

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 Mgmt 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

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 & restrictionsSee 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

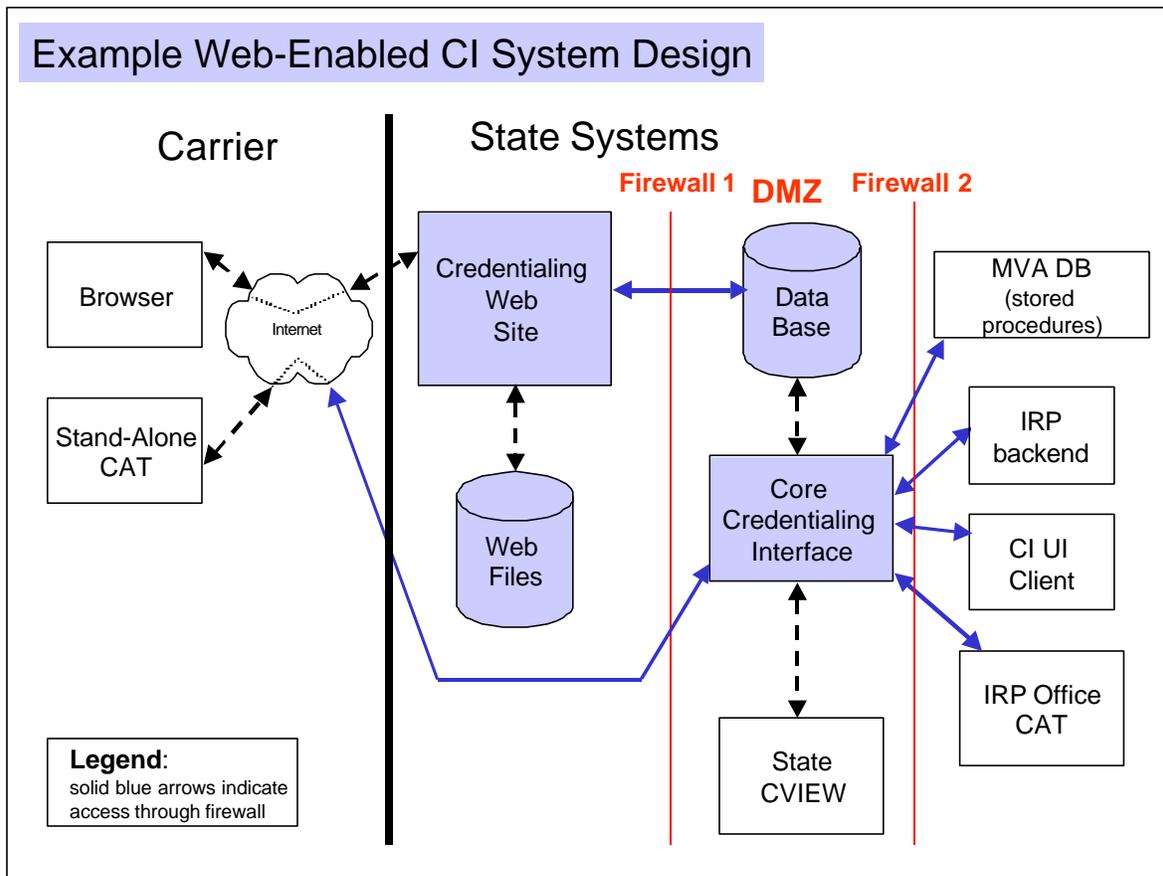


Figure 6–2. Example State System Design Including Credentialing Web Site

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)

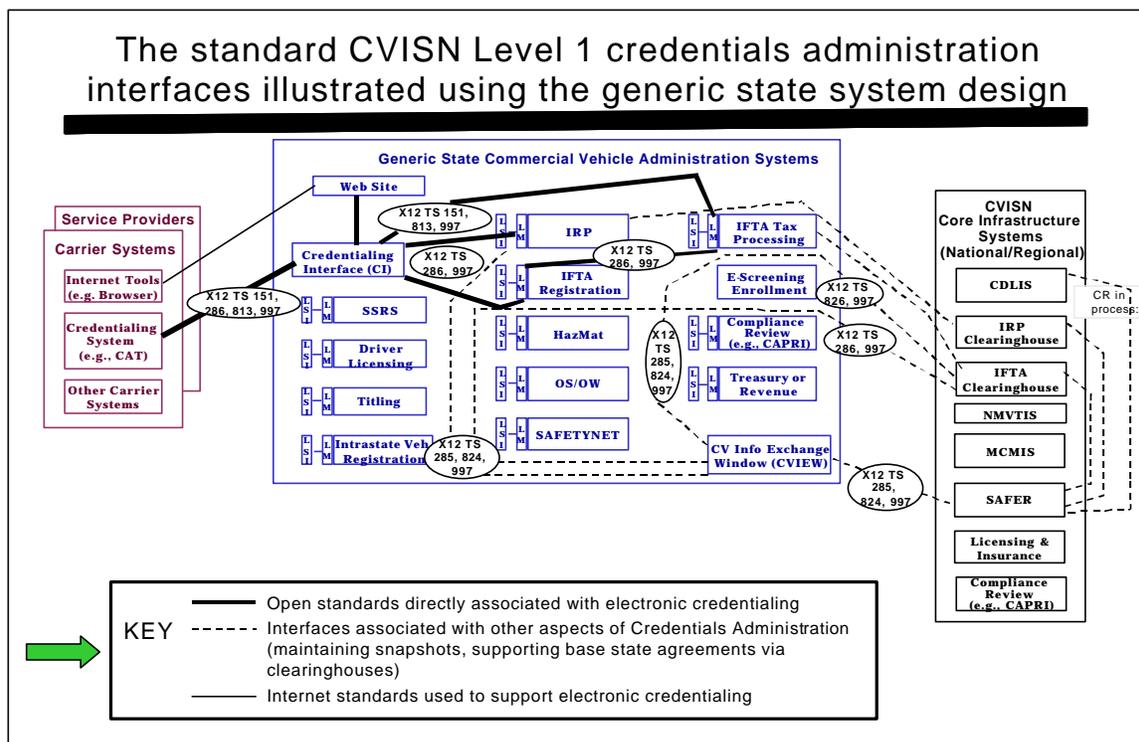


Figure 6–3. CVISN Level 1 Interfaces Related to Credentials Administration

Several documents provided detailed specifications for the EDI interfaces. The applicable standards are contained in the latest version of ANSI ASC X12 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.

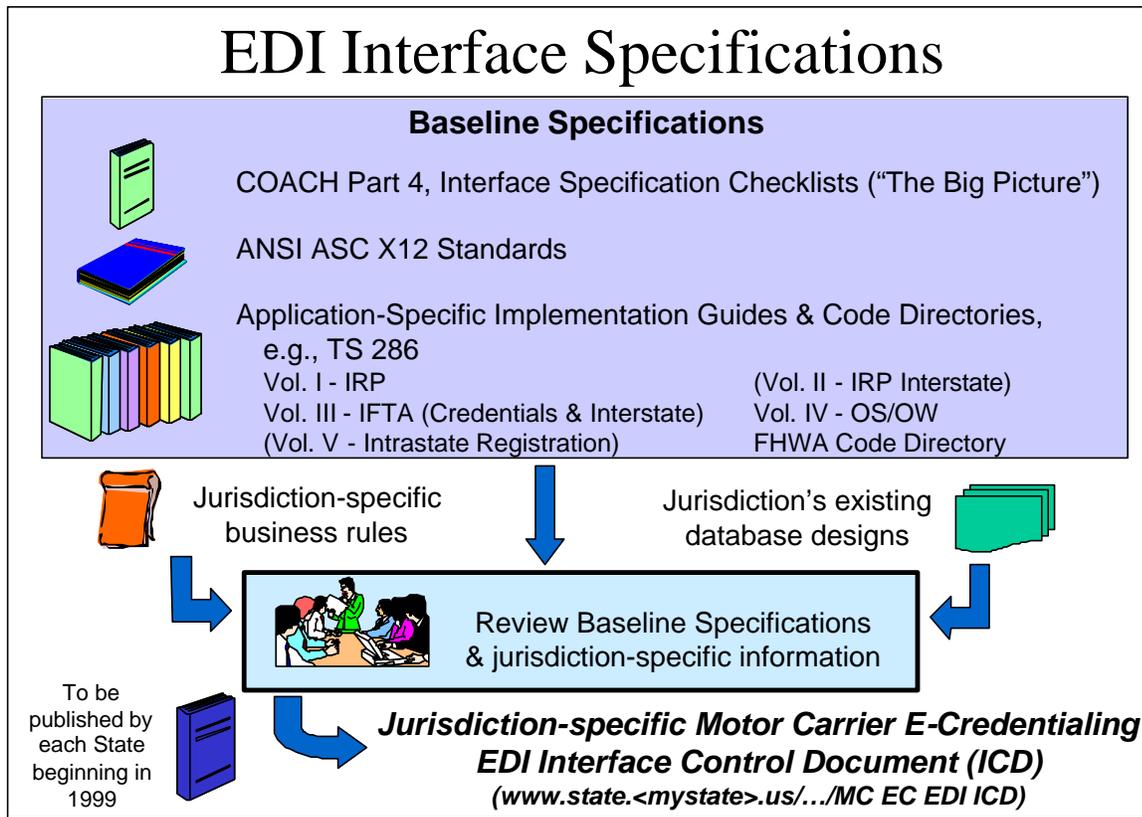


Figure 6-4. Defining EDI Constraints Unique to the State

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.

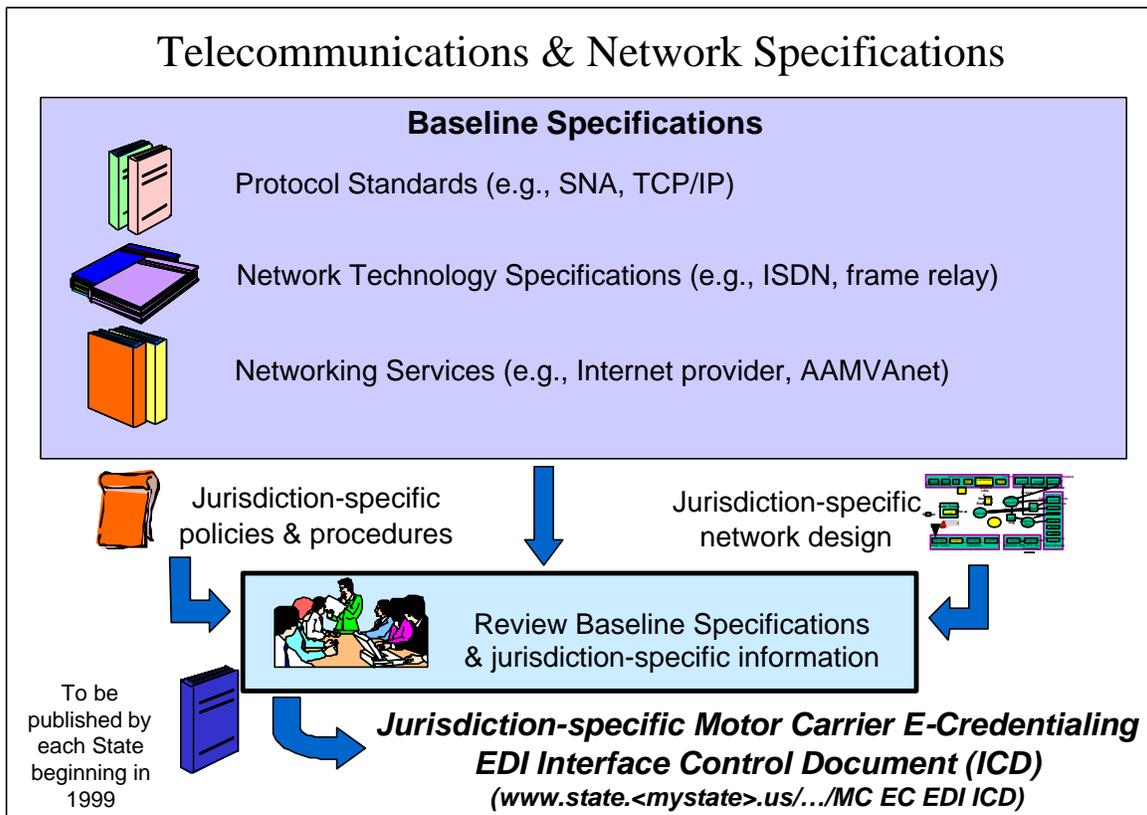


Figure 6-5. Defining Telecommunications & Network Constraints Unique to the State

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.

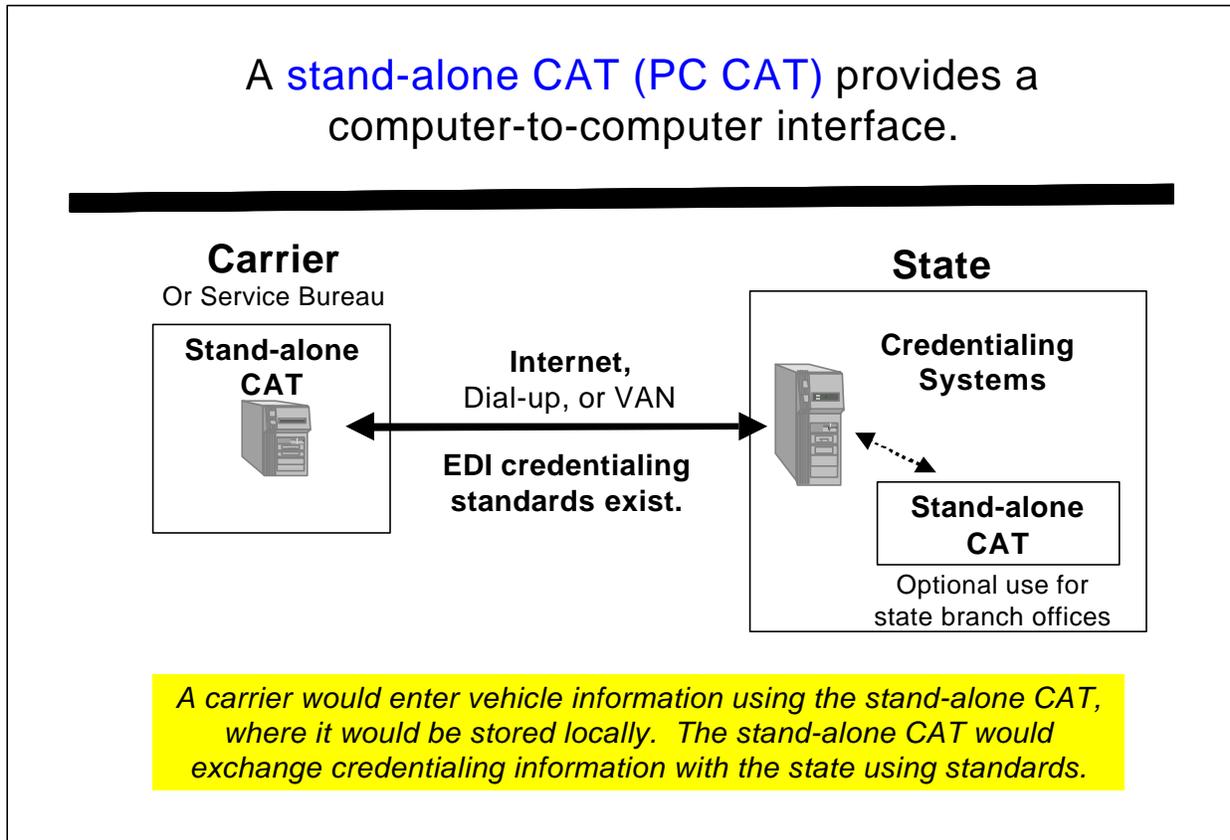


Figure 6–6. State Provides An X12 EDI Computer-To-Computer Interface; Applicant Uses CAT

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.

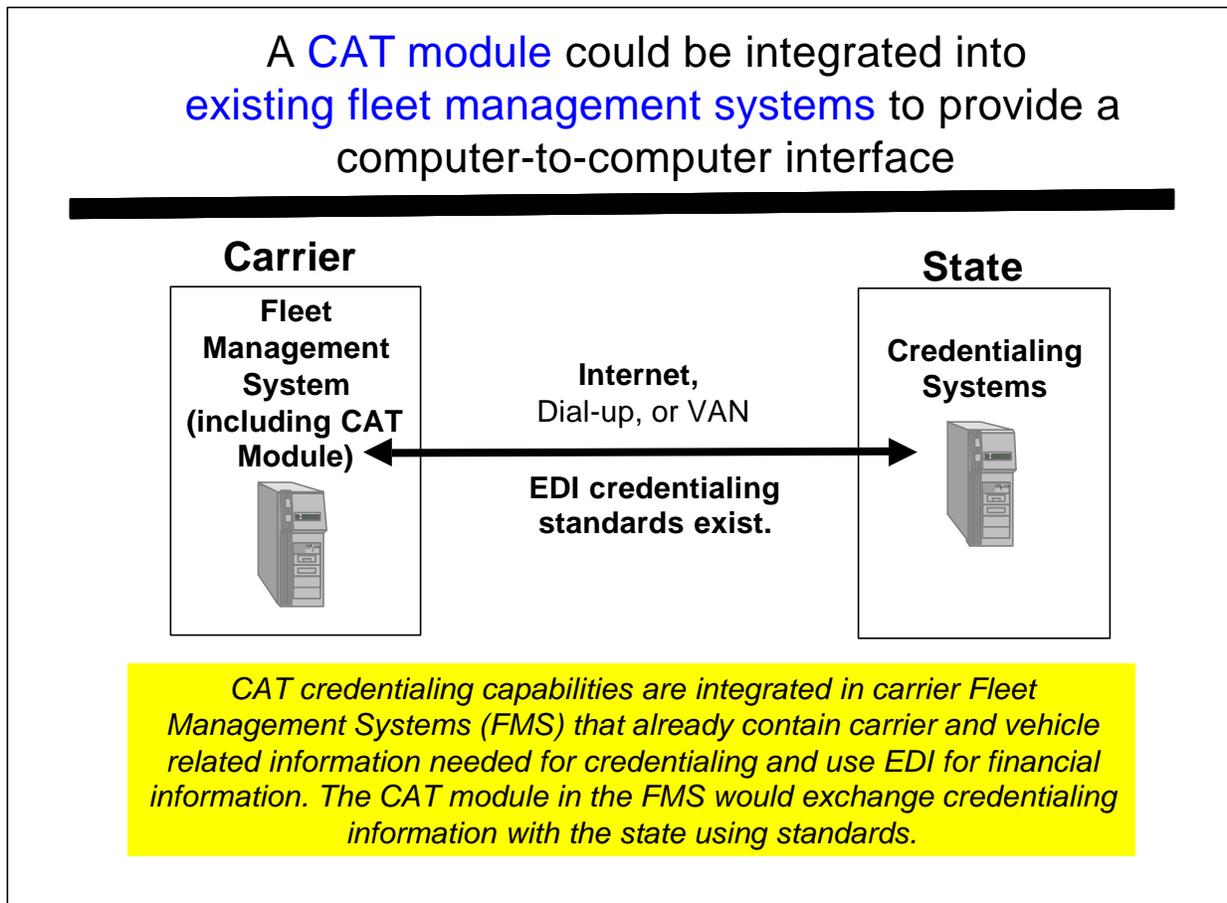


Figure 6–7. State Provides An X12 EDI Computer-To-Computer Interface; Applicant Uses FMS CAT Module

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.

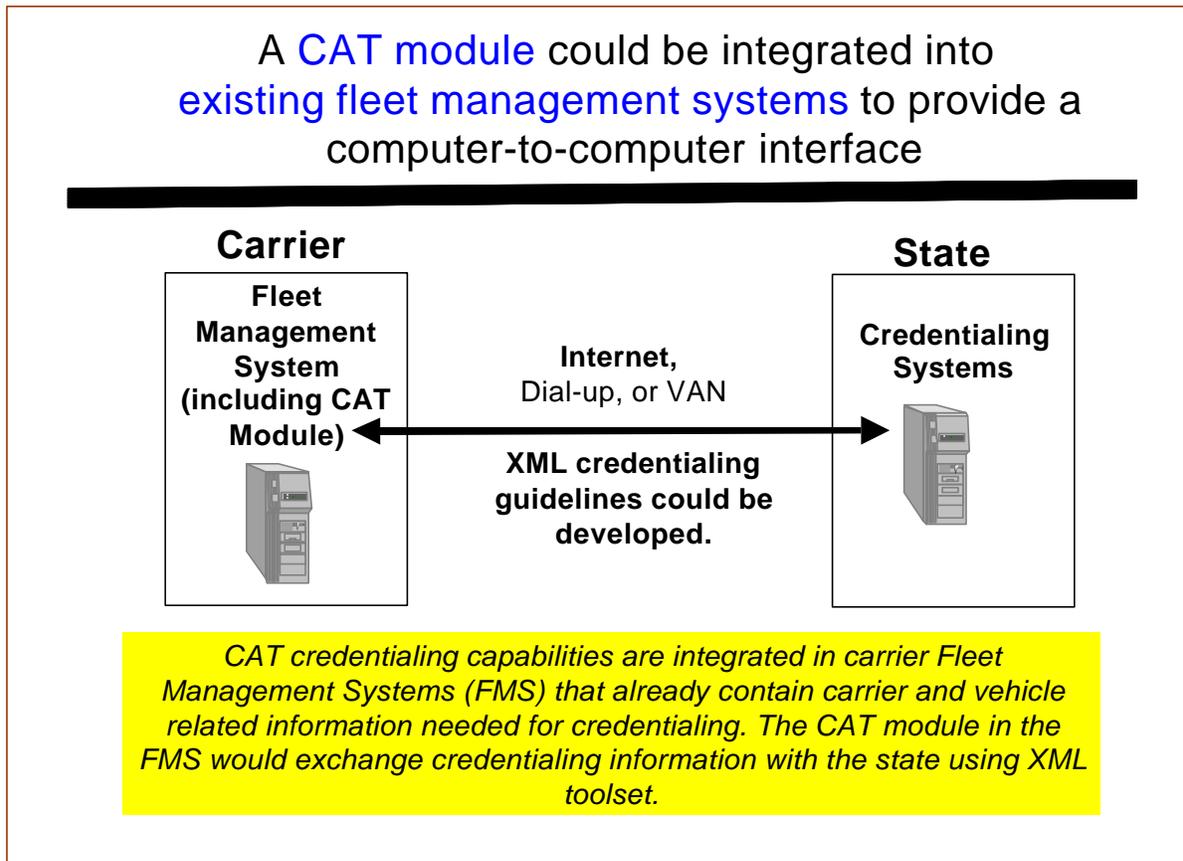


Figure 6–8. State Provides An XML Computer-To-Computer Interface; Applicant Uses FMS CAT Module

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.

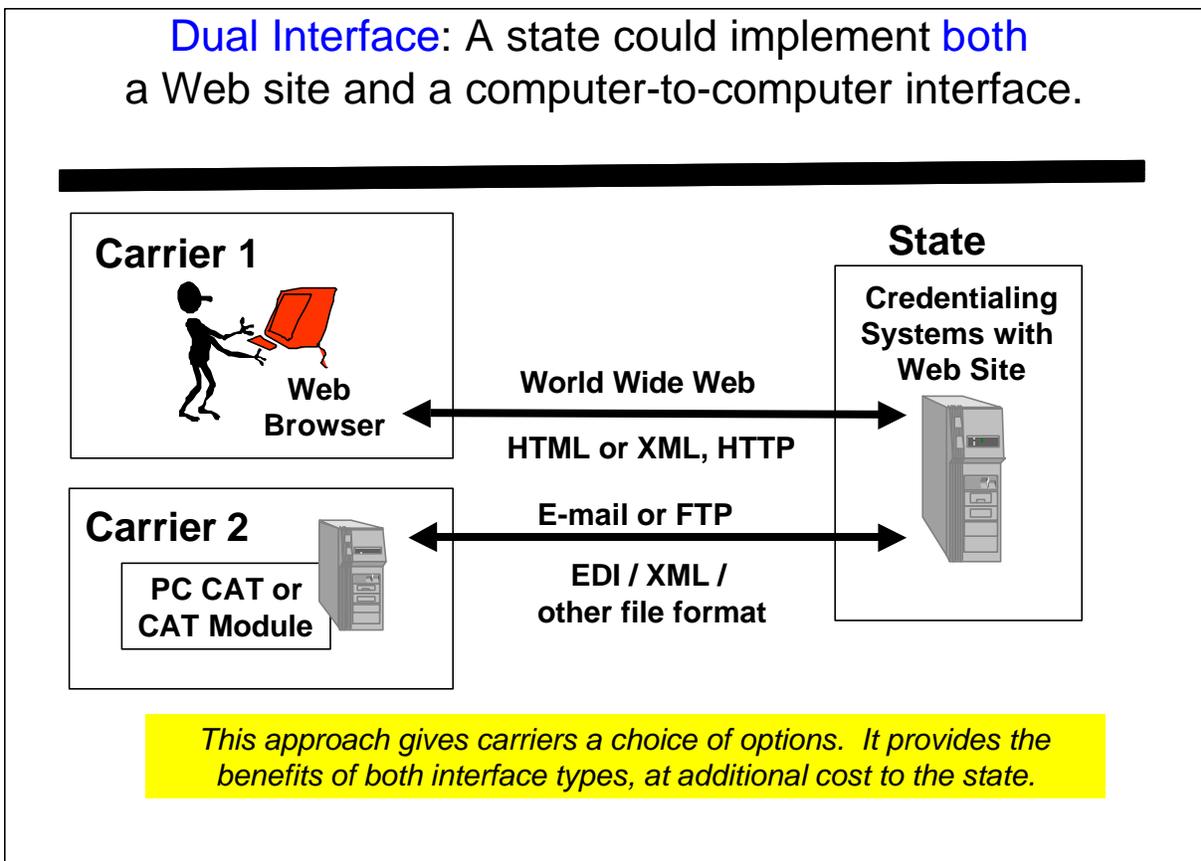


Figure 6–9. State Provides Both Computer-To-Computer Interface and Web Site

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.

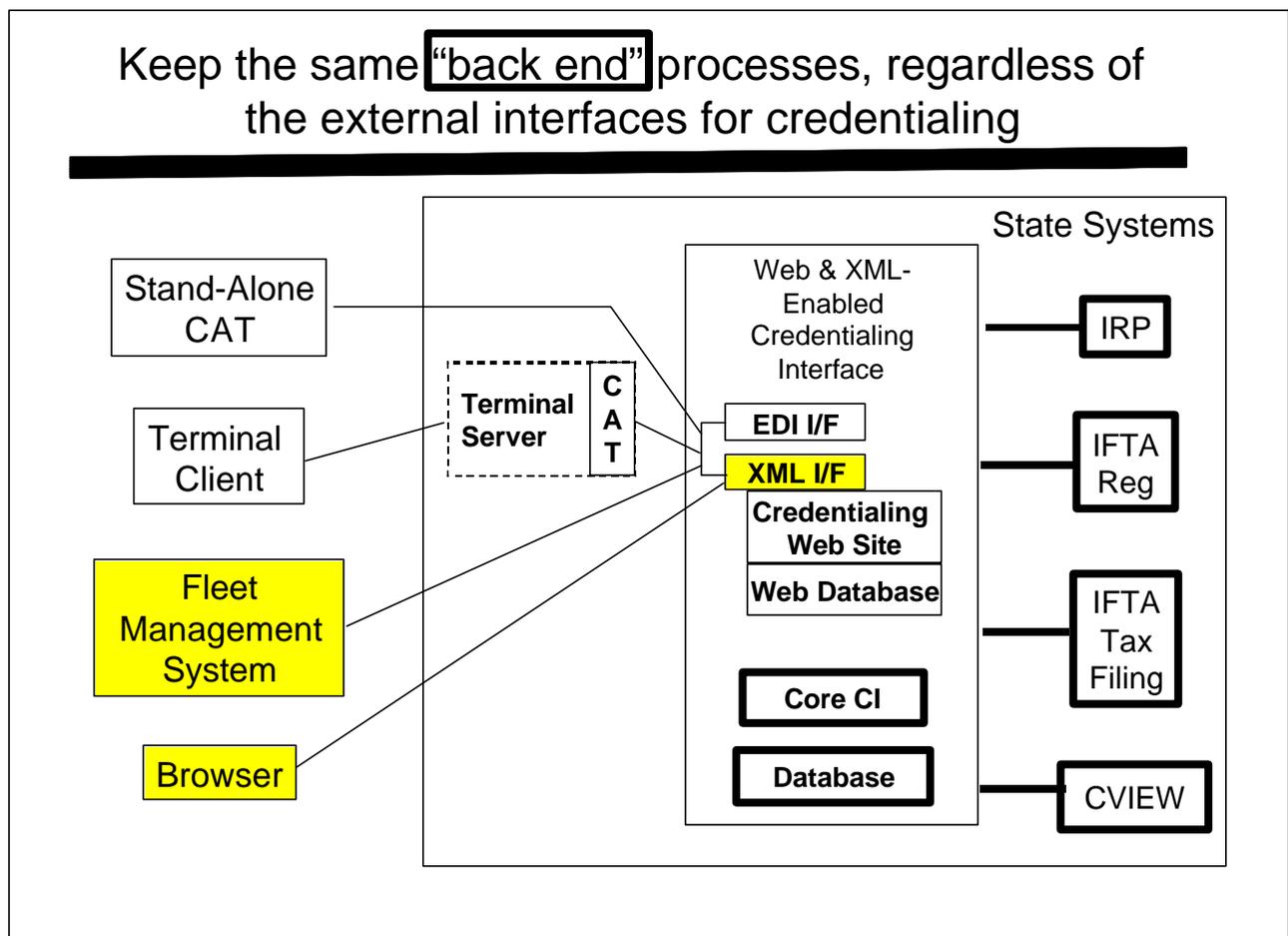


Figure 6–10. Approach to Multiple External Interfaces

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.