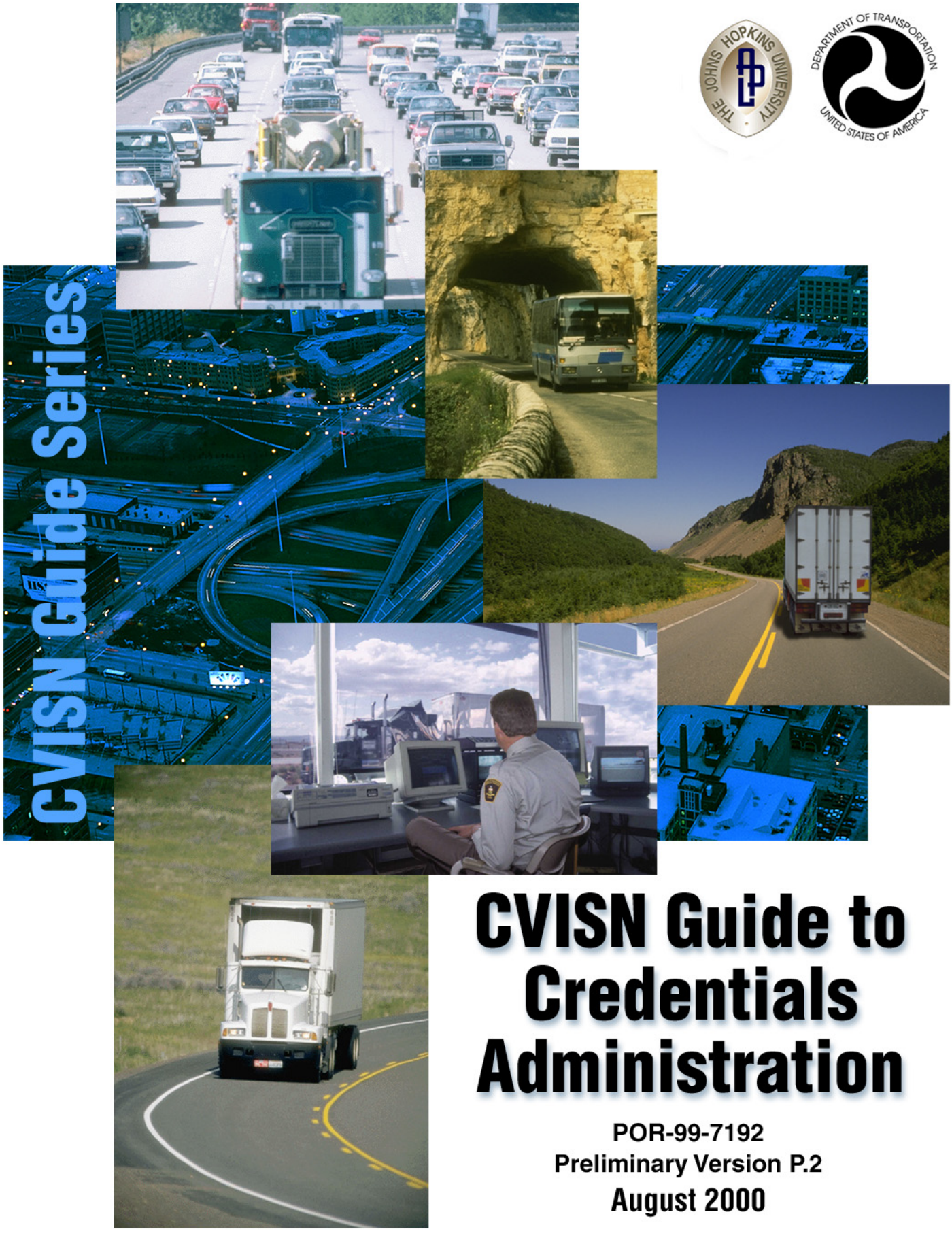


CVISN Guide to Credentials Administration

POR-99-7192

Preliminary Version P.2

August 2000

CVISN Guide to Credentials Administration

POR-99-7192
Preliminary Version P.2

August 2000

Note

The Motor Carrier Safety Improvement Act was signed into law on December 9, 1999. This act established a new Federal Motor Carrier Safety Administration (FMCSA) within the U.S. Department of Transportation (DOT), effective January 1, 2000. Prior to that, the motor carrier and highway safety program was administered under the Federal Highway Administration (FHWA).

The mission of the FMCSA is to improve truck and commercial passenger carrier safety on our nation's highways through information technology, targeted enforcement, research and technology, outreach, and partnerships. The FMCSA manages the Intelligent Transportation Systems (ITS) / Commercial Vehicle Operations (CVO) program, a voluntary effort involving public and private partnerships that uses information systems, innovative technologies, and business practice re-engineering to improve safety, simplify government administrative systems, and provide savings to states and motor carriers. The FMCSA works closely with the FHWA ITS Joint Program Office (JPO) to ensure the integration and interoperability of ITS/CVO systems with the national ITS program.

Preliminary Issue

It is important to note that this is a preliminary document. All sections included are complete and have been reviewed by JHU/APL, but not by other DOT contractors or state/federal government agencies. The purpose of this issue is to obtain comments and feedback on this document from those external organizations before a baseline version is published.

This document is disseminated in the interest of information exchange. JHU/APL assumes no liability for its contents or use thereof. This report does not constitute a standard, specification, or regulation. JHU/APL does not endorse products or manufacturers. Trade and manufacturer's names appear in this report only because they are considered essential to the object of this document.

Note: This document and other CVISN-related documentation are available for review and downloading by the ITS/CVO community from the JHU/APL CVISN site on the World Wide Web. The URL for the CVISN site is: http://www.jhuapl.edu/cvisn/

Review and comments to this document are welcome. Please send comments to:

Ms. Sandra B. Salazar
JHU/APL CVISN Project
11100 Johns Hopkins Road
Laurel, MD 20723-6099

Phone: 240-228-7610
Fax: 240-228-6149
E-Mail: sandra.salazar@jhuapl.edu

CVISN Guide to Credentials Administration

Table of Contents

List of Tables

List of Figures

This Page Intentionally Blank

1. INTRODUCTION

Credentials Administration is one of the three key capability areas in Commercial Vehicle Information Systems and Networks (CVISN) Level 1. The CVISN Guide to Credentials Administration provides reference information and offers advice about implementing credentials administration functions in CVISN.

This is one in a series of guides. The other guides (please see, for example, References 8–10) will be available from the CVISN Web site http://www.jhuapl.edu/cvisn/. The CVISN Glossary (Reference 1) provides definitions of terms and abbreviations used in this document.

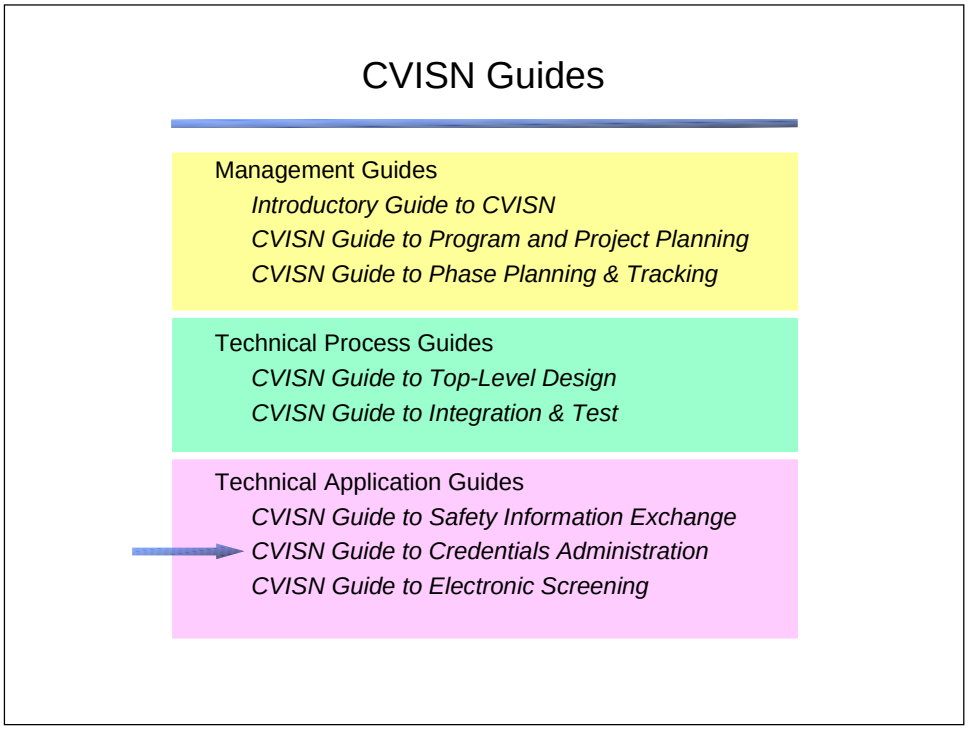


Figure 1–1. The CVISN Guide Series

Subsequent chapters of this guide discuss the concepts, systems, development processes, and issues associated with Credentials Administration.

Factors to Consider in Credentials Administration

Some factors that should be considered when working in the credentials administration area are:

- The most critical interface is that between the motor carrier and the state. The state must provide either a person-to-computer interface, such as a Web browser-based interface, or a computer-to-computer interface.
- If a computer-to-computer interface is chosen, an open, X12 Electronic Data Interchange (EDI) interface should be used, unless the state has evidence that customers support another approach, such as eXtensible Markup Language (XML).
- Different types and sizes of motor carriers will have different needs and preferences. It is likely that your state will need to provide both a Web browser- based interface and a computer-to-computer interface to meet all their needs.
- When the CVISN architecture was baselined in 1996, it focused on the use of ANSI ASC X12 EDI transaction sets for carrier – state credentialing interactions. With the explosion of Web services and Internet popularity over the past few years, FMCSA has reviewed its EDI policy and surveyed CVO stakeholders on electronic credentialing preferences (Reference 59). The new policy will be that FMCSA requires that states implement either a person-to-computer or a computer-to-computer interface. FMCSA also recommends that, in the near term (over the next ~2 years), carriers and states use X12 EDI for computer-to-computer interfaces unless the state has evidence that customers support another approach. FMCSA encourages the exploration of XML as an alternative to EDI.
- The area consists of several somewhat independent sub-areas corresponding to each credential. These may be integrated in the state's Credentialing Interface (CI) software, but are generally handled by independent processing systems within the state.
- The development process adopted will need to accommodate the characteristics of legacy systems that process credentials currently. If these systems are commercial-off-the-shelf (COTS) products (as opposed to custom state systems), close cooperation with the product vendors is essential to success. Procurement and subcontract management will be very important components of a successful credentials administration program.
- As time goes on, there should be more solutions readily available off-the-shelf.
- One of the reasons the cost of implementing electronic credentialing remains high is that states do not follow uniform business processes. Even though the International Registration Plan (IRP) and International Fuel Tax Agreement (IFTA) promote some level of uniformity, there is still a lot of room for individual state variation. Joining with other states and associations to standardize credentialing processes and data will help to reduce the cost for all states. This can be done at one level by simply studying and adopting the processes of another state that has already implemented electronic credentialing. Hopefully as time goes on, state associations like the American Association of Motor Vehicle Administrators (AAMVA), IFTA, Inc. and IRP, Inc. will set up mechanisms to allow states to come together for the purpose of defining more uniform credentialing processes.

- It is important for states to establish the habit of monitoring external events as the project proceeds. The CVISN Deployment Workshops are intended to provide a snapshot of the "CVISN world status", but time marches on and things change. The project manager should identify useful Web sites and points of contact to monitor key external factors that may benefit (or harm) the project. Some examples of these are:

  - Status of EDI standards and implementation guides
  - IRP and IFTA Clearinghouse status
  - Status of vendor credentialing products
  - Development of new technologies and related implementations such as the eXtensible Markup Language (XML)
  - Progress of credentialing efforts in other states
  - Activities of state associations such as AAMVA, American Association of State Highway and Transportation Officials (AASHTO), IFTA, Inc. and IRP, Inc.
  - Reports such as the National Governors Association's State Fiscal Implications of ITS/CVO Deployment (Reference 51) and Booz-Allen & Hamilton's ITS Field Operational Test Cross-Cutting Study Commercial Vehicle Administrative Processes (Reference 52)

This Page Intentionally Blank

2. WHAT IS CREDENTIALS ADMINISTRATION?

Operating a commercial vehicle in the United States requires many "credentials." A **credential** is some form of evidence of meeting specified qualifications. Vehicles must be titled and registered. Some credentials are required for carriers, vehicles, or drivers that will operate only within a single state (intrastate), and different credentials are required for those that will be operate in multiple states (interstate). Carriers must have adequate liability insurance and be authorized to carry certain types of "cargo" (e.g., hazardous materials, people, and household goods). Special permits are required to operate vehicles that are over the standard legal weight or size. Drivers must be licensed to drive whatever size vehicles they intend to operate, and must meet medical standards. Carriers must pay fuel taxes for operating vehicles in each jurisdiction. Some states have additional credentialing requirements.

States have reached agreements on vehicle registration and fuel tax payments for interstate operators. These are called "base state agreements." According to the IRP, the states agree that a vehicle registrant can file with a "base state," and receive one license plate and cab card. The base state will charge the registrant the sum of the fees due to all states in which the vehicle operates, based on miles driven in each state. The base state sends apportioned fees to other states. The IFTA is a similar arrangement in which a carrier files quarterly fuel tax returns with a base state on its operations in all states. The base state apportions the fuel taxes to the appropriate jurisdictions. All mainland states in the U.S., as well as some Canadian jurisdictions, are part of the IRP and IFTA.

Credentials administration comprises:

- all aspects of applying for, reviewing, and granting commercial vehicle credentials; paying the associated fees
- filing returns on fuel taxes, paying the associated taxes and fees
- managing information about credentials and tax payment status, providing information to users
- supporting base state agreements and associated fee payment reconciliation

The regulatory requirements associated with credentials administration include:

- registering to operate as a motor carrier
- having the required liability insurance
- registering and titling vehicles
- paying fuel taxes
- applying for special oversize/overweight permits
- applying for special hazardous materials hauling licenses and permits
- paying Federal heavy vehicle use tax
- complying with other state-specific regulation

In discussions about CVISN projects, Credentials Administration is usually split into three segments: electronic credentialing, interstate credentials data and fee exchange, and interagency (within your state) credentials data exchange. Figure 2–1 shows an overview of the Credentials Administration processes, focusing on the responsibilities of the major stakeholder groups, and the kinds of information exchanged.

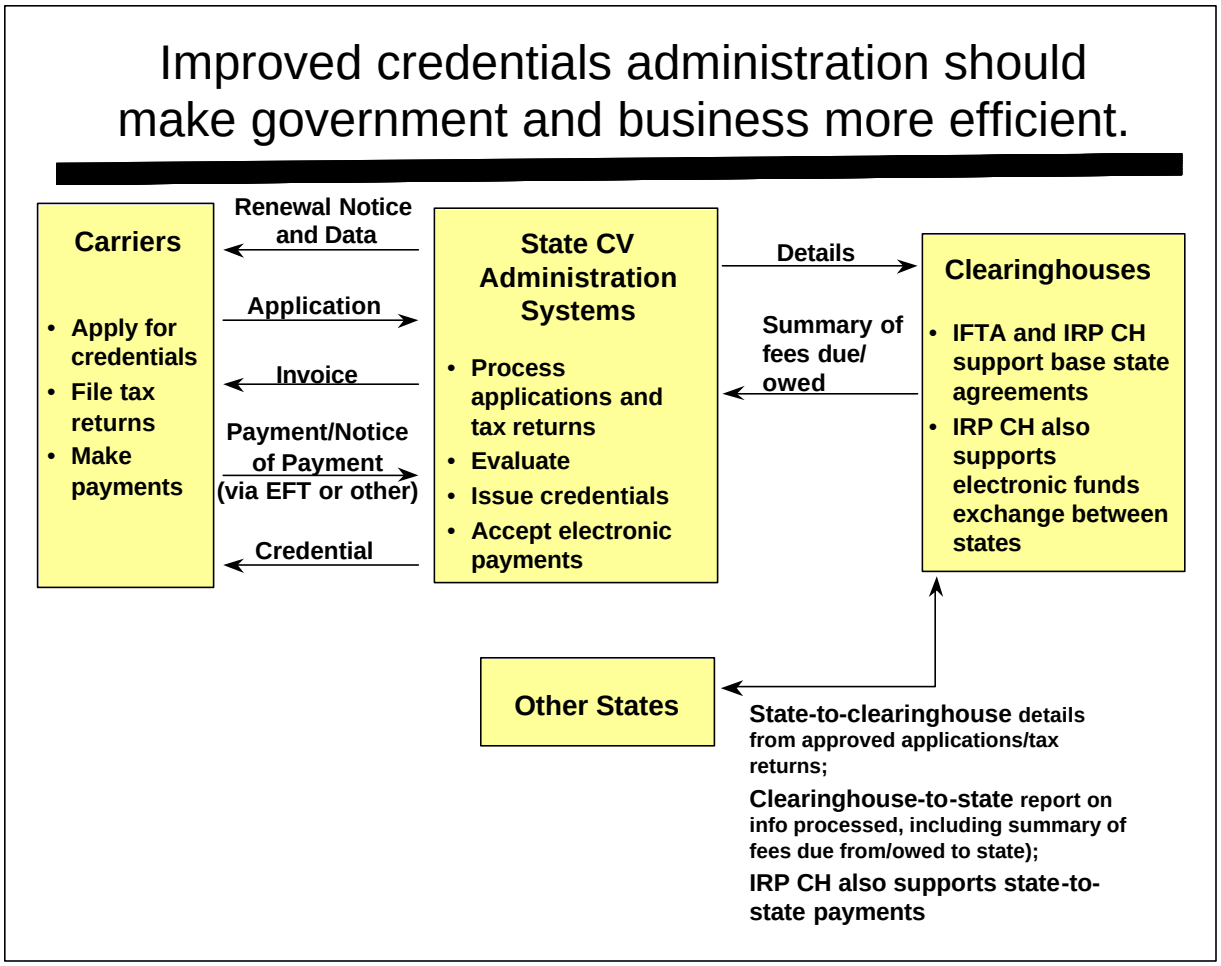


Figure 2–1. Credentials Administration Overview

2.1 Electronic Credentialing

A **credential** is some form of evidence of meeting specified qualifications. It is issued by an authorized source and it entitles the holder to specified rights, privileges or authority. Today, most credentials are issued in paper form, with supporting records on file in the issuing jurisdiction's system. An electronic credential is an electronic record of the credential.

The authoritative source for an electronic credential is the issuing agency. The holder of the credential may be issued an electronic copy that represents the same authority as today's paper copy.

Electronic Credentialing is defined to mean an operational process that uses software under the applicant's control to send credentials applications (including fuel tax returns) to the state, and to get electronic notification of credentials status in return. When feasible, the credential itself is returned electronically. Electronic payment is an option associated with electronic credentialing.

2.2 Interstate Credentials Data and Fee Exchange

To support base state arrangements, states must collect fees from operators, apportion the fees collected to other states according to pre-determined criteria, and transfer funds to those states accordingly. To facilitate that process, clearinghouses have been developed for the IRP and the IFTA. The IRP and IFTA governing documents are listed as references 11 and 12.

A state also exchanges interstate credentials data with other states through Safety and Fitness Electronic Records (SAFER) snapshots. Snapshots contain limited identifier/census, safety, and credential information. Snapshots are used primarily by systems to support making quick decisions. Each state is responsible for maintaining the credentials information in the carrier and vehicle snapshots. The CVISN states, to date, have chosen to implement a state Commercial Vehicle Information Exchange Window (CVIEW) system that collects information from the state credentialing systems. CVIEW then forwards the credentials snapshot segments to SAFER. SAFER distributes the snapshot data to subscribers.

2.3 Interagency (Within Your State) Credentials Data Exchange

Typically, different state agencies need access to credentials information. For instance, before a vehicle is registered, it must be titled. Before a carrier is issued a HazMat permit, it must be authorized to operate in the state. Roadside officers often help enforce credentials regulations by issuing citations to those who are operating without the proper credentials.

Credentials information is exchanged within the state via snapshots (and CVIEW) or by direct interaction among state systems.

Figure 2–2 illustrates the vision for handling CVO electronic business transactions by the Year 2005. It is envisioned that by then, the vast majority of credentials administration business transactions will be handled electronically.

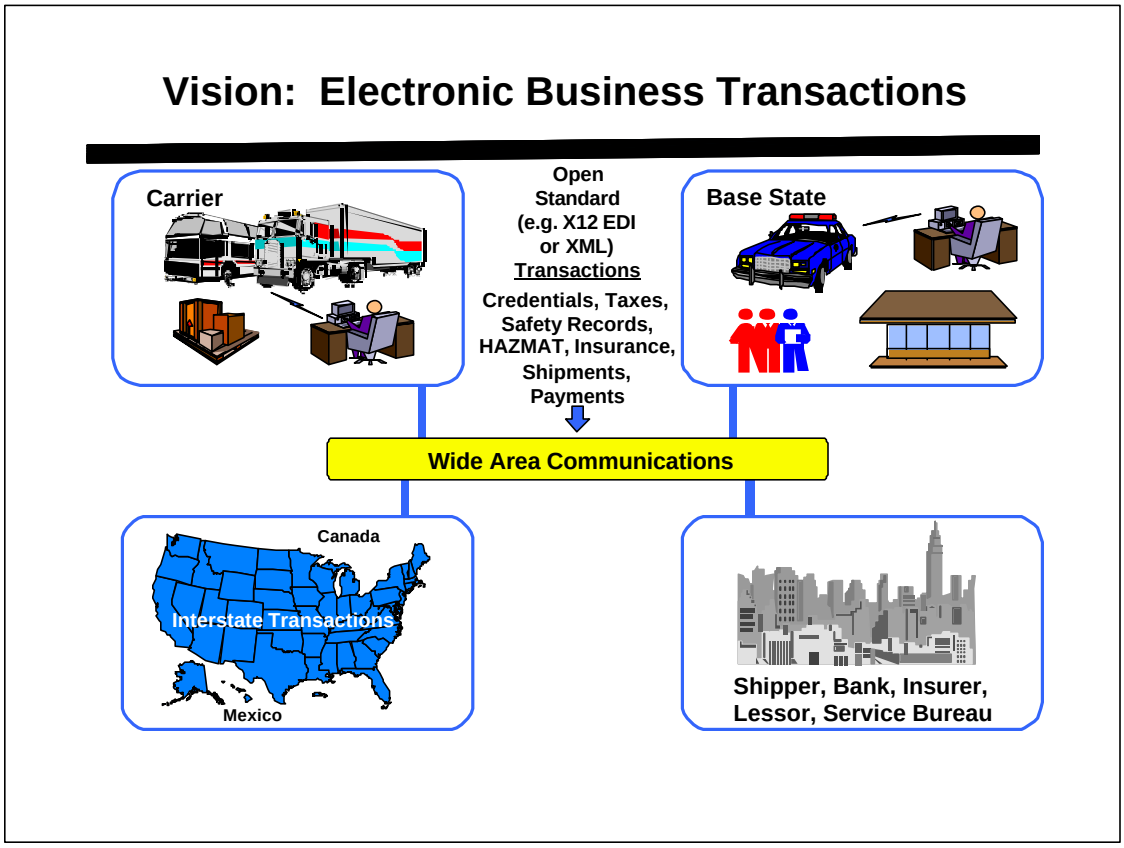


Figure 2–2. Vision: Electronic Business Transactions

2.4 Electronic Screening Enrollment

Electronic screening (e-screening) is the application of technology to make more informed screening decisions. Properly implemented, electronic screening results in improved traffic flow, focuses vehicle inspections and ultimately achieves the goals of increased safety and reduced operating costs. Prior to participation in e-screening programs, the carrier, vehicle and transponder information must be provided through an enrollment process. When applying to an electronic screening program, the motor carrier may also request participation in other screening programs or states. Strictly speaking, e-screening enrollment is a credentialing operation. However, it is not discussed in this guide, but in the *CVISN Guide to Electronic Screening*, Reference 10.

3. WHAT ALREADY EXISTS?

Key necessary components already exist for the carrier, state and CVISN core infrastructure systems. These include legacy credentialing systems, communications systems to exchange information, Internet capabilities, and Web sites to distribute information. In addition there are commercially available products that support CVISN in terms of data mapping and translation between systems. The following sections provide a summary of products used by carriers, states, and the CVISN core infrastructure, plus a summary of the data interchange standards that are the backbone of the CVISN architecture.

3.1 Products Used By Carriers/Applicants

Many large carriers already use sophisticated software packages to support fleet and freight management and administrative functions. Some of those packages assist in the preparation of credentials applications and fuel tax filing.

Service providers offer support for credentials administration to mid-sized carrier operations.

In the future, carriers are expected to be able to obtain CVISN-compatible software from the vendor of their choice. Compliance with the CVISN standards will ensure that it will be compatible with state systems.

An example of a CVISN-compatible software package is the Carrier Automated Transaction (CAT) system. This product allows a motor carrier or service provider to enter credentials applications through a program running on a PC, and then send these applications to the state Credentialing Interface (CI) using a modem, a standard phone line, and, perhaps, an Internet service provider or other network service. The CAT software also processes responses coming back from the CI. FHWA sponsored the proof of concept of PC-based CAT software as part of the Midwest and Southwest One-Stop Shopping operational test projects. States in the CVISN Model Deployment Initiative are sponsoring the development of a CAT for their carriers. For the CAT and CI systems that have been developed to date, all messages passed between CAT and the CI are formatted according to the American National Standards Institute (ANSI) X12 Electronic Data Interchange (EDI) standards. The use of X12 EDI was initially required for the carrier-to-state computer-to-computer interface. However, technology is changing rapidly and the eXtensible Markup Language (XML) has emerged as an alternative to X12 EDI. The use of an open interface standard, other than X12 EDI, is now permissible under the CVISN architecture. Some states that are not already committed to using X12 EDI are now exploring the use of XML, but no CAT software implementing XML is currently available to carriers.

With the development of the Internet and the "information highway," carriers have access to electronic information exchange via e-mail and various communications protocols. States in the CVISN Model Deployment Initiative are sponsoring the development of Web sites for credentialing. The state-operated Web site will interface with the state's credentialing system. A state-operated Web site will allow a carrier to access electronic credentialing services using a

commercial World Wide Web browser. This makes it possible for them to participate in CVISN with on-site desktop computer hardware and general-purpose, user-friendly software, an option that many carriers can feel comfortable with.

3.2 Products Used By States

Most states today have extensive information systems used to process all the credentialing aspects of commercial motor vehicle operations. The state processes the applications with a combination of manual and automated processes. Often some sort of invoicing and payment is involved, which may or may not use electronic payment mechanisms.

Commercial products and service providers are available to support different credentialing activities such as:

- IRP
- IFTA registration and tax filing
- oversize and overweight permitting
- hazardous materials permitting and route planning

CVISN Model Deployment Initiative states are working with commercial vendors to enhance their products to use open interface standards, and are upgrading their home-grown (legacy) credentialing products to support new interfaces and new operational concepts. Most of the existing state systems will fit in with the CVISN architecture with the introduction of either a legacy system interface, or a legacy modification which would allow the EDI or other open standard data format to be translated into a form required by a particular system. Some CVISN states are exploring use of the World Wide Web for electronic credentialing.

In the CVISN prototype effort, the state Credentialing Interface software package (CI) was developed to facilitate the flow of credential data from input (the carrier) to its destination (the legacy credentialing systems). If a state implements a computer-to-computer interface, credential applications may be entered by the carrier through a CAT and sent to the state CI. If a state implements a Web site for credentialing, the application information entered by the carrier via a Web Browser will also be sent to the state CI. The CI provides a single point of contact for receiving all commercial vehicle credentials applications. The functions performed by the CI are these:

- receive, parse, and acknowledge application
- maintain status information on transaction processing
- validate certain aspects of the application data and eligibility of applicant
- check carrier, vehicle, and account information for consistency with data on file
- route data to appropriate legacy systems and translate formats as needed
- route invoices, e-credentials and other transactions from legacy systems back to the carrier system

- manage interfaces with legacy systems
- maintain logs and archives
- display and print application data, transaction status, and log/archival data

Commercial vendors are available to develop and implement state-specific requirements.

3.3 CVISN Core Infrastructure Systems

The Safety and Fitness Electronic Records (SAFER) system collects and distributes snapshots. Snapshots contain safety and credentials information and support safety assurance, credentials administration, and electronic screening activities.

The IRP Clearinghouse supports the IRP base state agreement. The IRP Clearinghouse streamlines the exchange and reconcilement of registration information and fees by:

- enabling jurisdictions to electronically exchange motor carrier and fee information between jurisdictions
- providing an electronic remittance netting function with concurrent Electronic Funds Transfer (EFT) capability through a central IRP bank
- tracking all amounts due to/from a base jurisdiction, from/to all foreign jurisdictions
- providing reports on the information exchanged and netted fees processed

The IRP Clearinghouse uses the AAMVAnet AT&T Global Network Systems Network Architecture (SNA) for communication. Network Job Entry (NJE)/Remote Job Entry (RJE) is used for batch transfer. 3270 terminal emulation is used for interactive inquiries. E-mail or fax services are used for notifying jurisdictions of Clearinghouse updates and issues. To keep the network from clogging, some transfers from jurisdictions to the clearinghouse are done in batches, which can be transferred in approximately two hours over the existing network. Longer transfers are accomplished using removable media. More information about the IRP Clearinghouse can be found at http://www.aamva.org/IRP/public/html/projects/clear.html.

The IRP Clearinghouse is fully operational now. Currently, 19 of the 56 IRP jurisdictions are members of the IRP Clearinghouse; however, 70% of the IRP jurisdictions plan to participate in the Clearinghouse by the end of 2000. Today, there are 15 jurisdictions that are actively participating in the Clearinghouse, electronically exchanging registration information and fees. These fifteen jurisdictions include Arizona, British Columbia, Georgia, Idaho, Kansas, Kentucky, Maine, Maryland, Minnesota, Montana, Nebraska, Nevada, Vermont, Virginia, and West Virginia. Within the next several months Arkansas, Mississippi, New Hampshire, New Jersey, New Mexico, New York and Washington, who have attended the Clearinghouse training, are expected to become active Clearinghouse participants, too. Preliminary discussions are underway regarding implementing a data interface between the IRP Clearinghouse and SAFER.

The IFTA Clearinghouse supports the IFTA base state agreement. The IFTA Clearinghouse was devised to replace paper exchange of data with automated exchange to support business processes. The Clearinghouse will store information regarding carrier demographics and transmittal records. This information will only be shared by participating jurisdictions, except for reports that will be generated and distributed by IFTA, Inc. The Clearinghouse will also provide readily available information on carriers.

The IFTA Clearinghouse provides a client/server approach using Dial-up communication access methods. The clients will be able to send their files to the Clearinghouse using the File Transfer Protocol (FTP). The upload process will consist of X12 EDI files created at the jurisdiction, then sent to the IFTA clearinghouse database. Jurisdictions will be responsible for updating the IFTA Clearinghouse database with registration and tax filing information on a timely basis. An Open Database Connectivity (ODBC) connection to the IFTA Clearinghouse database is provided to allow ad hoc query/reports capability. In the future, jurisdictions may be able to download an "extract" file containing all demographic data submitted by all participating jurisdictions in X12 EDI format. More information on the IFTA Clearinghouse can be found at the IFTA Web Site http://www.iftach.org/.

The IFTA Clearinghouse went into production in July, 2000. As of mid-July, Maryland is sending daily updates of demographic/licensee data to the IFTA Clearinghouse. Rhode Island and Ohio have also registered to use the Clearinghouse.

The Commercial Driver's License Information System (CDLIS) was developed to support the commercial driver's licensing process performed by the states. CDLIS is a transaction routing (or "pointer") system that permits states to share CDL information. More information on CDLIS can be found at http://www.aamva.org/aamvanet/Driver/appCDLIS.html. CDLIS has been operational since 1992.

NMVTIS is the National Motor Vehicle Titling Information System. The American Association of Motor Vehicle Administrators (AAMVA) is developing this system. The initial focus is not on commercial vehicles. NMVTIS will allow jurisdictions to verify the validity of titles prior to issuing new titles. More information on NMVTIS can be found at http://www.aamva.org/aamvanet/Vehicle/NMVTIS.htm.

3.4 Data Interchange Standards

When the CVISN architecture was baselined in 1996, it focused on the use of ANSI ASC X12 EDI transaction sets for carrier – state credentialing interactions. With the explosion of Web services and Internet popularity over the past few years, FMCSA has reviewed its EDI policy and surveyed CVO stakeholders on electronic credentialing preferences (Reference 59). The new policy will be that FMCSA requires that states implement either a person-to-computer or a computer-to-computer interface. FMCSA also recommends that, in the near term (over the next ~2 years), carriers and states use X12 EDI for computer-to-computer interfaces unless the state has evidence that customers support another approach.

Certain X12 EDI transaction sets are part of the CVISN architecture. The CI and CAT use transaction set (TS) 286 for processing credential applications and returning credentials data. In addition, TS 813 and TS 150 are used for IFTA Quarterly Tax Filing. TS 997 is used to functionally acknowledge that a transaction is received, and to report syntax problems. TS 151 is used as an application-level acknowledgment, and to report problems with tax filings. When the analysis of financial system interfaces is completed, the CI may also be required to process TS 820 for Electronic Funds Transfers (EFTs). The following transaction sets support credentials administration:

	TS 150	Tax Rate Notification
	TS 151	Electronic Filing of Tax Return Data Acknowledgement
*	TS 285	CV Safety & Credentials Information Exchange (snapshots)
	TS 286	Commercial Vehicle (CV) Credentials
	TS 813	Electronic Filing of Tax Return Data
	TS 820	Payment Order/Remittance Advice
	TS 826	Tax Information Exchange
*	TS 824	Application Advice
	TS 997	Functional Acknowledgement

(means primarily used for safety assurance and electronic screening; the transaction sets so marked indirectly support credentials administration since credentialing systems supply information for snapshots)*

Commercial products are available that map standard data formats to and from the format required by the standard, if necessary. For instance a state legacy system interface (LSI) could process a TS 826 message into the format required by a legacy processing system, and re-map the output to a TS 286 to interface with other CVISN components.

Implementation Guides (see references) are available for the transaction sets currently used in CVISN.

This Page Intentionally Blank

4. OPERATONAL CONCEPTS AND SCENARIOS

The term "operational concept" generally means "how a system is used in various operational scenarios". "System" is used here in a broad sense to include people and manual processes as well as automated information, sensor and control systems. New operational concepts are adopted in order to solve a problem in the current operations or to take advantage of new knowledge or technology that enables improvements in current operations.

The operational concepts are related to the guiding principles developed by the stakeholder community. The concepts were derived by first analyzing the user services that discuss how to improve commercial vehicle operations, then interpreting the stakeholder-developed guiding principles, and finally applying knowledge about the state of existing and emerging technologies. The combination of the desired commercial vehicle operations improvements, guiding principles about making those improvements, and the reality of technological advances are reflected in the operational concepts.

CVISN Credentials Administration operational concepts include all aspects of applying for, reviewing, and granting commercial vehicle credentials; filing tax returns on fuel taxes; paying the associated taxes and fees; managing information about credentials and tax payment status; and conducting other state, regional, and federal administrative functions associated with those activities.

Many stakeholders are interested in and concerned with the operational concepts relating to how they will conduct their business. The concepts that support credentialing are designed to complete the credential life cycle electronically. Information necessary to carry out credential administration would be captured, processed, and stored electronically and made available to authorized users over commercially available communication networks. Standard snapshots and reports would be available to review and evaluate the carrier's safety performance and credentials.

4.1 Key Operational Concepts

The *CVISN Operational and Architectural Compatibility Handbook (COACH) Part 1*, Operational Concept and Top-Level Design Checklists (Reference 2), provides a comprehensive checklist of key operational concepts relating to Credentials Administration. The operational concepts should be used to guide the state design process. The credentials administration operational concepts stated in the COACH Part 1 are repeated and further explained here.

- Credential applications and fuel tax returns are filed electronically from Commercial Vehicle Operations (CVO) stakeholder facilities. Carriers may use a Web browser to fill in electronic forms at a state World Wide Web site. Another choice is that the carrier uses a credentialing software package to support electronic credentialing and tax filing. One example of this kind of package is a stand-alone personal computer (PC) product referred to as CAT (Carrier Automated Transactions). A third option is

that the credentialing software is integrated with other carrier operations systems. In all cases, the credentials information is submitted electronically to some state-controlled system.

- Internal state administrative processes are supported through electronic exchange of application data, safety records, carrier background data, and other government-held records. Information exchange is enabled through the use of standards. Many elements of CVO require information about the credentials history for carriers and vehicles. Collecting the most-used information into standard messages simplifies systems since interfaces can be defined once, rather than negotiated between every pair of stakeholders. Credentialing actions may be based, in part, on a review of the safety information available from snapshots. The support of internal administrative processes rests on fostering a communications infrastructure that allows the state to collect data electronically so that it can be passed on to the state's own processing software and data bases with little or no manual intervention. A typical example might be when a carrier's safety record is evaluated during the vehicle registration process using the Performance and Registration Information Systems Management (PRISM) approach. PRISM is a program sponsored by the Federal Highway Administration (FHWA) that seeks to improve safety by linking vehicle registration to acceptable carrier safety performance. An explanation of the relationship between PRISM and CVISN is provided in Section 8. Reference 15 provides more information on PRISM.

Key Operational Concepts for Credentials Administration

- Electronic credentialing & tax filing
- State administrative processes supported by electronic information exchange
- Base state agreements supported electronically
- National electronic access to interstate credentials information
- Access to data controlled
- Able to correct errors
- Fees paid electronically
- Electronic access to administrative processes available from public sites
- Status information available electronically to qualified stakeholders
- Carrier audits use electronic support
- Paperless vehicle concept

- IRP and IFTA base state agreements are supported electronically. The International Registration Plan (IRP) and International Fuel Tax Agreement (IFTA) Clearinghouses were developed to provide electronic support for the exchange of financial information to support IRP and IFTA. The IRP and IFTA Clearinghouses are both operational.
- Credential and fuel tax payment status information for interstate operators is made available electronically nationally to qualified stakeholders. Making the information

available electronically exploits the value of collecting and processing the information electronically. Credentials information is made available through the carrier, vehicle, and driver snapshots maintained by the Safety and Fitness Electronic Records (SAFER) system. While the SAFER credentials information may not be up-to-the-minute, it provides a useful window into credentials information for interstate operators. For absolutely current information, users must contact the authoritative source.

- User access to data is controlled (restricted and/or monitored) where necessary. Information sharing within a single jurisdiction and across jurisdictions using electronic networks is a cornerstone of the Intelligent Transportation Systems (ITS)/CVO initiative. Information systems are only as good as the quality of the data they use. Data must be accurate, current, and safe from tampering or unauthorized disclosure. Authoritative sources are the official repositories for the data. Some information will be sensitive and not all stakeholders can be allowed to have it. The systems must include techniques for controlling access to information so that inappropriate disclosure does not take place.
- Mechanisms are made available for operators to dispute credentials records held by government systems. If errors exist in government-held records pertaining to credentials, standard procedures must be available to note and correct the error.
- Fees and taxes are paid electronically. Electronic commerce allows government administrative systems to streamline the base state agreements, exchanging fees and taxes for interstate operators. Applicants should also be able to pay credential and tax fees via electronic funds transfers (EFTs), debit cards, credit cards, or other electronic means.
- Electronic access to administrative processes and information is available from "one stop shops" in public sites. States or commercial vendors can provide kiosks for carriers who do not own the appropriate computer and communications hardware or software to otherwise access the electronic credentialing capabilities offered by the state. Access to administrative processes and information can be provided via the World Wide Web.
- Credential and fuel tax payment status information for intrastate operators is made available electronically to qualified stakeholders throughout the state. Just as information about interstate operators should be accessible nationwide, information about intrastate operators should be accessible within the state. The use of snapshots provides a common method for sharing key data, whether for intrastate or interstate operators. For the concept to work, some state system equivalent to CVIEW must maintain snapshots for intrastate operators.
- Carrier audits are accomplished with electronic support. Supporting conduct of carrier audits refers to two functions: permitting state administrators to perform electronic scans of state records in selecting candidates for audits, and permitting auditors access to state and carrier records on a particular carrier during the actual conduct of an audit of that carrier.

- The "paperless vehicle" concept is supported; i.e. electronic records become primary and paper records become secondary. Electronic access to credentials information makes it possible to contemplate no longer requiring commercial vehicles to carry copies of credentials and decals on-board. Instead, credentials would be checked and verified electronically. The concept is to support the complete credential life cycle electronically: application, fee payment, credential issuance, revenue distribution, modification, renewal, audit, sanctioning, appeals, and inspection. Data exchanges between the public and private sector are accomplished using formats and protocols defined in open standards. Paper could be produced from the electronic information if and when required.

4.2 Credential Life Cycle

At a relatively abstract level all credentials follow a similar administrative path, which we refer to as the **"credential life cycle."** The recognition of similarity in credentials processing allows unified design of credentialing data interfaces and automated processes. Regardless of the CVO credential involved, many of the processes and functions are the same. Stakeholders in the administration of credentials and the collection of fuel taxes take the following steps.

- **Application** – A user (an "applicant") typically initiates the credentials process by filing an application requesting a particular credential. Often, it is not practical to handle the initial application process electronically. For example, for initial vehicle registration in a new jurisdiction, the new state usually requires that the old license plates must be turned in – a manual process. Also, to embark on electronic credentialing, the state and applicant must establish trading partner agreements, a process that usually involves paper documents and physical signatures. So, electronic credentialing usually starts with renewals or modifications ("supplements") to the initial application.
- **Fee Payment** – Applicants must usually pay a fee, ranging from a nominal administrative charge to a substantial fee or tax, in order to receive a credential. The amount due may be a fixed fee or (as in the case of some taxes) may require complex algorithms to determine.
- **Issuance** – Upon furnishing a proper application and paying the required fee, an applicant receives the credential certifying that these requirements have been met. The credential may be a certificate, a sticker, a stamp, or a plate, and in the future it may be a remotely accessible electronic record. In some cases, the state may issue controlled credential stock to a trusted agent, and allow the agent to print the actual credential.
- **Revenue Distribution** – When a jurisdiction acts as a base state it collects fees and taxes for all other participating jurisdictions within which the applicant will operate. These collected funds must be properly disbursed to the other jurisdictions, together with records that allow tracking funds, and permit each jurisdiction to determine whether carriers and vehicles are properly registered to operate within its borders.

- **Modification** – Most systems for administering credentials include some method for modifying information on record to reflect changes in an applicant's circumstances. Depending on the nature of the change, the applicant may be required to remit additional fees, no fee, or be entitled to a refund.
- **Error Correction –** Jurisdictions must provide some method for applicants to review and correct credential-related information held by the jurisdiction. State or Federal freedom of information legislation may apply.
- **Renewal** – Almost all credentials have a finite period of applicability after which they must be renewed if they are to remain valid.
- **Audit** – Most systems for administering credentials have some provision for physically checking historical records of selected applicants to verify that information used to secure credentials is accurate.
- **Sanctions** – Systems for administering credentials provide for sanctions of applicants who fail to properly register and pay fees as required. Possible sanctions include levying fines, placing vehicles out of service, revocation of a carrier's authority to operate, and prosecution.
- **Appeals** – Most systems for administering credentials provide applicants a mechanism to appeal fee determinations and sanctions that they believe to be incorrect or unjustified.
- **Roadside Inspection** – Credentials are distributed (in paper or electronic form) so that regulatory agents and law enforcement officers can establish whether or not vehicles operating in their jurisdiction have properly obtained all required credentials.

Starting with this basic life cycle in mind, it is often easier to see the common processes and establish common design approaches as operational scenarios for particular credentials are developed.

4.3 Operational Scenario

The expected benefits resulting from applying the credentialing concepts are more efficient and responsive administrative processes for carriers and government agencies. It has been estimated that the cost of compliance with regulations for both carriers and government may be as high as $6B annually. Prior to CVISN deployment, the estimated time to register a vehicle in the state of Maryland, from start to finish, finish being defined as when the vehicle is legal to operate, was reported to be 4 to 7 business days. This time has been reduced to roughly 15 minutes per vehicle.

A state must develop or otherwise acquire new systems and modify some existing systems to implement the CVISN Level 1 capabilities. There are many ways to do this and still be in conformance with the architecture and standards. Chapter 6 illustrates several approaches to electronic credentialing that are consistent with the architecture.

Regardless of the design approach chosen, all states need to model their intended business processes in a way that is easy for all stakeholders to review and understand. The functional thread diagram is the tool recommended to illustrate operational scenarios.

This section depicts an example functional thread diagram. The scenario chosen is one of the CVISN Level 1 capabilities. **The high-level CVISN Level 1 operational scenarios related to Credentials Administration functions are listed below:**

- accept and process electronic IRP credential applications for supplements (e.g., adding a vehicle to an existing account)
- accept and process electronic IRP renewal applications
- accept and process electronic IFTA credential applications for supplements (e.g., changing ownership)
- accept and process electronic IFTA renewal applications
- accept and process electronic filing of and payment for IFTA quarterly tax returns

For each of the scenarios, it is sometimes useful to divide the steps in the scenario into these three subgroups:

- interact with the applicant electronically
- maintain snapshots for interstate operators by providing credential data for carriers and/or vehicles based in your state to SAFER
- connect to the appropriate clearinghouse to support the base state agreement

It is often more convenient to test the implementation of the scenarios in the shorter subgroups of steps.

The operational scenarios related to enrolling in one or more electronic screening programs are included in the *CVISN Guide to Electronic Screening*, Reference 10.

The example operational scenario illustrates the first operational scenario in the list: an IRP Supplement for a carrier adding a vehicle to its fleet. The method used to demonstrate the scenario is called a "functional thread diagram." The activities in the scenario are listed as steps. To differentiate between different time schedules, numbers are used to show the interaction between the applicant and the state, and the state's update of snapshots. Those interactions occur as soon as possible after the supplemental application is received by the state. Letters are used to show the state's connection to the IRP Clearinghouse, since that occurs at a regular period instead of being triggered by the carrier's supplemental application.

A diagram corresponding to the steps listed is presented in Figure 4–1 for a graphical view of the scenario. The lines represent data flow between products, with arrows indicating the direction of flow. Each line is labeled with a number or letter. The complete set of lines constitutes a thread of activities that accomplish a function. Hence, the diagram is called a "functional thread diagram."

The IRP Supplement "Add Vehicle" scenario addresses three areas: transactions between the motor carrier and state agencies, transactions among agencies within the same state including the update of snapshots, and transactions among state agencies and the IRP Clearinghouse. This example is loosely based on Maryland's design. The state uses a commercial product to support IRP processes. The state has contracted the implementation of a Credentialing Interface (CI) software package to interact with the carriers' credentialing software. In this example, the carrier uses a CAT product whose development is being sponsored by the state. The state is also implementing a CVIEW software package to provide snapshot segment updates to SAFER. Please see Reference 14 for more information about snapshots.

4.4 Example Operational Scenario: IRP Supplement, Add Vehicle

1. Carrier enters an IRP credential application via a Carrier Automated Transaction (CAT) system which submits it to the Credentialing Interface (CI) as an EDI X12 TS 286.
2. The CI submits a query to its state database to perform preliminary checks as part of evaluating the application.
3. The state database reports the status, i.e., flags and condition to the CI.
4. If a satisfactory status is received, the application is sent to the IRP system for processing via EDI X12 TS 286.
5. The IRP system processes the application and sends an invoice notice to the CI via EDI X12 TS 286.
6. The CI sends the invoice notice to the CAT via EDI X12 TS 286 and maintains archival/audit copies of all transactions.
7. The carrier reviews the invoice data and verifies that the application data matches the intent. The CAT sends payment method information to the CI via EDI X12 TS 286.
8. If a Temporary Authority (TA) is requested, the CI releases it to the CAT via EDI X12 TS 286.
9. If a TA was granted, the CI sends a vehicle snapshot segment update to CVIEW via EDI X12 285.
10. CVIEW sends updated snapshot data to SAFER via EDI X12 TS 285.
11. CVIEW sends updated snapshot data to Roadside via EDI X12 TS 285.
12. SAFER sends updated snapshot data to subscribers via EDI X12 TS 285.
13. The CI verifies payment method information (financial system interfaces are not shown) and passes payment approval to the IRP system via EDI X12 TS 286.
14. The IRP system validates payment amount and updates application status to indicate the permanent credential granted and notifies the CI via EDI X12 TS 286.

15. The CI passes the permanent credential to the CAT via EDI X12 TS 286. Cab Cards may be printed in the carrier's office or state office.
16. The CI updates CVIEW with permanent credential information via EDI X12 TS 285.
17. CVIEW sends updated snapshot data to SAFER via EDI X12 285.
18. CVIEW sends updated snapshot data to Roadside via EDI X12 285.
19. SAFER makes updated snapshot data available to subscribers via EDI X12 TS 285.

A. Periodically (daily), the IRP system sends updates to the IRP Clearinghouse on IRP registration information and fee payments (recaps).

B. Monthly, the IRP Clearinghouse makes available the fee information (pre-netting transmittals) to the participating jurisdictions for approval and/or correction. Today, the states review the information interactively using terminals. In the future, it may be possible to receive the transmittals using EDI TS 286. If an EDI interface is provided, the interaction will occur with the CI.

C. The IRP Office and also other participating jurisdictions report back to the IRP Clearinghouse the approvals or corrections. Today, the approvals/corrections are made via terminals. In the future, it may be possible to use TS 286. If an EDI interface is provided, the interaction will occur with the CI.

D. The IRP Clearinghouse performs the actual netting and makes available corrected/approved vehicle and fee actions (post-netting transmittal) and netting results (remittance netting reports) to the participating jurisdictions. Today, the information is reviewed via terminals. In the future, it may be possible to use TS 286. If an EDI interface is provided, the interaction will occur with the CI.

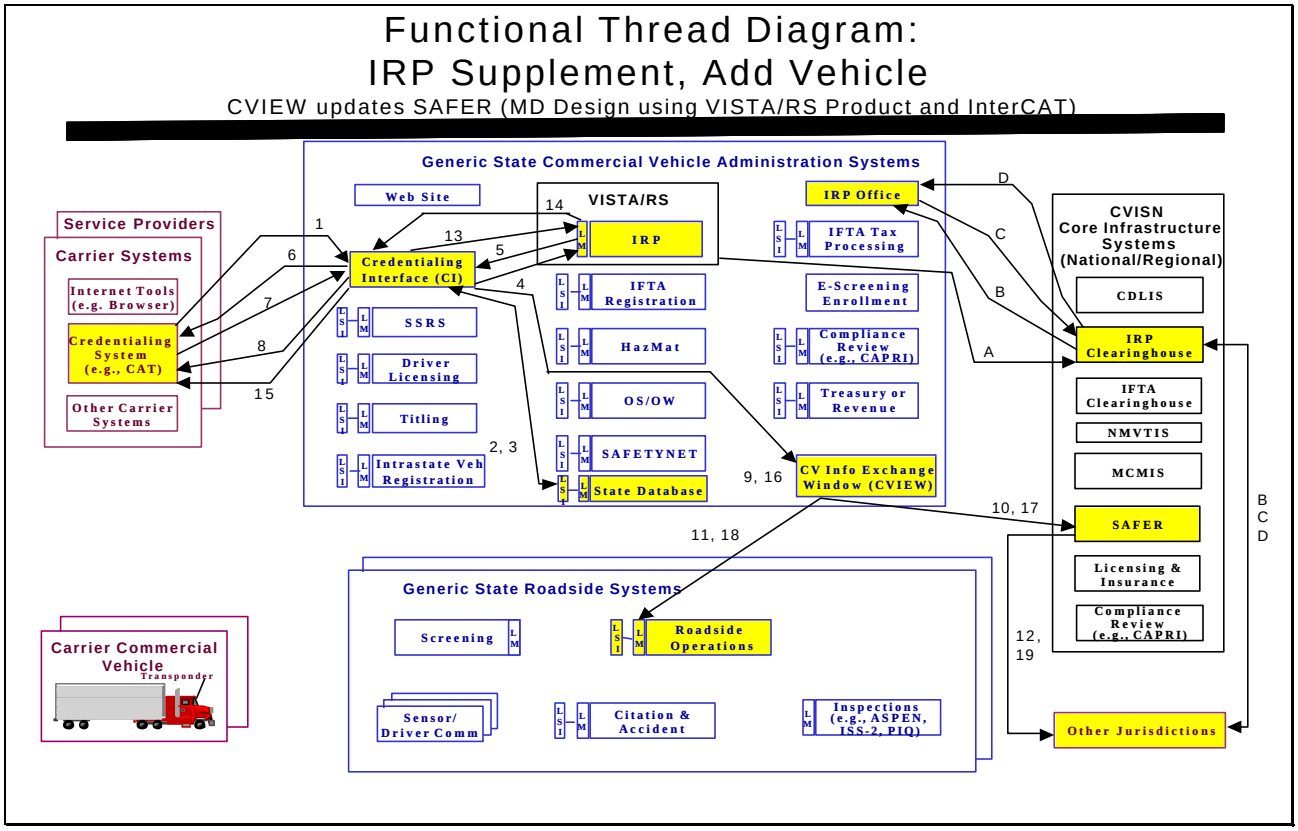


Figure 4–1. Functional Thread Diagram: IRP Supplement, Add Vehicle

NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. Content errors in a received TS 286 are noted by also replying with a TS 286. The results of processing an incoming TS 285 are reported via TS 824.

Additional examples of operational scenarios and functional thread diagrams are in Appendix C. They are included for reference, and as starting points for states that plan to implement similar processes.

A list of scenarios geared to interoperability testing CVISN Level 1 capabilities is shown in Table 4–1. The list shows details such as different kinds of supplemental credentials. Interaction between the state and the clearinghouses is listed separately from interaction between the state and the carrier for testing purposes. Error handling scenarios are not included in the table, but must be addressed as part of the design process. A state may need to add scenarios to address additional functions. More information about interoperability testing can be found in Section 7 and in References 6, 26-28, and 65.

Table 4–1.
Credentials Administration Scenarios for Interoperability Testing

Scenario
Accept & process electronic IRP credential applications
* IRP Supplemental: Add Vehicle - *pairwise and end-to-end*
* IRP Supplemental: Add Jurisdiction - *end-to-end*
IRP Supplemental: Delete Vehicle
IRP Supplemental: Change Unit Number
IRP Supplemental: Change Weight
IRP Supplemental: Replacement Credential
IRP Supplemental: Transfer Plate
* IRP Renewal - *end-to-end*
IRP Trip Permit
Reconcile IRP fees state-to-state through IRP Clearinghouse
IRP Pre-Netting Transmittal
IRP Post-Netting Transmittal
IRP Remittance Netting
IRP Recaps
IRP Recap Correction
Accept & process electronic IFTA credential applications
IFTA Supplemental: Change Ownership
IFTA Supplemental: Add Jurisdiction
* IFTA Renewal - *pairwise and end-to-end*
IFTA Trip Permit
Transmit IFTA information from carrier IFTA credential application to IFTA Clearinghouse
IFTA Demographic Information
Accept electronic filing of and payment for IFTA quarterly tax returns
* IFTA Quarterly Tax Filing - *pairwise and end-to-end*
IFTA Tax Return Correction
IFTA Copy of Tax Return
Retrieve tax rates from IFTA, Inc.
Get IFTA tax rates
Transmit IFTA tax payment information to IFTA Clearinghouse
IFTA Transmittals
Check IFTA Clearinghouse data
IFTA demographic data
IFTA transmittal data

Tests denoted by "*" have been included in the *CVISN Interoperability Test Suite Package, Part 2 - Test Cases and Procedures* (Reference 27). The type of test, pairwise and/or end-to-end, is also indicated for implemented tests.

5. CRITICAL DECISIONS

In this chapter, we identify some of the decisions that are critical to successful implementation of CVISN Level 1 credentials administration functions. The chapter is intended to serve as a checklist to remind states about some of the major planning and design issues they should settle as early in the process as possible. Other decisions may be just as critical for a given state; this list reflects the critical credentials administration-related decisions commonly faced by states implementing CVISN Level 1.

5.1 Design Decisions

The decisions listed below are categorized as "design" because they have a significant impact on the design approach. They all impact planning as well.

For which credentials will the state implement electronic credentialing?
IRP and IFTA credentialing are part of CVISN Level 1. Many states also choose to implement intrastate vehicle registration, single state registration system (SSRS), titling or other credentialing functions as well.

Are there some parts of a credentials process where automation is impractical or the benefit of automation isn't worth the cost?
For example, it may be impractical to automate every single aspect of the IRP registration process in your state. You may have some legal requirements to have a signature on file or other supplemental paperwork. This transaction may only occur once when a carrier first starts its operation. Automating this may be more trouble than it is worth. So you may want to consider continuing to have initial transactions being manual, while subsequent ones are all automated. You might provide a Web site to give out information on how to go through the first manual step, to make this process easier on carriers. Even if you decide to automate everything completely, you may want to defer automation of some parts of the process until later phases of your CVISN program. Recall that the Level 1 requirements include end-to-end electronic processing for IRP and IFTA, and connection to both the IRP and IFTA Clearinghouses.

Will the state implement a person-to-computer or a computer-to-computer interface for electronic credentialing? Will the state elect to implement both?
The CVISN architecture initially required that an EDI interface be provided so that carriers could submit credentials applications using open standards. That solution suits carriers with sufficient software and hardware capability. Some carriers, however, do not have ready access to credentialing software, and prefer to enter applications through a Web site. Designing a solution that is effective for both the carriers and the state makes sense. Many CVISN Model Deployment Initiative states implemented an X12 EDI interface, using the CAT and CI model, for carrier-state transactions. Some states have deployed credentialing Web sites. Some states have determined that both interface methods are necessary to meet their customers' varying needs, and so are implementing both a Web site and some type of computer-to-computer interface. FMCSA recommends that states survey their stakeholders to determine whether both interfaces would be

appropriate. An example survey, based on the questionnaires used by FMCSA in the recent CVISN Electronic Credentialing Preferences Survey, that a state could use to develop a profile of its carrier and service bureau customers, will be promulgated soon.

If the state elects to implement a computer-to-computer interface for carrier-to-sate transactions, what interface method will be used (X12 EDI, XML, or other)?
FMCSA recommends that, in the near term (over the next ~2 years), carriers and states use X12 EDI for computer-to-computer interfaces, unless the state has evidence that customers support another approach. X12 EDI is a standard for data exchange based on a 20-year history of consensus on data semantics, and is in use by many large carriers in their customer and supplier interfaces. However, FMCSA also encourages the exploration of XML as an alternative to EDI. XML is the hot new technology, which may prove to be cheaper to implement than X12 EDI, for those who are not already using EDI for e-commerce. However, industry-specific standards have not yet been developed.

For each credential, will the state modify the legacy system (LM) to handle the electronic data interchange (EDI) open standards, or translate the incoming transactions in some legacy system interface (LSI) and pass the credential application data to the legacy system in the native form?
Many CVISN Model Deployment Initiative states chose a mixed approach, modifying some legacy systems to handle EDI, and building LSIs for others. A deciding factor is often whether the legacy system is state-owned or whether service is provided by a vendor's product. If a vendor's product provides services, the states have most often elected to have the vendor's product modified to handle EDI. This makes it easier for the state to use different vendors, since the interfaces are defined using open standards.

How will requirements be specified?
Arriving at a specific process and format for requirements definition can be a challenge, especially in the credentials administration area. There are three types of requirements:

- requirements for the whole end-to-end process
- requirements for each product
- requirements for the interfaces between products

As a lesson learned from the prototype states, it is difficult to do a comprehensive, detailed end-to-end requirements specification up front prior to picking software vendors. It takes too long, is difficult to maintain, and the vendors will still need to do their own requirements analysis when they begin to work. A recommended alternative is to do a high level requirements end-to-end specification up front with several key sample scenarios. Then, for each phase, complete the process by defining more detailed requirements for the capabilities to be implemented in that phase. Please see the section on Requirements Specification in Chapter 7 of this guide for further discussion.

How will snapshots be updated to reflect credentials actions?
Many CVISN Model Deployment Initiative states have elected to build a state Commercial Vehicle Information Exchange Window (CVIEW) by starting with the generic CVIEW product developed under FMCSA funding. That generic CVIEW supports EDI interfaces for snapshot segment updates. The generic CVIEW will continue to be made available to any requesting state through the CVISN prototype period, i.e. through 2000. There has also been discussion among some states regarding working together to develop one or more "regional CVIEWs".

If a state uses EDI to send snapshot segment updates to CVIEW, the decision about which state product(s) will send those updates is tightly coupled to the LSI/LM decisions. If the legacy product is being modified to handle EDI, then it makes sense for the legacy product to send the snapshot segment update to CVIEW. If an LSI is being created to avoid modifying the legacy product to handle EDI, then often the state chooses to have the Credentialing Interface (CI) provide the snapshot segment update. In some states, the state chooses to have the CI provide the snapshot segment update in lieu of requiring that the vendor's product make the update. That approach keeps the snapshot update completely under the state's control. The state can also choose to tailor the generic CVIEW to accept non-EDI inputs.

Where and how will snapshots be used in the credentialing processes?
Snapshots were devised to support roadside operations, but work equally well in credentialing processes. States participating in the Performance and Registration Information Systems Management (PRISM) program intend to use snapshots to check the carrier's safety status before renewing vehicle registration. Other uses of snapshots are being considered by CVISN states.

Where will error checks be performed?
Many errors in incoming applications can be detected by software. The earlier the checks are performed, the faster the corrections can be obtained from the submitter. The decision about what error checks to perform and which product should perform each one (CI, LSI, legacy system) is a factor that affects the complexity of each product's development or modification.

How can the state leverage the automation to help with paper forms processing?
Not all carriers will immediately start using electronic credentialing. In Maryland, they are enhancing the impact of the automation by installing CAT-like software in the state credentialing offices so that the state personnel can enter the information from paper forms supplied by the applicants. The CAT-like software performs error checking, and submits the application to the CI, where it is processed like any electronic application.

5.2 Planning Decisions

The decisions listed in this category usually do not impact design as much as they impact the preparation of task lists, assignments, schedules, and budget considerations.

Build vs. Buy?
One of the most important decisions the project team must make is the "build-vs.-buy" decision. What should you buy and what should you get off the shelf? This question needs to be addressed for each subsystem, e.g., the CAT, CI, IRP system, etc. As the decisions are made, keep in mind license considerations for commercial-off-the-shelf (COTS) products.

Will the state update current legacy systems or re-compete/re-develop?
Sometimes a major project like implementing CVSIN is the catalyst to re-evaluate existing systems and address lingering problems. As the design options are considered, the legacy systems in place today and other possible substitutes should be examined. The decision to build a new product (or modify an existing one) using in-state resources, or to contract for the development of a new product (or modification to an existing product) with an outside vendor should take into account the risks associated with each option, the available resources, existing contractual arrangements, and the state's experiences with the current products.

Will the state sponsor the development and deployment of a CAT? Who will provide CATs to early-adopter carriers?
The generic CVISN state design includes a carrier-based credentialing product called a CAT. Many of the CVISN Model Deployment states chose to sponsor the development of a CAT to support their business rules, and then provided that CAT to the carriers participating in the early CVISN deployment. One of the key goals of CVISN is to allow motor carriers to select their own fleet management software that includes some type of "CAT module". However, in the early stages of deployment, it is recommended that states pay for a "model CAT" for their states and provide this to at least a few selected carriers. The state may wish to also use this CAT in branch offices to handle walk-up traffic. This gives the state control of the end-to-end process initially. As this process stabilizes, carriers can begin to use packages of their own choosing as the front end.

When will the state join each clearinghouse?
Some initial and recurring costs, as well as training, should be expected as the state joins the IRP and IFTA Clearinghouses.

Will the state participate in PRISM?
Some PRISM funding may be available. Please see Reference 15 for contact information. In addition, the PRISM processes should be considered as the top-level CVISN design for the state is established.

What are the priorities and sequence for implementing capabilities?
For every state, some priorities and sequences for implementation make more sense than others. Both design and cost factors should be considered when establishing the baseline schedules. The relationship of CVISN activities to other state activities must also be considered. For example, many states were forced to divert CVISN personnel resources to address the Y2K problem. The process of incremental deliveries and testing may be new to some stakeholders. Defining the priorities and development sequence helps everyone understand when each capability will be ready, and what kinds of tests must be executed to verify the delivered components.

Who is the system integrator?
A decision closely related to the build-vs.-buy decision is who will provide the system integration function. System integration refers to the process of integrating each subsystem into the whole, testing the interfaces, testing the functionality, testing the overall flow, and testing for interoperability, performance and reliability. Some alternatives are:

- state builds everything in-house and does the system integration with in-house staff
- state buys some products, builds some in-house, and integrates them with in-house staff
- state hires a system integrator to integrate all the purchased and in-house systems in the credentials area
- state contracts with a system integrator to serve as prime contractor and deliver a complete working system

Should the state have an independent verification and validation (V&V) agent?
Some states have policies that encourage them to hire an independent verification and validation agent to provide an independent technical assessment and guidance as the project proceeds. If the agent has experience from other similar projects, they can be very helpful. They may serve as an acceptance test conductor or witness to ensure independence in the test process.

Sole Source or Competitive Contracting?
Sole source contracting is sometimes selected if the state believes that a particular vendor is uniquely qualified. In some cases, sole source contracts can be put in place more quickly than contracts established through a competitive bidding cycle. Sole source contracting may not be an option since most states require competition whenever possible.

Has the state planned to involve its carriers at each step in the planning process?
Carrier involvement is crucial to project success. Knowing what improvements the carriers in the state are capable of and interested in making helps drive the state's decisions. It is worthwhile for both sides to set realistic expectations about the improvements that carriers and the state can make.

Could other state or local agencies use the CVO data?
Much of the data that is collected under CVISN deployment may be useful to other State and local transportation entities (e.g., traffic management center) outside the CVO community. The state may wish to evaluate the data that is being collected for CVISN initiatives to determine whether sharing the data with other agencies would be beneficial.

5.3 Funding and Contracting Phase Key Decisions

These are issues that must be faced during the funding and contracting phase of the project. They are not unique to credentials administration.

- How much funding is required to complete the project?
- Where will the funding be obtained?
- What type of procurement should be used for each product or service?
- What can be done to expedite procurements?
- What type of incentives and remedial mechanisms should be included in the contracts?
- What software rights should be included in the contracts?
- How can the RFPs be written to assure architectural conformance and interoperability?

5.4 Development Phase Key Decisions

These are issues that must be faced during the development phase of the project. They are not unique to credentials administration.

- How should the initial design be modified based on the experience gained in each phase?
- How should the initial phase plan be modified based on progress actually made in each phase?

6. REQUIREMENTS & DESIGN GUIDANCE

According to the Transportation Equity Act for the 21st century (TEA-21), states using federal funds (Highway Trust Funds) must conform with the National Intelligent Transportation System (ITS) architecture and standards, which include the Commercial Vehicle Information Systems and Networks (CVISN) and International Border Clearance (IBC) architecture and standards. Two Notices of Proposed Rulemaking (NPRM), References 23 and 24, published in the Federal Register, with a comment period extending into August 2000, that propose requirements for meeting this section of the law and accelerating the integrated deployment of ITS. The essence of the proposed rules is to realize these policy objectives:

- Implement TEA-21
- Support key Federal priorities:
  - Integration
  - Interoperability
  - Use of the National ITS Architecture and applicable standards
- Incorporate ITS into existing transportation planning and project design procedures
- Provide flexibility to states by emphasizing architecture and systems engineering process, rather than mandating use of the National ITS Architecture

The *CVISN System Design Description* (Reference 7) illustrates the top-level requirements for Credentials Administration, and shows the generic CVISN state design approach. The COACH Part 3 (Reference 4) takes the COACH Part 1 state credentials-related requirements and allocates them to components of the generic CVISN state design, providing a model for states to tailor.

Recall the high-level definition of CVISN Level 1 as stated in Reference 8:

- automated processing (i.e., carrier application, state application processing, credential issuance, tax filing) of at least IRP and IFTA credentials, ready to extend to other credentials [intrastate, titling, oversize/overweight (OS/OW), carrier registration, hazardous materials (HazMat)]. Note: Processing does not necessarily include e-payment.
- connection to IRP and IFTA Clearinghouses
- at least 10 percent of the transaction volume handled electronically, ready to bring on more carriers as carriers sign up, ready to extend to branch offices where applicable

The final statement in that list is further explained as follows. The intent is that the state will work closely with its carriers as CVISN capabilities are being implemented. To claim that the state is successfully handling IRP and IFTA functions electronically, the somewhat arbitrary figure of 10 percent was selected. The idea is that at least 10 percent of all credentials transactions for which electronic credentialing is offered (at least IRP and IFTA) will be handled electronically once the state has achieved CVISN Level 1. The 10 percent figure should be readily achievable if carriers have embraced the state's approach to electronic credentialing.

The architecture requires that states implement either a person-to-computer or a computer-to-computer interface for electronic credentialing. The options are summarized in Table 6–1.

Table 6–1.
CVISN Guidelines for Carrier-to-State Interface Design

Interface	Design	Technology Choices
Carrier-to-State	Person-to-Computer: • Carrier to Web Site	WWW and Internet standards; HTML or XML
	Computer-to-Computer: • CAT to CI • Fleet Mgmnt System to CI	Open standard (EDI); exploring XML

In this section, we illustrate various approaches for the carrier-to-state interface that conform to the architecture. The options depicted on the following pages do not exhaust the possibilities, but do represent a variety of choices that have been explored by CVISN prototype and pilot states. It is recommended that states survey their stakeholders to determine whether both a computer-to-computer interface and a Web site would be appropriate. Many states are planning to implement more than one option (e.g., a personal computer version of the Carrier Automated Transaction (CAT) software, and a Web site).

Public and private entities may choose to implement additional open standards for electronic credentialing-related functions (i.e., more than those identified on the previous pages).

The architecture may be updated to include use of additional standards, if recommended by a consensus of the stakeholder community. These may include one or more electronic methods of payment [automated clearinghouse (ACH) debit or credit, credit card, electronic funds transfer (EFT)].

6.1 State Operated Web Site for Credentialing

Since its creation in 1992, the World-Wide Web has been the major reason for the acceleration of the growth of the Internet. The Web allows users to interact with documents stored on computers across the Internet as if they were parts of a single hypertext. Hypertext is the organization of information units into connected associations that a user can choose to make. An instance of such an association is called a link or hypertext link.

Technical standards for the Web are now defined by the World-Wide Web Consortium (W3C). The Hypertext Markup Language (HTML) is a standard recommended by the W3C and adhered to by the major browsers, Microsoft's Internet Explorer and Netscape's Navigator. HTML is the set of "markup" symbols or codes inserted in a file intended for display on a Web browser. The

markup tells the Web browser how to display a Web page's words and images for the user. The individual markup codes are referred to as tags. The eXtensible Markup Language (XML) is also a formal recommendation of the W3C. XML is a metalanguage that lets a group of stakeholders create their own customized markup languages for exchanging information. Both XML and HTML contain markup symbols to describe the contents of a page or file. HTML, however, describes the content of a Web page (mainly text and graphic images) only in terms of how it is to be displayed and how the user is to interact with it. XML is gaining in popularity among developers of Web sites.

Electronic commerce in many industries is migrating to the Web-site-based solutions. In the approach depicted in Figure 6–1, a carrier would connect to a state credentialing Web site using a browser and enter the information on the Web-site page(s). An advantage to this approach is that it supports carriers with minimal carrier investment. For small carriers this option appears optimal, but for medium to large carriers the manual data input may not be efficient.

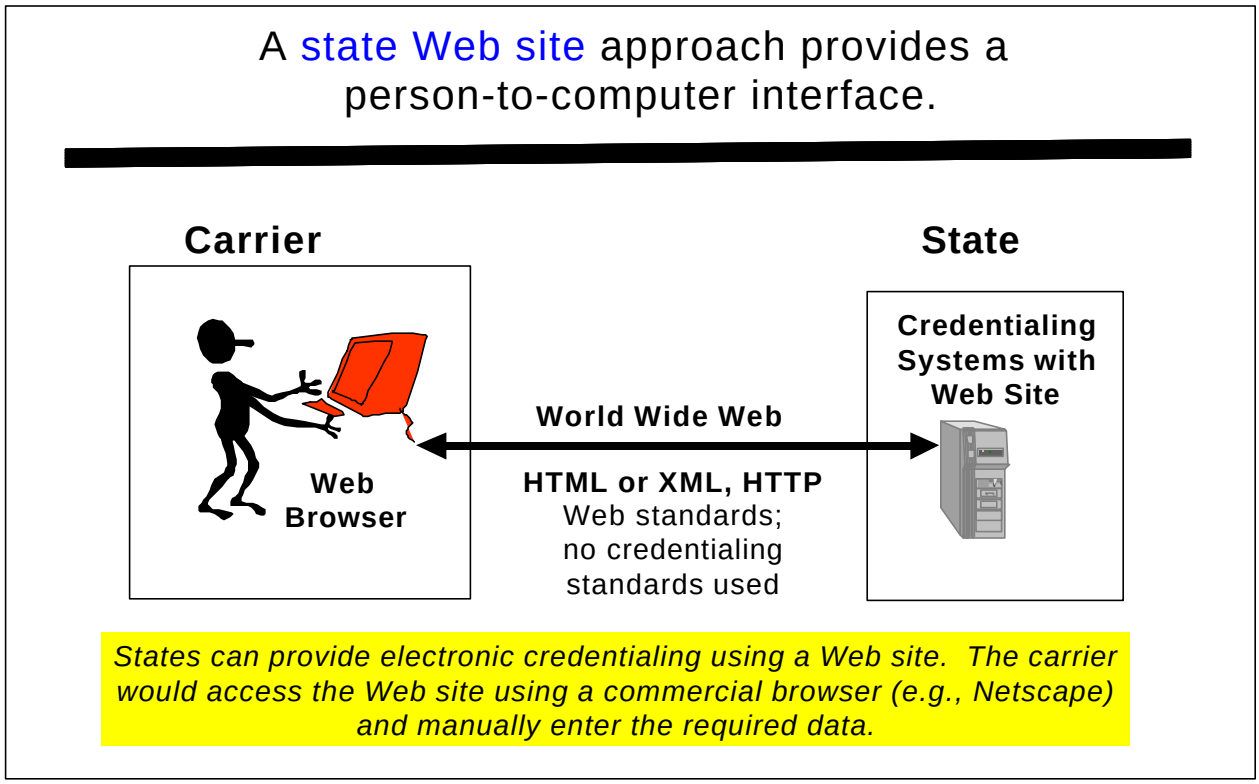


Figure 6–1. State Provides Web Site; Applicant Uses Web Browser

This approach conforms to the architecture if it supports all popular commercial browsers and provides the CVISN Level 1 functionality.

6.1.1 Operational Concept Guidance for Web Credentialing

Following are operational concepts for developing a credentialing web site.

- Review the business process before implementing the Web site. Don't automate a bad process.
- Make it easy for the customer. For instance, after you know who the customer is, populate the screen with information you have in your database. (State law may require that users type in some information, even though the state already knows it.)
- Make your CVO credentialing Web site consistent with other state Web sites. Adopt a common look and feel.
- You may not want to do initial registration for IRP or IFTA over the Web. It's okay to require a visit to the state office to establish an account.
- Provide one entry point for all CVO processes. Make available links to other useful CVO-related sites. This is the concept of a 'portal', that is, a Web site that users tend to visit as an anchor site.
- Provide temporary credentials, if feasible. This serves the applicant's immediate need, while allowing the state to continue checking the application and payment.
- Remain customer friendly. Give email and "live" contact information for urgent questions. Plan for human support as backup.
- Think about security. Put security only where you need it There are many issues and considerations, including:
  - Authentication
  - Levels of access
  - Different levels of privileges
  - Trading partner agreement
  - Access from wireless mobile devices
  - Multiple passwords for an account /company & user categories
  - State privacy laws & restrictions

  See Appendix F for a more detailed discussion of Web security issues.
- Learn from others. For instance, look at some of the highly rated Web sites or textbooks, such as Reference 60, which discusses human factors and web development.

6.1.2 Planning Guidance for Web Credentialing

Planning steps for Web site development are similar to those for any other type of software development.

- Find out what your customers and operations staff want. There is no benefit in implementing capabilities, no matter how elegant, if there is no end user interest.
- Deliver end-to-end capability incrementally. For instance, complete the integration of one Web-based function before you add other Web front-ends.
- Prototype to get feedback. When customers try out the system, they may discover that their requirements are not as they originally thought. The earlier in the process that changes are made, the less expensive they will be.
- Start with something easy (perhaps an easy supplement like Delete Vehicle). Next, move to another fairly easy function, choosing one with high value to your customers (like another supplement - Add Vehicle).

6.1.3 Design Guidance for Web Credentialing

Design guidelines for a Web site for credentialing include:

- Link to other sites for explanatory or background information, rather than replicating it. For instance, link to your on-line Trucker's Handbook to explain IRP, IFTA, etc.
- Check data as early as possible. For instance, check the validity of an identifier as soon as it's entered.
- Use the same "back end" regardless of the input mechanism. For instance, if you support either EDI or Web inputs for IFTA quarterly tax filing, use the same process to determine the tax owed, regardless of whether the return was filed using EDI or the Web. This is depicted in figure 6-10.
- Use the CVISN recommended primary identifiers. The CVISN Architecture recommends that the CVO community use the primary identifiers in all data exchanges and business processes.
- Strive for single entry of common data across all CVO applications.
- Let users back out, correct errors, avoid inadvertently making a duplicate record.
- Include a view to see and print a familiar form (not necessarily to fill it out that way on-line).
- Consider methods to enable users to print credentials, for example, a mechanism to print once.
- Consider providing a "confirmation message" showing the results of the application processing. This could be in computer-readable form, thereby allowing the user to update their database.
- Provide a synchronization report showing everything the state holds about the applicant. This may help carriers maintain consistency between their vehicle database and the state's vehicle database.
- Obey state laws and policies regarding privacy, data protection, etc. For example, it may not be permissible to automatically populate fields on a Web page with certain data, such as the Social Security Number.

- Make key information secure, but be aware that encryption slows down performance. Put security where you need it, and only there.
- Consider higher thresholds/security/access controls for folks with more power (e.g., those who can create accounts).
- Use new technological advances cautiously. Make sure that the techniques you want to use are stable enough, and are supported in the development tool set that you have. For instance, wait until more than one commercial browser has implemented support for a new feature.
- Don't re-invent the wheel. For instance, use standard authentication techniques.

Figure 6–2 illustrates one possible design and shows the firewalls. In this figure, the "Core Credentialing Interface" performs functions such as:

- receive, parse and acknowledge application
- maintain status information on transaction processing
- validate certain aspects of the application data and eligibility of applicant
- check carrier, vehicle, and account information for consistency with data on file
- route data to appropriate legacy systems and translate formats as needed
- route invoices, e-credentials and other transactions from legacy systems back to the carrier system
- manage interfaces with legacy systems
- maintain logs and archives
- display and print application data, transaction status, and log/archival data

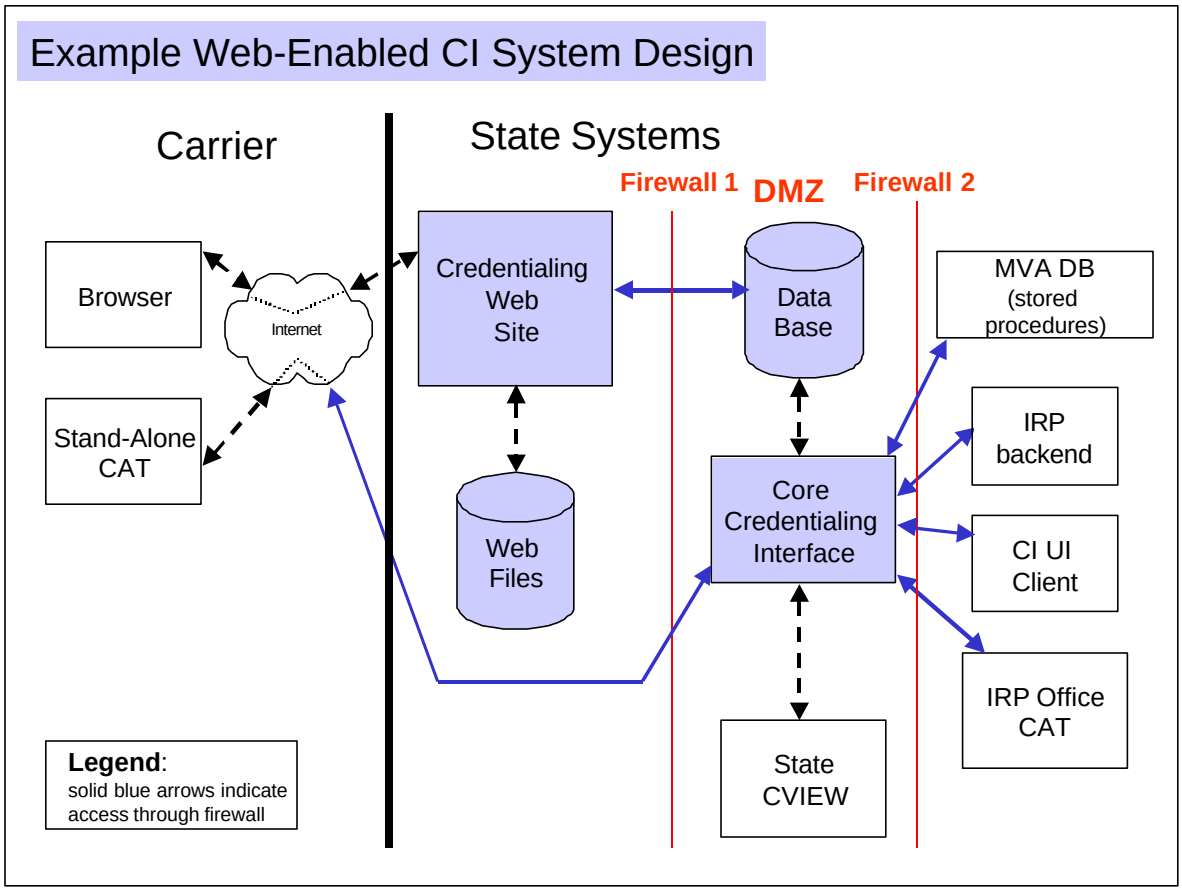


Figure 6–2. Example State System Design Including Credentialing Web Site

6.1.4 Implementation Guidance for Web Credentialing

The guidance in this section applies to implementation of Web sites in general, and is not CVO Web site specific in most cases.

- Decide and advertise what browsers/versions you will support. At least for some period of time after browsers upgrade, offer a backward-compatible, less capable version of your Web site.
- Make the user interface friendly and consistent. For example, always use TAB to go from one data entry field to the next across the page.
- Provide on-line help. Keeping user manuals on-line and accessible via hypertext links is easier and friendlier.
- Provide contact information for off-line help. For instance, tell the user how to report errors in the information they aren't allowed to change.
- Especially during the early stages of deployment, provide a method for users to get help in real time from staff trained in how the Web interface works, and what the business processes and data requirements are.

- Make it easy for the user to perform different functions. For instance, if the user simply wants to correct an error on the last page, make it easy to bypass information that isn't being changed and get to that last page.
- Use Commercial Off the Shelf Software (COTS) whenever possible. For instance, there are COTS products that can help you track usage, instead of writing unique code to meet legal requirements.
- Develop on a different platform than where the real Web site is, for security reasons, and to stay sane.
- Provide different output options depending on the user. For instance, some trusted customers may have controlled stock to print their own cab cards.

6.1.5 Test Guidance for Web Credentialing

Testing the Web site is just as important as testing any other software before release.

- perform rigorous testing before promoting a new build for customer use
- run regression tests to make sure all capabilities work, even the ones you don't think you've changed
- establish "test accounts" so that you don't disturb real customers' data as you test
- test using several different browsers to access the Web site
- ask real users to help with testing
- conduct interoperability tests

6.2 Computer-to-Computer Interfaces

Since the use of open standards is a key architectural concept, it is important that states providing a computer-to-computer electronic credentialing option consider using the identified X12 EDI transactions. It is recommended that, in the near term (over the next ~2 years), carriers and states use X12 EDI for computer-to-computer interfaces unless the state has evidence that customers support another approach. However, eXtensible Markup Language (XML) is a promising emerging technology and the exploration of XML as an alternative to EDI by carriers and states is encouraged.

6.2.1 X12 EDI Computer-to-Computer Interface

ANSI X12 EDI standards and user implementation guides (IGs) define the structure and meaning of computer-to-computer messages passed between trading partners. EDI transaction sets describe data structure, data type, data interdependencies, and data usage. X12 EDI is a standard for data exchange based on a 20-year history of consensus on data semantics. Commercial translators are available for EDI and EDI cost is reduced by using the Internet, rather than a value added network (VAN) to send and receive data. Many large carriers use EDI for e-commerce. From the state's perspective, conformance with the architecture requires an EDI interface for certain state-to-core infrastructure systems.

The EDI transaction sets (TSs) associated with electronic credentialing are:

TS 150	Tax Rate Notification (not required for Level 1)
TS 151	Electronic Filing of Tax Return Data Acknowledgement
TS 286	Commercial Vehicle (CV) Credentials
TS 813	Electronic Filing of Tax Return Data
TS 997	Functional Acknowledgement

Figure 6–3 and the following list summarize the EDI requirements related to electronic credentialing from the COACH Part 4 (Reference 5).

- to conform with the architecture, if the state implements an X12 EDI carrier-to-state interface, a state should accept and respond to X12 EDI standard transactions with the public (286, 813, 151, 997) for CV credentialing.
- to conform with the architecture, if the state implements an X12 EDI carrier-to-state interface, a state should provide invoice data for credentials electronically (using X12 EDI 286 for EDI-based credentialing).
- to conform with the architecture, if the state implements an X12 EDI carrier-to-state interface, a carrier's software product should generate and respond to X12 EDI standard transactions (286, 813, 151, 997).
- to conform with the architecture, if the state implements an X12 EDI carrier-to-state interface, tax rate information should be provided using X12 EDI TS 150 (not required for Level 1)

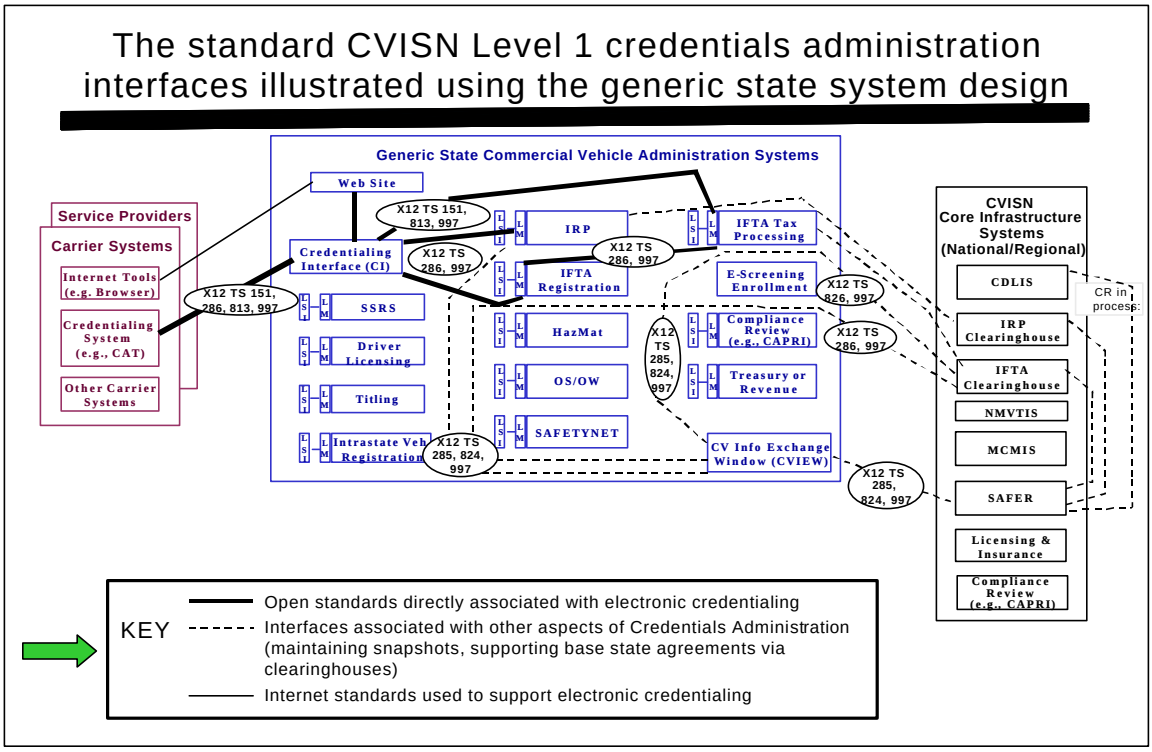


Figure 6–3. CVISN Level 1 Interfaces Related to Credentials Administration

Several documents provided detailed specifications for the EDI interfaces. The applicable standards are contained in the latest version of ANSI ASC Xl2 EDI standards (Reference 17). Application-specific guidelines are found in the implementation guides (IGs) (References 18-21). Individual jurisdictions sometimes have particular business rules that further define how the standard and conventions should be used. Figure 6–4 illustrates the process of defining those jurisdiction-specific EDI constraints/differences.

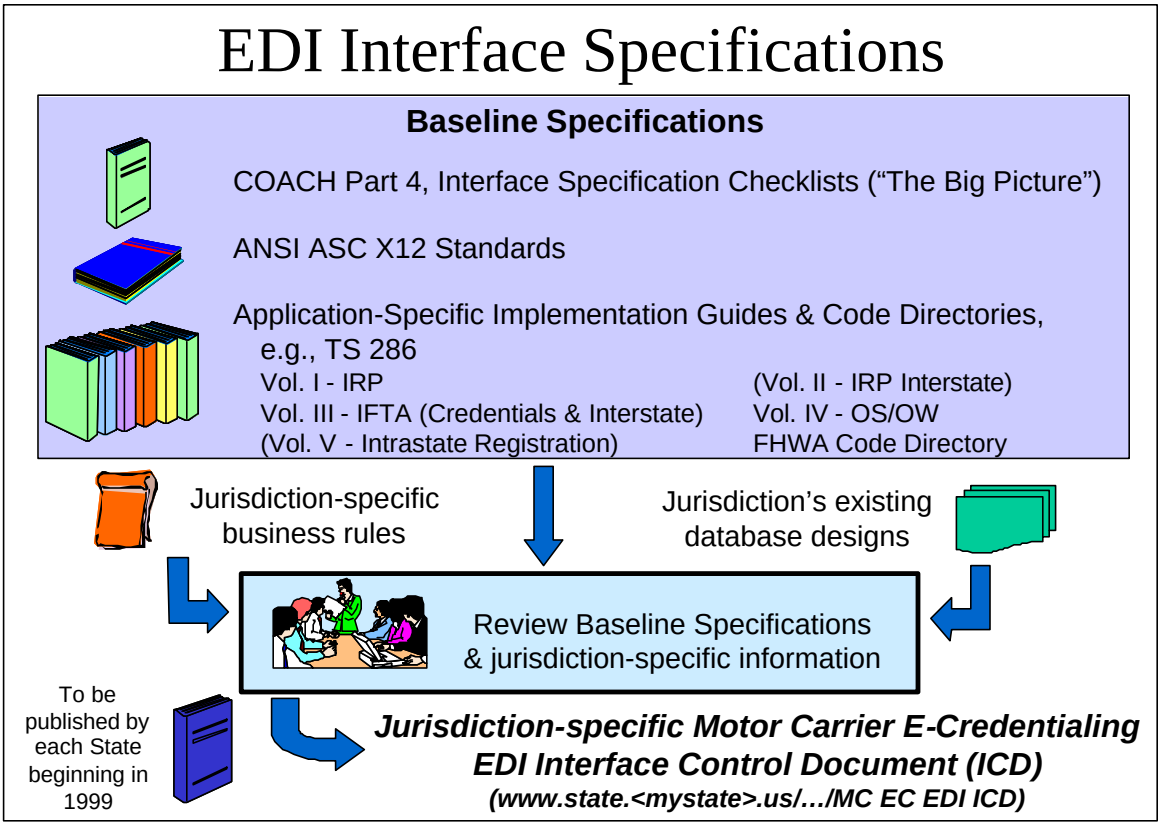


Figure 6–4. Defining EDI Constraints Unique to the State

Each jurisdiction also has unique telecommunications and networking constraints and options. Information about supported protocols, connection methods, security procedures, and configuring individual workstations is necessary to complete the process of developing and installing a system to support electronic credentialing. Figure 6-5 illustrates the process of defining those jurisdiction-specific telecommunications and networking constraints.

Research into data requirements, application processes, and database design is a necessary part of the EDI implementation process. The jurisdiction-specific constraints/differences that have been identified in the CVISN model deployment effort are listed below. The list is intended as a reminder for the EDI developer and for the jurisdiction. Getting a clear picture of these constraints and differences is central to the research process for a jurisdiction. If these topics are

researched adequately, the developed EDI package should meet the jurisdiction's and applicant's business needs.

- Policies
- Validation procedures
- Error-handling protocols
- Credentials issued (temporary, permanent, etc.)
- Data element requirements (optional, mandatory)
- Data element attributes (length, valid codes, etc.)
- Application procedures
- Acknowledgment protocols
- Electronic payment options

The combination of the information provided in the implementation guides and the jurisdiction-specific constraints/differences should be sufficient for developers to build software products that meet users' needs. It is important to note that tailoring the implementation guides to meet a specific jurisdiction's business needs should not include changing the mapping solution that is specified in the IGs.

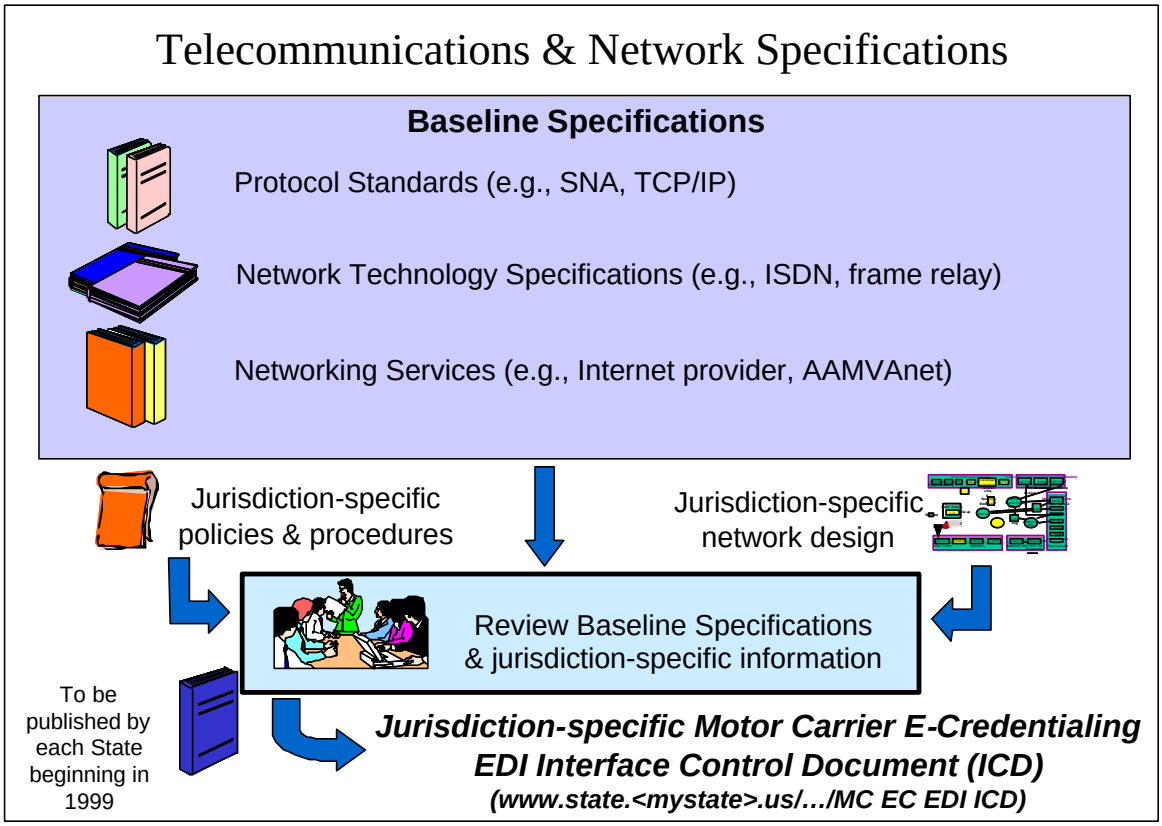


Figure 6–5. Defining Telecommunications & Network Constraints Unique to the State

In the following diagrams, options are presented for a state and its carriers to implement an X12 EDI interface.

The initial implementation of the CVISN architecture was the Carrier Automated Transaction (CAT) system residing on a PC shown in Figure 6–6. A state would accept electronic transactions to the Credentialing System (through the Credentialing Interface (CI)) using EDI standards. A state could also make the PC CAT available for carriers on a walk-up basis at a state's branch offices. The PC CAT solution may be most useful as an interim step during the next couple of years until CAT modules become commonly available as part of Fleet Management System packages.

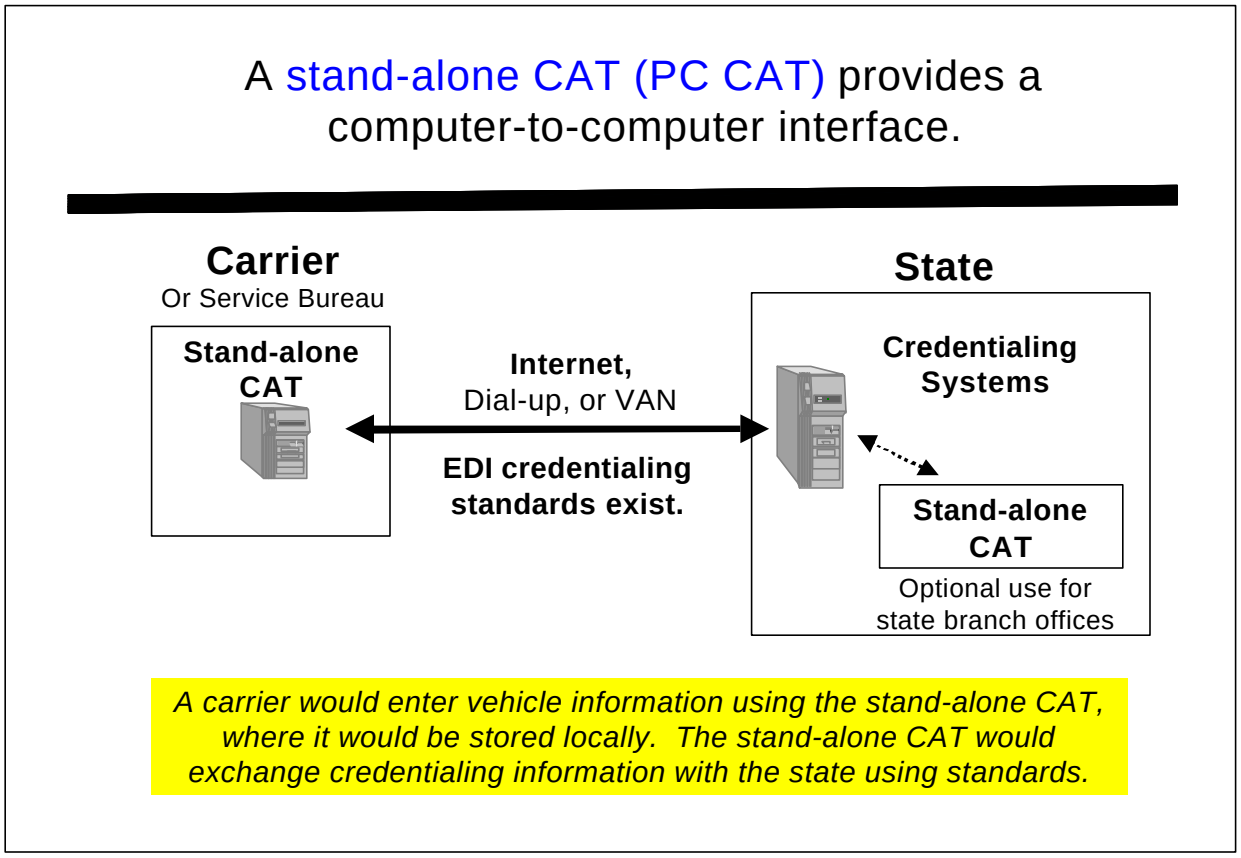


Figure 6–6. State Provides An X12 EDI Computer-To-Computer Interface; Applicant Uses CAT

Typically medium and large size carriers have fleet management software (FMS) systems that support many of the tasks associated with their operations. These systems often exchange financial and billing information using EDI standards. They also contain inventory information on the carrier's fleet of vehicles. Incorporating CAT capabilities into the FMS, as shown in Figure 6–7, would allow the motor carriers to leverage their existing investment in FMS systems by automating and integrating the credentials administration process with other business functions.

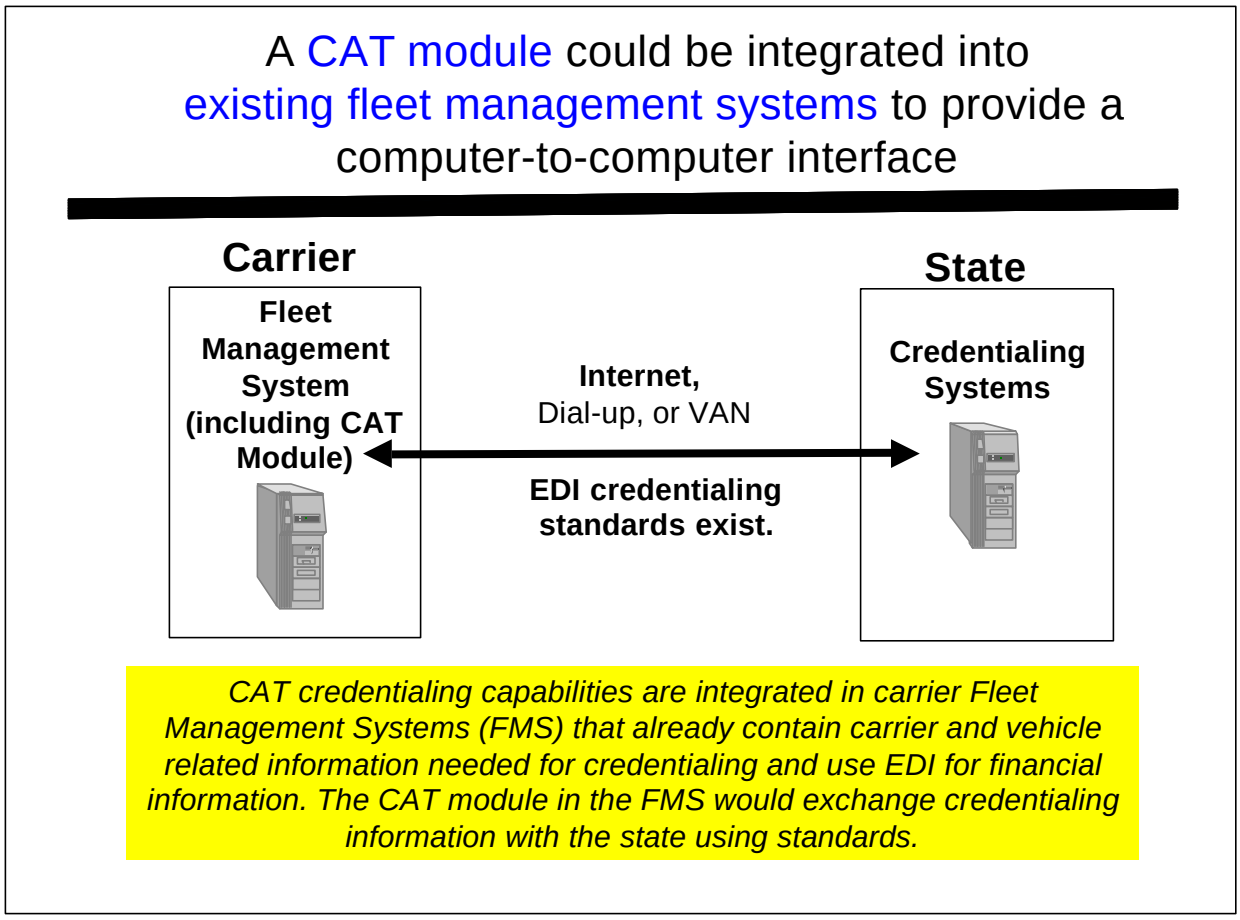


Figure 6–7. State Provides An X12 EDI Computer-To-Computer Interface; Applicant Uses FMS CAT Module

FMS systems may be "home grown", if the carrier is large enough, or they can be purchased from software vendors. Software vendors may see that including automated credentialing capabilities provides a marketing advantage, and develop the CAT capabilities as part of their product. However, it will not be cost effective for a software vendor to develop the software until a sufficient number of states commit to using automated credential transactions using standards; then the development costs can be spread over their customer base.

Integrating credentialing into FMS systems is consistent with CVISN Architecture for computer-to-computer interface, if open standards are used.

6.2.2 XML Computer-to-Computer Interface

XML is a metalanguage for creating a customized mark-up language to describe the structure and content of documents (References 58, 61-64). It is an outgrowth of document publishing and display technologies which is becoming popular in World Wide Web applications. It is a method, not a standard, for data interchange. An XML document alone does not tell you about the data type, data relationships, or meaning of the data exchanged. However, there are associated XML technologies that enhance its power:

- Document Type Definition (DTD): Provides rules for using XML to represent documents of a certain type. Defines the tags used.
- Schema: Goes beyond the DTD and describes meaning, usage, and relationships of data elements. Schemas are likely to replace DTDs in XML applications within a year or two, but standards are still being developed and tools are not available.
- XML Parser: Checks for well-formed XML document (matching tags, proper nesting). A validating parser checks that an XML document conforms to an associated DTD.
- Style sheet: Describes how an XML document is presented or displayed.
- XML Query Language: Notation for addressing and filtering the elements of XML documents.

The CVISN architecture encourages the exploration of XML as an alternative to EDI. Both of the solutions shown for the EDI Computer-to-Computer Interface (Figures 6–6 and 6–7) would conform to the architecture if the carrier-to-state interface were implemented using XML rather than X12 EDI. Figure 6–8 is an example of the FMS CAT approach.

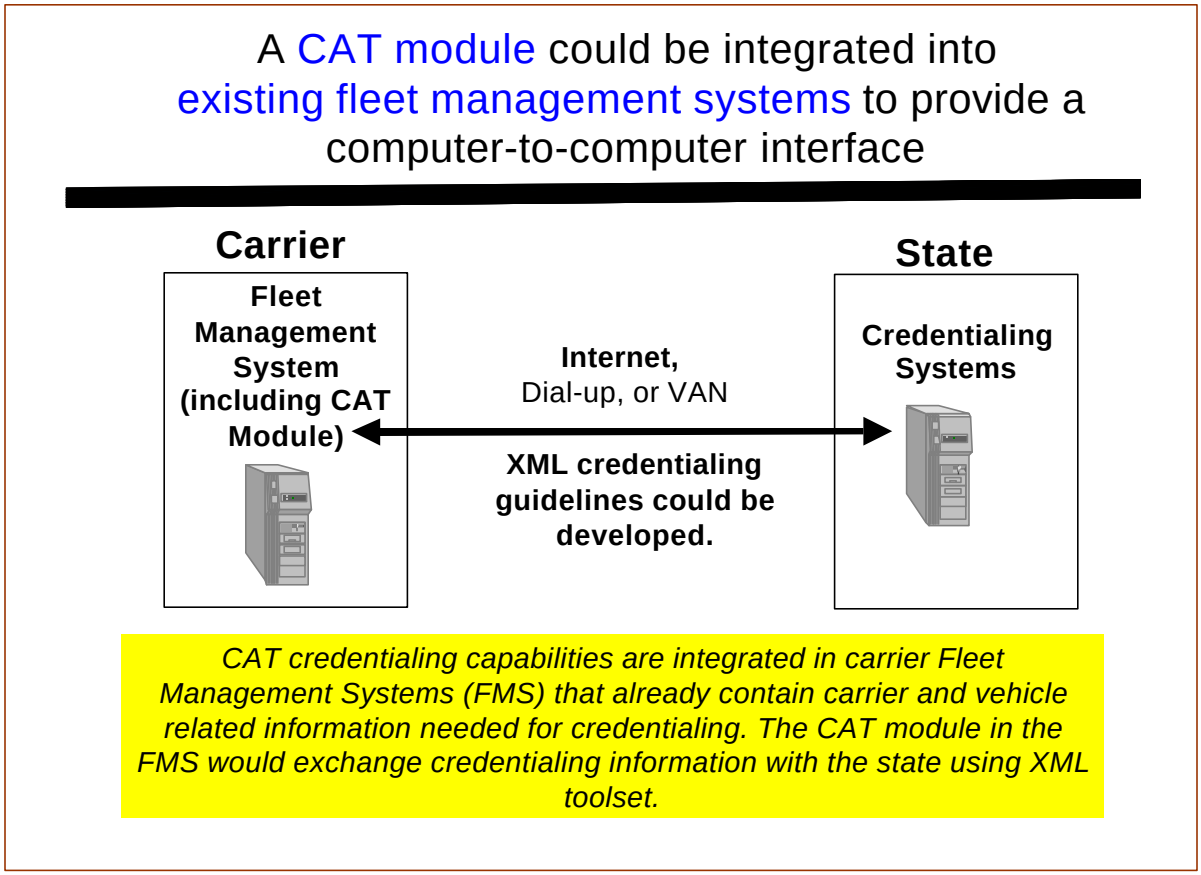


Figure 6–8. State Provides An XML Computer-To-Computer Interface; Applicant Uses FMS CAT Module

XML is becoming a de facto standard. The Organization for the Advancement of Structured Information Standards (OASIS), a nonprofit international consortium dedicated to accelerating the adoption of product-independent formats based on public standards, and the World Wide Web Consortium (W3C) are two of the key organizations involved in developing XML standards. Standards organizations and industry experts are working via the ebXML initiative, endorsed by leading industries and the ANSI X12 Committee, to combine the rich data semantics of EDI with the emerging XML technology. More information can be found at the OASIS website http://www.oasis-open.org/index.html and the W3C website http://www.w3.org/.

XML is a potential alternative approach for CVO information exchange. Using XML for CVISN applications is not likely to require modifications to the XML standard. However, XML and its associated family of tools are still under development. It will be necessary to analyze XML technology and standards and determine how to apply it to CVO applications. For example, mutually defined tags are needed for data exchange and industry-specific DTDs or schemas are required to give the data meaning. There are no guidelines at this time for the use of XML in the domain of commercial vehicle operations, and no equivalent aids to users as the implementation

guides for EDI. Regardless of whether X12 EDI or XML is used to exchange information, developers need to map data from the existing (legacy) format to the interface, and back again. Custom software is needed to extract and insert data into your applications.

6.3 Implementing both a Computer-to-Computer Interface and a Web Site

The CVISN architecture recommends that states survey their stakeholders to determine whether both a person-to-computer and a computer-to-computer interface would be appropriate.

Some states have had discussions with their state trucking associations or have conducted surveys of their customers to determine preferences for electronic credentialing. They have determined that their large carriers, even though they may represent less than 20% of their customers, believe that a Web site will not satisfy their needs for transferring large volumes of data (Reference 59). Figure 6–9 depicts a state implementing both a computer-to-computer interface and a Web site.

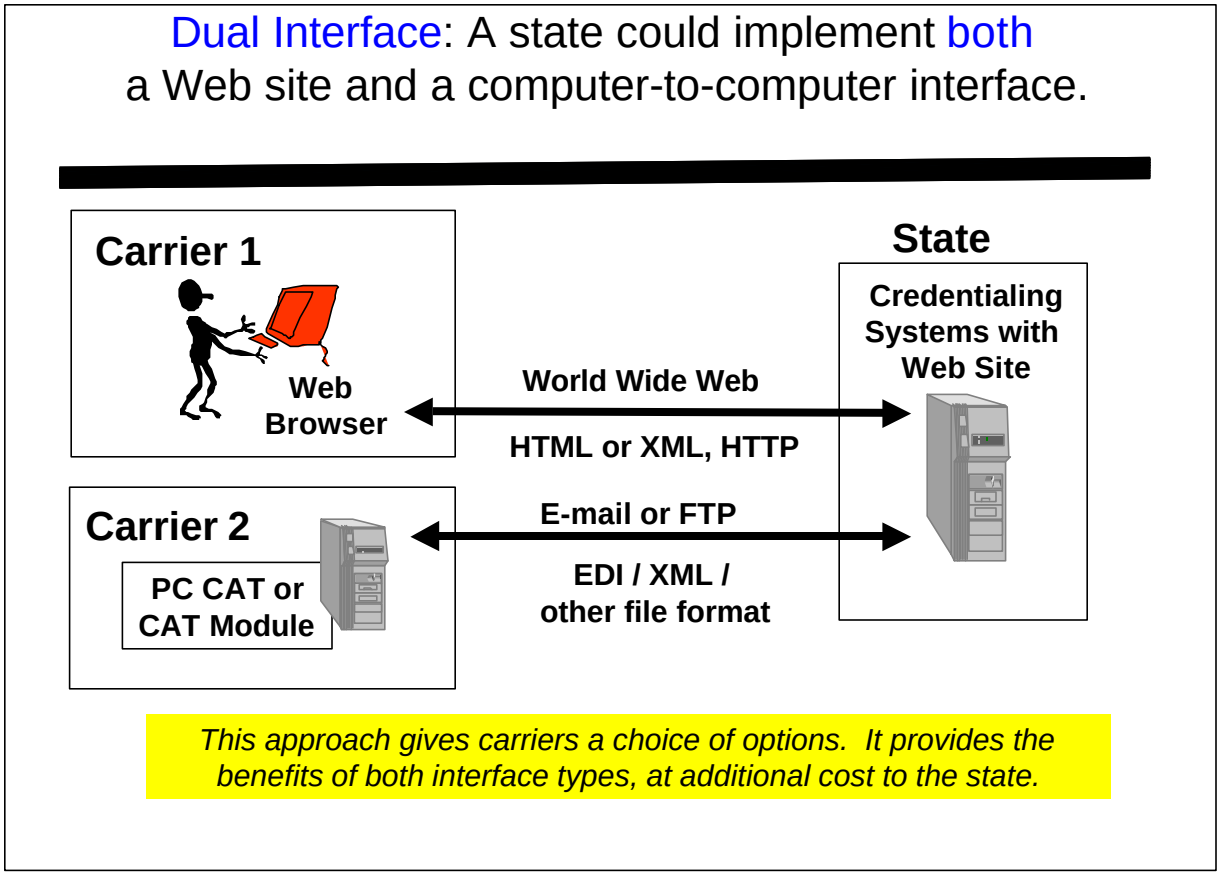


Figure 6–9. State Provides Both Computer-To-Computer Interface and Web Site

There are at least three choices for interfaces: EDI or XML file exchanges or an interactive Web interface, and many approaches to implementing these interfaces. Regardless of the interface used to interact with the carrier, the processing of the carrier-provided inputs should be the same in the CI and the legacy credentialing systems. Keep the same "back end" processes (snapshot, clearinghouse interface, etc.) regardless of the front end.

Figure 6–10 shows four approaches. The first approach shown is the stand-alone CAT. The CAT exchanges information with the state's Credentialing Interface. The carrier (or service provider) owns or leases the CAT product, and data are stored on the carrier's (or service provider's) system.

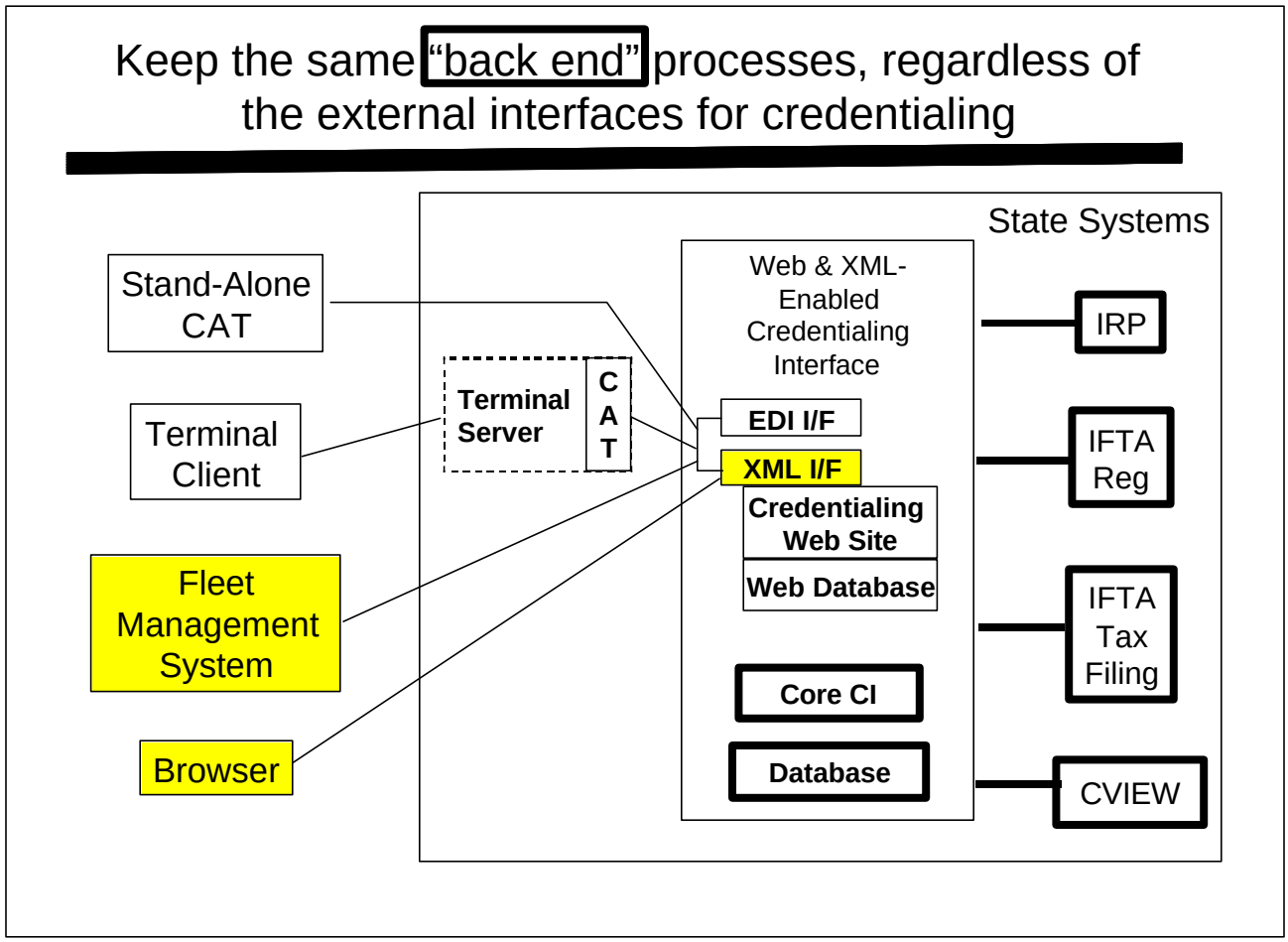


Figure 6–10. Approach to Multiple Extemal Interfaces

The second approach is for the carrier to access electronic credentialing services through a Terminal Client. In this approach, the CAT is owned or leased by whoever owns the Terminal Server (the state or a service provider). Both CAT-based approaches use the same interface choice, X12 EDI.

The third approach shown is for the carrier to use a fleet management system that has built-in electronic credentialing support. The interface could be either XML or EDI.

The fourth approach is a Web site solution. The carrier uses a browser to access the state's Web site for electronic credentialing. A combination of HTML, XML, dynamic HTML, and/or XHTML may be used.

7. INTEROPERABILITY ISSUES/STATUS

The interoperability issues related to Credentials Administration are concentrated on the ability to exchange credentials information and relate it to other information. Different legacy systems typically use different identifiers as look-up keys. The white paper on standard identifiers (Reference 16) provides detailed guidance on establishing a workable approach.

7.1 Issues

1. How will credentials-related identifiers be crossed-referenced to safety-related identifiers?

   First, an assessment of interstate carrier identifiers: For safety purposes, the United States Department of Transportation (USDOT) number is the main identifier (ID). For the International Fuel Tax Agreement (IFTA), the taxpayer ID is the main identifier. For the International Registration Plan (IRP), the IRP account number is used. The MCS-150 form captures many key identifiers (USDOT number, motor carrier operating authority number issued by the Federal Highway Administration or Interstate Commerce Commission, Dun & Bradstreet business number, taxpayer identifier) for carriers. Data from the MCS-150 are entered into the Motor Carrier Management Information System (MCMIS) database. The data from MCMIS is entered into the Safety and Fitness Electronic Records (SAFER) snapshot database. From a user's point of view, the SAFER/CVIEW systems make the information accessible electronically. However, at this time, there is no requirement to keep that part of the MCMIS database up to date.

   Under the Performance and Registration Information Systems Management (PRISM) processes, each vehicle must be associated with a safety carrier (using USDOT number to identify the carrier). The carrier's safety record is checked when the vehicle is registered. This provides an annual opportunity to confirm the carrier ID associated with each vehicle, and hence, to tie safety and IRP data together.

   IFTA registration allows, but does not usually require that the USDOT be captured. If applicants routinely supplied the USDOT number, then a linkage between safety and IFTA data could be established.

   The availability of all related identifiers for a given intrastate carrier in a single state system varies from state to state. Until all intrastate carriers are assigned USDOT numbers by a similar mechanism to that used today for interstate carriers, it will be difficult to assemble the cross-reference in the SAFER/CVIEW snapshots.

   Cross-referencing credentials and safety data will require a concerted effort. Linking the data together provides a better opportunity to identify high-risk operators. The snapshot should be used to collect all identifiers for all carriers. The CVO community should adopt a primary identifier for each CVO entity (e.g. motor carrier, commercial vehicle, etc.); such an identifier would permit a cross-reference between two databases that are designed around

different physical identifiers. Use of the primary identifier in all exchanges that update carrier snapshot updates should help to establish the cross-reference between the primary ID and other IDs for the same carrier.

2. What must be done to use "electronic signatures?"

   State procedures generally require original signatures on paper documents for:

   - carrier certification that application content is accurate
   - affidavits for a variety of purposes including application for refunds
   - power of attorney to allow a third party to act on behalf of the carrier

   The Electronic Signatures in Global and National Commerce Act was approved by Congress and signed into law in June 2000. The digital signature bill gives an electronic signature entered over the Internet the same legal validity and effect as a traditional signature on paper. While digital signatures are legally valid and must be accepted by all states, the states to will need to determine precisely how contracts are carried out. The intent of the legislation was not to overturn state contract laws, but simply to give a baseline.

   Digital signature technology is viable but immature

   - public key/private key cryptography
   - digital certificates
   - hardware keys/smart cards
   - biometric methods
   - user id & personal identification number (PIN)

   Simple approaches are readily available that probably provide higher security than is provided by current paper base level. Electronic processes require an electronic signature (or substitute) to be a replacement for pen and paper systems if the full benefits of automation are to be received. Technologies for electronic or digital signatures exist and this technology is evolving rapidly, now that the digital signature bill has become a federal law. States should position themselves institutionally to be able to evolve with the technology. That means that states may need to change laws to allow electronic signatures. States should not legislate a specific technology solution. The electronic data interchange (EDI) Trading Partner Agreement can be used to define the rules for signatures, affidavits, certifications & power of attorney.

3. How are CVISN states going to deal with the Heavy Vehicle Use Tax (HVUT) electronically?

   This tax affects both inter- and intra-state vehicles with gross taxable weights of 55,000 lb. or more. Vehicle owners must report and pay this tax using IRS Form 2290 (Heavy Vehicle Use Tax filing). There are exceptions for vehicles traveling less than 5000 miles per year; a 25% reduction for vehicles registered in Canada or Mexico; and some other special cases.

Enforcement is via FHWA, which will withhold Federal Aid funding for states that do not verify proof of HVUT payment. Therefore, states are mandated to require proof of payment of the tax before they may issue a truck registration or license. Reference 54 says that it is the policy of FHWA that each state require proof of HVUT payment either: before registering, or within 4 months after registering if a suspension registration system is implemented.

As related to electronic credentialing, the problem is with the current procedures that utilize paper to fulfill the state's mandate to verify proof of payment*: the IRS stamps "received" on a paper copy of Form 2290, indicating receipt of the taxes*. Currently there is no provision to query an IRS database for payment status. The high degree of privacy afforded to tax records is a barrier to the IRS releasing this information.

Some of the solutions that have been proposed include:

- Any state should be able to automatically query the IRS using a vehicle identification number (VIN) and a taxpayer identification number (TIN or EIN). IRS would then confirm (or deny) that HVUT has been paid for that vehicle by that taxpayer for the current period, avoiding the need for stamped paper copies.
- Every state could send the IRS a file of HVUT-qualified vehicles that are registered in that state, and push the compliance burden onto the IRS.
- States could collect the tax as part of the vehicle registration process, then pass it on to the IRS. (States should be reimbursed for doing so.)
- The cumbersome filing and checking of the Heavy Vehicle Use Tax could be replaced with a slight increase in the existing fuel tax structure.
- Use existing Safety and Fitness Electronic Records (SAFER) System for distributing HVUT payment status; or use a new or exiting registration clearinghouse. This minimizes the number of interfaces.

The IRS is interested in automating the HVUT process. The IRS will enable Form 2290 to be submitted electronically as part of their overall program for electronic filing, and per a recent change of policy will develop some kind of query capability such that a state could electronically verify HVUT payment at the time of vehicle registration. AAMVA and JHU/APL have been in contact with the IRS concerning the architectural approach. Unfortunately, production capability should not be expected before approximately 2002 or 2003, so CVISN states will need work-arounds until then.

So, how are CVISN states dealing with HVUT electronically in the meantime? Some states issue a temporary credential until HVUT proof is sent in, and only then issue the permanent credential. Some states issue the permanent credential immediately, but suspend it 30-60 days later unless the carrier has mailed in a confirming paper copy of Form 2290. A few states collect the HVUT on behalf of the IRS – that way they immediately know it has been paid and can proceed to issue the permanent credential; they do this as a customer service to streamline the process. Some states do nothing until and unless they have a stamped copy of Form 2290.

7.2 Interoperability Tests

Interoperability tests for credentials administration functions are being defined according to the criteria in the *CVISN Operational and Architectural Compatibility Handbook (COACH) Part 5, Interoperability Test Criteria* (Reference 6). The CVISN Interoperability Test Suite Package (References 26-28 and 65) explains the test scenarios, cases, procedures, and data. The tests are divided into two categories: those that test the interaction between pairs of products (pairwise tests) and those that verify a more complete functional thread (end-to-end tests). The list of available tests for credentials include:

- accept and process electronic IRP credential applications using EDI
- accept and process electronic IFTA credential applications using EDI
- accept electronic filing of and payment for IFTA quarterly tax returns using EDI

A similar set of tests are being developed for IRP and IFTA for Web-based applications.

8. BEYOND CVISN LEVEL 1

This section includes a summary of potential credentialing capabilities beyond CVISN Level 1 and an overview of PRISM and its relationship to CVISN.

8.1 Credentials-Related Aspects Beyond CVISN Level 1

CVISN Level 1 was defined as a pragmatic means of setting a goal that was ambitious but achievable. It purposely excluded many capabilities that were desirable and feasible with today's technology in order to control project scope and cost. If funding is available, these capabilities will be included in a future phase of the CVISN Program.

A preliminary definition of the capabilities a state would implement beyond CVISN Level 1, in the credentialing area, is provided in the Table 8-1. The final definition will evolve in a cooperative effort among FMCSA, states, and other CVO stakeholders.

Table 8–1.
Preliminary State Requirements for Credentials Administration Beyond CVISN Level 1

State Capabilities for Credentials Administration Beyond CVISN Level 1
▪ Electronic payment for credentials.
▪ End-to-end processing (i.e., carrier application, state application processing, payment, and credential issuance) of intrastate registration, titling, OS/OW, carrier registration and HAZMAT credentials.
▪ Connection to the Unified Carrier Registry (UCR), the electronic federal carrier registration system.
▪ "Paperless" vehicle: no requirement for paper credentials on vehicle.
▪ At least 50 percent of the total transaction volume handled electronically.

8.2 PRISM Concepts

PRISM (Performance and Registration Information Systems Management) is a FMCSA-sponsored program that seeks to improve safety by linking vehicle registration actions to an evaluation of the related carrier's safety rating. The program includes procedures for a carrier to improve their safety rating.

PRISM is a comprehensive program of motor carrier safety assessment, enforcement and improvement. The core concept of PRISM is the linking of vehicle registration at the State level to acceptable carrier safety performance. Through the PRISM program, the safety performance of the carrier responsible for a vehicle being registered is considered at vehicle registration time. As a part of vehicle registration, participating States assure that the carrier is registered and meets the required safety criteria. Ultimately, subject to State laws, vehicle registration may be

denied to unsafe carriers. As part of this process, the USDOT number of the carrier is recorded as part of the vehicle registration electronic record, thus linking the vehicle to the carrier responsible for the safe operation of the vehicle. That linkage can also be used at the roadside during screening operations and inspections. Six states (CO, IN, IA, MN, OR, and PA) currently participate in the PRISM program. Other states have been approved to participate.

The other major process in PRISM is the **MCSIP (The Motor Carrier Safety Improvement Program).** MCSIP tracks carrier safety improvement through a series of levels intended to bring the carrier into full safety compliance. The MCSIP level is a crucial measure of a carrier's current status in this improvement process.

The safety assessment algorithm at the core of PRISM is **SafeStat**. From a comprehensive array of MCMIS carrier performance data (inspections, crashes, reviews, enforcement cases, citations) SafeStat computes an indicator and a category for carriers that have sufficient data. The SafeStat indicator and category can be used to prioritize carriers for a possible on-site review. The SafeStat values are also available at the roadside for use in screening algorithms.

How are PRISM and CVISN Related?

CVISN (Commercial Vehicle Information Systems and Networks) - The information systems and communications networks that support commercial vehicle operations. CVISN includes information systems owned and operated by governments, carriers, and other stakeholders. It excludes the sensor and control elements of ITS/CVO.

The **CVISN Architecture** provides a standardized framework for linking new and existing systems and networks to facilitate the exchange of information. The CVISN Prototype & Pilot states are deploying **CVISN Level 1 capabilities**: safety information exchange through snapshots, inspection reporting using ASPEN, electronic screening using transponders and snapshot data, electronic credentialing for IRP and IFTA, and supporting base state agreements via the IRP and IFTA Clearinghouses. Ten states (CA, CO, CT, KY, MD, MI, MN, OR, VA, and WA) are currently deploying CVISN Level 1 capabilities.

Access to safety information is necessary to support the safety performance evaluations that serve as a basis for accomplishing PRISM program goals. Information systems and networks that are part of the CVISN Architecture provide that access.

- To facilitate information exchange, several systems are being developed under CVISN. One of those systems is **SAFER (Safety and Fitness Electronic Records).** SAFER and other information systems (e.g., SAFETYNET, MCMIS, ASPEN, CAPRI) are used to supply data for the PRISM processes.
- The values generated by PRISM's SafeStat algorithm are included in SAFER snapshots. Snapshots are used in roadside screening and inspection activities to focus resources on high-risk operators.

Thus, the PRISM system concepts and approach are compatible with and utilize components of the CVISN Architecture.

The PRISM operational concepts are illustrated in the figure below. Originally, the **PRISM Central Site** was maintained by the IOWA DOT. Today, modifications to SAFER are underway to provide PRISM Central Site data exchange support for participating PRISM states using open standards.

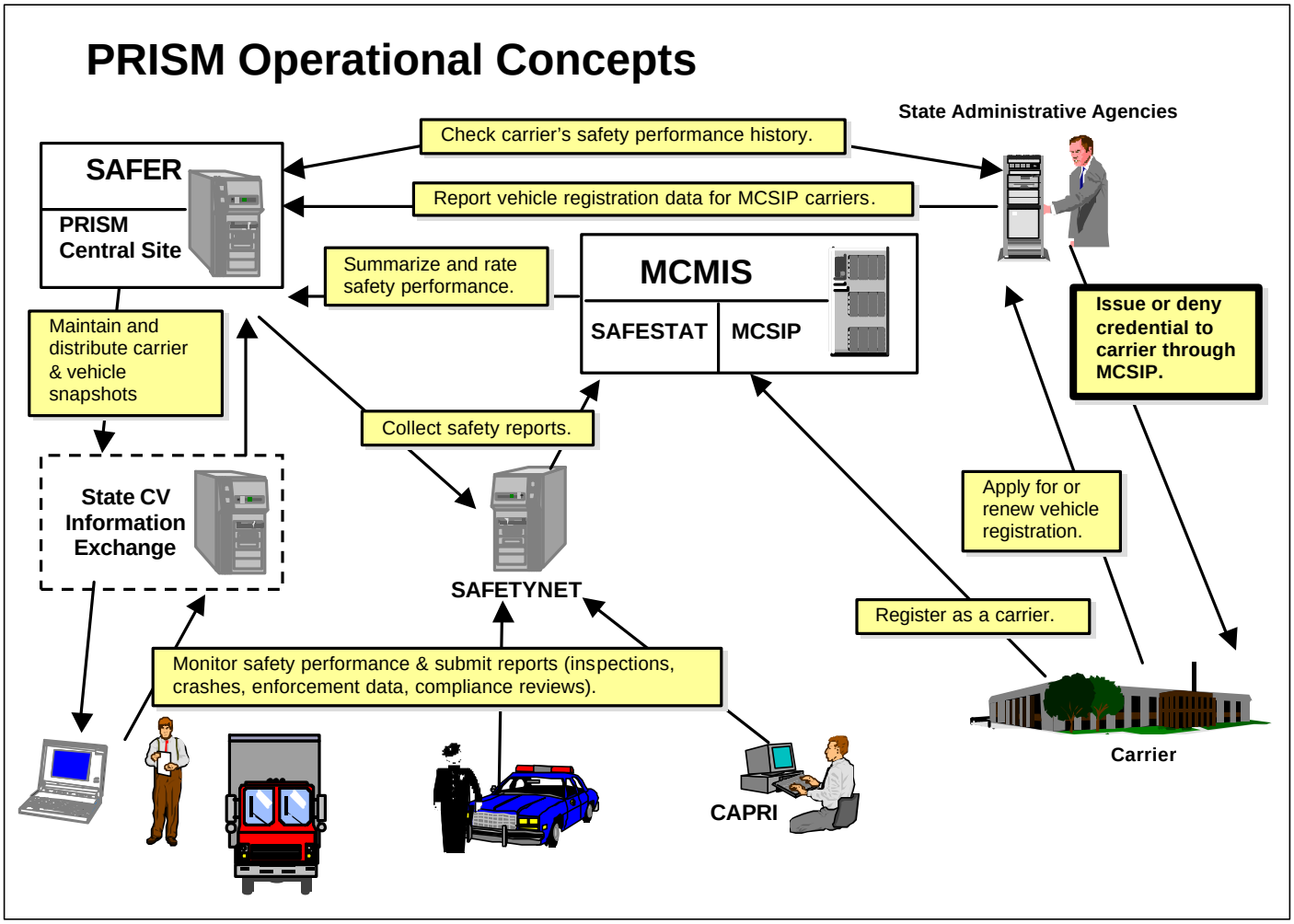


Figure 8–1. PRISM Operational Concepts

PRISM and CVISN share key concepts:

- focus safety enforcement on high risk operators
- use open standards for data communications
- use standardized algorithm for determining a carrier's safety fitness
- use data exchange systems, e.g. SAFER that conform with the National ITS Architecture

These concepts, implemented through state and national systems, link CVISN deployment and PRISM Program activities.

SAFER is being modified to:

- provide users with a logical view of the existing PRISM Target File, i.e., access to carrier and vehicle records for those carriers in the MCSIP
- accept, process, and output MCSIP carrier vehicle records to requesting PRISM state systems
- generate an historical audit of MCSIP carrier activities
- support batch and interactive communications
- provide PRISM users with enhanced query support and report generation capabilities

Appendix A. REFERENCES

This Page Intentionally Blank

Note that not all of these references are explicitly cited in the text of this guide.

1. JHU/APL, *ITS/CVO CVISN Glossary*, POR-96-6997 V1.0, dated December 1998. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
2. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 1 – Operational Concept and Top-Level Design Checklists*, SSD/PL-99-0243, POR-97-7067 V2.0, dated August 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
3. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 2 – Project Management Checklists*, Preliminary Version, POR-97-7067, P2.0, September 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
4. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 3 – Detailed System Checklists*, Baseline Version, POR-97-7067, P1.0, May 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
5. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 4 – Interface Specification Checklists*, Draft Version, POR-97-7067, D1.0, April 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
6. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 5 – Interoperability Test Criteria*, SSD/ PL-99-0470, POR-98-7126, D.1, dated July 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
7. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) System Design Description*, POR-97-6998 V2.0, August 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
8. JHU/APL, *Introductory Guide to CVISN*, POR-99-7186 P.1, dated May 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
9. JHU/APL, *CVISN Guide to Safety Information Exchange*, POR-99-7191, D.1 (Draft), March 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
10. JHU/APL, *CVISN Guide to Electronic Screening*, POR-99-7193 D.1 (Draft), October 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
11. IFTA Articles of Agreement, last updated July 2000. Available from the IFTA Clearinghouse at their World Wide Web site http://www.iftach.org/Manual1.htm.
12. INTERNATIONAL REGISTRATION PLAN, INC. with official commentary, August 22, 1994. Available from IRP, Inc. at their World Wide Web site http://www.aamva.org/IRP/index.html.

13. *reference deleted*

14. JHU/APL, *Safety and Fitness Electronic Records System (SAFER) and Commercial Vehicle Information Exchange Window (CVIEW), Carrier, Vehicle, and Driver Snapshots*, Preliminary Version P1.0, White Paper, October 15, 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

15. FHWA, *PRISM Overview*, published on the World Wide Web at http://www.mcs.dot.gov/factsfigs/prism.htm.

16. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) Recommendations for Primary Identifiers*, Preliminary Version, P1.0, June 23, 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

17. ANSI ASC X12, *Electronic Data Interchange X12 Standards*, Draft Version 4, Release 3, (a.k.a. Release 4030), December 1999.

18. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume I - IRP Credential Transactions, ANSI ASC X12 Version 4 Release 3*, POR-96-6993 D.5, dated March, 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

19. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume II – IRP Interstate Credential Transactions*, Draft Version originally published in December 17, 1996. Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

20. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume III - International Fuel Tax Agreement (IFTA) Credential Transactions, ANSI ASC X12 Version 4 Release 3*, POR-97-6996 D.4, dated March, 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

21. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume IV - Oversize / Overweight (OS/OW) Credential Transactions*, POR-97-7068 D.3, dated March, 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

22. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Safety and Credentials Information Exchange (Transaction Set 285)*, POR-96-6995 D.5, March, 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

23. Notice of Proposed Rulemaking, Statewide Transportation Planning, Metropolitan Transportation Planning; US DOT Federal Highway Administration 23 CFR parts 450 and 1410; Federal Transit Administration 23 CFR Part 1410, 49 CFR Parts 613 and 621; FHWA Docket No. FHWA-99-5933, FHWA RIN 2125-AE62; FTA RIN 2132-AA66; published in the Federal Register Volume 65, No. 102, Thursday May 25, 2000; Proposed Rules.

24. Notice of Proposed Rulemaking, Intelligent Transportation System Architecture and Standards; US DOT Federal Highway Administration 23 CFR Parts 655 and 940; FHWA Docket No. FHWA-99-5899; RIN 2125-AE65; published in the Federal Register Volume 65, No. 102, Thursday May 25, 2000; Proposed Rules.

25. JHU/APL, *CVISN Guide to Top-Level Design*, POR-99-7187 P.1.1 (Preliminary), June 25, 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

26. JHU/APL, *CVISN Interoperability Test Suite Package, Part 1 – Test Specifications*, Draft, POR-98-7122 D.2, dated January 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

27. JHU/APL, *CVISN Interoperability Test Suite Package, Part 2 – Test Cases and Procedures*, Draft, POR-98-7123 D.0, dated September 1999. Note: This document is scheduled for a significant update in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

28. JHU/APL, *CVISN Interoperability Test Suite Package, Part 4— Test Data, Draft*, POR-98-7125 D.0, September 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

29. JHU/APL, *The Maryland Commercial Vehicle Information Systems and Networks (CVISN) Prototype Top-Level Design Description*, Preliminary, POR-99-7235, dated November 1999.

30. Intelligent Transportation Society of America, *ITS CVO Guiding Principles*, published on the World Wide Web at http://www.itsa.org, last updated March 27, 1998.

31. Intelligent Transportation Society of America, *Fair Information Principles for ITS/CVO*, published on the World Wide Web at http://www.itsa.org, last updated January 12, 1999.

32. Intelligent Transportation Society of America, *Interim ITS/CVO Interoperability Guiding Principles*, published on the World Wide Web at http://www.itsa.org, last updated January 12, 1999.

33. FHWA, Letter from HAS-20 to States, *Call for New CVISN States - What states are interested in CVISN Workshops*, J. Loftus e-mail dtg 981222 5:10 PM

34. ASTM 1 Physical Layer, The DSRC standards are still in the approval cycle. For current status information, see http://www.its.dot.gov/standard/standard.htm.

35. ASTM 2 Data Link Layer, The DSRC standards are still in the approval cycle. For current status information, see http://www.its.dot.gov/standard/standard.htm.

36. IEEE P1455, *Draft Standard for Message Sets for Vehicle/Roadside Communications.* The DSRC standards are still in the approval cycle. For current status information, see http://www.its.dot.gov/standard/standard.htm.

37. The U. S. Department of Transportation, ITS Joint Program Office, *Policy for Dedicated Short Range Communication (DSRC)* draft January 15, 1998.

38. James A. Obrien, *Introduction to Information Systems*, Irwin McGraw-Hill, 1997, ISBN 0-256-20937-5.

39. JHU/APL, *Introduction to ITS/CVO Training Material*, version 2.1, February 1999. The participant's manual is available from the Electronic Document Library at http://www.its.dot.gov/welcome.htm. Search for document number 8103.

40. JHU/APL, *Understanding ITS/CVO Technology Applications Training Material*, version 2.0, January 1999. The student's manual is available from the Electronic Document Library at http://www.its.dot.gov/welcome.htm. Search for document number 8143.

41. ASC X12D/W456, *ASC X12 Guideline for Electronic Data Interchange, EDI Implementation Reference Manual Guidelines*, Data Interchange Standards Association (DISA), February 1991.

42. Margaret A. Emmelhainz, Ph.D., *EDI: A Total Management Guide*, Van Nostrand Reinhold, 1993.

43. Richard H. Baker, *EDI: What Mangers Need to Know About the Revolution in Business Communications*, Tab Professional and Reference Books, 1991.

44. Data Interchange Standards Association (DISA) Home Page: http://www.disa.org/ - (DISA Reference Desk, Product Catalog, Internet Services).

45. JHU/APL, *Scope Workshop Notebook*. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

46. Meiler Page-Jones, *The Practical Guide to Structured Systems Design*, Yourdon Press, New York , New York, 1980, ISBN 0-917072-17-0.

47. ANSI/IEEE Std 1042-1987 (R1993), *An American National Standard IEEE Guide to Software Configuration Management*, 1988.

48. JHU/APL, *Intelligent Transportation Systems (ITS) Commercial Vehicle Information Systems and Networks (CVISN), State of Maryland, Credentials Administration Requirements Specifications (CARS)*, SSD/PL-96-0613, Draft Issue D.1, dated November 1997.

49. JHU/APL, *Intelligent Transportation Systems (ITS) Commercial Vehicle Information Systems and Networks (CVISN), Commonwealth of Virginia, Credentials Administration Requirements Specifications (CARS)*, SSD/PL-98-0485, Version 2.0, dated September 1998.

50. JHU/APL, *CVISN Guide to Integration and Test*, POR-99-7194 to be published in 2000. The document will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

51. National Governors Association (Thom Ruble), *State Fiscal Implications of Intelligent Transportation Systems/Commercial Vehicle Operations Deployment*, 1998, ISBN 1-55877-299-5. The report is available from the Electronic Document Library at http://www.its.dot.gov/welcome.htm. Search for document number 5484.

52. Booz-Allen & Hamilton, *ITS Field Operational Test Cross-Cutting Study Commercial Vehicle Administrative Processes*, FHWA-JPO-99-037, September 1998. The document is available from the Electronic Document Library at http://www.its.dot.gov/welcome.htm. Search for document number 6324.

53. JHU/APL, *ITS/CVO Architecture Conformance: Interoperability Testing Strategy,* Draft, POR-98-7076 D.1, dated January 16, 1998. This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

54. Federal-Aid Policy Guide 23 CFR Part 669, *Enforcement of Heavy Vehicle Use Tax*, December 9, 1991, Transmittal 1. Available at: http://www.fhwa.dot.gov/legsregs/directives/fapg/cfr0669.htm

55. Federal-Aid Policy Guide NS 23 CFR 669, *Non-Regulatory Supplement*, September 30, 1992, Transmittal 5. Available at: http://www.fhwa.dot.gov/legsregs/directives/fapg/0669sup.htm

56. *1997 Federal Highway Cost Allocation Study, Final Report*. Published by the U.S. Department of Transportation, Federal Highway Administration. Chapter IV, "Trends and Forecasts of Highway User Revenues". Available at: http://www.ota.fhwa.dot.gov/hcas/final/four.htm

57. *Rand McNally Motor Carrier's Road Atlas 2000*. ISBN 0-528-84129-7.

58. JHU/APL, *Extensible Markup Language (XML) in CVISN*, Draft Version D1.0, White Paper, January 21, 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

59. JHU/APL, *CVISN Electronic Credentialing Preference Survey Results*, dated July 10, 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

60. Chris Forsythe, Eric Grose, and Julie Ratner, *Human Factors and Web Development*, Lawrence Erlbaum Associates, 1998.

61. World Wide Web Consortium (W3C), http://www.w3.org/XML/ This copyright notice applies to all documents from the reference: Copyright © World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. W3C® is a registered trademark of the Massachusetts Institute of Technology on behalf of the World Wide Web Consortium. http://www.w3.org/Consortium/Legal/.

62. Peter Flynn, *Frequently Asked Questions about the Extensible Markup Language*, Version 1.5, 1 June 1999, maintained on behalf of the World Wide Web Consortium's XML Special Interest Group at http://www.ucc.ie/xml/

63. Robin Cover, *XML website* is hosted at Organization for the Advancement of Structured Information Standards (OASIS), http://www.oasis-open.org/cover/xml.html

64. Electronic Business XML (ebXML) Home Page. UN/CEFACT (United Nations body for Trade Facilitation and Electronic Business) and OASIS have established the Electronic Business XML Working Group to develop a technical framework that will enable XML to be utilized in a consistent manner for the exchange of all electronic business data. Home page is http://www.ebxml.org/

65. JHU/APL, *CVISN Interoperability Test Suite Package, Part 3 – Test Tool Description, Draft,* POR-98-7124 D.1, dated July 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/

Appendix B. OPERATIONAL SCENARIOS AND FUNCTIONAL THREAD DIAGRAMS

This Page Intentionally Blank

Operational Scenarios and Functional Thread Diagrams

- An “operational scenario” is a description of how a state intends that their customers and the state, or the state and core infrastructure systems should interact to accomplish key CVISN functions. An example was given in chapter 4. More examples are provided here.
- The operational scenario is shown as a list of sequential steps. To differentiate between different time schedules, numbers are used to show the interaction between the applicant and the state, and the state’s update of snapshots. Those interactions occur as soon as possible after the initial application is received by the state. Letters are used to show the state’s connections to the clearinghouses, since that occurs at a regular period instead of being triggered immediately by the carrier’s actions.
- Each operational scenario is illustrated by overlaying information onto the state system design template. The lines represent data flow between products, with arrows indicating the direction of flow. Each line is labeled with a number or letter. The complete set of lines constitutes a thread of activities that accomplish a function. Hence, the diagram is called a “functional thread diagram.”
- This appendix provides examples of operational scenarios and functional thread diagrams. They are included for reference, and as starting points for states that plan to implement similar processes.

CVISN Level 1 Credentials Administration Key Operational Scenarios

- **Accept and process electronic IRP credential applications for supplements (e.g., adding a vehicle to an existing account)**
  - ***Example 1*: VISTA/RS, PC-CAT, CVIEW**
  - ***Example 2*: Web Browser/Web Site, CVIEW**
- **Accept and process electronic IRP renewal applications**
- **Accept and process electronic IFTA credential applications for supplements (e.g., changing the carrier's address)**
- **Accept and process electronic IFTA renewal applications**
  - ***Example 3*: RPC, PC-CAT, CVIEW**
  - ***Example 4*: Web Browser/Web Site, CVIEW**

Accept and process electronic IRP credential applications for supplements **Example 1**: VISTA/RS, PC-CAT, CVIEW

1. Carrier enters an IRP credential application via a Carrier Automated Transaction (CAT) system which submits it to the Credentialing Interface (CI) as an EDI X12 TS 286.
2. The CI submits a query to its state database to perform preliminary checks as part of evaluating the application.
3. The state database reports the status, i.e., flags and condition to the CI.
4. If a satisfactory status is received, the application is sent to the IRP system (VISTA/RS) for processing via EDI X12 TS 286.
5. The IRP system processes the application and sends an invoice notice to the CI via EDI X12 TS 286.
6. The CI sends the invoice notice to the CAT via EDI X12 TS 286 and maintains archival/audit copies of all transactions.
7. The carrier reviews the invoice data and verifies that the application data matches the intent. The CAT sends payment method information to the CI via EDI X12 TS 286.
8. If a Temporary Authority (TA) is requested, the CI releases it to the CAT via EDI X12 TS 286.
9. If a TA was granted, the CI sends a vehicle snapshot segment update to CVIEW via EDI X12 285.
10. CVIEW sends updated snapshot data to SAFER via EDI X12 TS 285.
11. CVIEW sends updated snapshot data to Roadside via EDI X12 TS 285.
12. SAFER sends updated snapshot data to subscribers via EDI X12 TS 285.
13. The CI verifies payment method information (financial system interfaces are not shown)and passes payment approval to the IRP system via EDI X12 TS 286.
14. The IRP system validates payment amount and updates application status to indicate the permanent credential granted and notifies the CI via EDI X12 TS 286.
15. The CI passes the permanent credential to the CAT via EDI X12 TS 286. Cab Cards may be printed in the carrier's office or state office.
16. The CI updates CVIEW with permanent credential information via EDI X12 TS 285.
17. CVIEW sends updated snapshot data to SAFER via EDI X12 285.
18. CVIEW sends updated snapshot data to Roadside via EDI X12 285.
19. SAFER makes updated snapshot data available to subscribers via EDI X12 TS 285.

A. Periodically (daily), the IRP system sends updates to the IRP Clearinghouse on IRP registration information and fee payments (recaps).

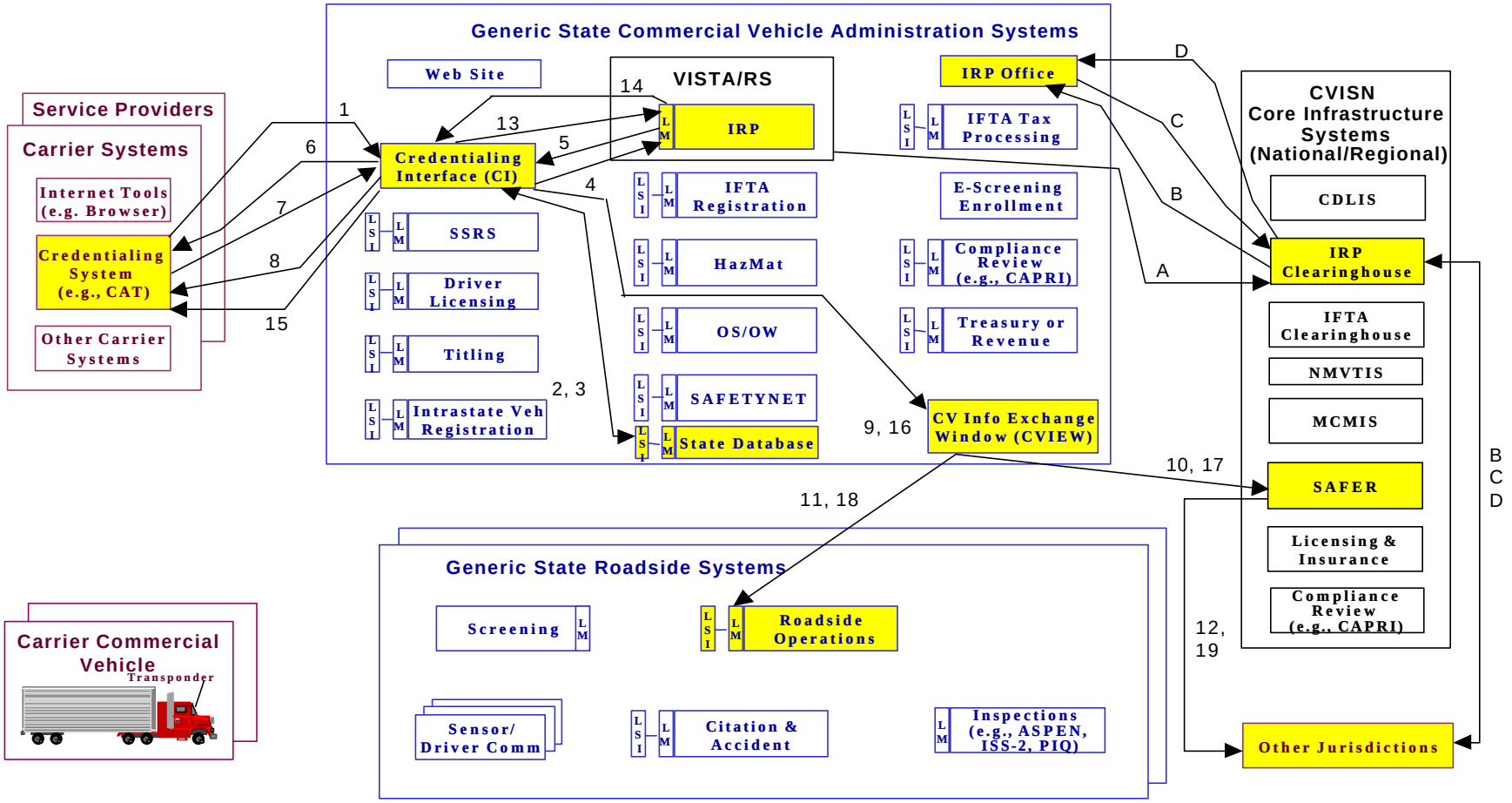
B. Monthly, the IRP Clearinghouse makes available the fee information (pre-netting transmittals) to the participating jurisdictions for approval and/or correction. Today, the states review the information interactively using terminals.

C. The IRP Office and also other participating jurisdictions report back to the IRP Clearinghouse the approvals or corrections. Today, the approvals/corrections are made via terminals.

D. The IRP Clearinghouse performs the actual netting and makes available corrected/approved vehicle and fee actions (post-netting transmittal) and netting results (remittance netting reports) to the participating jurisdictions. Today, the information is reviewed via terminals.

NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. Content errors in a received TS 286 are noted by also replying with a TS 286. The results of processing an incoming TS 285 are reported via TS 824.

Accept and process electronic IRP credential applications for supplements
Example 1: VISTA/RS, PC-CAT, CVIEW

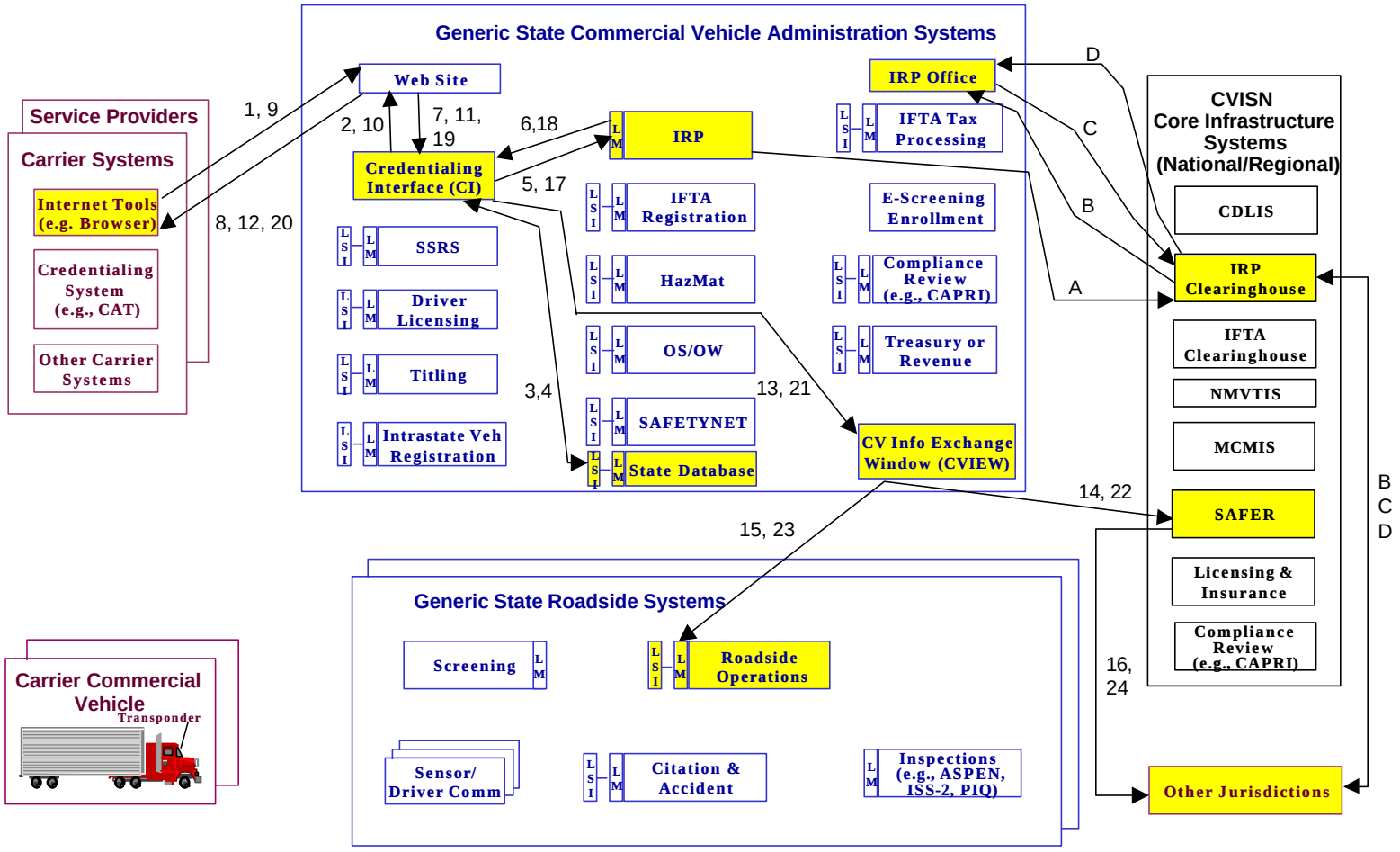


Accept and process electronic IRP credential applications for supplements **Example 2**: Web Browser/Web Site, CVIEW (1 of 2)

1. Carrier enters an IRP credential application via a Web browser to a state-based Web Site.
2. The Web Site passes it to the Credentialing Interface (CI).
3. The CI submits a query to its state database to perform preliminary checks as part of evaluating the application.
4. The state database reports the status, i.e., flags and condition to the CI.
5. If a satisfactory status is received, the application is sent to the IRP system for processing via EDI X12 TS 286.
6. The IRP system processes the application and sends an invoice notice to the CI via EDI X12 TS 286.
7. The CI sends the invoice notice to the Web Site and maintains archival/audit copies of all transactions.
8. The carrier retrieves the invoice notice from the state Web Site using a Web Browser.
9. The carrier reviews the invoice data and verifies that the application data matches the intent. The carrier indicates payment method information via the Web Browser to the Web Site.
10. The Web Site passes it to the Credentialing Interface (CI).
11. If a Temporary Authority (TA) is requested, the CI releases it to the Web Site.
12. The carrier prints the TA from the Web Site.
13. If a TA was granted, the CI sends a vehicle snapshot segment update to CVIEW via EDI X12 285.
14. CVIEW sends updated snapshot data to SAFER via EDI X12 TS 285.
15. CVIEW sends updated snapshot data to Roadside via EDI X12 TS 285.
16. SAFER sends updated snapshot data to subscribers via EDI X12 TS 285.
17. The CI verifies payment method information (financial system interfaces are not shown)and passes payment approval to the IRP system via EDI X12 TS 286.
18. The IRP system validates payment amount and updates application status to indicate the permanent credential granted and notifies the CI via EDI X12 TS 286.
19. The CI passes the permanent credential to the Web Site via EDI X12 TS 286.
20. The carrier prints the Cab Cards from the Web Site.
21. The CI updates CVIEW with permanent credential information via EDI X12 TS 285.
22. CVIEW sends updated snapshot data to SAFER via EDI X12 285.
23. CVIEW sends updated snapshot data to Roadside via EDI X12 285.
24. SAFER makes updated snapshot data available to subscribers via EDI X12 TS 285.

NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. Content errors in a received TS 286 are noted by also replying with a TS 286. The results of processing an incoming TS 285 are reported via TS 824.

Accept and process electronic IRP credential applications for supplements
Example 2: Web Browser/Web Site, CVIEW



Accept and process electronic IRP credential applications for supplements
Example 2: Web Browser/Web Site, CVIEW (2 of 2)

A. Periodically (daily), the IRP system sends updates to the IRP Clearinghouse on IRP registration information and fee payments (recaps).

B. Monthly, the IRP Clearinghouse makes available the fee information (pre-netting transmittals) to the participating jurisdictions for approval and/or correction. Today, the states review the information interactively using terminals.

C. The IRP Office and also other participating jurisdictions report back to the IRP Clearinghouse the approvals or corrections. Today, the approvals/corrections are made via terminals.

D. The IRP Clearinghouse performs the actual netting and makes available corrected/approved vehicle and fee actions (post-netting transmittal) and netting results (remittance netting reports) to the participating jurisdictions. Today, the information is reviewed via terminals.

NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. Content errors in a received TS 286 are noted by also replying with a TS 286. The results of processing an incoming TS 285 are reported via TS 824.

This Page Intentionally Blank

Accept and process electronic IFTA renewal applications
Example 3: RPC, PC-CAT, CVIEW

1. The IFTA Registration System sends a registration renewal notification to the Credentialing Interface (CI) via EDI X12 TS 286.
2. The CI sends the notification to the Carrier Automated Transaction (CAT) via EDI X12 TS 286.
3. The carrier enters an IFTA registration application using a Carrier Automated Transaction (CAT) system, and sends it to the Credentialing Interface (CI) via EDI X12 TS 286. The carrier pays for the application (through EFT, credit card, debit card,…)
4. The CI checks the carrier's status (delinquent, non payment etc.…) with the IFTA Registration System and IFTA Clearinghouse via Regional Processing Center (RPC).
5. The CI sends the application to the IFTA Registration System via EDI X12 TS 286.
6. Once the application is processed by the IFTA Registration System, a message is returned to the CI via EDI X12 TS 286. If processing was completed successfully, credential information is returned. If problems were found, an error message is returned.
7. The IFTA Registration System also proactively updates the CI whenever the carrier's status changes, (e.g., from Active to Inactive, Active to Revoked).
8. The CI sends a return message to the CAT via EDI X12 TS 286.

A. Periodically (no more than daily), the IFTA Registration System creates a file reflecting IFTA credential renewals, additions, and changes. The information is sent to RPC in RPC proprietary format.

B. Daily, RPC updates new or changed IFTA credential information (Demographic) and sends it to the IFTA Clearinghouse, for all client jurisdictions, via EDI X12 TS 286.

C. The IFTA Clearinghouse database is updated with registration information (Demographic) received from participating jurisdictions. Jurisdictions can query the IFTA database using reporting tools. Jurisdictions may be able to download an "extract" file containing all demographic data submitted by participating jurisdictions in EDI X12 TS 286 format.

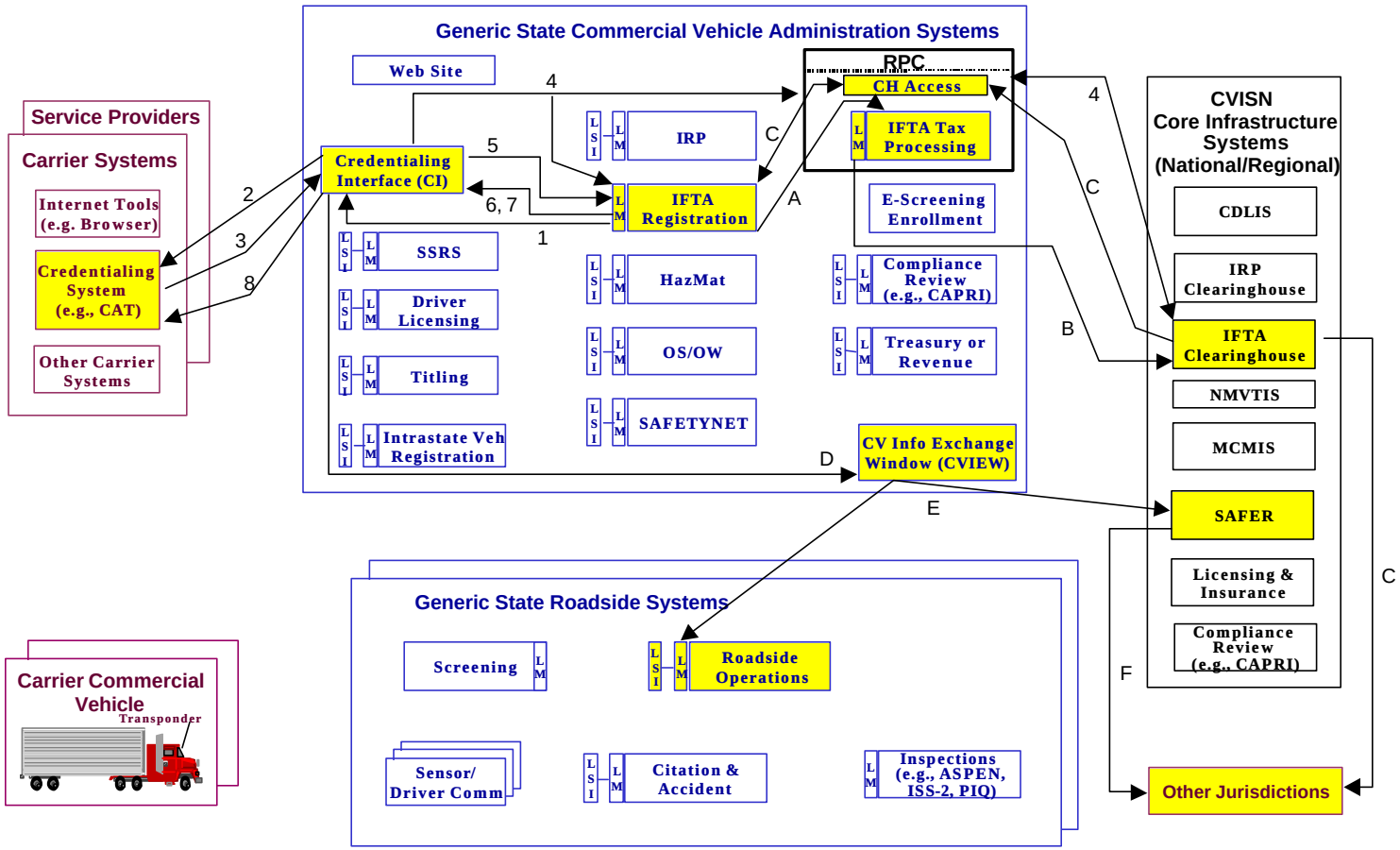
D. Nightly, the CI generates a new or modified carrier snapshot IFTA segment and sends it to CVIEW via TS 285.

E. CVIEW updates the carrier snapshot with IFTA credential data and forwards it to subscribers, including SAFER and the State roadside sites via EDI X12 TS 285.

F. SAFER updates (or creates) a carrier snapshot with IFTA credential data and forwards it to subscribers via EDI X12 TS 285.

NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. Content errors in a received TS 286 are noted by also replying with a TS 286. The results of processing an incoming TS 285 are reported via TS 824.

Accept and process electronic IFTA renewal applications
Example 3: RPC, PC-CAT, CVIEW



Accept and process electronic IFTA renewal applications
Example 4: Web Browser/Web Site, CVIEW

1. Carrier enters an IFTA registration application via a Web Browser to a state-provided Web Site. The carrier pays for the application (through EFT, credit card, debit card,…).
2. The Web Site passes it to the Credentialing Interface (CI) via EDI X12 TS 286.
3. The CI sends the application to VISTA/TS via EDI X12 TS 286 for processing.

   Note:

   The Web Site and/or the CI validates the application data to determine completeness, format, agreement with business rules, payment status, and whether to grant or deny the credential.
4. Once the application is processed by the IFTA Registration System, a message is returned to the CI via EDI X12 TS 286.
5. If processing was completed successfully, credential information is returned to the Web Site via EDI X12 TS 286.
6. The carrier retrieves the credential information from the Web Site using a Web Browser.

A. Nightly, the IFTA Registration System updates new or changed IFTA credential information (Demographic) and sends it to the IFTA Clearinghouse via EDI X12 TS 286.

B. The IFTA Clearinghouse database is updated with registration information (Demographic) received from participating jurisdictions. Jurisdictions can query the IFTA database using reporting tools. Jurisdictions may be able to download an “exact” file containing all demographic data submitted by participating jurisdictions in EDI X12 TS 286 format.

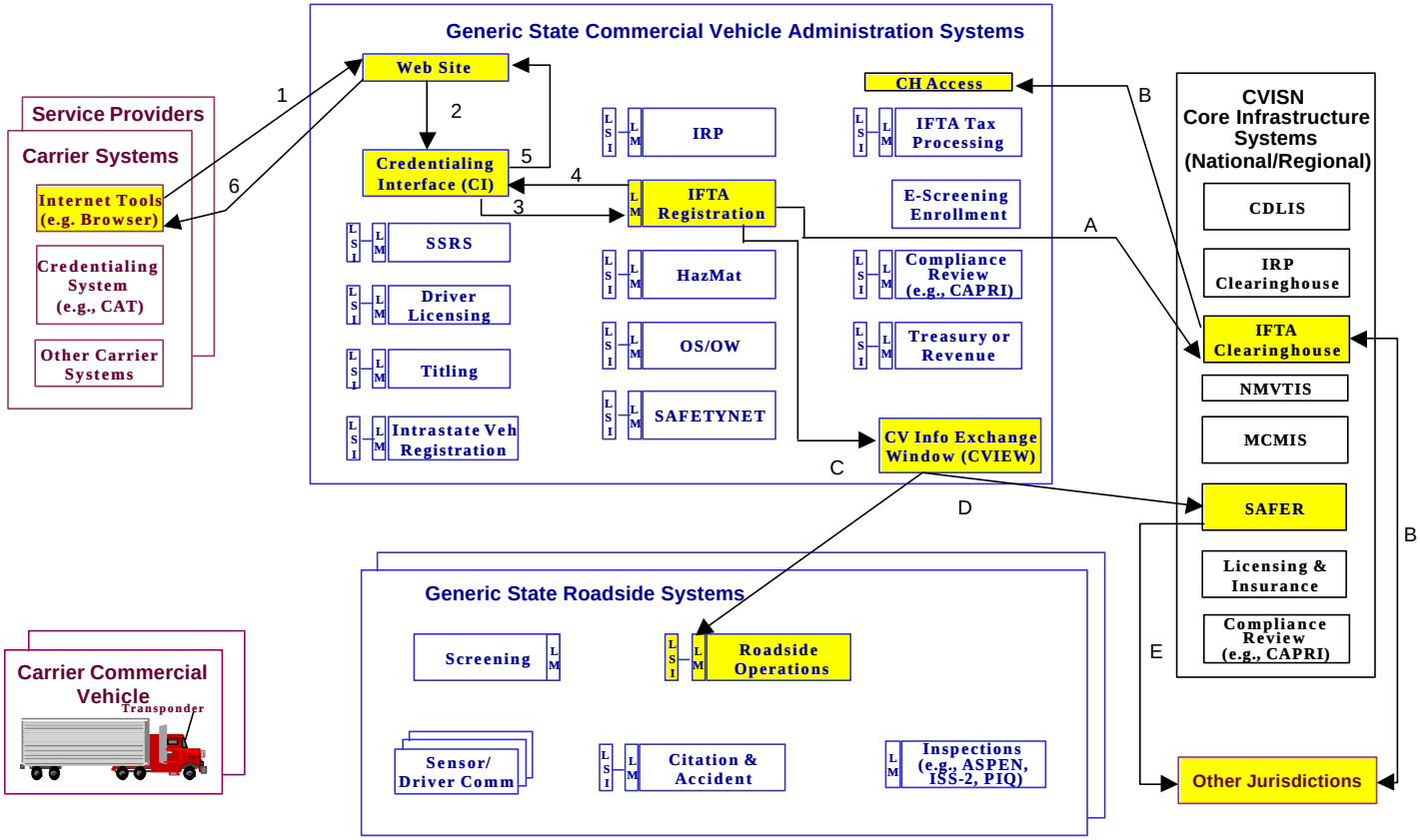
C. Nightly, the IFTA Registration System generates a new or modified carrier snapshot IFTA segment for all VISTA/TS clients and sends it to CVIEW via TS 285. (Alternatively the IFTA Registration System could generate a new or modified carrier snapshot IFTA segment and provide it to the CI and then CI sends it to CVIEW).

D. CVIEW updates the carrier snapshot with IFTA credential data and forwards it to subscribers, including SAFER and the State roadside sites via EDI X12 TS 285.

E. SAFER updates (or creates) a carrier snapshot with IFTA credential data and forwards it to subscribers via EDI X12 TS 285.

NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. Content errors in a received TS 286 are noted by also replying with a TS 286. The results of processing an incoming TS 285 are reported via TS 824.

Accept and process electronic IFTA renewal applications
Example 4: Web Browser/Web Site, CVIEW



Appendix C. RECOMMENDED DEVELOPMENT PROCESS

This Page Intentionally Blank

RECOMMENDED DEVELOPMENT PROCESS

The Commercial Vehicle Information Systems and Networks (CVISN) Guide to Top-Level Design and the CVISN Guide to Project Planning describe fundamental principles and generic processes. This chapter applies and tailors this guidance to the credentials administration area. Some states may already have a well-documented methodology for information system development. If so, the state should follow that process, possibly making some adjustments to incorporate any ideas included here that aren't reflected in the state's standard procedures.

The first section in this chapter provides an overview of the entire process. Subsequent sections address each successive phase of the process, including these topics:

- phase process
- phase products
- factors to consider
- list of key decisions (refer to Chapter 5 for a description of each)
- advice and lessons learned

A final section addresses requirements specification, a topic that impacts all phases.

C.1 Development Process Overview

The *Introductory Guide to CVISN* outlined a model development process for implementing CVISN capabilities. Figure C–1 is repeated from that document as a reminder of the model.

Deploying CVISN Level 1 capabilities is a major undertaking that typically takes several years. In order to reduce risk, it is strongly recommended that states use an incremental deployment approach. It is critical that this large project be broken into a series of 3–6 month time periods called project phases. Specific results or products are defined for each phase. These are defined in detail for each phase just before it begins, and more broadly for subsequent phases. The use of phases allows taking a big job and breaking it into small, manageable pieces. If a state completes the first couple development phases on time and meets all the objectives, this provides assurance that the plan is realistic. If not, it allows the state to revise the plan and take other corrective actions prior to committing extensive resources to a project that is not properly structured for success. Incremental development and measurable milestones ensure stakeholder participation and feedback and real visibility into project progress.

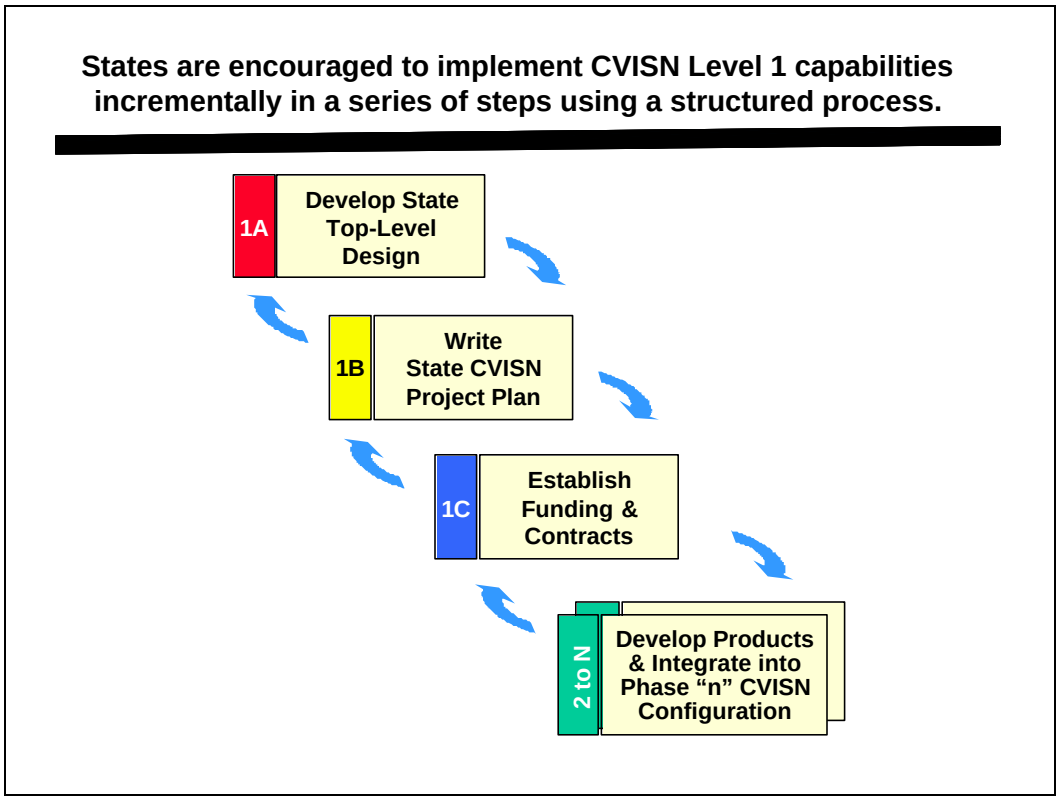


Figure C–1. Overview of CVISN Deployment Process

The figure shows that the first phase is devoted to developing the state top-level design, preparing the State CVISN Project Plan, establishing full funding for the project, and issuing major contracts for products and technical services. Each subsequent phase is a development phase that results in some type of demonstration or operational capability. More information on phases is provided in the *CVISN Guide to Project Planning* and the *CVISN Guide to Phase Planning and Tracking*.

This Guide to Credentials Administration has been prepared with the experience of early CVISN deployments in mind. It assumes that states will have to do considerable requirements analysis and state-specific planning. As time goes on and CVISN moves into the mainstream, this will be less the case. Some of the aspects of CVISN will become routine. This may be true for your state even now.

For example, if your state uses an existing fuel tax processing system (e.g., the Regional Processing Center (RPC) or the Lockheed Martin IMS VISTA/TS product) and this system has a proven electronic data interchange (EDI) front-end interface to allow electronic credentialing using open standards, you can move quickly through these processes and eliminate some of the detailed requirements analysis. Similarly, if your state uses an International Registration Plan (IRP) product that already has an interface to the IRP Clearinghouse, you should be able to shortcut the process and move to a quick implementation of that capability.

The approach defined herein assumes that your state is providing some level of system integration. If you decide to subcontract the role of system integrator, you may not follow the detailed steps outlined herein. Most likely, your system integrator will propose an approach based on their methodology. Nevertheless, the material herein can help you to understand what they must accomplish.

C.2 Top Level Design Phase

Top-Level Design Phase Process

The CVISN Guide to Top Level Design describes the general process for developing a top-level design. Figure C–2 describing this process is repeated below as a reminder.

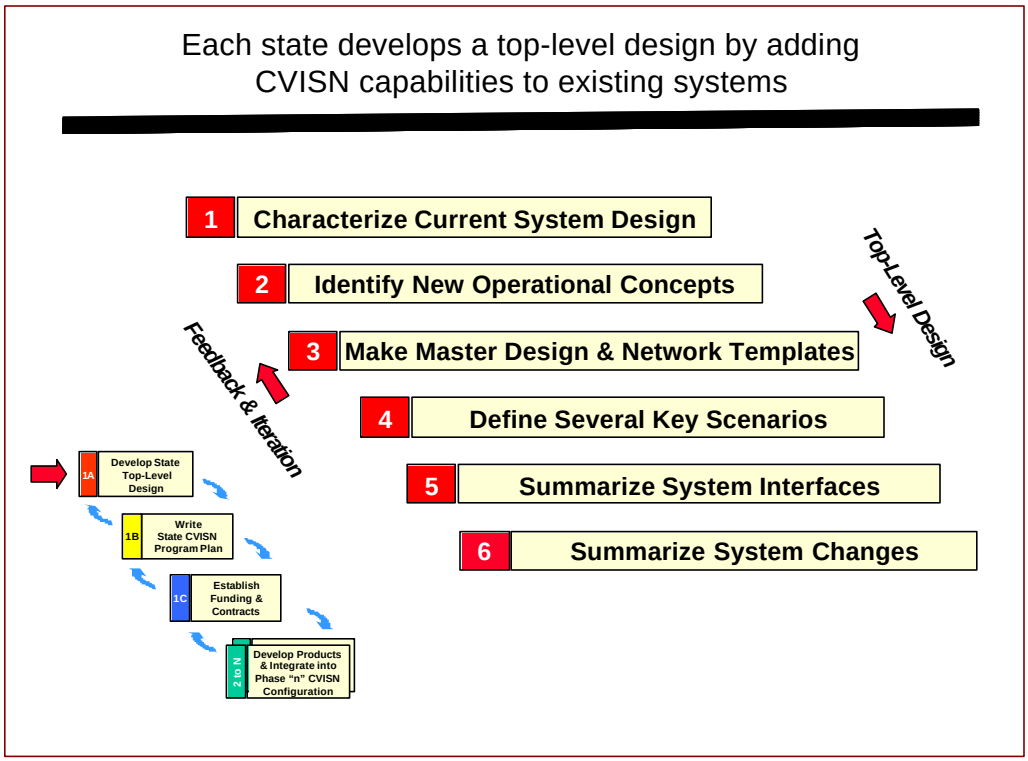


Figure C–2. Top-Level Design Process

Even though the steps are shown as sequential, the process actually involves a great deal of feedback and iteration. Throughout the process, identify issues, actions and decisions. At the end of this process, your state will have decided what products it wants to develop or acquire, what modifications it wants to make to existing systems, and how it wants to interface systems to each other. This phase establishes the technical framework for everything that follows.

Top-Level Design Phase Products

- A State CVISN Top Level Design Description that shows how credentials administration fits into the statewide CVISN design. It should include:
  - System Requirements
    - ✓ State-specific goals
    - ✓ CVISN Operational and Architectural Compatibility Handbook (COACH) Part 1 tables from Chapters 2, 3, 4, 5, 6
    - ✓ COACH Part 4 tables
    - ✓ Other state requirements
  - System Design
    - ✓ Allocation of requirements to system components
      - ➢ COACH Part 3 tables, tailored as needed
      - ➢ Description of functions for each new component
    - ✓ System Interface Summaries
    - ✓ Top-Level Physical System Design
  - System Change Summary
  - Operational Scenarios
  - Issues
- In addition to the State CVISN Design Description, your state may want to prepare a separate, more detailed Credentials Administration Requirements Specification (CARS) document. This document provides a description of how transactions flow end-to-end through all the systems supporting credentials administration. It also allocates requirements to each subsystem, legacy system interface and legacy modification. (Please see section C.6 for more on requirements specification.)

Factors to Consider in the Top-Level Design Phase

- The credentials administration area is the most complex of the three CVISN Level 1 capability areas. It involves multiple systems with complex interfaces. Different vendors or state organizations often develop these systems. A single transaction, such as registering a vehicle, may initiate other transactions that thread their way through 5 to 10 systems before the task is accomplished. A Carrier Automated Transaction (CAT) (or fleet management package) or Web site, Credentialing Interface (CI), IRP system, IRP Clearinghouse, state financial system, several bank systems, flags and conditions checks in related state databases, and an interface to Commercial Vehicle Information Exchange Window (CVIEW) (or equivalent) must all work properly for this function to work as a whole.
- Because of the complexity of the credentials administration area, it is especially important to limit the level of detail in the top-level design. The top-level design should provide a technical framework that allows the various parties involved to proceed with their parts relatively independently. For example, the top-level design can not specify every possible transaction scenario that can occur. But it can describe key scenarios and establish the framework for others. Similarly, it can not specify

precisely every possible error condition that can occur and how to handle it. But it can establish a systematic framework for dealing with errors.

- As part of the system design process, the state needs to deliberately assess the expected transaction volume and what that implies for computer, storage, and networking needs. This assessment should be updated periodically as the project proceeds.

Key Decisions

- For which credentials will the state implement electronic credentialing?
- Are there some parts of a credentials process where automation is impractical or the benefit of automation isn't worth the cost?
- Will the state implement a person-to-computer or a computer-to-computer interface for electronic credentialing? Will the state elect to implement both?
- If the state elects to implement a computer-to-computer interface for carrier-to-sate transactions, what interface method will be used (X12 EDI, XML, or other)?
- For each credential, will the state modify the legacy system (LM) to handle EDI, or translate the incoming transactions in some legacy system interface (LSI) and pass the credential application data to the legacy system in the native form?
- How will requirements be specified?
- How will snapshots be updated to reflect credentials actions?
- Where and how will snapshots be used in the credentialing processes?
- Where will error checks be performed?
- How can the state leverage the automation to help with paper forms processing?

Advice and Lessons Learned

- Develop requirements in multiple levels of detail. Use clear, concise top-level, testable, requirements as the basis for procurements and contracts. Develop more detailed business process descriptions as required by each phase as the work proceeds. (Please see section C.6 Requirements Specification for more discussion.)
- The use of a CI to serve as a single electronic interface from motor carriers to states has proven to be a useful concept. It allows a state to control and standardize its external interface to carriers independently from internal processes. It then preserves the ability to contract to different vendors for IRP, International Fuel Tax Agreement (IFTA), oversize/overweight (OS/OW), intrastate registration, hazardous materials (HazMat), electronic screening enrollment, titling, and carrier registration without impacting the motor carrier community each time a change is made. The state can hide internal changes from motor carriers by developing custom legacy system interfaces (LSIs).
- Survey carrier and service bureau customers to determine whether both a Web site and a computer-to-computer interface are required to support the needs of all segments of the carrier community. If both are warranted, plan for both from the outset.

C.3 Project Planning Phase

Project Planning Phase Process

The CVISN Guide to Project Planning describes the general process for developing a project plan and organizing the project. Figure C–3 that portrays this process is repeated below as a reminder.

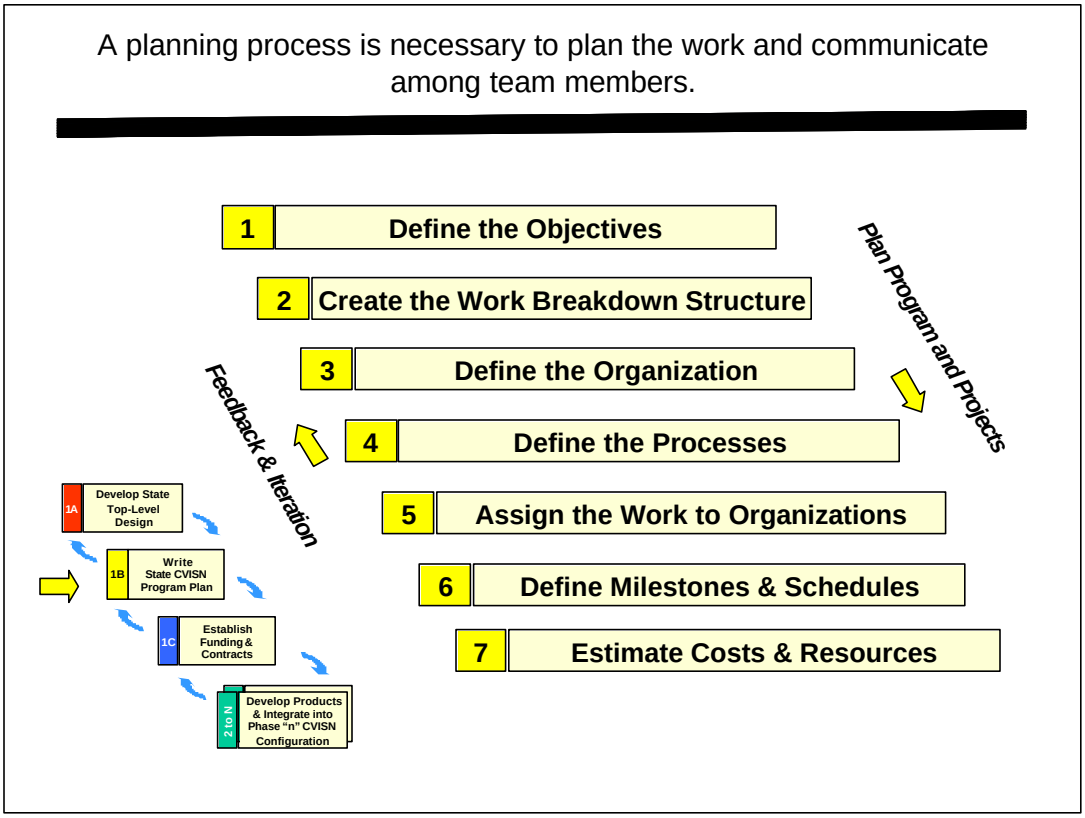


Figure C–3. Project Planning Process

Planning Phase Products

- A completed project plan that reflects the results of all the decisions made in this step. The top-level plan for credentials administration should be reflected in the State CVISN Project Plan.
- Documents necessary to support acquisition of full project funding. The plan should support this, but other proposals and state-specific documents may be required.
- Preliminary Phase Schedule for credentials administration systems and capabilities.

Factors to Consider in the Project Planning Phase

- What other projects are going on in your state that may impact the CVISN project. For several of the pilot states, Y2K efforts had such a high priority that resources were not available for CVISN tasks. Are there any major projects ongoing in your state that will compete for resources? Are major upgrades already taking place in the systems that support credentialing? Are major upgrades planned in the hardware and communications systems that will support the credentialing applications?
- If you are modifying existing systems in-house, will state staff be able to dedicate sufficient time to accomplish the modifications? Does this project have sufficient priority among all the on-going efforts? Does the management structure support the project?
- What policies does your state have on the use of the Web? Is there a program in your state to actively promote "electronic government" and deliver more services over the Web and the Internet? Can you leverage on these programs?
- What type of internal methodology has your state used in the past for information system development in the credentialing area? Is the process outlined in the CVISN guide series compatible with that approach? Are there any special requirements for feasibility studies or cost/benefit analysis studies?
- What is the typical procurement cycle in your state? What steps are required? How long does it take? What can be done to expedite this?
- What have other nearby states done towards implementing CVISN? Can you leverage what they have done, learn from them or partner with them in some way?

Key Decisions

- Should the state build or buy each subsystem?
- Will the state update current legacy systems or re-compete/re-develop?
- Will the state sponsor the development and deployment of a CAT? Who will provide CATs to early-adopter carriers?
- When will the state join each clearinghouse?
- Will the state participate in the Performance and Registration Information Systems Management (PRISM) program?
- What are the priorities and sequence for implementing capabilities?
- Who is the system integrator?
- Should the state have an independent verification and validation (V&V) agent?
- Sole Source or Competitive Contracting?
- Has the state planned to involve its carriers at each step in the planning process?
- Could other state or local agencies use the CVO data?

Advice and Lessons Learned

- If you are going to implement a computer-to-computer interface, your state should support the development (or modification) of at least one or two CAT or fleet management packages to interface to your state CI. Forcing carriers to pay for the development of a CAT capability to an undemonstrated state interface is asking a lot. Your program is likely to expand faster if you select a few carriers to test out a state-sponsored CAT capability. Ideally, CAT's (or equivalent fleet management products) would be used from two different vendors to provide choice and promote competitive pricing.
- If you are using X12 EDI, you need to test that your state has a working EDI interface to the state system(s), e.g., the CI, that are handling EDI credentials transactions.
- If you are implementing a CAT, the state should establish testing requirements and a test environment so that motor carriers and their software vendors can develop CAT packages on their own and easily test that they interfaced correctly with state systems. If you are implementing a Web site, testing is important as well and should be considered part of your CVISN program. Johns Hopkins University/Applied Physics Laboratory (JHU/APL) has developed a series of standardized interoperability tests and a CVISN Test Facility that can help. (Please see the *CVISN Guide to Integration and Test*, Reference 50.)

C.4 Funding and Contracts Phase

Funding and Contracts Phase Process

The CVISN Guide to Project Planning describes the general process for the funding and contracting phase. Figure C-4, which portrays this process, is repeated below as a reminder. The process for this phase is very dependent on state specific details. The figure is intended to give a conceptual framework and starting point. You should develop a specific process that meets the needs of your state.

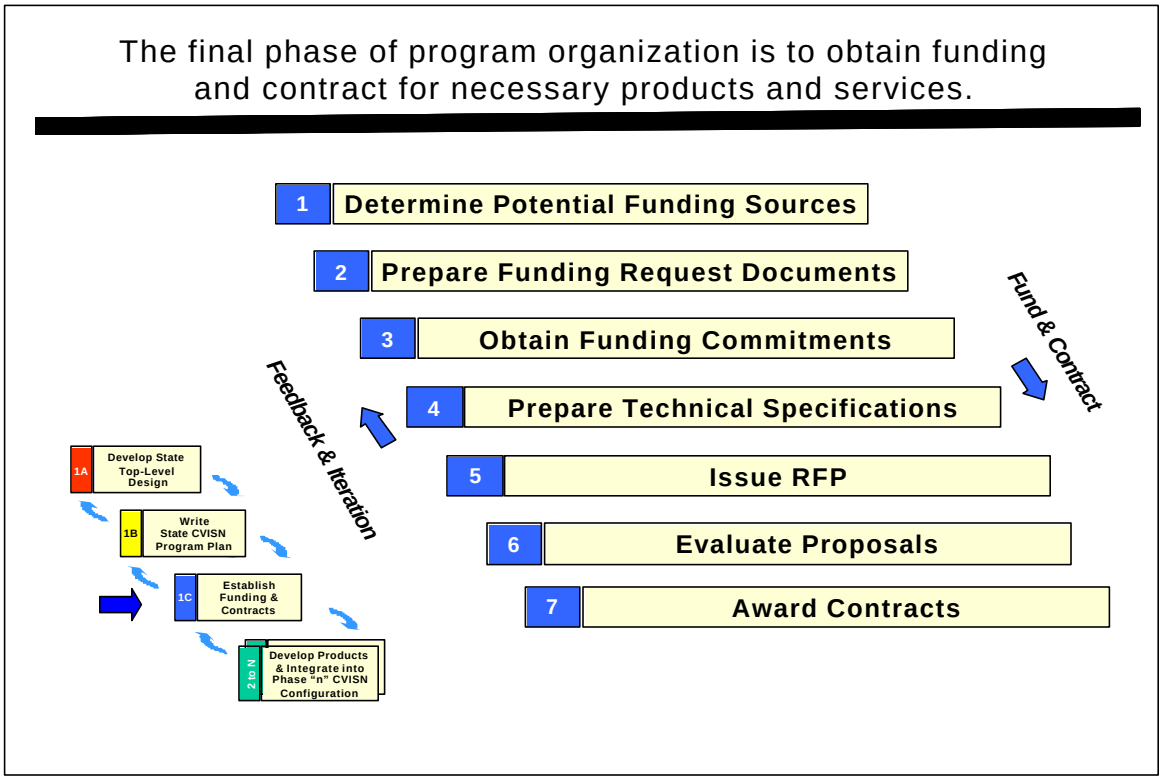


Figure C–4. Funding and Contracts Phase Process

Funding and Contracts Phase Products

- Documents needed (PR material, feasibility studies, cost/benefit studies, grant applications or proposals) to obtain funding
- Commitments for funding from state, federal and private sources on a schedule that meets project cash flow requirements.

- Procurement documents (e.g., request for proposal (RFP), evaluation plan, feasibility study, and sole source justification) to acquire hardware and software products as well as software development, system integration, communication, and verification and validation services.
- Flexible contract mechanisms are in place to support a team of contractors as required to complete all aspects of the project.

Factors to Consider in the Funding and Contracts Phase

- The credentials administration area is particularly complex. It is too complex to form an iron-clad specification of just how everything is going to work prior to issuing contracts. The state needs contractual vehicles that allow work to be defined and costs estimated at a high level before all the details are known. The contractual mechanism must also have the flexibility to define detailed process and system design as the work proceeds.
- Be sure to include measurements of performance and remedies for non-performance in contracts.
- Be sure to account for operations and maintenance in the budget estimates.
- *If the state is pursuing a mostly custom development approach:* The requirements analysis approach is critical. The requirements will guide the activities of the contractors. Consider including a proof-of-concept phase in which the state can judge the contractor's commitment and ability to meet the technical and schedule requirements.
- *If the state is using mostly commercial-off-the-shelf (COTS) packages:* The requirements analysis approach is required, but not as critical as with custom development. Basically, you are buying what vendors already have. You want an opportunity to "try before you buy". Consider including a preliminary demonstration phase in your contract that allows your state personnel to see the basic (unmodified) package they are getting before making the final commitment to it.

Key Decisions

- How much funding is required to complete the project?
- Where will the funding be obtained?
- What type of procurement should be used for each product or service?
- What can be done to expedite procurements?
- What type of incentives and remedial mechanisms should be included in the contracts?
- What terms and conditions related to software rights should be included in the contracts?
- How can the RFPs be written to assure architectural conformance and interoperability?

Advice and Lessons Learned

- If possible, set up some type of indefinite delivery/indefinite quantity (ID/IQ) contract vehicle with your systems integration agent and software services vendors. This allows you to define specific task orders as the work proceeds. It lessens the need to have a "frozen" set of requirements up front. It allows the team a lot more flexibility in solving problems. It allows adapting to changes in technology as the project proceeds.
- To assure architecture conformance, be sure to require that vendors prove that their deliverables conform to the architecture through the execution and analysis of interoperability tests. Also require design reviews so that the state's Conformance Assessment Team can check the design for conformance.
- When states decide to do a mostly COTS approach, they expect the costs to be very small. This expectation is often not met. For example, if your state purchases an existing CI, it is likely to require substantial modification and customization to fit in your environment. It may need custom legacy system interfaces. Your state may have slightly different processes than other states using the product. You may require additional data fields. The result is that the COTS product may still cost hundreds of thousands of dollars. Nevertheless, it is still cost effective because a development from scratch may cost millions of dollars.

C.5 Development Phase "n"

Development Phase "n" Process

The *CVISN Guide to Phase Planning and Tracking* describes the general process for developing and maintaining a Phase Plan and tracking progress as the phase proceeds. Figure C–5, which portrays this process, is repeated below as a reminder.

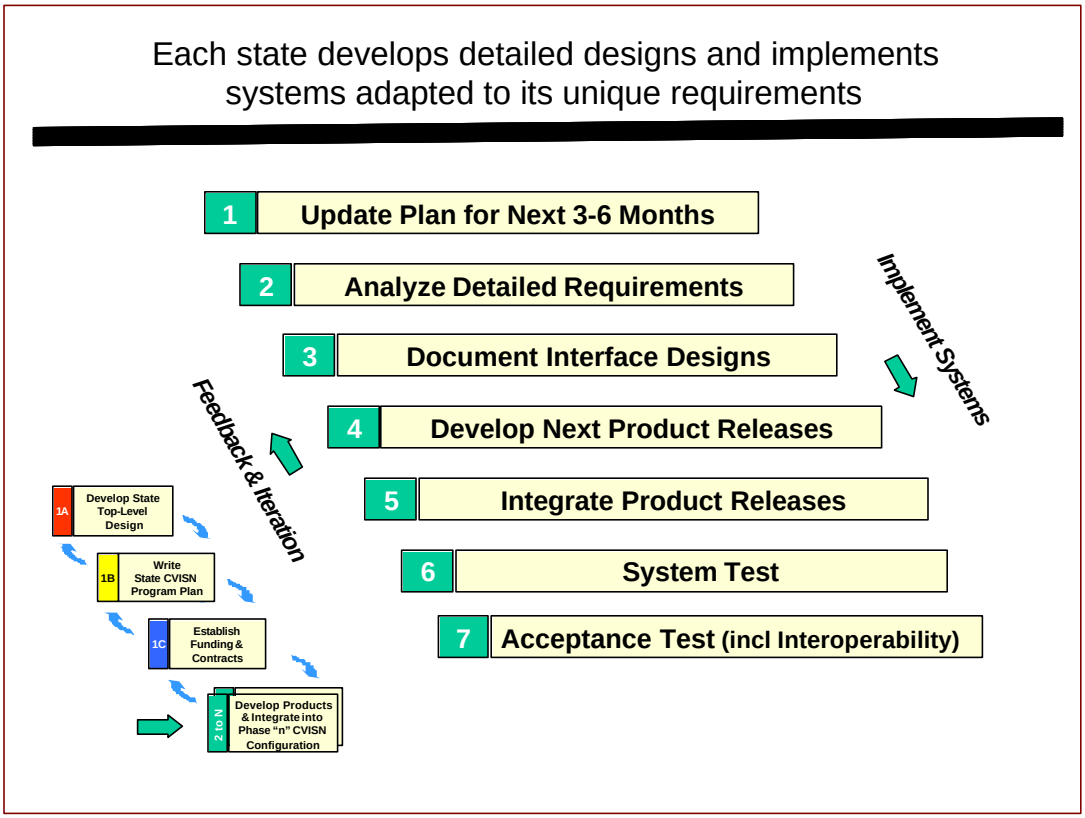


Figure C-5. Development Phase "n" Process

Development Phase "n" Products

- Working products (e.g., CATs, CI, LSIs, legacy modifications (LMs), Web site)
- Products integrated into the operational environment
- Test documentation showing proof that products worked as required
- Operation and maintenance documentation
- Net result: New operational capabilities

Factors to Consider in Development Phase "n"

- You need to be able to incrementally define details. Allow time in the schedule to define more scenarios and to document the state specific interface requirements at the beginning of each phase. If you are implementing X12 EDI, the state-specific EDI requirements should be published in a *State of ___ Motor Carrier Electronic Credentialing EDI Interface Control Document* that is made available on a state Web site.
- As components are developed, tests should be executed to verify that the components meet the design. As components are integrated, interoperability tests should be

executed to verify that the standard interfaces were implemented correctly, and that the components and products work together correctly.

- Configuration management becomes very important when integrating products from multiple vendors. A change management process must be in place. As changes are made to interface designs, everyone must be kept informed of changes and planned updates. Updates to systems on each end of the interface must be synchronized. Version numbers must be systematically assigned to all products and version description documents prepared to coordinate updates and make sure that compatible versions are installed together.

Key Decisions

- How should the initial design be modified based on the experience gained in each phase?
- How should the initial phase plan be modified based on progress actually made in each phase?

Advice and Lessons Learned

- Incremental deliveries reduce the risk for both the state and the vendor. Use them.
- Assuming that you are doing incremental development, allow time at the beginning of each phase for a "mini-business process reengineering (BPR)" study of just the processes for that phase. For example, maybe the next step focuses on the "IRP Add Vehicle" supplemental transaction. Allow a few days to define detailed processes. Also, refine the interface specifications at this time. Finalize any state specific details related to EDI interface maps (the software that converts legacy system data from or to EDI) at this time. This "just-in-time" analysis will present topics to the development team when they are ready to handle them and need the results. It will avoid "warehousing" a thick specification on a shelf to gather dust.
- An early delivery that shows tangible progress is critical to building the team, establishing forward momentum, establishing credibility, and securing funding. For example, Maryland established an electronic credentialing capability with several carriers with early versions of the CAT and CI. This was done even before the CI was interfaced to the state's processing systems. This allowed the carriers to try out the electronic credentialing concept. The state still needed to print out the application from the CI and retype it into their legacy system. Nevertheless, this was a good first step because it established the most critical interface, that between the carrier and the state.
- Schedule management is especially important in the credentials administration area because of the need to coordinate multiple vendors. The state needs an integrated schedule that has top level milestones and any external dependencies among the various vendors and organizations involved. The system architect needs to have clear authority to adjust the schedule details in response to technical issues. However, everyone must make a firm commitment to meet major milestones.

- The credentialing area will probably require close coordination among a number of vendors. Vendors will be dependent on each other for achieving their goals. These external dependencies need to be identified and carefully managed. When problems come up (as they always will, even in the best programs) there will be a tendency for everyone to blame the problem on someone else. You need a strong system integrator and problem resolution process to deal with this.
- An early indicator of a vendor's ability to perform is to check the level of effort being applied. There is no substitute for a visit to the vendor's development facility. Ask to meet the people working on your system. Ask what other assignments they are working on. Step back and perform a "sanity check" on staffing levels. Ask yourself if it is realistic to expect the work you want with the effort that is being applied.
- Hopefully, careful planning will allow things to go well with your vendors. But be sure to have contractual remedies in place just in case they don't. These can include progress payments based on performance, incremental funding, and cancellation clauses.
- Test data can be time consuming to prepare. Build on existing test data (e.g., the CVISN interoperability test suite package) when possible. Lack of test data can cause insufficient test and allow problems to go undetected until systems are put into production.
- Changes in requirements can kill project schedules and cause cost overruns. An effective configuration management (CM) process is necessary to ensure that changes are only made when the impacts on cost and schedule are understood and approved. For more information about CM, please see Reference 47.

C.6 Requirements Specification

Development of accurate requirements specifications that are detailed enough (but not too detailed) is a critical success factor in a credentials administration project. It is discussed here as a separate topic because it is a consideration that has impact on all phases of the development process, from top-level design through final acceptance testing. Several alternatives to specifying requirements are discussed below.

Alternative A: Simplified Requirements Specification Document.

If your state is not experienced in using detailed requirements specifications effectively, a simplified approach may be a better choice. Consider not writing a very detailed credentials administration requirements specification up-front. Some folks think that a thick, detailed requirements document will ensure that the contractor will produce what you want. Experience has shown that this is not necessarily the case. Instead, a concise requirements document that states the end results and leaves the details to be developed as part of the phased development process is more likely to succeed. Remember that your objective is to produce a top-level requirements specification that limits the project scope and is concise, testable, and provides a basis for establishing and managing a contract.

One suggested approach is to use your *State CVISN Top Level Design Description* as the basic source of requirements for your credentials administration subsystems. The design description should include the completed sections of the various parts of the COACH:

- COACH Part 1, Operational Concept and Top-Level Design Checklists
- COACH Part 3, Detailed System Checklists
- COACH Part 4, Interface Specification Checklists

Review and edit these, filling them out and customizing them as required to meet the needs of your state.

Your request for proposal (RFP) should refer to specific sections of the design description relevant to the item or items being procured. It can also reference these guides and any other state specific documentation (e.g., strategic plans) that provide background or describe your concept of operations. The RFP should require that the product pass the interoperability tests. Please see the COACH Part 5 (Reference 6) and the CVISN Interoperability Test Suite Package (References 26-28) for further information. The RFP should require that as part of the project, the vendor perform systems analysis and develop more detailed process descriptions and related requirements with operations personnel during each phase of the project. These process descriptions may be done in joint application design sessions using participant flows or some equivalent method and diagramming technique. When evaluating proposals, pay particular attention to the vendors' experience and proposed approaches to working with your team to develop these detailed process designs.

Alternative B: Delta Requirements

If your state is using a largely COTS approach, you may want to consider a variation on Alternative A. Do the simplified requirements specification based on your State System Design Description and COACH as described above. Then ask the contractor to install their COTS products for a trial period of 1-3 months. During this time, ask the contractor to develop a "delta" (i.e., difference) requirements specification that just describes what changes you want to make to their product. The contractor may use checklists, focus groups, interviews and other techniques to collect these delta requirements.

Preparation of the delta requirements is in lieu of a detailed description of each scenario or business process. If you are basically satisfied with the process as it exists, there is no need to spend a lot of effort documenting it.

Alternative C: Comprehensive Requirements Specification Document

Traditional software life cycle models advise having comprehensive, detailed, requirements nailed down in a requirements specification before the project starts. We have noted some problems with this approach, including:

- Developing the document is costly and time consuming
- Processes change and the document quickly becomes obsolete
- If the people developing the document aren't the ones developing the system, much of the investment remains locked in the heads of the analysts who wrote the specs and is not transferred to the developers. The developers will likely want to redo this work themselves and get the users' perspective first hand.
- User personnel often don't have time to invest in really studying requirements documents and making sure the documents reflect their needs
- It is very difficult for even the most dedicated user personnel to review the documents and actually understand what they are getting. When they finally see the system, they will realize that there were lots of things they wanted that didn't occur to them when reviewing the specs.

However, if your state has worked successfully with comprehensive, detailed requirements specifications before and this is what you want on this project, consider issuing a partial draft of the requirements specification as part of your RFP. Then have the successful bidder complete the draft as you require as part of their contract. Have them finalize sections with each phase of the project as it proceeds.

In Maryland and Virginia, comprehensive *Credentials Administration Requirements Specifications (CARS)* (References 48 and 49) were prepared up front. These documents provided a description of how transactions flow end-to-end through all the systems supporting credentials administration. They also allocated requirements to each subsystem, legacy system interface and legacy modification and defined interfaces between those elements. Because the prototype states were the first to initiate the credentialing project, it was felt that a comprehensive document like the CARS was needed. In retrospect, the CARS documents provided a wealth of information and were useful to the projects. In particular, the participant flows (in CARS Chapter 3, Business Processes) were very useful for gaining an understanding of how the users wanted the final system to work. However, the more technical sections of the CARS (Chapter 4, Systems Business Processes and Chapter 5, System Functional Requirements) were less useful and are not recommended for future efforts because of the time and cost of preparation.

Appendix D. CREDENTIALS ADMINISTRATION IN THE CVISN MODEL DEPLOYMENT STATES

This Page Intentionally Blank

CREDENTIALS ADMINISTRATION IN THE CVISN MODEL DEPLOYMENT STATES

Several of the Commercial Vehicle Information Systems and Networks (CVISN) Model Deployment States provided information about how they are implementing credentials administration functions (see subsequent sections in this chapter). This information is included below as written by the states without further editing. All information is as of July 2000 unless otherwise noted. It is subject to change and is provided as background only.

D.1 California

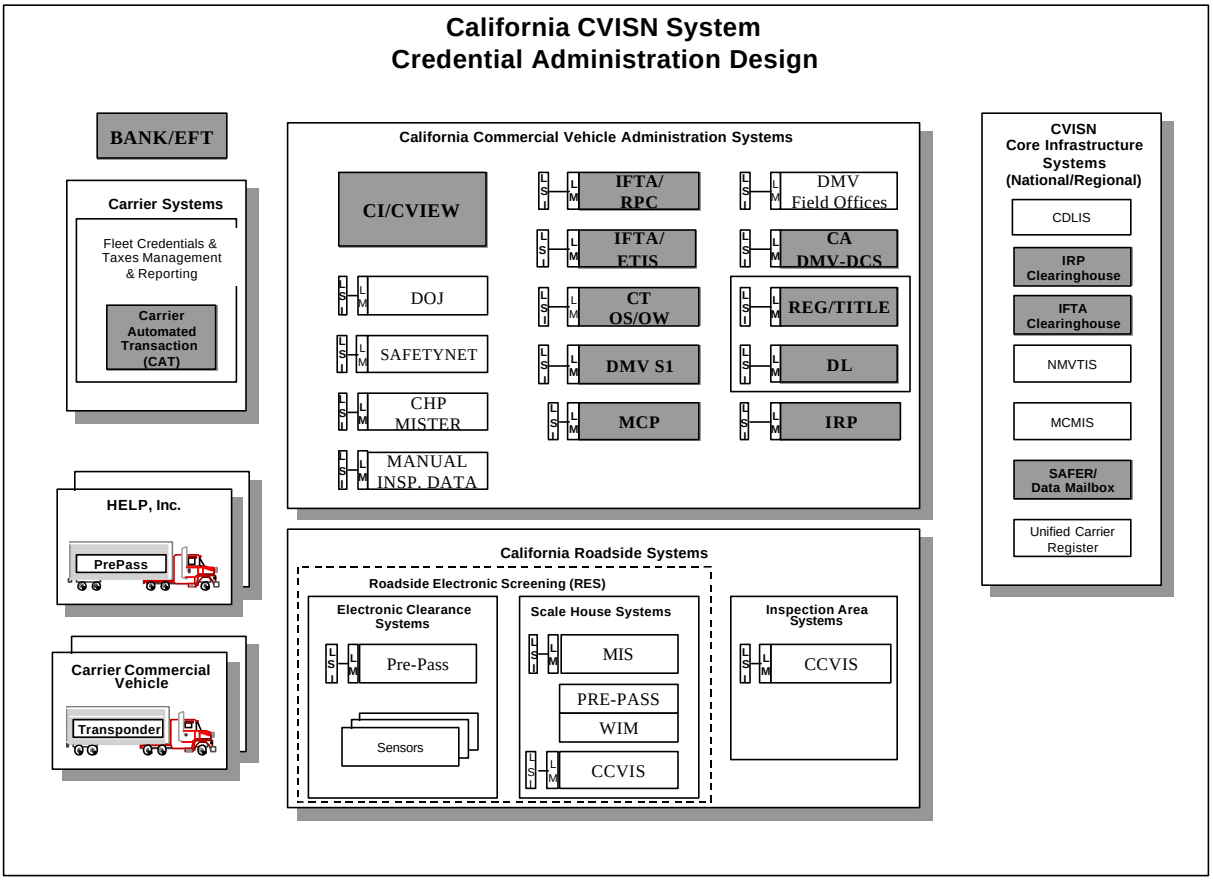


Figure D-1. CA CVISN System Design Template

Highlights of California Credential Administration modifications and planned or existing capabilities include:

- Develop a CAT requirement document. The CAT will provide capabilities for complete point of sale credential application processing for IRP, IFTA, OS/OW, SSRS, and then adding MCP and intrastate registration.
- Will determine the applicability of the CAT software for use in DMV field offices. Plan to use the Internet, using EDI transaction specifications, for communications between the carrier's CAT system and the state's CI system.
- Develop a CI/CVIEW requirement document. The CI will provide an interface among the carrier's CAT system, the state legacy systems in its native mode, the core infrastructure systems, and the connection and use of the public domain CVIEW software.
- Using the Regional Processing Center (RPC) to support IFTA functions.
- Using the Illinois Single State Registration System (SSRS) to support interstate insurance functions.

D.2 Colorado

(April 1999) Colorado has been maintaining a database of commercial vehicle credentials for many years. This process began in 1985 with the installation of computer systems in each port of entry location. Although we used extracts from various State credential legacy systems, and merged the data with tapes provided by major carriers operating in the state, we relied mostly on our field officers to populate and maintain our database. This meant that, at a minimum, a driver would have to come in at least once a year to produce proof of current credentials so that our expiration dates could be updated. Since credentials expire at different times during the year, drivers who frequently clear our ports could be called in multiple times.

With the advent of CVISN we are attempting to minimize the data entry effort for our officers. This will have a direct benefit for the drivers as well as for their corporate staff that insures they are properly credentialed. We are also integrating *more* data into our credential processes, such as SAFER information

Colorado has contracted with Intelligent Decision Technologies (IDT) Ltd. to provide us with a Web-based application system. This system will provide the carrier the ability to electronically apply for, and receive, credentials for IRP, IFTA, IFTA Quarterly tax returns, SSRS and Hazardous Material licenses. We intend to add additional credentials once we exhibit success with the initial offering, such as the Oversize and Overweight permits, USDOT application and Emissions Exemption waivers. The greater benefit here is to the carrier who will no longer need to deal in person with multiple agencies and multiple departments in order to obtain their operating authority.

We are also in the process of sending this data electronically to the roadside. The officers will no longer have to stop drivers and do a physical check of their credentials in order to update the

database. Since we can receive necessary data from different state and federal agencies, more information can be provided at the roadside in a quicker manner.

One problem with this attempt is how to link different data elements from different agencies to the same vehicle. In order to resolve this we are asking our officers to capture US DOT numbers whenever possible. Matching US DOT number to VIN numbers seems to be our best possible means of identifying a vehicle and tying their credential information to it.

In addition to our in-state efforts, Colorado will begin the process of connecting to the IRP and IFTA Clearinghouses and sharing our data nation-wide.

D.3 Connecticut

In Connecticut, three agencies are involved in credentials administration: DMV for vehicle registration, SSRS, title, and driver's licenses, DOT for Oversize/Overweight Permits, DRS for fuel taxes.

D.4 Kentucky

(April 1999) Figure D–2, a high-level system design template highlights those credentials administration functions targeted for inclusion in Kentucky's CVISN deployment strategy. Additional information relating to CVISN and CVO activities can be found at http://www.kytc.state.ky.us/motorcarrier/Motorcar.htm and http://acvo.uky.edu.

It should be noted that the ALTS Terminal located in Roadside Systems is part of an existing operation for verifying certain credentials; this operation will be retired once a certain level of CVISN functionality is achieved.

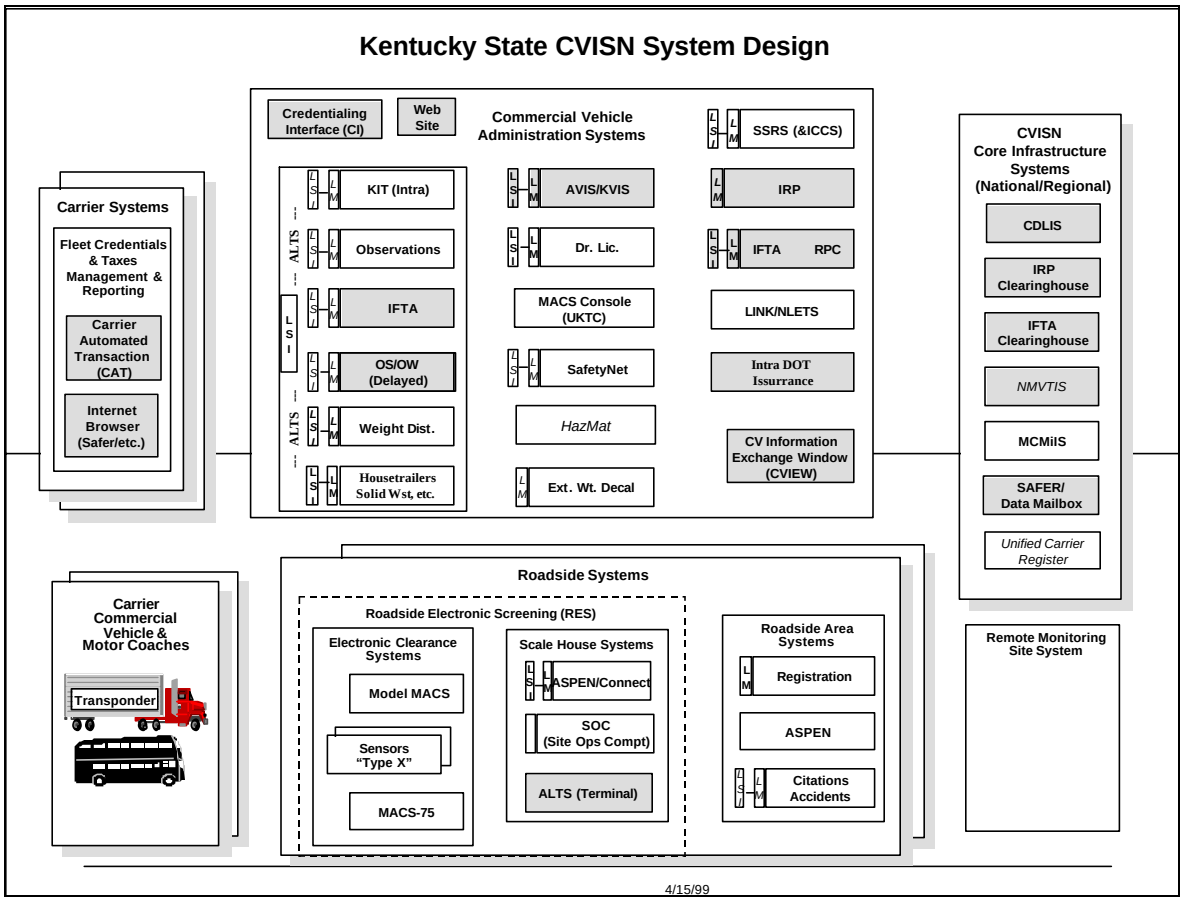


Figure D–2. KY CVISN System Design Template

Highlights of Kentucky's plans include:

- Implementing a credentialing interface (CI) to serve as the primary focal point for incoming and outgoing electronic credentialing activities with carriers.
- Preference of a commercial carrier automated transaction (CAT) package to assist in building and testing the various CI and CVISN systems and applications.
- Link existing credentialing system beginning with the IRP and IFTA followed by OS/OW.
- Working with a select and representative group of carriers to obtain carriers' perspectives and to foster communication.
- Installation of CAT functionality at regional public sites for access by the smaller carrier operations.
- Use of the Internet as the means of data communications
- Use of existing applications and systems containing the business rules where feasible.
- Connection to the CDLIS, IRP Clearinghouse, IFTA Clearinghouse, and NMVTIS.
  - Use of the public domain version (core modules) of CVIEW as the communication link to SAFER.

- Placing all CVO credentialing manuals and procedures on Web servers for access by carriers.
- Developing a Web interface containing basic credentialing functionality in addition to providing for commercial CAT and EDI interfaces
- Use of Regional Processing Center (RPC) to support IFTA functions.

D.5 Maryland

(April 1999) Figure D–3 shows Maryland's system design template, with the credentials administration-related functions highlighted. More information about the MD CVISN project can be found at http://www.mdot.state.md.us/mmcp/index.html. Information about the MD Business Licensing Information System can be found at http://www.blis.state.md.us/.

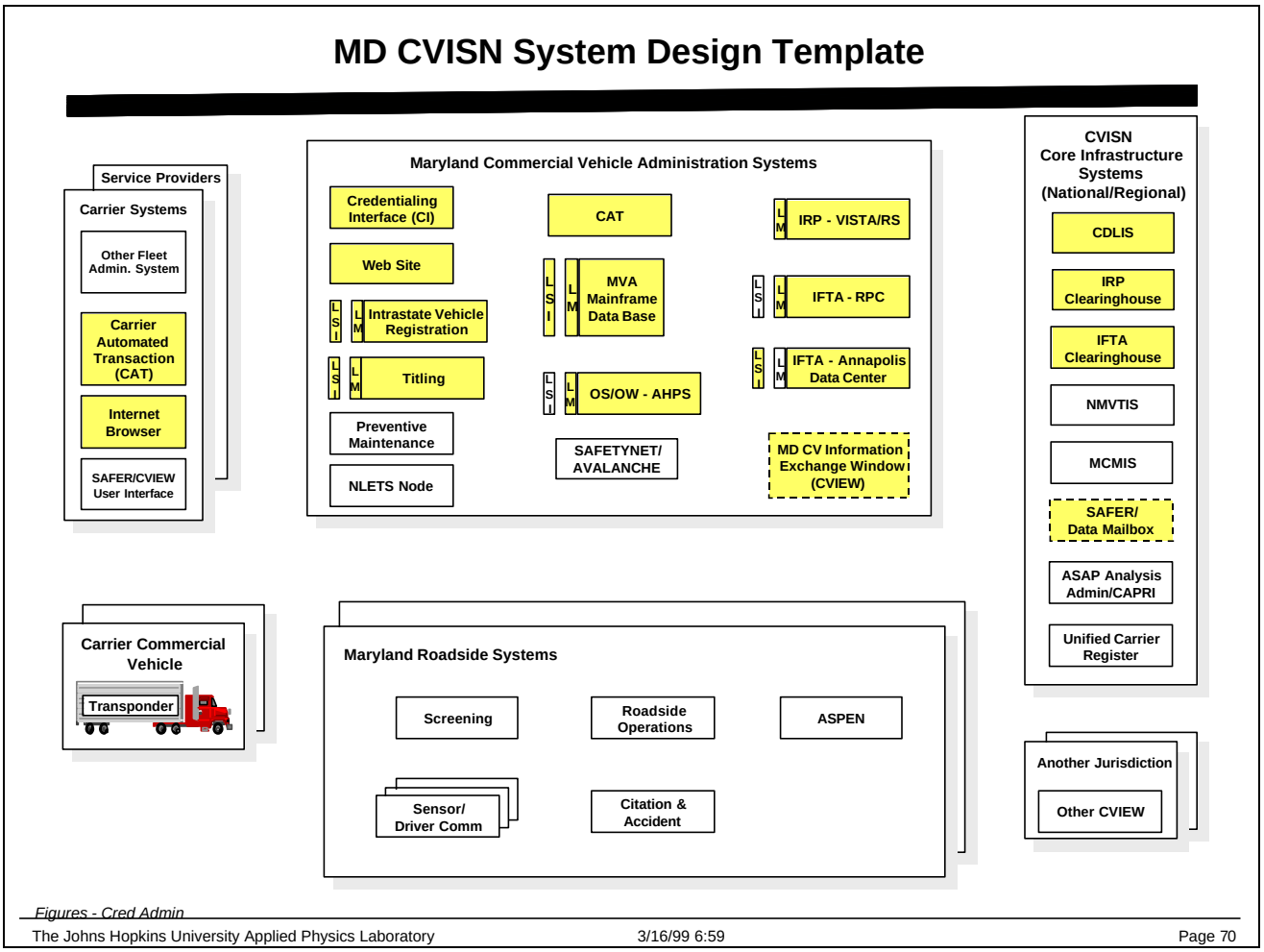


Figure D-3. MD CVISN System Design Template

Highlights of Maryland's credentials administration modifications and planned or existing capabilities MD include:

- implementing a CI and CAT, starting with IRP, then IFTA.
- also plan to implement electronic credentialing for titling, intrastate vehicle registration, and oversize/overweight permitting
- also installing the CAT at regional MVA offices, so that MD staff can use the product to enter information from paper applications received over the counter
- developing a WebCAT for IRP initially
- connected to the IRP and IFTA Clearinghouses as part of their pilots
- using the Regional Processing Center (RPC) to support IFTA functions
- using a commercial product for IRP functions
- put Motor Carrier Handbook on the MD DOT WWW page
- added 2 Servers to support the CI, state office CATs, and CVIEW, with plans for two more to support operational mode
- improved existing connectivity between VISTA/RS and MVA to support additional traffic associated with IRP; between MVA mainframe and MDOT networks for access to MVA Legacy Database; MDOT networks and MD Comptroller's networks for IFTA; MVA and weigh station facilities for carrier and vehicle snapshots; MDOT networks and the Internet (firewall upgrades, domain name services, etc.) for IRP, IFTA, intrastate, Web CAT.

D.6 Michigan

Figure D–4 provides a general schematic of the recommended CVISN architecture for the State of Michigan. The architecture encompasses 11 existing legacy systems and four new systems, and provides secure communications between agencies, with motor carriers, and with third parties such as national information systems, banks, and insurance companies. The implementation uses the state's existing Lansing communications network to link state agencies, and a mix of communications networks to introduce motor carriers and third parties. There is a central hub for all CVISN communications that incorporates the federal architecture concepts of the "Credentialing Interface" and the "CVIEW" data exchange window or "snapshot" database.

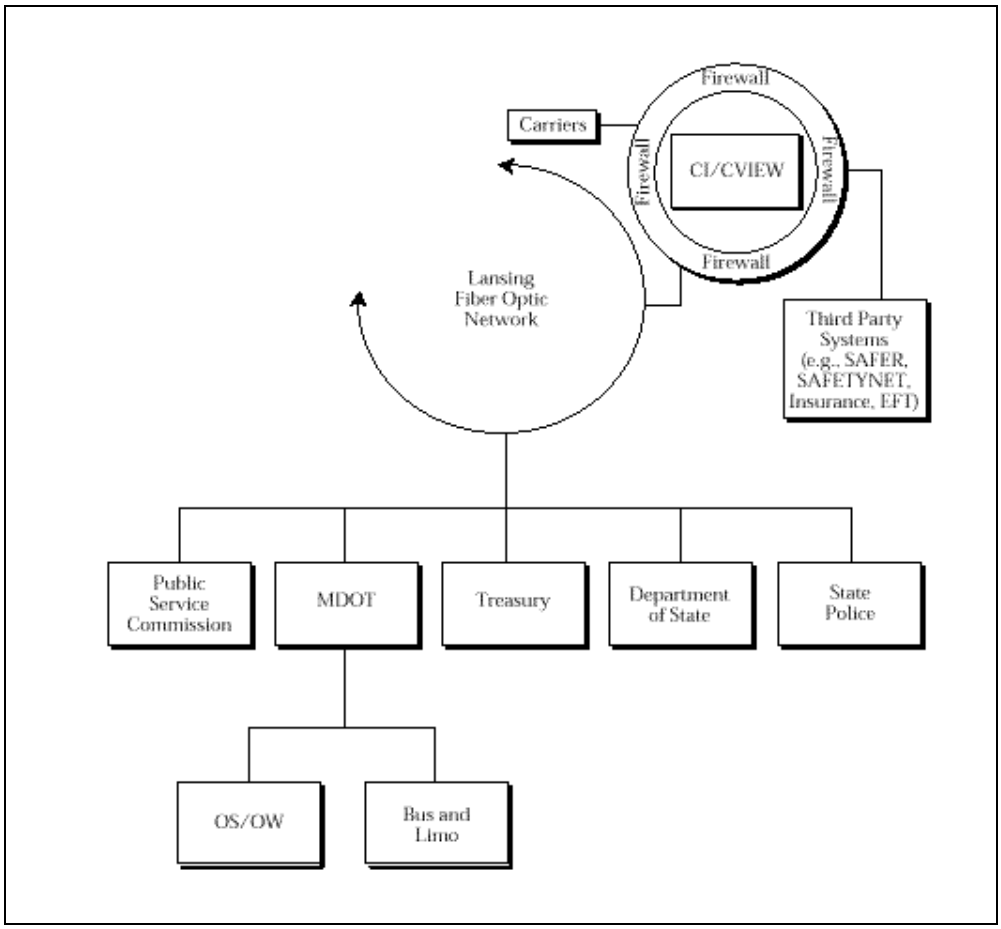


Figure D–4. MI General Schematic

From an agency perspective, there will need to be changes to existing legacy systems, both to accommodate the submission of credential requests by motor carriers and to be able to query the snapshot database for additional information not previously available. The general look and feel for the individual agency employee, however, will not drastically change – mainframe users will remain mainframe users, and PC users will remain PC users. Behind the scenes, a "Legacy System Interface" and a revamped security firewall will handle the interaction with the rest of CVISN.

Motor carriers will have the biggest set of new functionality. Participating motor carriers and their agents will be able to use computer software to submit and retrieve credential requests electronically using a dial-up approach called a "Virtual Private Network" (VPN) that is based on the Internet backbone. Since the CVISN network will be available nearly 24 hours per day as opposed to the regular, more restrictive business hours, this electronic capability will increase the level of service available to carriers.

The recommended system architecture for Michigan CVISN uses the core national standards for a CVISN architecture as a starting point, then customizes the national architecture to fit the specific situation found in Michigan. The customization process used interviews with agency staff about existing systems, and desired CVISN process and system requirements. The process then reviewed the state of the practice in over 20 different systems and business process areas, and recommended the best approaches for Michigan CVISN.

The customization process followed a series of design goals with respect to the agencies involved:

- Adherence to the functionality of the national CVISN architecture;
- Availability of the ANSI X12 Electronic Data Interchange Standard when connecting to external systems as required by the national architecture;
- Minimal intrusion on existing legacy systems;
- Minimal changes to the agency processes used to handle paper-based carrier credential submissions, which still will take place;
- Usage of existing infrastructure whenever possible;
- A modular design that allows for individual components to fail without shutting down the entire system;
- A single point of connectivity between each agency (the firewall) and the rest of CVISN (the CI/CVIEW); and
- A generic approach to processes and systems that is suitable for all agencies.

The last point is critical from a design and maintenance standpoint. While each agency has its own unique systems and processes, it is necessary to consider a generic "agency-blind" approach in designing the overall architecture. The alternative would consume significantly more resources in the implementation phase of physical and detailed system design.

Figure D–5 provides an overview of the architecture from the perspective of a generic Michigan agency. Each agency has between one and four deskside systems. These systems are used either for credential management, or for the manipulation of inspection and compliance information. These systems currently exist at each agency; no new legacy systems are proposed. A legacy system interface (LSI) will be built to facilitate transactions between systems. Conceptually, we have drawn a different LSI for each legacy system, but the actual implementation approach will be left to the discretion of each agency.

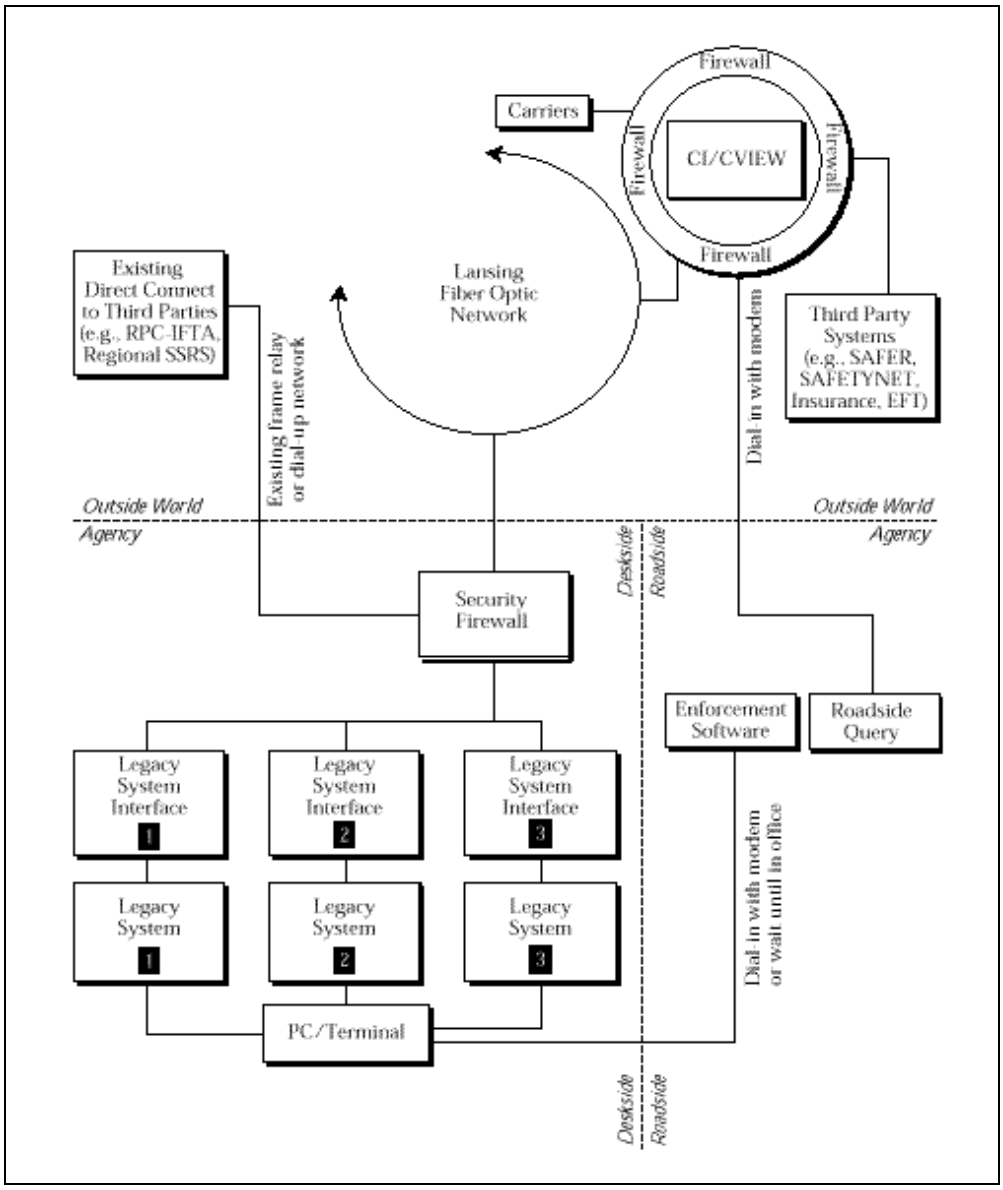


Figure D–5. MI Architecture from Agency Perspective

Participating motor carriers will submit their credential requests through the Carrier Automated Transaction (CAT) software. The CAT software will connect to the CI/CVIEW, which will gather carrier requests for each legacy system. For some transactions, the CI/CVIEW may augment the request with additional data from the carrier or vehicle snapshot. The agency's LSI then will connect to the CI/CVIEW, will download the requests, and will manage the data transfer and storage into the legacy system. Once credential requests have been processed, electronic notification will be sent back to the carrier.

The process is the exact reverse for the carrier notification and snapshot update process. The legacy system will provide data to the LSI about the credential and its resolution. The LSI will build the appropriate message for the carrier, as well as any changes to the carrier or vehicle snapshot. On a periodic basis, the LSI will connect to the CI/CVIEW, and will transfer the information. The submission will be kept at the CI/CVIEW until the carrier's next connection.

Paper-based credential submissions generally include a check for payment. With electronic submissions through CVISN, an alternate method is needed. Therefore, the CVISN architecture will support electronic payments through three different payment types (bank debit, credit card, and third party managed escrow) on a nightly basis. Each LSI will be responsible for managing payment request information at a per-credential basis. The CI/CVIEW will gather payment requests for all carriers, and will forward them to the appropriate institution for payment.
The intention of the recommended CVISN architecture is to minimize the number and scope of changes to agencies' existing legacy systems. Unfortunately, some modifications will be necessary for most systems to handle the new functionality provided by CVISN. Most modifications involve the carrier submission of credential requests that are "waiting for approval" into the legacy system databases.

D.7 Minnesota

(April 1999) Figure D-6 summarizes the system interactions in Minnesota's credentials administration design.

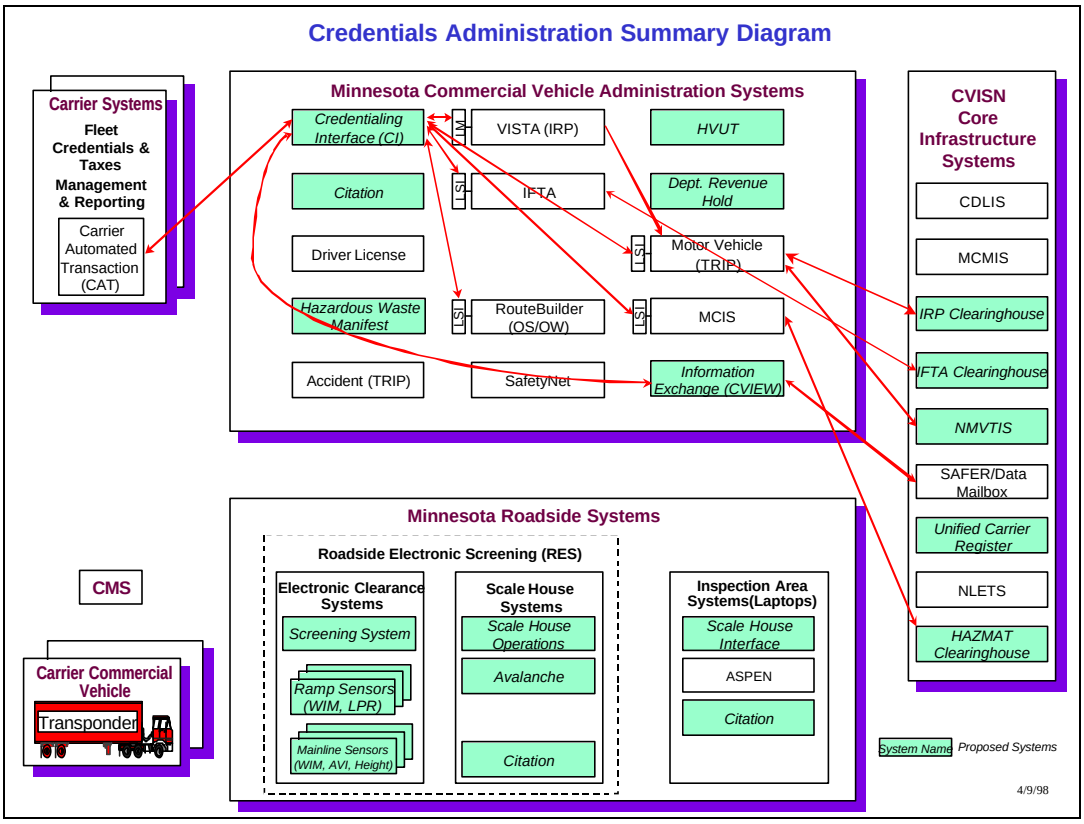


Figure D–6. MN Credentials Administration Summary

Highlights of Minnesota's credentials administration include:

- Implementing a CAT system with capabilities for IFTA, interstate operating authority (SSRS), and intrastate vehicle registration in the first release in April, 2000. Release 2 in December, 2000 will add IRP, OS/OW, and Uniform Hazardous Materials Permit functionality.
- Developing a customized, combined CVIEW and CI systems on the same installation.
- Designing a generic LSI structure to reduce redundancy and future maintenance costs.

D.8 Oregon

No information was available from Oregon at the time of publication of this document.

D.9 Virginia

Figure D-7 shows Virginia's Top Level Data Flow for Credentials Administration.

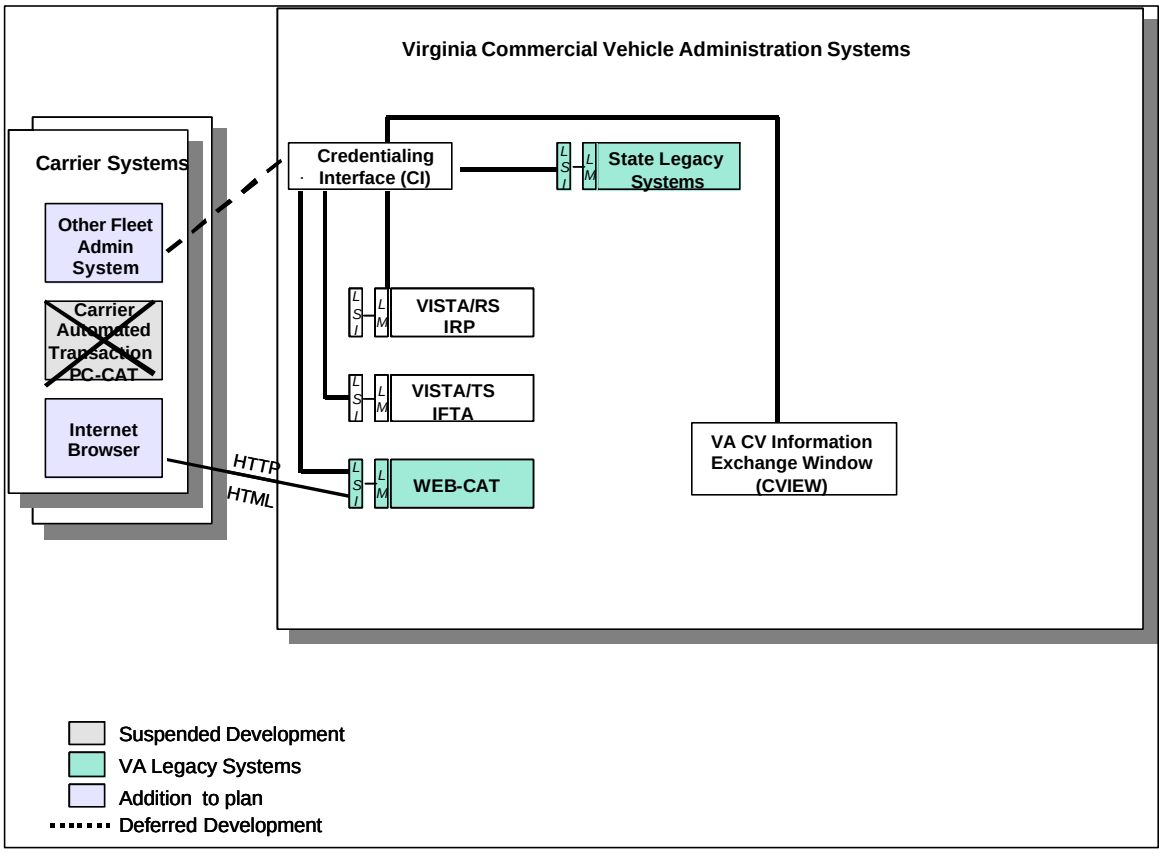


Figure D–7. VA System Design Template

Highlights of Virginia's Credentials Administration current and planned capabilities include:

- Deployed PC-CAT in five Carrier's offices. Conducted technical assessment and evaluated carrier feedback during limited operations period. Abandoned PC-CAT efforts in favor of internet web based solution.
- Installed and evaluated Kentucky version of Credential Interface (CI). Documented Virginia specific delta requirements for IRP.
- Developed legacy modifications to Intrastate Operating Authority and Titles and Registration systems for interface with CI. Will reevaluate these modifications when

Virginia moves forward with integrating Intrastate Operating Authority, titling and intrastate registration into their web based solution.

- Contracted with new vendor to assist DMV in the development of the webCAT (internet web based solution). webCAT business requirements completed and are continually being updated. Developed a project management web site.
- Participated in IRP Clearinghouse pilot; automated interface is operational. IRP Clearinghouse in production with 15 jurisdictions.
- IFTA Clearinghouse pilot jurisdiction. EDI interface for demographic data and transmittal data is operational. Anticipate moving into production mode before the end of calendar year 2000.
- Reached agreement with FHWA to pursue web solution utilizing flat files.
- Deployed web front-end to DMV production web server at https://www.dmv.state.va.us/webcat
- Level I functionality has been developed plus interfaces to Virginia legacy and payment systems. Further capability to be developed.
- WebCAT should be fully operational and in production for IRP, IFTA and Virginia Motor Fuel Road Tax during the summer of 2000. Transaction services that will be available include:

IRP

1. Add vehicle
2. Add jurisdiction
3. Delete vehicle
4. Transfer plate
5. Transfer and exchange plate
6. Change vehicle unit number
7. Replace credential
8. Increase weight
9. Address change
10. Renewal notices
11. Renewal
12. Add fleet
13. Convert Virginia plate to IRP plate
14. Pay invoice

IFTA/Virginia Motor Fuel Road Tax

1. Tax return filing
2. Miscellaneous tax payment
3. Additional decal order
4. Renewal notices
5. Renewals

General webCAT System Features and Capabilities

1. Secure environment (user ID and password protection)
2. On-line user registration
3. Storage of account, fleet, and vehicle data
4. Database management to ensure webCAT and legacy system databases are synchronized
5. Transaction manager which organizes transactions into three categories: (a) saved but not submitted, (b) submitted, (c) historical
6. Business rule edits
7. On-line help
8. Credit card, ACH debit and ACH credit payment options
9. Options to receive credentials through mail, pick them up at any DMV Customer Service Center, or self issue credentials
10. Validations to ensure vehicles are titled in Virginia prior to registration
11. Validations to ensure compliance with Heavy Vehicle Use Tax (HVUT)
12. System checks to ensure credentials are not issued if stops or suspensions are on file

- Virginia will begin to develop additional webCAT services later in 2000 to include titling, Intrastate Operating Authority and Single State Registration. Later in 2001 it is anticipated that webCAT services will include electronic notification of overweight violations and the option to pay for such violations through webCAT.

D.10 Washington

Figures D–8 and D–9 show Washington's system design template.

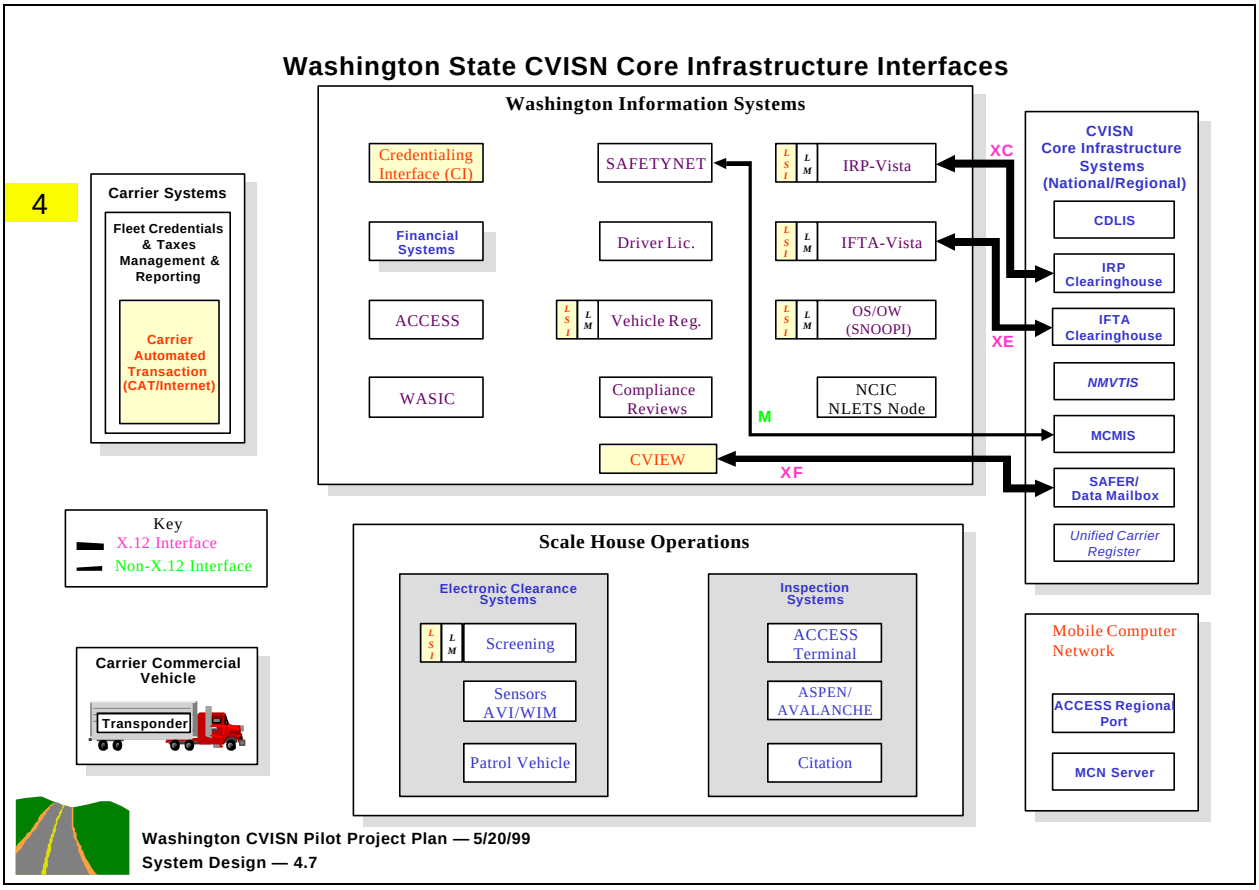


Figure D–8. WA CVISN System Design Template

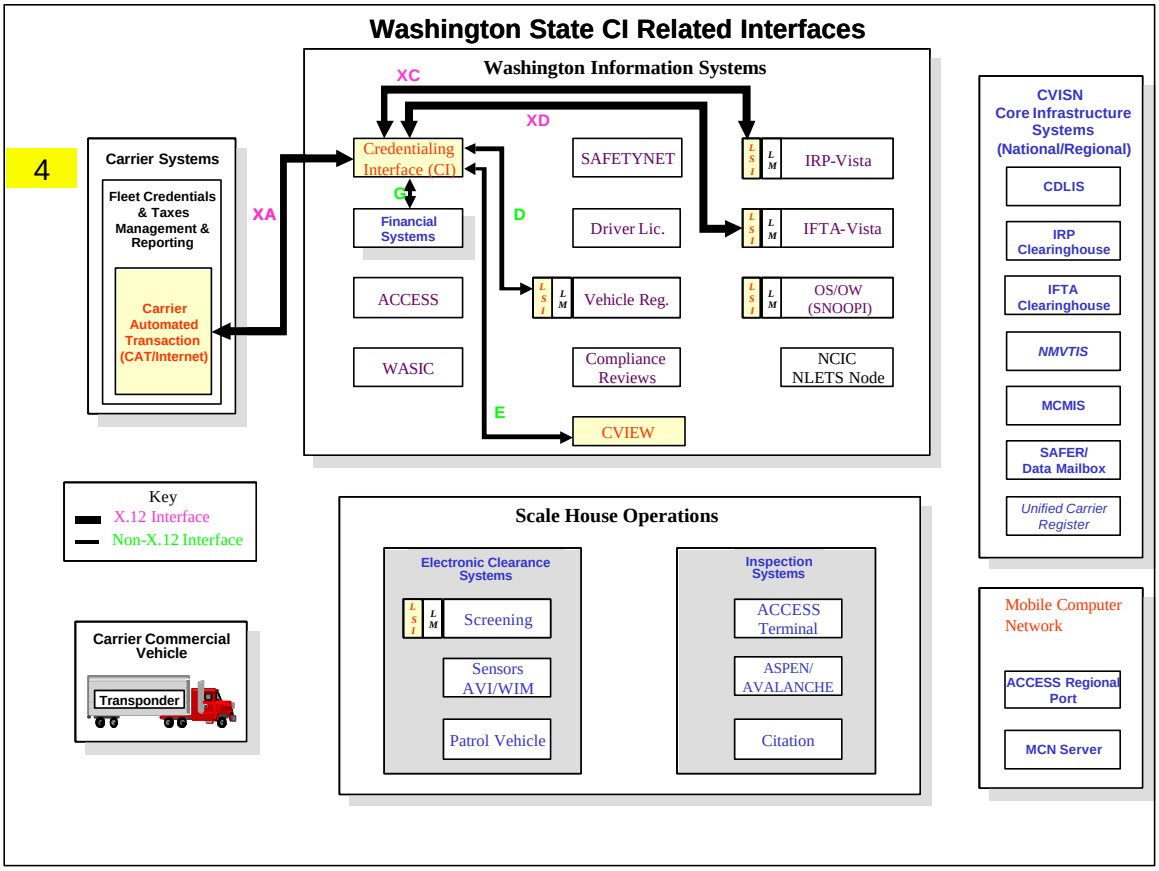


Figure D–9. WA CI Related Interfaces

Washington used:
Microsoft NT Server
Windows Based Applications
in VB6 and C++6
MS SQL Database

More information about the WA CVISN project can be found at ftp.CVISN.WSDOT.WA.Gov

Please note: this is a secured site and you will need a user id and password for access. Call Anne Cline, CVISN Project Coordinator, at (360) 705-7341 for a user id and password.

Highlights of Washington's credentials administration modifications and planned or existing capabilities:

- Lockheed Martin was the selected vendor for developing the Credentialing Interface
- Current IRP and IFTA data (from Lockheed) has been loaded onto the Screening Database at WSDOT headquarters
- Received current IRP data from Oregon, extracted the Washington specific data and loaded onto the Screening Database at WSDOT headquarters
- In the process of obtaining Washington vehicle registration information (flat file via ftp)
- Developed Oversize/Overweight permitting program with SNOOPI
- Developed Web site for use by the Transponder Administrator
- Established pre-clearance and enrollment vehicle criteria

This Page Intentionally Blank

Appendix E. LESSONS LEARNED – CREDENTIALS ADMINISTRATION

This Page Intentionally Blank

LESSONS LEARNED – CREDENTIALS ADMINISTRATION

This chapter contains "Lessons Learned" in the area of Credentials Administration. Several of the CVISN Model Deployment States responded to these questions in July 2000:

What did you do right that you'd recommend to other states?
What you didn't do that you wish you had?
What issues do you wish you could have settled earlier?
What requirements turned out to be key drivers for design?
What design choices did you consider and reject/choose and why?
In general, what lessons learned about Credentials Administration would you like to share?

E.1 Lessons Learned – California

- Agreed to the concept that CVISN required a multi-agency and industry effort.
- Approved over 100 carriers who volunteered to participate in this demonstration project either directly, through agents, or through leasing companies.
- Should have demanded significant break out sessions at workshops for open state interaction.
- Should have been concerned about lack of qualified vendors to support CVISN development.
- Should have been proactive in discussing multi-state development contracts to minimize cost.
- Design the interfaces to all legacy systems in their native mode rather than EDI.
- Combining the CI/CVIEW functionality into a single computer platform.
- Rejected a separate CI and CVIEW to minimize maintenance of test and operational systems.
- Chose to develop a PC CAT versus a Web CAT system to allow for distribution of inventory items (plates, stickers, decals, etc.) and handling of group payment options.
- Chose to produce final documents versus temporary documents as requested by the industry.
- Should have resolved the dependency for paper documents to satisfy the FHVUT reporting requirements.

E.2 Lessons Learned – Colorado

(Updated April 1999)

- It always takes more time, money, staff and effort to do these projects than is economically feasible. At least if you're one of the pilot or prototype states.
- It is our hope that over time vendors will have gained the necessary experience and knowledge that will allow them to give reasonable estimates and to rely less on state staffing in order to insure project success.

- With few vendors willing to take the risk and provide these services to the states, there isn't the competitive marketplace that the states need to insure reasonable pricing.
- The majority of benefits associated with electronic credentialing side are for industry. The majority of the work effort and costs rests with the state.
- Get industry involved and keep them there. Besides our monthly meetings, which are well attended by both state and industry representatives, we have hired an industry representative to act as a "go between" to insure that the concerns and needs of both sides are being communicated.

E.3 Lessons Learned – Connecticut

What did we do right? Involved the heads of the business units in each agency that are responsible for credentials administration. These units have historically worked together to successfully address common issues. It was not difficult to get them to address CVISN issues in the same manner.

We probably could have spent more time on design issues with this group. There is still work to be done that we expect to hire a systems integration firm to define and address. How to provide for electronic payment functionality is an issue. At the present time each agency has evolved its own process. It would be beneficial if the State adopted a standard approach and assigned a single point of responsibility for this function, but this may not happen in the CVISN time frame.

At this point we anticipate most of the design requirements for vehicle registration to be driven by DMV, for tax systems by DRS and for OS/OW by DOT. CVISN drives the requirements for data sharing among these systems, and we expect most sharing to occur through Connecticut's CI/CVIEW System. We reject the idea of connecting all the systems to each other. Instead they will each be linked to CI/CVIEW, a much simpler arrangement.

In general, we've tried to identify the stakeholders in this area and invite them to participate in the process and in the decision making. To date, this approach has served us well in the credentials administration area. .

E.4 Lessons Learned – Kentucky

(Updated April 1999)

- Sufficient funding and personnel resources are necessary for supporting DUAL Systems
- Uniformity/compatibility among numerous states is necessary before the full benefits of CVISN can be realized
- Coordination efforts are directly proportional to the number of organizational units involved. The fewer the number of organizational units (departments) containing the credentialing, safety, and electronic screening processes, the easier it is to administer the CVISN activities

E.5 Lessons Learned – Maryland

(Updated April 1999)

- Involve operations staff from day one: describe the business process first, then identify the functions of the system. Improve the process if you can, rather than just automating it, but don't stake the project on your ability to change the business process.
- Learn what the most-responsible agency's engineering staff needs, and what they like and hate. They, too, will have to live with the system after it's built.
- Use CVISN as a catalyst: stick your neck out to make "the right thing" happen for the state staff in areas broader than CVISN. You make friends and build momentum that way. *(Examples: promote use of TCP/IP network access and make it available to other projects; eliminate dumb terminals in favor of client/server systems- let others get onto the CVISN workstations; deploy capabilities where they belong, not just where they are now.)*
- Set small milestones very early; make them larger and farther apart only when confident in the capabilities and commitment of the vendors.
- CVISN makes waves. You'd better learn to surf: exploit the win-win opportunities that CVISN presents. *For example, in Maryland we were able to take advantage of a pent-up desire to convert many Mainframe-SNA network functions to Client/Server-TCP/IP. We gained a lot of support among top managers, line supervisors and hands-on staff, all of whom felt they had something to gain by making their part of CVISN work.* If the wave is too wild to surf, or you're in the wrong position to catch the ride, you'd better learn to put your bow into the wave and make headway in the rough seas. *For example, Y2K issues postponed action on IFTA registration, but we've kept up as well as we could while awaiting resource availability, and now we're in pretty good shape to proceed.*
- There is a gap between system developers and end-users that is hard to fill. Products may be finished and put on the shelf, and there is nobody whose job it is to take it off the shelf and get it into operation. *Example: we've had a couple months delay in getting subscriptions working routinely to ROCs (Roadside Operations Computers) because of logistics about data sets and mail accounts.*

E.6 Lessons Learned – Michigan

In summary, Michigan has found that proper staffing and a strong commitment at the very beginning can avoid many pitfalls and lead to a much smoother project.

E.7 Lessons Learned – Minnesota

No information was available from Minnesota at the time of publication of this document.

E.8 Lessons Learned – Oregon

No information was available from Oregon at the time of publication of this document.

E.9 Lessons Learned – Virginia

- Design driver: Requirement for a Credential Interface (CI).
- Design driver: Requirement for a CAT product that was little/no cost to carrier and integrated well into other state supported services.
- Design driver: By using a low level browser such as 3.0, one eliminates client-side scripting. Therefore, server side scripting must occur, which can affect performance.
- Design driver: By duplicating business rules between webCAT and legacy systems, we experienced an increase in additional development and maintenance. Control and security of the front-end system is the benefit for the jurisdiction.
- Rejected development of a PC-CAT. Market does not appear to be emerging. State cannot assume cost of ownership and maintenance.
- Selected webCAT option as most viable product.
- Integrated design to share components between webCAT & CI.

E.10 Lessons Learned – Washington

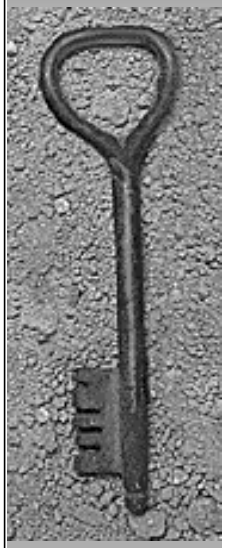
- As an incremental step, developed simple interfaces between state legacy systems. Example: The story here is to do things as easily as possible. Since we have a site up and running now, and no clearinghouses to connect with, we developed our own data base by using our own licensing agency's data, Oregon's data, and data returned from our IRP/IFTA provider. We are using periodic updates and hope to let this portion through an RFP in the very near future.
- It takes longer than you think for mapping to legacy systems.
- CVISN architecture should be folded into or required as legacy core system functionality with your IRP/IFTA vendor. Example: Most states have a contract with their IRP/IFTA provider. We had just signed a contract with our vendor before CVISN came along. We weren't lucky enough to have them fall in the reverse order. Had it been so, we would have demanded that the CVISN architecture be folded in as core functionality with our state system.
- For leverage, partner with other states that use the same vendor. Example: It was easy for our vendor to stall us and keep making empty promises of a delivery date. However, our state is no different than other states using the same vendor. We should have partnered with other states in making our early demands to our vendor. If we had done so, we would already have a functioning CI.

Appendix F. WORLD WIDE WEB SECURITY ISSUES

This Page Intentionally Blank

Wide Open to the World's Web

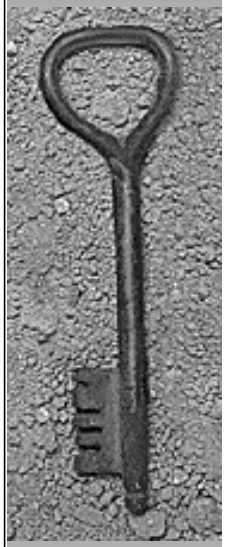
Security Issues for Web Users and Providers



Scramble to Fix Computer Security Flaws

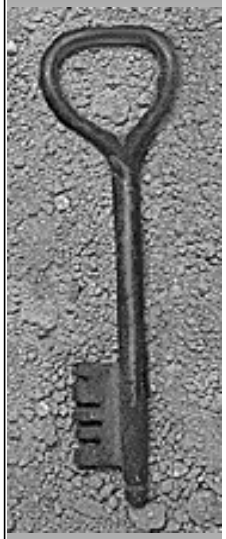
- By SARA ROBINSON, August 3, 1999

  Three giants of the computer industry Microsoft, Hewlett-Packard and Compaq Computer -- found themselves scrambling today to address a rash of serious security vulnerabilities in software designed to interact with Microsoft's Internet Explorer Web ...



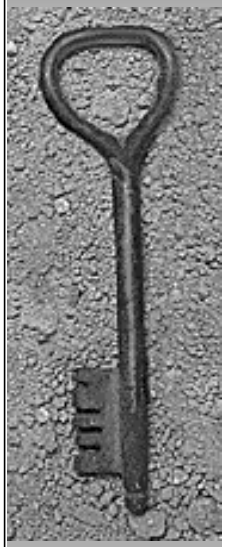
Secure or Not, the Internet Has Become a Part of Life's Routine

- By AMY HARMON - February 13, 2000 "When Jon Tara first heard that unknown vandals with unclear motives had managed to sabotage several of the Internet's most prominent businesses last week, the San Diego software engineer posted a probing message to an online investing forum…"



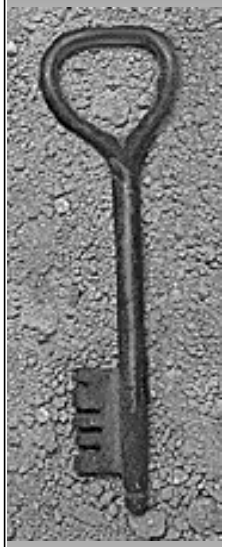
Britain Closes Web Site With Spies' Names

- By WARREN HOGE - May 14, 1999
  "An embittered former British spy has used the Internet to make public the names of a large number of secret agents, but officials in London said today that the Web site had been shut down and that no duplicates had surfaced…"



New Security Fears As Hackers Disrupt 2 Federal Web Sites

- By MICHAEL JANOFSKY - May 29, 1999 “An enduring cat-and-mouse game between Federal agents and computer hackers took a novel twist this week as the hackers turned on their pursuers, disrupting the Web sites of the Federal Bureau of Investigation and the United States Senate…”

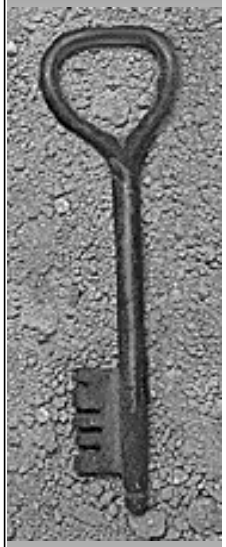


HacK, CouNterHaCk

- By Bruce Gottlieb - October 3, 1999 "Would you like to see how to knock someone off the Web?" Silicosis asks. Sili, as he is known, is a slim young man with serious eyes set deeply into a delicate face. He's the newest member of a hacker collective known as L0pht (pronounced "loft‘) …”

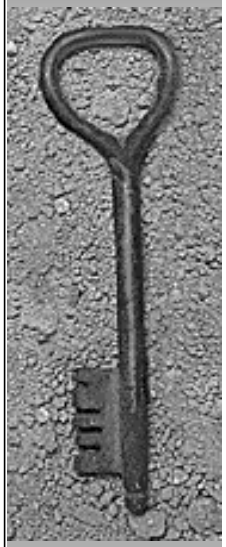
Web Attacks Might Have Many Sources

- By MATT RICHTEL and SARA ROBINSON - February 11, 2000
  "Computer security experts said today that evidence now suggests that the three days of attacks on leading Web sites may have been the work of more than one person or group. The analysis that more than one group was at work…"

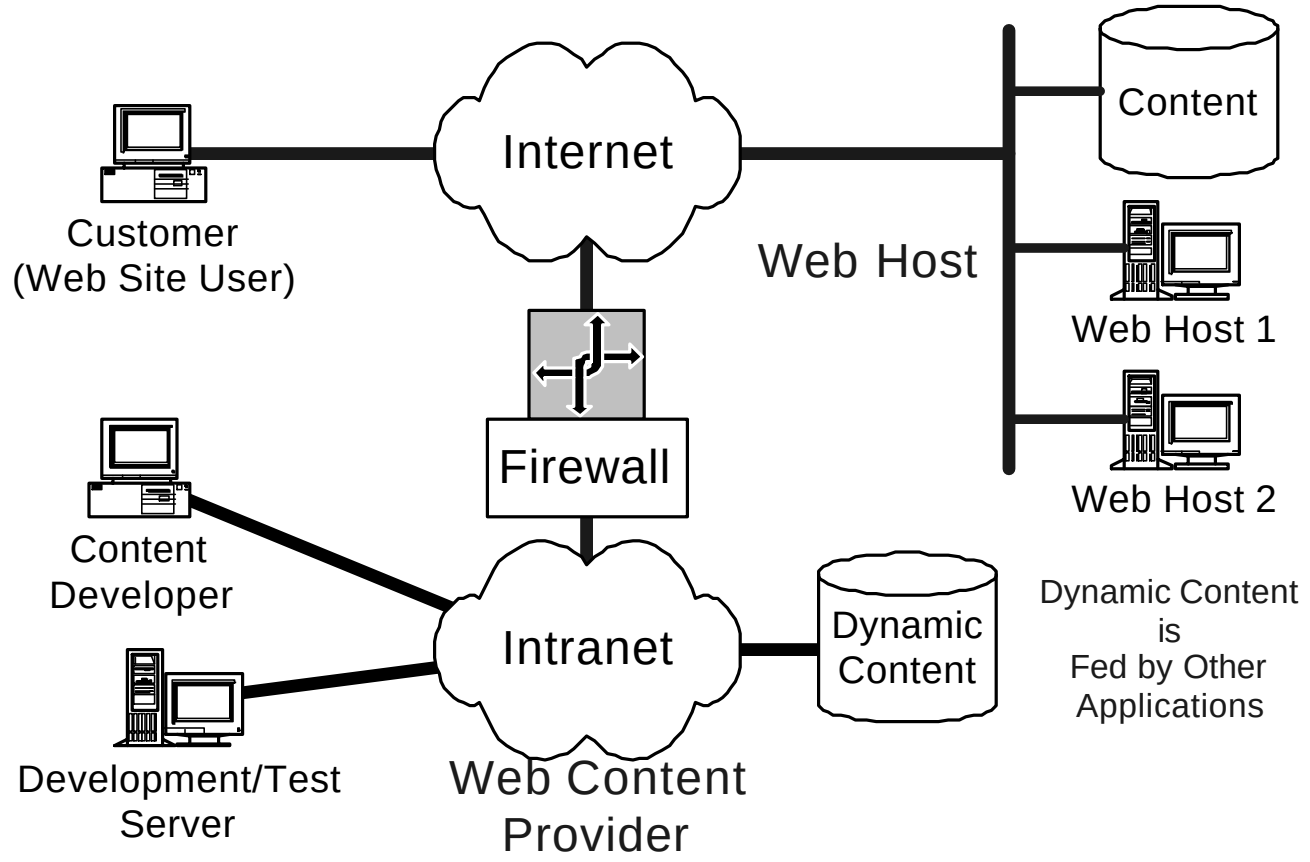


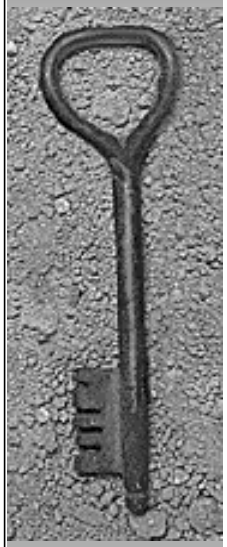
Are there real Web Security Issues?

Obviously



The Model for Web Services

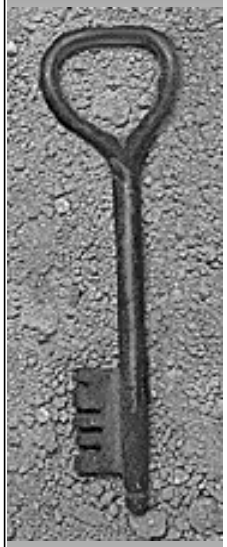




Who needs to be concerned?

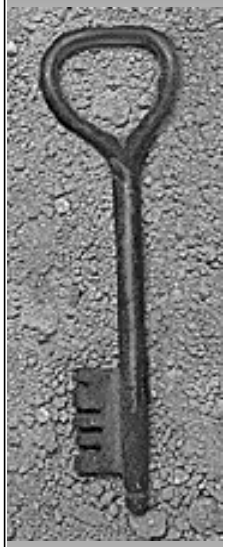
- Each and every Web Host
- Each and every Web Content Provider
  - As a provider you may have ethical and legal issues
  - At a minimum you are at risk of embarrassment
- Each and every Web Site User
  - It doesn't matter if you use Netscape or Microsoft's Internet Explorer
  - The problems are real either way, although they may be different

Issues and Responsibilities for the Web User



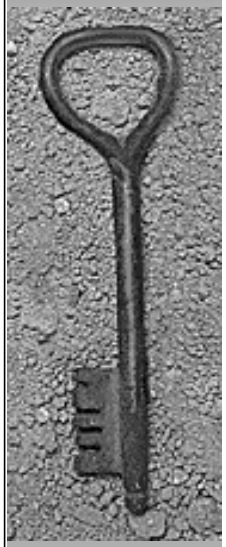
What are the issues for Web users?

- Damage may be done to your computer.
- Information may be stolen from your computer.
- Information that you provide to Web sites may be wrongly used or distributed.
- You may receive misinformation from web sites.
- You may receive stolen property from web sites.
- You may not be able to get the service you need.



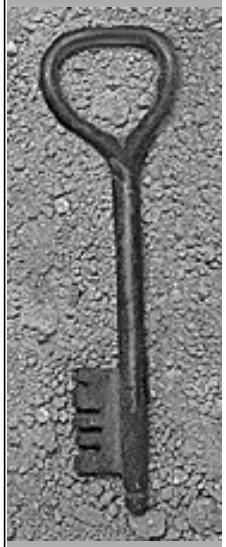
How can a hacker steal or damage my information?

- Hacker's Goal: Install or run a program on your computer
- Approach: Run a script ("active content") through the browser (CGI, Java Applet, ActiveX, JavaScript) or cause you to run a program (a .COM, .BAT, .EXE, or a document with macros)
- Damage: Destroy information with a virus or plant a program that provides a conduit to steal information



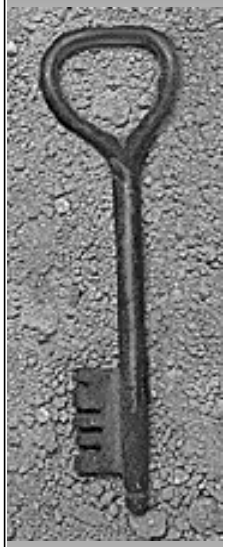
How do I protect my computer?

- Keep an up-to-date backup of key data
  - Keep your documents in one place (e.g., My Documents) and back that up every day
  - Don’t worry as much about application software (e.g., Windows, Word, etc.) – you can always reinstall that
- If you have any sensitive or valuable information
  - Either store that information on removable disks (floppy, Zip, etc.) and lock it up, or
  - Encrypt any sensitive information on your hard disk



How do I protect my computer?

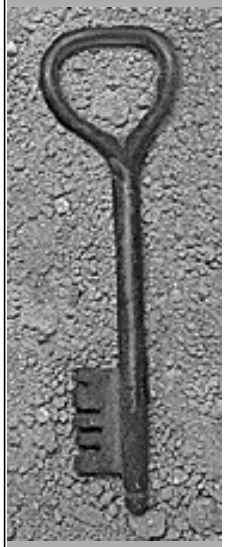
- Run virus protection software and keep the virus definitions up to date
- Try not to visit questionable sites
  - Stick to the sites you need, know, and trust
  - Don’t surf
- Be very careful when downloading and running programs
  - If possible, don’t do it
  - Don’t “click” on programs you get through E-mail



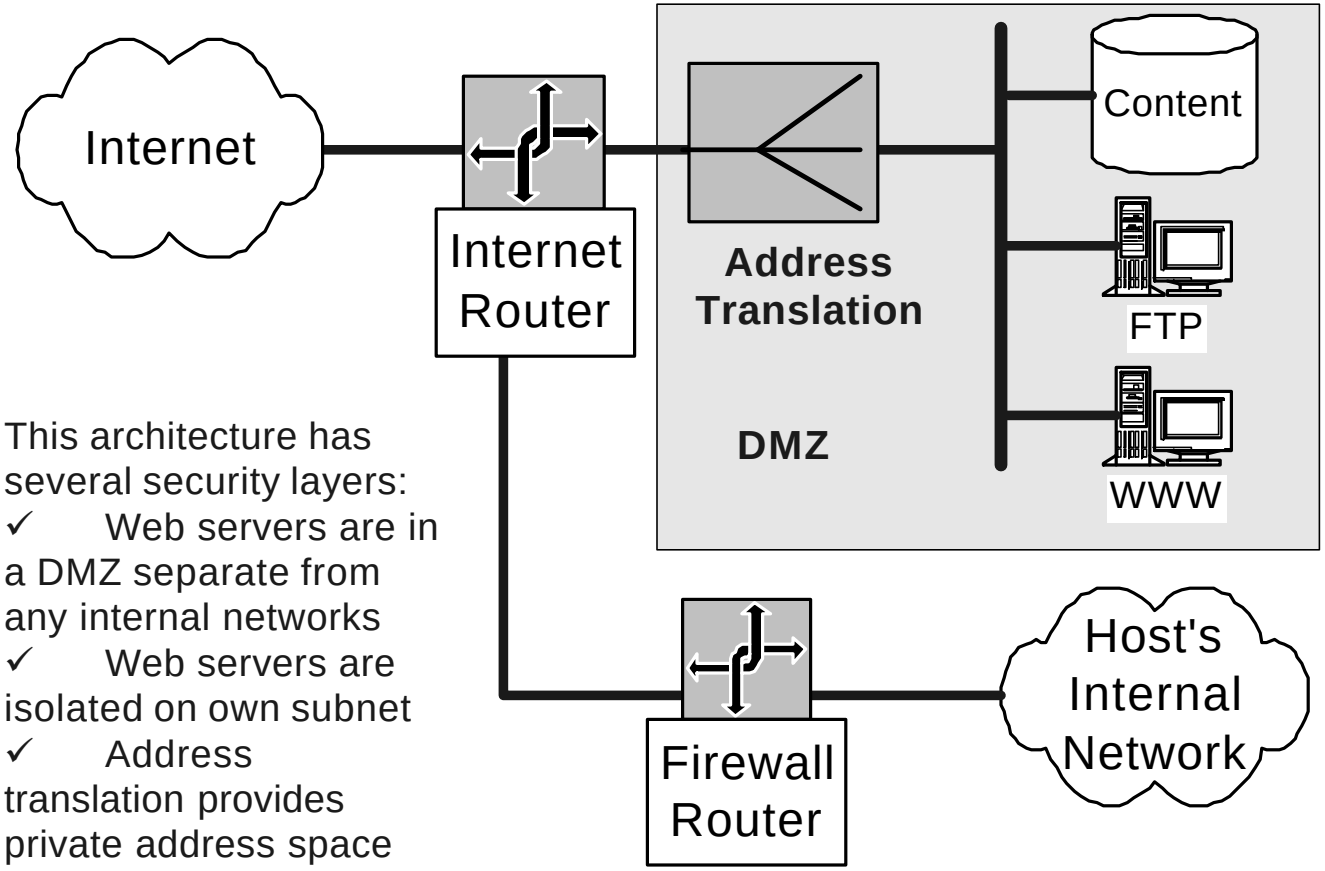
Summary: Recommend that Your Web Users...

- Treat active content as suspicious and potentially dangerous
- Stick to the web sites they know, trust, and need
- Avoid downloading and running executable programs
- Keep security controls, such as certificates, in place

Issues and Responsibilities for the Web Host and Web Content Provider

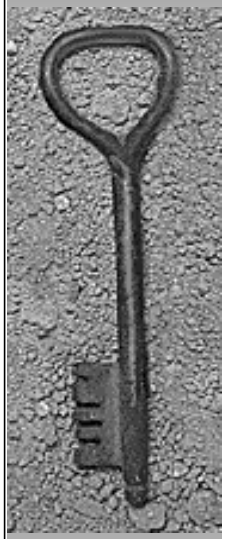


Network Architecture Can Enhance the Host's Security



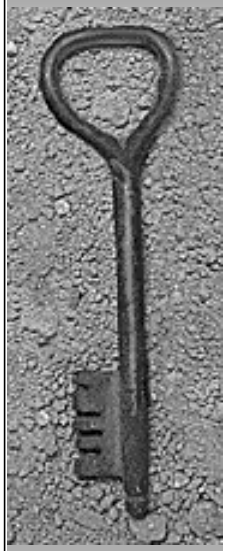
This architecture has several security layers:

- ✓ Web servers are in a DMZ separate from any internal networks
- ✓ Web servers are isolated on own subnet
- ✓ Address translation provides private address space for Web servers



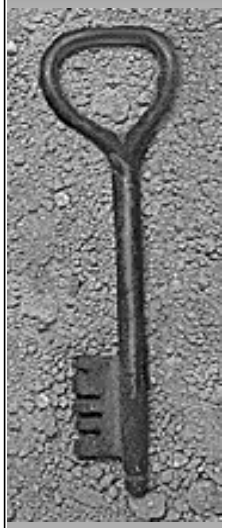
Summary: Your Web Host Should...

- Have a published security and privacy policy
- Use good physical security
- Configure servers properly
- Administer the servers for security with the latest patches

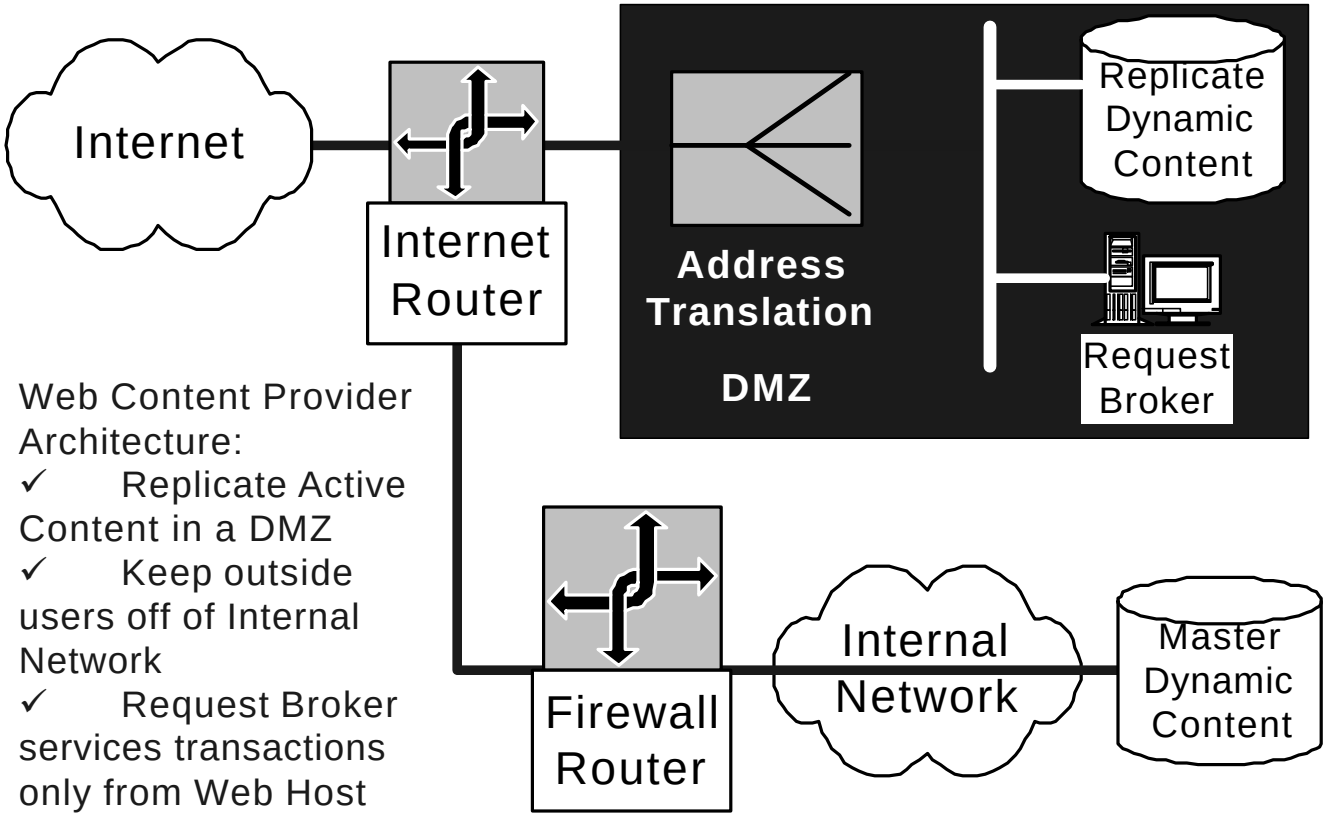


Keeping the Server Secure

- Rule #1: Don’t do development on the web server!
  - Web site development should be done in a development environment
  - Port code to the server after extensive testing
- Take footprints and look for unexpected changes
  - Take a snapshot of the working server with a tool like TripWire
  - Periodically compare the server to the snapshot
  - Investigate unexpected changes

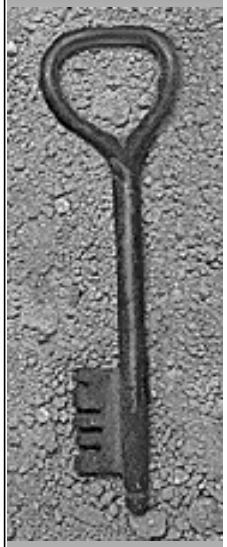


Network Architecture Can Enhance the Provider's Security



Web Content Provider Architecture:

- ✓ Replicate Active Content in a DMZ
- ✓ Keep outside users off of Internal Network
- ✓ Request Broker services transactions only from Web Host

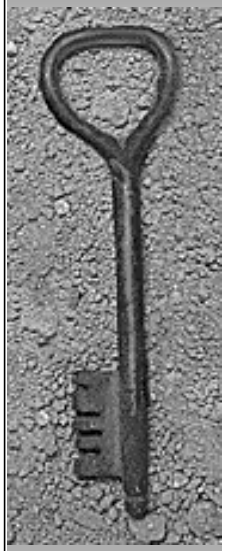


Summary: Your Web Content Provider Should…

- Treat web content like software and use good systems for review, documentation, change, publication, and testing
- Test code thoroughly before production
- Have one person who releases production code
- Have one Web Master (a different person) who installs production code

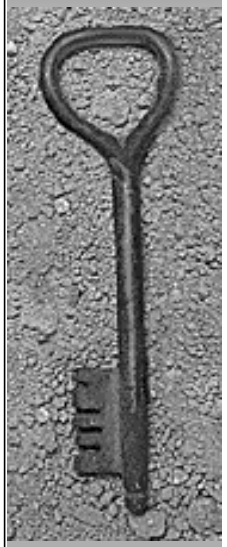
More detail follows on Host and Content Provider security issues

Issues and Responsibilities for the Web Host



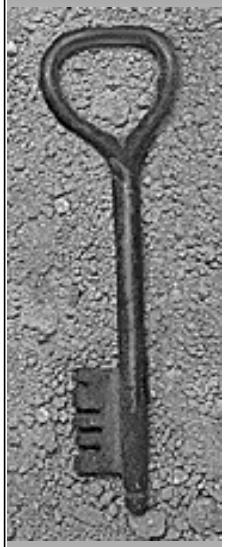
Web Host: Make or Buy Decision

- Should we provide our own web servers?
  - More control, tailored and tuned to our requirements (security and performance)
  - Significant overhead and responsibility
- Should we buy this service?
  - Many organizations in the business: Digital Nations; BBN/GTE; Digital Island; AT&T
  - Those heavily involved as service providers, particularly for E-Commerce, have a strong vested interest in security



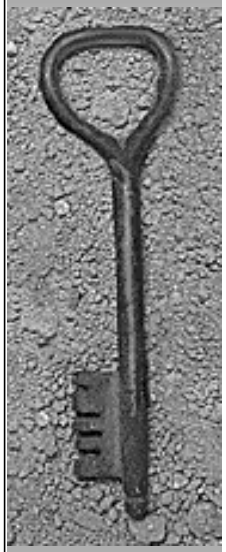
What security can we expect from our host?

- Very difficult to mandate a specific security solution
  - Requirements are difficult to construct without detailed knowledge of vendor's architecture
  - Many reasonably safe solutions; no absolutely safe solution
- Probably should be an evaluation criteria for source selection



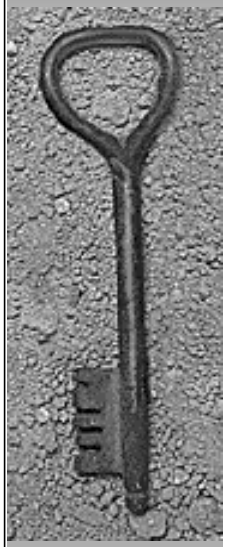
Policies are the Basis for Security

- Web host must have a written Privacy policy
  - Under what circumstances will they distribute information about clients
  - See http://www.TRUSTe.org
- Web host should have a written and published security policy
- You should ask for both of these policies as part of any RFP for web services



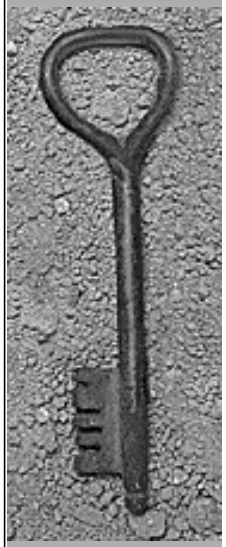
Physical Security for Web Servers

- Protected from unauthorized physical access
  - Located in a locked room with limited access
  - Located on a secure site with 24x7 security
  - Protected with power-on passwords
- Protected from water, fire, and theft
- Protected with clean power and standby power



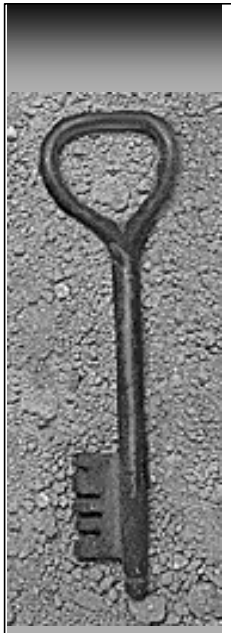
How is your web site spread between host servers?

- There are distinct advantages for you if you have one or more dedicated servers for your site
  - Multiple servers are more robust
  - Less susceptible to denial of service attacks
  - Avoid sharing a server with a prime hacker target
- This is more expensive for the host provider, so it may be more costly for you
- One cost-effective solution may be your own “slice” of a mainframe web server



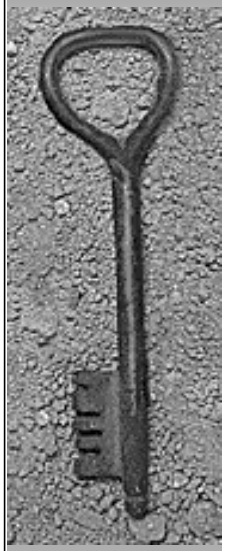
Proper Server Configuration and Administration is Most Important

- Web servers are designed for outside access, so blocking the path to the server is not an option
- Three considerations for server defense:
  (1) Which web server
  (2) Which operating system
  (3) How is security administered?
- The last of these is by far the most important



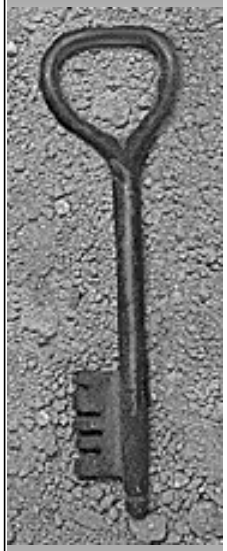
Which web server software is more secure?

- The main key is whether or not the web server software has to run as a privileged application
- Of the big three
  - Apache is great for security because it does not run in a privileged mode
  - Netscape Server runs privileged but has a good security reputation
  - Microsoft Information Index Server (IIS) both runs privileged and has a poor reputation
- IBM Web Sphere on OS/390 is potentially very secure



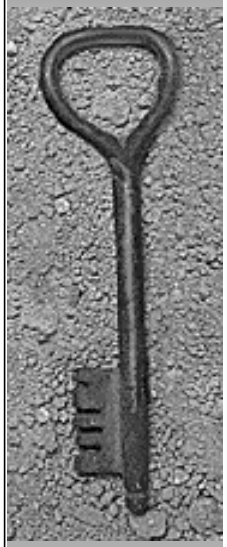
Which operating system is more secure?

- IBM's OS/390 is far more secure than UNIX or NT
  - Only economical at large scale
  - Big role in E-Commerce
- Both UNIX and NT can be made secure with proper administration, configuration, and tools



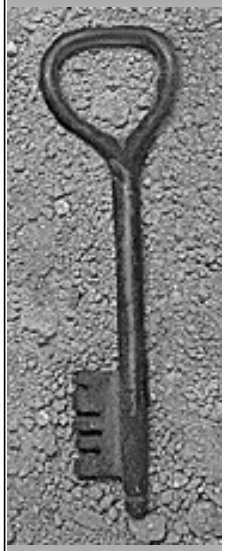
Key Points for Operating System Security

- Install all security patches promptly
- Carefully control account access
  - No unattributed accounts; e.g., root logons
  - No Guest accounts
  - Limit privileges to only those needed
- Don’t share web server with other applications
- Pay attention! Log access and examine the logs for security problems



Run Only Those Services Needed for Web on the Web Server

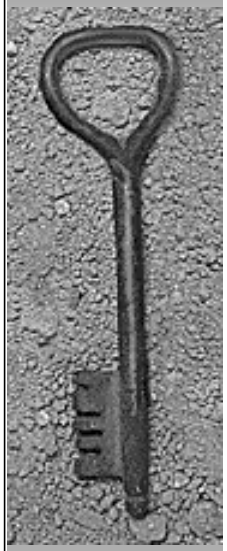
- On NT run
  - Server, TCP/IP, and WebServer
  - If required, RPCBind and Domain Authentication
- On UNIX some replacements of infamous services can increase security
  - Run the latest version of the Perl 5 scripting language
  - Run the latest version of Xntpd, network time protocol
  - Run the latest version of DNS (domain name services)
  - Run PRO FTP if a File Transfer Protocol server is required
  - Wietse's replacements for rpcbind and the infamous UNIX mail program sendmail



Use Security Tools to Help; Keep Up With the Bug Tracks

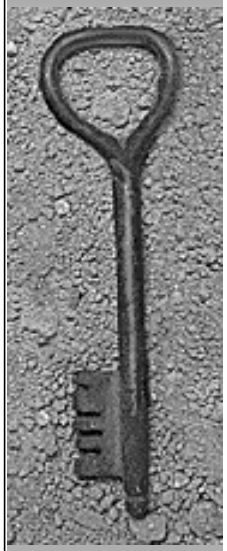
- Security monitoring tools should be part of a security architecture
- Some common tools include
  - Tripwire (ftp://coast.cs.perdue.edu/pub/COAST/Tripwire/)
  - COPS (ftp://ftp.cert.org)
  - Swatch (ftp://ftp.standford.edu.general/security-tools/swatch)
- One has to keep up with the security bugs that are constantly discovered
  - http://www.ntsecurity.net
  - http://www.sans.org/
  - http://www.cert.org/nav/training.html#infosecurity

Issues and Responsibilities for the Web Content Provider



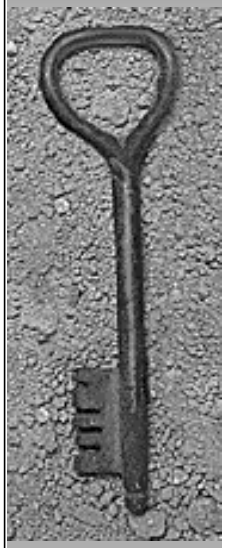
What are the concerns for Web Content Providers?

- Information meant to be private may be stolen from your site.
- Your site may be used to present misinformation.
- Your site may be damaged or destroyed.
- Access may be disrupted (Denial of Service).
- Your site (or intended site) might be used to cause damage to or steal information from your users.



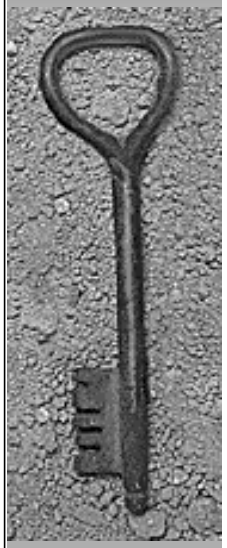
Is the content secure?

- All the host security is of no value if the content is not secure:
- Who is authorized to place content on your web site?
- Under what rules do they operate?
- What types of tools and languages are they allowed to use?



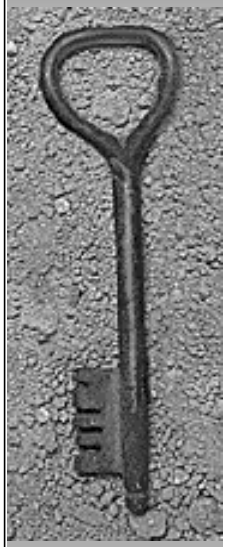
Develop On a Test Environment

- The ability to compose HTML with Notepad does not make one a Web Master
- Do not develop on the Web Host Server
- Test all code thoroughly before it is ported to the web server
- Only one or two Web Masters should have authority to port code to the Web Host



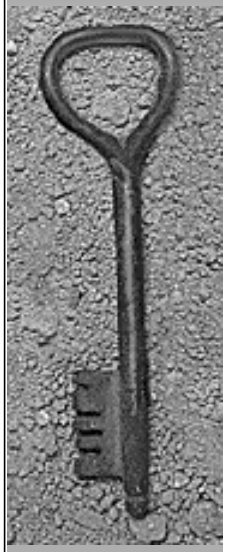
Quality Control for Content

- Get code reviews in place: Peer review and senior review
- Have a single approval authority for production code
- Have a single web master for placing code in production
- Implement change control for content
- Monitor code footprint for changes



Not All Content is Safe

- Active X controls can be spoofed into real controls which can attack client machines
- Java and (especially) JavaScript have active hacker exploitation
- Neither Active X nor Java Script are confined to their own “sandbox”
- Both Java and Active X support third-party certificates to guarantee original code: “Original” is not the same as “safe.”



References

- SANS Security, “Fundamentals of Web Security,” presented at SANS Security Conference by John Stewart and Dave Kensiski, December 13, 1999
- Hacking Exposed: Network Security Secrets and Solutions, by Stuart McClure, Joel Scambray, and George Kurtz, published by Osborne, 1999
- Hacker Proof, by Lars Klander, JAMSA Press, 1997, Chap. 6, 7, and especially 19
- Go to the World Wide Web Consortium at http://www.w3.org and search on “security”