

Key requirements of the Real ID Act

Federal rules will clarify these requirements. Here is what is known now:

- **Card specifications** – Specifies minimum information to be included on driver licenses and identification cards, such as legal name, date of birth, digital photograph, residence address and customer signature.
- **Card security features** – Specifies minimum physical security features to be included on the cards to prevent tampering, counterfeiting or duplication for fraudulent purposes.
- **Machine-readable technology** – Establishes a common machine-readable technology, such as bar codes or magnetic strips, with minimum data elements.
- **Electronic verification** – Requires verification with the issuing agency of specific data on the identity source documents, such as birth certificates, Social Security cards and immigration documents.
 - Birth certificates – No system exists today.
 - Social Security cards – Connect to Social Security Administration.
 - Immigration documents – Federal system must be expanded.
- **Legal Presence** – Requires evidence of lawful status in the country as either a U.S. citizen or legally present immigrant.
 - State-issued card must expire when legal status in the U.S. expires, such as a visa expiration date.
 - If the customer's authorized stay in the U.S. is indefinite, the state-issued card is valid for one year.
 - DMV cannot accept foreign documents other than an official passport.
- **Imaging ID documents** – Collect and store copies of identity source documents and retain them for at least seven years in paper form or 10 years in electronic format. DMV is choosing to store them in electronic format for 10 years.
 - Allows renewal without customer presenting identity documents again.
 - Makes documents available to law enforcement for investigations and prosecution.
- **Digital photos** – Requires retention of the photograph of every applicant, including applicants who are denied a license for insufficient documents or documents that may be fraudulent.
 - Makes photos available to law enforcement for investigations and prosecution.
- **Electronic access** – Each state must be able to electronically access information contained in another state's database.
 - Must have access to all data fields printed on the card.
 - Allows states to confirm the validity of original issuances.
 - No such data-sharing system exists today.
- **One person / one license** – The goal is to not issue a card until confirmation that the applicant's license in another state has been terminated.
- **Physical security** – Ensures the physical security of facilities where driver licenses and ID cards are produced and sensitive inventory is stored.

- **Background checks** – All persons who manufacture or produce driver licenses and ID cards are subject to appropriate security clearance requirements.
- **Employee training** – Requires DMV employees to receive training on recognizing fraudulent documents.
- **Expiration dates** – Limits the validity of cards to no more than eight years.
- **Driving-only cards** – Allows for issuance of driving-only cards for applicants whose identity or lawful presence in the U.S. is not determined. If a state issues these card, the card must:
 - Clearly state that it may not be accepted for identity purposes by any federal agency.
 - Use a unique design or color to alert federal agencies and law enforcement that it may not be accepted for federal purposes.