State and Local

Solution Profile

The DMV of the 21st Century—Modernization in the Application Economy

DMV Modernization

Within the next decade, many DMVs across the states will consider replacing legacy systems. Traditionally, the options are custom development, COTS, MOTS, and component-based development. These modernization efforts have resulted in varying degrees of success due to the complicated business requirements. Today, the modernization effort is even more challenging with the rapid advance in technology, the proliferation of social media platforms, and heightened security concerns which collectively have changed the landscape of how DMVs deliver services to the public. CA Technologies believes fundamentally these areas can be addressed to reduce the risks and enhance the success of these multi-million dollars investments.

DMVs provide primary services to citizens: driver's licenses, vehicle registration and titling, and motor carrier credentialing. They also support all local government agencies with information for law enforcement, courts and tax assessors, and provide information to automobile dealerships and insurance agents. But DMVs do a lot more for their state. They support transportation safety through programs to increase seat belt use and decrease alcohol-related injuries and death.

Modernization is not just about replacing old servers and out-of-date code. It is about providing better service to customers, and improving services across the board. This means decreasing wait times in line for a driver's license. It means using new technology like document imaging or new websites that support mobile devices. It means providing alternate ways to deliver services such as innovative apps for renewals or new processes for titling a new car at the dealership. Modernization is about bringing the DMV into the 21st century.

Looking at successful modernization projects, there are many lessons learned. Strong project management is always key. Modernization and business process improvement always go hand in hand. Data is priority number one, and all data issues should be addressed early and up front.

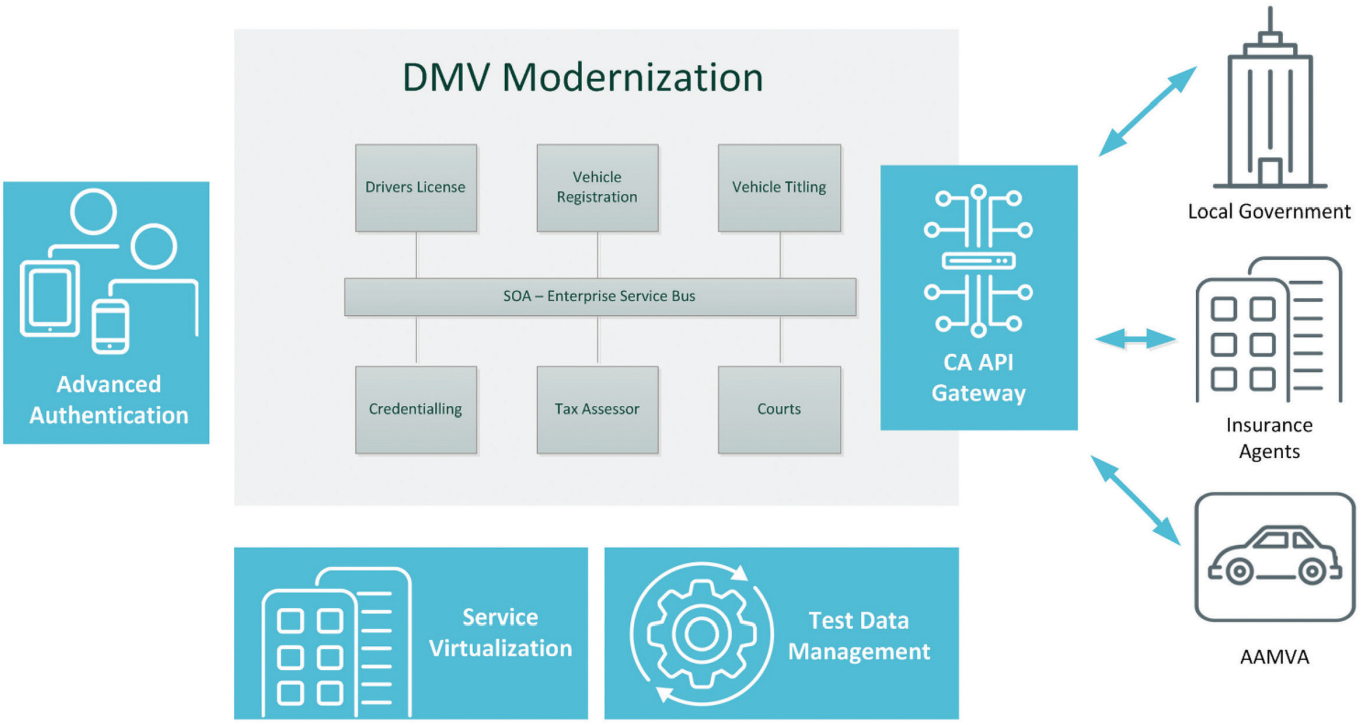
While states will rely on system integrators for the expertise in modernizing their systems, there are four areas that states can look to new technology to help ensure success.

1) State DMVs are both consumers and providers of data. They supply data to law enforcement, tax assessors and other agencies. They provide licensing and titling information for auto dealerships and insurance agents. As consumers, they get data from the Department of Homeland Security (DHS), HHS and commercial licensing agencies. API Gateways working in tandem with SOA can facilitate and secure this communication as DMVs modernize their systems. 2) Managing and protecting data is a top priority for states. When states put their modernization projects out to bid, system integrators become responsible for the project, yet states are still responsible for the security of their data. While DMVs focus on securing their production data, test data protection has increasingly become an area of concern. Test Data Management protects personally identifiable data (PII) and helps states manage test data. 3) During a modernization project, access to back-end and legacy systems for testing is one of the biggest constraints, causing delays and high costs to a project. Service Virtualization is a unique technology that virtualizes the services developers need to build their new systems. 4) States are looking for alternative ways to provides services to their citizens. Citizens want to do business on their smart phones, tablets, and kiosks. Multi-factor authentication and risk based authentication ensure secure on-line business.

CA Solution

CA API Management

DMVs are both consumers and providers of information. DMVs consume information from DHS, the State Department, the Department of Justice and Commercial Driver's License Information Systems (CDLIS). And DMVs provide information to car dealerships, insurance companies and a host of local government agencies, including tax assessors and law enforcement agencies. CA API Management with secure gateways provides backend SOA connectivity across databases, applications, mainframes and middleware to easily connect external data sources to SOA.



CA Solution (cont.)

In the DMV Architecture, the CA API Gateway is a virtual appliance that is scalable and can be clustered and easily managed through a central console. It is easily deployed in the DMZ or outside the firewall to provide secure communication with external data sources. It provides XML firewalling, and protocol translation from legacy sources to REST and JSON. It makes exchanging authentication and authorization data easy with security assertions with support for advanced SAML, OAuth, and XACML. The CA Mobile Access Gateway can be deployed to secure access to external customers using mobile devices.

CA Service Virtualization

As DMVs modernize their systems, states are moving to a modern Services Oriented Architecture with a business rules engine (BRE) and enterprise services bus. DMV internal processes rely on external data. This presents challenges when developing new services as these services are often constrained or unavailable to developers and they cannot test interfaces with partners or local agencies.

When developers cannot get to these services and backend hosts, it can cause serious delays in the overall project. Even though states contract out the development of new systems, they are responsible for providing test and development labs and access to existing services. The high costs of integration labs often leads to incomplete QA and user acceptance testing (UAT).

With Service Virtualization, developers no longer have to rely on others for their testing resources. CA Service Virtualization captures, models and then simulates the behavior of constrained or unavailable systems. The DMV can even virtualize mainframe services to run on a Window platform. CA Virtualization allows state to create a low-cost virtual, “life-like” environment where services are available to developers all the time. This reduces development costs and means the DMV can go live sooner with higher quality software and less project risk.

For developers, the benefits of virtualizing services is the reduction in the testing cycle time, the ability to test exception scenarios with no disruptions, and an increase in test coverage. Service Virtualization allows developers to increase their test runs and regain more development and testing time in the lab. This means higher quality development and more effective regression and system testing. For state agencies, the benefits of service virtualization is a significant reduction in the cost of creating and maintaining development and test environments, and the ability to create realistic integration labs at lower costs. When states virtualize services running on the mainframe, they can realize significant saving in MIPs fees.

CA Solution (cont.)

Test Data Management

When modernizing DMV systems, nothing is more important than protecting and managing data. The DMV is both a consumer and provider of data and has access to privileged data from federal, state and commercial data. CA Test Data Management (CA TDM) provides a comprehensive suite of tools that compliment CA Service Virtualization. Unlike traditional data masking and sub-setting technologies, CA TDM generates synthetic test data and makes it easy for users to get the data they need when they need it through a self-service portal.. These more modern approaches can be blended with CA TDM masking and sub-setting algorithms to meet almost any customer data need. To generate data CA TDM combines innovative data masking rules with synthetic test data generation create test data sets that DMV can use to modernize their legacy systems.

Synthetic test data contains all of the characteristics of production data but without any Personally Identifiable Information (PII). Exposing PII doesn't carry the same fines as exposing HIPAA data, but it is still critical for states to protect citizen data during development, something traditional masking does not provide. Masking can easily miss sensitive data and sub-setting doesn't provide adequate data coverage when building new services. CA TDM uses powerful data profiling techniques to take an accurate picture of your data and uses this model to quickly generate smaller, richer, more sophisticated sets of test data to facilitate development while allowing states to protect citizen PII. CA TDM increases testing efficiencies. It generates data to ensure coverage where production data is insufficient to test new services. CA TDM provides a test data warehouse where developers can find and reserve data through a self-service interface, saving developers from having to create or manipulate their own data sets. CA TDM increases efficiencies for developers while protecting critical data and citizen PII.

CA Advanced Authentication

DMVs are looking for ways to provide alternative access to traditional services. Citizens today live in an application economy and now expect anytime anywhere access on their mobile phone and tablets. As the DMV modernizes their applications, they need ways to provide secure access to their services online or at Kiosks. They need to confirm identities before access is granted. But they also need a way to make it easy for users. CA Advanced Authentication is transparent to uses. It reduces the risk of improper access and fraud without burdening valid users.

CA Advanced Authentication provides a wide variety of multi-factor, strong authentication credentials, plus risk-based authentication methods like device identification, geolocation and user activity, techniques that the banking industry has adopted for years. This allows the DMV to create the appropriate authentication process for each application or transaction, while supporting all of the popular mobile devices. It reduces the risk of data breaches and fraud, requires step-up authentication for suspicious activities, and helps states meet compliance guidelines such as FFIEC, HIPAA, PCI, and SOX.

CA Advanced Authentication uses patented technology to protect against man-in-the-middle and man-in-the-browser attacks. It offers a wide variety of integration options such as SAML, API and RADIUS, and can also use OpenID and Oauth.

Finally, if DMVs are going to accept payments online, CA Advanced Authentication offers payment security technologies like Card Not Present (CNP), 3-D Secure, EMV CAP/DPA, mobile wallet and mobile OTP transactions. This helps increase customer adoption of online payments while ensuring security.

CA Technologies (NASDAQ: CA) creates software that fuels transformation for agencies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with state agencies to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments.

To learn how government agencies are partnering with CA Technologies on modernization, visit ***ca.com/publicsector***