercially available credentials or existing implementations that are certified or equivalent to NIST Level 2 or above may be used provided the identity attributes are verified in a manner that satisfies the jurisdictional needs for identifying a customer.

States should consider referring to either OMB M-04-04 E-Authentication Guidance or NIST SP800-63 E-Authentication Guideline for guidance when determining the authentication requirements. For background information on E-Identity refer to Appendix A.

5.9 Retention of Electronic Signature

Ultimately, the purpose of the electronic signature is to prove a link between the e-odometer disclosure statement and the individuals who executed it so they cannot later claim they were not involved. The process used to electronically "sign" the statement must permit the storage of pertinent information (or metadata) that can be used to prove that connection. The electronic system must retain that information along with the e-odometer statement so it can be retrieved if it is needed. The requirement to store this information should have the same retention requirement as the e-odometer statement.

5.10 Same Electronic Signature Process for Power of Attorney

Because implementing the electronic processing of a POA in compliance with the guidance in §580.13 through §580.16 of The Rule could be complex, many states may choose to defer that effort relating to disclosure under POA. The Task Force is of the opinion that if a state chooses to undertake the effort, there is no reason why the signature on the POA should be at a higher level of confidence than for the odometer disclosure statement itself. These documents may be phased out going forward in an e-title environment.

5.11 Ancillary Matters

All state electronic processing of vehicle records is already governed by state and federal laws or regulations in areas such as accessibility, privacy, and security. Changes to the requirements relating to these subjects can be relatively frequent as new threats are detected and new technologies become available. The Task Force recognizes that regulations on these subjects would apply to electronic processing of odometer disclosures and did not believe this report needed to address the accessibility, privacy, and security from a technology perspective specific to e-odometer disclosure.

5.12 Use of E-Odometer Disclosures for Dealer to Dealer Transfers

States are still determining the best way to track odometer disclosures when a vehicle is transferred from one dealer to another. Resolving this will be a key to a state implementing electronic processing of odometer disclosures for used vehicles (i.e., vehicles that already have been titled at least once). Currently, states generally do not require a dealer to obtain a title for a used vehicle when transferring it to another dealer, partly to allow quick resale by the receiving dealer. For this type of transfer, the odometer disclosure statement, recorded either on the certificate of title or on a separate document, is kept with the current title from the previous owner. Ultimately, all of these odometer disclosure statements are presented to the state when a new owner applies for a new title. However, in an environment using e-titles, it is not clear how best to handle an odometer disclosure when a dealer transfers a used vehicle to another dealer. The Task Force believes that each transfer should continue to be captured and there shall not be any skipped title re-assignments in an electronic environment.

One solution, but perhaps not the only solution, for dealer-to-dealer transfers in an e-titling environment would be to have the dealers electronically submit the odometer disclosure statements to the state at the time of the dealer-to-dealer transaction. Because the Task Force is recommending an incremental approach, it is the Task Force's belief that states should not be prohibited from collecting odometer disclosure

information on dealer-to-dealer transactions as soon as resources are available to do so.

5.13 Assuring the Accuracy of Reported Mileage

Verifying the accuracy of the declared mileage would require a state to visually or electronically read the odometer, and, in most cases, the state does not have the resources to perform such checks, nor is this a current practice in most states. The state should verify with existing title records that the mileage declared is consistent with previous declarations, usually meaning that it is not less than what was previously reported. The Task Force does not anticipate a change in the practice of authenticating odometer disclosures in an electronic approach.

5.14 Transferor and Transferee Typing Names into System

The Rule presently contains requirements for individuals to print their names in addition to signing the odometer disclosure statement. The printed name has value during a fraud investigation because it provides additional clues that a forensic examiner can use in determining who actually signed an odometer disclosure statement in a paper odometer disclosure environment. Having a person type their name into a system when providing an electronic signature does not normally provide any similar forensic capability, and therefore should not be a separate requirement in an e-odometer disclosure approach to keystroke their own individual name.

Section Six Roadmap: Future Actions That Will Inhibit Odometer Fraud

As the use of electronic processing of odometer disclosure statements grows, there will be opportunities to make improvements that will inhibit fraud as well as simplifying the process for those involved. However, taking advantage of these opportunities will require that a number of issues be resolved. This section of the report discusses some of the key areas that the Task Force will begin to address in 2015. In many cases, coordination and cooperation among states and stakeholders will be necessary to accomplish what is needed.

6.1 Used Vehicles Sold or Traded-In to Dealers

As discussed in section 5.12, dealer-to-dealer odometer disclosure statements are normally received by the state when the final purchaser makes an application for a certificate of title, not at the time a vehicle is re-assigned from one dealer to another. In an electronic processing environment, when a vehicle is assigned to a dealer, the dealer itself could be required to execute an e-odometer disclosure at the time of assignment and have to submit it to the state. The state will make this statement a permanent part of the title record. However, the Task Force needs to consider the following questions:

- How will the customer who ultimately buys the vehicle receive the odometer disclosure? This customer is, after all, the one who the disclosure is meant to protect.
- How will the odometer disclosures be made and reported as the vehicle passes from dealer to dealer? Keeping the existing process will likely result in the current owner always needing to obtain a paper certificate of title when selling the vehicle, somewhat defeating the purpose of having e-titles.
- Should e-odometer disclosures be required for dealer-to-dealer transfers? Requiring an e-odometer disclosure to be made every time a vehicle changes hands, even when there is not a title application submitted, could help to inhibit fraud through more frequent reporting. Currently, the relatively long period between when the initial odometer disclosure is executed until it is submitted to a state provides an opportunity for unscrupulous dealers to commit odometer fraud. If all disclosures were made to the state in near real time, there would be significantly less opportunity for anyone to subsequently alter the disclosure statement. An additional benefit would be that this type of reporting would virtually eliminate the need for using a POA. This might also be accomplished with voluntary odometer statements reported by the transferor, as discussed in section 6.4.

6.2 Transfers of Vehicles across State Borders

For transfers across state borders, the electronic processing of odometer disclosure statements is closely related to the electronic processing of titles in general. Until electronic processing of odometer disclosures for interstate transfers can be done, it will not be possible to do electronic processing of titles for interstate transfers. However, interstate transfer issues that impede the electronic processing of odometer disclosures may best be addressed by solutions that address interstate processing of titles in a broader context.

The following are some of the questions that will need to be addressed to enable electronic processing of odometer disclosures for interstate transfers:

- Which state will handle the on-line interaction with the parties executing the odometer disclosure statement? Should it be that state to which the vehicle is being transferred or the state that houses the current title for the vehicle?
- If the old state and the new state have different electronic signature processes, which process will be used for the transfer?
- How will the states communicate to effect the necessary exchanges of data?
- What role can or should the National Motor Vehicle Title Information System (NMVTIS) have in the transfer?
- How will the states handle an interstate dealer-to-dealer transfer if the receiving dealer does not plan to apply for a title? What needs to happen if the vehicle is then transferred to a dealer in a third state before being sold to a customer who applies for a title?

The implementation of electronic processing for interstate transfers will require cooperation among states and stakeholders to find answers to these questions and to establish standards for procedures, communication links, data, etc. Such cooperation will require a forum similar to the Task Force on at least a regional, preferably national, level. Developing disparate regional standards is less than optimal since it will inevitably raise issues for transfers between regions.

6.3 Use of NMVTIS to Inhibit Odometer Fraud

NMVTIS provides a means for states to exchange vehicle title and brand information. Federal law requires all of the states to inquire against the NMVTIS data and submit title and brand data.[3] Although a state can perform all the required inquiries required for its participation by using batch processing with NMVTIS, a large number of states are using online real-time inquiries at the time a title is processed and issued. The federal regulations require the states to complete the following:

- Perform a check of NMVTIS title and brand inquiry before issuing a new title on a motor vehicle when an out-of-state certificate of title is being surrendered.
- Provide title and brand information to NMVTIS at the time a title is issued.
- Pay NMVTIS user fees.

The current implementation of NMVTIS requires a state to provide the odometer reading associated with the current title[4] when the title information is added to NMVTIS. When the title information is for a previously titled vehicle, the information from the previous title is retained in the title history for that vehicle.

When a state receives an application for a new title for a vehicle being transferred from out-of-state, it must send an inquiry to NMVTIS before issuing the new title. In response to the inquiry, NMVTIS provides the mileage recorded on the latest title on file[5] and also the mileage from any older titles NMVTIS has for the history of the vehicle.

The inquiring state can then use this information to compare with the mileage from the odometer

3 49 U.S.C. 30502, 28 C.F.R. 25.54

4 This will be the mileage from odometer disclosure statement executed when the ownership of the vehicle was transferred. 49 C.F.R. 25.54(a)(5)

5 Depending on the state, NMVTIS uses title numbers and/or the title issuance date to differentiate between titles it has on file for a given vehicle. In many states, the state assigns a new title number when issuing a new title for a vehicle. In other states, the state always keeps the same title number associated with a vehicle, and when issuing a new title only the issuance date is changed.

disclosure statement presented with the title application. In this way, NMVTIS currently provides support for the e-odometer disclosure program. There is the possibility that NMVTIS could provide even more support in the future.

The regulations that govern NMVTIS allow for subsequent capture of odometer disclosures from sources other than the issuance of a title.[6] Some examples of these other disclosures include the mileage recorded during safety inspections or emissions tests. These events often occur between the issuance of one title and the next, so storing the recorded mileage in NMVTIS would provide more recent information for comparison with the latest disclosure being presented to the state.

While NMVTIS is authorized to store this information, it does not currently have the capability to do so. If NMVTIS were to be enhanced to enable the capture and storage of additional odometer information, it would play a key role in contributing to the integrity of the odometer disclosure program.

One possible benefit of having NMVTIS store odometer mileage reported between the issuance of titles is that it could be used to record the mileage for an interstate transfer of a vehicle from one dealer to another.

6.4 Voluntary E-Odometer Reporting by Transferor

As suggested in section 4.1 and elsewhere in this report, the gap between the time an odometer reading is recorded on the odometer disclosure statement and the time the odometer disclosure statement is reported to the state as part of an application for title can be considerable, and allows time to commit fraud. Related fraud can include falsifying or altering the odometer statement, adding or altering the transferee name after the transferor executes the odometer disclosure statement, or failing to identify each successive transfer and the odometer mileage readings at each undisclosed transfer. An electronic odometer reporting system can shorten that time between the odometer reading and reporting, but still relies upon the transferee to make that report. E-odometer should allow an odometer disclosure statement to be submitted unilaterally by the transferor, to be accepted as part of the title record only when confirmed by the transferee through subsequent title application, or other transaction or affirmation, rather than relying solely on reporting by the transferee. By allowing the transferor to report that a vehicle transfer has occurred and the vehicle mileage at the time of transfer, any delay in reporting by a transferee would become apparent, which visibility could reduce occurrences of fraud between the time of transfer and the time of application for new title. In addition, allowing reporting by the transferor could reduce title skipping, which can occur if intermediate owners, including insurers making total loss payments, fail to record themselves as owners even though a transfer of ownership has occurred. Allowing the transferor to report would impose no additional burden on any transferee, so high-volume transferees such as insurers or dealers purchasing at auction would be unaffected. A discrepancy between the transferor's voluntary report and the transferee's report will not necessarily indicate fraud, but it will identify a discrepancy and will provide additional information if the discrepancy is investigated. This could help ensure complete ownership history and facilitate proper branding of vehicles and reporting and collection of sales taxes and fees by states.

6 28 C.F.R. 25.53(a)(4)

Appendix A E-Identity Background

The Task Force used the background information in this appendix provided by the consultant when discussing the identity authentication and level of assurance they believed should be used for an e-odometer disclosure process. This appendix is not specific only to e-odometer disclosure identity verification.

Key Terms

- Digital identity is the representation of identity in a digital environment.
- Identity providers are entities that manage identity information on behalf of parties and provides assertions of authentication to other providers.
- Issuers are the entities responsible and trusted to issue identities to individuals, organizations, and/or systems.
- A credential is an object that authoritatively binds an identity to a token possessed and controlled by a person.
- An attribute is a distinct characteristic of an object. An object's attributes are often used to describe traits, such as size, shape, weight, and color.
- Authentication is used to confirm that system entities asserted principal identity with a specified, or understood level of confidence.
- Authorization is the process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Once a subject is authenticated, it may be authorized to perform different types of access.
- A relying party is a system entity that decides to take an action based on information from another system entity.

Overview

The formal identification process may consist of collecting information about a person and validating that information to provide some level of assurance that the person is who they claim to be (claimant). For the purposes of this document the claimant is the person signing the odometer disclosure. The identification process could then result in the issuance of both physical and electronic credentials dependent on future requirements. An issued credential is something that the user would then provide to validate a claim of their identity.

- A physical credential (e.g., DL or passport) can be issued by various authorities (e.g., Department of Motor Vehicles or State Department).
- An electronic credential (e.g., user name and password) may be issued during an online registration process or other process, whereas the validity of the requestor is checked against information currently stored in data repositories and is consistent with the same information for obtaining the physical credentials. Obtaining access to a controlled State asset or service will require the user to assert their identity by providing a pre-issued credential as proof of that identity.

However, not all credentials are equal. The level of assurance provided by a credential depends directly on the process that was used to issue a credential. Once issued, the credential must be validated as part of the authentication process. The individual must also have authorization to access the resource or service, regardless of the validity of the identity.

Before receiving credentials, an applicant must demonstrate that the identity claimed is real and that they are verified to use that identity. This process is referred to as identity proofing.

Credential issuance generally involves the following steps:

- Identity-proofing is where the claimed identity of the person is validated. In most states, this requires background checks and other means of verification processes which may include, at times, criminal history database checks, and other information provided by the claimant. Security managers will verify identity using an ID card(s) issued through an appropriately rigorous process prior to issuing local credentials. Where multiple proofs of identity are required, care should be taken to require use of ID cards which are issued using different identity proofing processes.
- Registration and naming, where the identity is assigned an identifier.
- Generation of an authentication credential. Depending on the business requirements and technology used, this may involve selection or generation of PINs, PKI certificates, photograph, and/or biometric reference samples.
- Binding the intended authentication method to the identity.

Authentication

Credentials are authenticated using one of three personal authentication factors or techniques.

The three categories of authentication factors are:

- Something claimant knows (e.g., a password)
- Something claimant has (e.g., a certificate with associated private key, smart card, or cookie)
- Something claimant is (e.g., a biometric attribute, such as fingerprint or facial)

Single-factor authentication is defined as the use of any one of these categories or authentication factors. If two factors are employed, this is considered two-factor authentication.

The level of assurance provided by a personal authentication method such as a smart card, key, or token, is increased as the number and types of authentication factors are increased.

Levels of Assurance

1	Little or no confidence in the asserted identity's validity. • Basic authentication
2	Some confidence in the asserted identity's validity. • Verified information • Various authentication (e-signatures, certificates, etc.)
3	High confidence in the asserted identity's validity. • Verified information and identity proofing • Multi-factor authentication

Level 1

Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data.

It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2 or 3. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plain text passwords or secrets are not transmitted across a network at Level 1. However, this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 2

Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Level 3, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by CSP. Approved cryptographic techniques are required.

Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 3

Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key, or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation, and man-in-the-middle attacks. A minimum of two authentication factors is required. While tokens may evolve, there are currently three kinds of tokens that may be used:

- "Soft" cryptographic tokens.
- "Hard" cryptographic tokens.
- "One-time password" device tokens.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by CSP; however, session (temporary) shared secrets may be provided to independent verifiers by CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved

methods), or are obtained directly from a trusted party via a secure authentication protocol.

Mapping Authentication Levels to Risk Assessment

Improper authentication of users can result in direct and dire consequences to an application, system, and organization. This approach emphasizes the development of authentication requirements based on risk. It is designed to approach the task from a business perspective, identify organization risk, and then match those risks to the appropriate technical solution. This is accomplished through a risk assessment for each transaction. The assessment identifies:

- Risks
- Likelihood of Occurrence

The results of the risk assessment should yield a determination of which level of assurance is appropriate, outline the potential harm or impact by not selecting the next highest level, and consider the likelihood of such harm or impact.

Examples of Authentication Credentials and Solutions

In order to offer flexibility to the states and to offer the proper amount of protection of fraud, the Task Force recommends that a state utilize a combination of mechanisms to assure the identity of the individual and the strength of the token are sufficient to reduce fraud that are equivalent to the controls expected in a Level 2 credential. This may be achieved via technology solutions or a combination of manual business processes that satisfy the identity verification necessary to reduce fraud.

It is recommended that an electronic signature utilizes one of two means, a token from Section A and a verification from Section B, or utilize a composite credential from Section C which encompasses the identity proofing and token issuance via a commercial solution and business process.

Section A	Section B	Section C
Something claimant knows • User ID/Password • Knowledge Based Authentication (KBA) • Key Identifier/ Personal Identification Number (PIN) • Jurisdiction provided token/code Something claimant has • Soft Token (Computer based/Mobile Device) • Short Message Service (SMS, aka Text Message) or other Out of Band (OOB) Message via a phone call or email. Something claimant is • Represented by a biometric contained on a token such as a Personal Identity Verification (PIV)/ Personal Identity Verification- Interoperable (PIV-I)/ Common Access Card (CAC) • Biometric Reader (Thumbprint, etc.)	Acceptable personally identifiable information (PII) to uniquely identify the individual through the use of automated verification systems such as Driver License Data Verification (DLDV), Social Security Online Verification (SSOLV), Utility, Financial, and other electronic verification services. Attributes can include: • Full Name (First, Middle, Last, Suffix) • Date of Birth • Address (Number, Street, City, State, Zip • Gender • DL# • Social Security Number • Phone Number • Email Address	• Digital Certificate issued to an individual from a trusted Certificate Authority that contain attributes that uniquely identify an individual and have sufficient confidence in the identity of the individual possessing the digital certificate. • Commercial e-signing solution that contain attributes that uniquely identify an individual and have sufficient confidence in the identity of the individual that applies the commercial signature. • Documented business process that verifies a government issued ID against an authoritative source (i.e. Driver License Data Verification (DLDV), state system, etc.).

Appendix B Making the Paper Process Electronic

During their deliberations, the Task Force discussed whether the objective was to automate the paper process or make the process less susceptible to fraud. Ultimately, the Task Force discussed both and believes an electronic process will significantly decrease fraud once e-titles have been implemented on a large scale. Through the discussion, the following information regarding odometer disclosures was clarified by NHTSA as a technical advisor.

With respect to making the paper process electronic, many, if not all, states have an electronic method that certain stakeholders (i.e., dealers) can use to electronically submit title applications. The one aspect of the application process that still requires paper is the odometer disclosure.

In discussion, it became evident that when a state receives the paper odometer disclosure, whether it be on a certificate of title or odometer disclosure statement (in the case of new vehicles), the state scans the paper, keeps the scanned copy, and destroys the paper.

The question was asked of NHTSA whether the scanning process could be done by the dealer, rather than the state. NHTSA responded that if the scanning process used for this purpose had high enough resolution to preserve the security features incorporated in the paper title, dealers could scan the document and send it electronically to the state. The Task Force believes that if the scanning process has sufficient resolution to ensure the image was taken from the original title and not on a substitute document, the scan could be sent electronically to the state. Such a process would be consistent with the objectives of NHTSA's current regulations as long as the original title is rendered non-negotiable once it has been scanned and sent electronically to the state. Dealers would be required to certify that titles have been made non-negotiable after being scanned electronically. States would need to establish penalties and other mechanisms to ensure that dealers fulfill this obligation. Additionally, states will need to ensure that the previous titles are canceled when applications for new titles are processed.

For the sale of new vehicles, either the MCO with the odometer disclosure on it, or another document with the odometer statement (dependent upon the state) would be scanned and electronically sent to the state. For a used vehicle, the existing certificate of title with the signed odometer disclosure, and any additional odometer statements, would be scanned and sent electronically to the state. If the state currently scans these documents for archival storage, having the dealer send scanned copies could reduce costs for the state.

Not every state will find this approach beneficial, so each state will need to determine for itself if this change is worth making.

If implemented, states are not required to obtain a waiver from NHTSA as it complies with existing regulation.

Appendix C Task Force List

WORKING GROUP CHAIR

Julie Baker
Chief, Bureau of Issuance Oversight
2900 Apalachee Parkway
Tallahassee, FL 32399-0500
T: (850) 617-3001
juliebaker@flhsmv.gov

AAMVA LEAD STAFF LIAISON

Casey Garber
Manager, Vehicle Programs
4401 Wilson Blvd., #700
Arlington, VA 22203
T: (573) 632-0245
cgarber@aamva.org

AAMVA CO-STAFF LIAISON

Cathie Curtis
Director of Vehicle Programs
4401 Wilson Blvd., #700
Arlington, VA 22203
T: (207) 395-4100
ccurtis@aamva.org

AAMVA TASK FORCE TECHNICAL ADVISOR

Geoffrey Slagle
Director of Identity Management
4401 Wilson Blvd., #700
Arlington, VA 22203
T: (703) 342-7459
gslagle@aamva.org

JURISDICTION MEMBERS

Donna Brouch
Vehicle Insurance Program Administrator
California Department of Motor Vehicles
2415 First Avenue M/S C383
Sacramento, CA 95818
T: (916) 657-8181
Donna.Brouch@dmv.ca.gov

Karen Grim
Senior Assistant Commissioner
Virginia Dept. of Motor Vehicles
PO Box 27412
Richmond, VA 23269
T: (804) 367-6659
Karen.Grim@dmv.virginia.gov

Thomas A. McCormick
Senior Assistant Attorney General
Vermont Department of Motor Vehicles
120 State Street
Montpelier, VT 05603-0001
T: (802)828-3432
Tom.McCormick@state.vt.us

Clint Thompson
Chief of Title Services
Texas Department of Motor Vehicles
4000 Jackson Ave
Austin, Texas 78731
T: (512) 465-4021
Clint.Thompson@txdmv.gov

Kay Kishbaugh
Division Manager
PA Department of Transportation
Bureau of Motor Vehicles, Vehicle Inspection Division
1101 South Front Street, 4th Floor
Harrisburg, PA 17104
T: (717) 783-4597
kkishbaugh@pa.gov

Andrew P. Lewis
Assistant Director Vehicle & Motor Carrier Services
Office of Vehicle & Motor Carrier Services
Iowa Department of Transportation
6310 SE Convenience Boulevard
Ankeny, IA 50021
T: (515) 237-3040
andrew.lewis@dot.iowa.gov

Scott Clapper
Chief of Vehicle Services
Delaware Division of Motor Vehicles
P.O. Box 698
Dover, DE 19903-0000
T: (302) 744-2533
Scott.Clapper@state.de.us

Paul Zelenski
Strategic Manager
Division of Motor Vehicles
Wisconsin Dept. of Transportation
PO Box 7902
Madison, WI 53707-7902
T: (608) 267-2404
Paul.zelenski@dot.wi.gov

Michael McCaskill
Business Resources Consultant
Department of Highway Safety and Motor Vehicles
2900 Apalachee Parkway C-408
Tallahassee, FL 32399-0560
T: (850) 617-2688
mikemccaskill@flhsmv.gov

Stacey Rockwell
Investigator
Bureau of Investigation & Identity Protection
Iowa Department of Transportation
2460 Gateway Dr.
Dubuque, IA. 52003
T: (563) 582-0112
stacey.rockwell@dot.iowa.gov

Paul Nilsen
Assistant General Counsel
Department of Transportation
4802 Sheboygan Avenue
Madison, WI 53702
T: (608) 261-0126
Paul.Nilsen@dot.wi.gov

TECHNICAL ADVISORS TO TASK FORCE REPRESENTING THE U.S. NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Otto Matheke
Office of the Chief Counsel
400 Seventh Street, S.W.
NCC-20, Room 5219
Washington, DC 20590
T: (202) 493-2290
Otto.Matheke@dot.gov

David Sparks
Director, Office of Odometer Fraud Investigation
400 7th Street, S.W.
NPO-503, Room 6240
Washington, DC 20590
T: (202) 366-5953
David.Sparks@dot.gov

Mary Versailles
Office of Safety Performance Standards
400 7th Street, S.W.
NPS-31
Washington, DC 20590
T: (202) 366-2057
Mary.Versailles@dot.gov

CONSULTANTS

Mike Farnsworth
7200 Ivakota Rd.
Clifton, VA 20124
T: (804) 334-1911
mike@id.me

Jay Maxwell
President & CEO
Clerus Solutions
3835 Breckinridge Lane
Clermont, FL 34711
T: (407) 697-5124
jmaxwell@clerussolutions.com

Thomas L. Osterbind, PMP
Senior VP, Technology and CTO
Clerus Solutions
T: (703) 994-3468
tosterbind@clerussolutions.com

Mr. Richard Alan Carter
Senior Vice President, Programs Division
Clerus Solutions
T: (410) 969-4858
rcarter@clerussolutions.com

American Association of Motor Vehicle Administrators
4401 Wilson Boulevard, Suite 700
Arlington, Virginia 22203
703.522.4200 | **aamva.org**