

## History of Changes

<b>Date</b>	<b>Modification</b>	<b>Author</b>
	<b>Application Development History</b>	
May 11 <sup>th</sup> 2010	Approved by Enterprise Architecture	Enterprise Architecture
June 9 <sup>th</sup> 2010	Approved by CIO	Enterprise Architecture
June 30 <sup>th</sup> 2010	Approved by the Information & Telecommunication Systems Executive Steering Committee	Enterprise Architecture
	<b>Web / eGovernment History</b>	
May 11 <sup>th</sup> 2010	Approved by Enterprise Architecture	Enterprise Architecture
May 26 <sup>th</sup> 2010	Approved by CIO	Enterprise Architecture
June 30 <sup>th</sup> 2010	Approved by the Information & Telecommunication Systems Executive Steering Committee	Enterprise Architecture
September 29 <sup>th</sup> 2010	Removed duplicated Best Practice and updated table of contents	Enterprise Architecture
	<b>Combined Document History</b>	
November 19 <sup>th</sup> 2010	Combined Application Development Domain and Web / eGovernment Domain documents into this single document. Updated road-map for Web Content Management Standard. Added On-Line Publication Standard.	Donna Camillone per Domain Team meeting 11/17/10.
December 13 <sup>th</sup> 2010	Updated Standards with the Portal Standard, Link Checker Standard, and Forum Standard voted on in the December 8, 2010 full domain team meeting.	Donna Camillone per Domain Team meeting 12/08/10.
December 14 <sup>th</sup> 2010	Updated document with changes requested in the DOIT Technical Architecture meeting.	Donna Camillone per DOIT Technical Architecture meeting review 12/13/10.
December 5, 2010	Approved by Enterprise Architecture	Enterprise Architecture
December 13, 2010	Approved by CIO/CTO	Enterprise Architecture
December 22, 2010	Approved by the Information & Telecommunication Systems Executive Steering Committee	Enterprise Architecture

## Table of Contents

Purpose.....	4
Overview.....	4
Technology categories in this domain .....	5
Application Development .....	5
Technical Standards .....	5
Web Browser .....	5
HTML/XML Editing .....	5
Application Development Languages.....	5
Application Development Toolsets (IDEs).....	6
Standalone Testing Tools.....	7
Source Code Management .....	7
Business Process Management .....	8
Modeling.....	8
Workflow .....	8
Messaging and Middleware .....	8
Application Middleware and Messaging Products .....	9
Technical Standards .....	9
Message Queuing.....	9
Reporting.....	9
Report Creation.....	9
Report Servers.....	10
Online Analytical Processing (OLAP) tools.....	10
Miscellaneous Applications .....	10
Help File/Facilities.....	10
Other .....	11
Geographic Information Systems (GIS) .....	12
Technical Standards .....	12
Enterprise GIS.....	12
Web Oriented Architecture (WOA).....	13
Technical Standards .....	13
Web Browser .....	13
HTML/XML Editing .....	13
Web publishing and Content Management.....	13
Technical Standards .....	13
Web Browsers.....	13
Portals .....	14
Web Page Creation and Editing.....	14
Web Content Management System (WCMS).....	14
Link Checker.....	14
Forums .....	14
Graphic/Photo Editors.....	14
Interactive Content Development .....	14
On-Line Publication.....	14
Video Editors .....	14

## Application / Web Development Technical Domain

Video Captioning Tools .....	15
Search Engines .....	15
eCommerce .....	15
Technical Standards .....	15
Online Payment Processing .....	15
Summary of principles .....	16
General Architecture Principles .....	16
Application / Web Development Specific Principles .....	16
Product/Technology Life Cycle Matrix .....	18
Life Cycle Definitions.....	18
Application/ Web Development Domain Products and Standards .....	19
Application Development .....	19
Business Process Management .....	21
Messaging and Middleware .....	22
Reporting.....	23
Miscellaneous Applications .....	24
GIS .....	25
Web Oriented Architecture.....	25
Service Oriented Architecture.....	26
Web publishing and Content Management.....	26
Graphic/Photo Editors.....	28
E-Commerce .....	30
Best Practices .....	31
State of Connecticut IT Policies Relevant to this Domain .....	33

# Application / Web Development Technical Domain

## *Purpose*

The purpose of this document is to set expectations of the agencies, bidders, vendors and consultants on life cycle and support for technical standards and products to be used by the agencies in acquiring, developing and deploying application and systems. This document defines the strategic standards and products for the Enterprise Architecture Standards Process (EASP) and provides technology road-maps or time frames for these standards and products. It does not address (at this time) patterns or implementation principles.

## *Overview*

The Enterprise Architecture Standards Project (EASP) covers two broad categories:

- Applied domains that identify specific technology in support of each Architecture Domain
- Integration or cross-over domains that combine and interface two or more technical domains

The Application Development Technical Architecture identifies criteria and techniques associated with the design of applications for the State's distributed computing environment that can be easily modified to respond quickly to the State's changing business needs, as well as to the rapidly evolving information technologies available to support those needs.

The State of Connecticut, like most large public and private enterprises, relies heavily on computer applications to support its business operations. Because the State's business processes change dynamically in response to both legislation and new demands from citizens, it is important that the State's computer applications also be able to change rapidly. Historically, the State's applications have been designed as 2-tier or 3-tier client/server applications. Systems were designed and implemented independently of each other, with little or no re-use of code or components.

The contemporary approach calls for considerably more modular, web-enabled applications with reusable components and sharing of information and processing resources. More importantly, application design is driven by business requirements, business activities and business processes. Applications and systems need to be designed for flexibility, scalability and agility, plus a lower total cost of ownership (TCO). Such systems generally conform to most or all of the principles of Service-Oriented Architecture (SOA), and the related Web-Oriented Architecture (WOA) and Event-Driven Architecture (EDA).

The W3C (Worldwide Web Consortium) is the primary organization for the development of interoperable technologies (specifications, guidelines, software, and tools) for Web-based architecture designs. (The Web is itself an application that rides on top of the internet and its associated technologies and standards.) Additional standard for WOA (and for SOA) are the province of the Organization for the Advancement of Structured Information Standards (OASIS).

The Web / E-Government Technical Architecture defines the policies, guidelines, best practices, technologies, and standards needed for adaptive deployment of electronic commerce and internet/intranet websites. This will allow for seamless platform-independent and secure anytime, anywhere access to state information.

## Application / Web Development Technical Domain

This domain is closely aligned with other domains including Collaboration/Directory Services, Database, and Middleware, sharing as it does technical standards, products and best practices.

### *Technology categories in this domain*

#### **Application Development**

Application Development identifies criteria and techniques associated with the design of applications for the State's distributed computing environment that can be easily modified to respond quickly to the State's changing business needs, as well as to the rapidly evolving information technologies available to support those needs.

For database standards please refer to the [Data Management Domain](#) document.

#### **Technical Standards**

XHTML, HTML, ASP

#### **Web Browser**

The primary interface for applications is a "standard" web browser, in keeping with web based architecture design. The choice of web browser is based on the target audience of the application. The technology in this category is defined in conjunction with the Platform Domain team.

The standards contained within this section are the "Code To" standards. Please refer to the Web / eGovernment section for the current desktop standards.

#### **HTML/XML Editing**

HTML or XML creation and editing is normally handled by the application development toolset; it can also be handled through the portal product or a stand-alone tool. (See Web Oriented Architecture below).

#### **Application Development Languages**

An application development language is a very-high-level programming language that generates coding in a conventional programming language or provides the user of a database management system with a programming language that is easier to implement than conventional programming languages. High-level languages permit a programmer to ignore many low-level details of the computer's hardware solving the problems of portability. Further, it is recognized that the closer the syntax, rules, and mnemonics of the programming language are to "natural language," the less likely the programmer is to introduce errors ("bugs") into the program.

C, along with its extensions, C++ and C#, has perhaps become the most widely used general-purpose language among professional programmers because of its ability to deal with the rigors of programming object-oriented programming. Object-oriented programming is a modular approach to computer program (software) design. Each module, or object, combines data and procedures (sequences of instructions) that act on the data. Java is an object-oriented

## Application / Web Development Technical Domain

language similar to C++ but simplified to eliminate features that are prone to programming errors. Java was developed specifically as a network-oriented language, for writing programs that can be safely downloaded through the Internet and immediately run without fear of computer viruses.

- ASP – including ASP Classic and ASP .Net is a framework for developing web applications and dynamically generated web pages.
- C++ - Object-oriented version of C that is popular because it combines object-oriented capability with traditional C programming syntax.
- C# - A Microsoft .NET language based on C++ with elements from Visual Basic and Java.
- COBOL - Developed in the 1960s. Widely used for mini and mainframe programming.
- Java - The programming language developed by Sun and repositioned for Web use. It is widely used on the server side, although client applications are increasingly used.
- JScript – Microsoft’s name for the scripting language used in web pages embedded into the HTML page. (Same as Sun’s JavaScript)
- JavaScript - A scripting language widely used on the Web. JavaScript is embedded into many HTML pages.
- VBScript - Subset of Visual Basic used on the Web similar to JavaScript.
- Visual Basic – A widely used Microsoft .NET language.
- Web Languages - Languages such as JavaScript, Jscript, Perl and CGI are used to automate Web pages as well as link them to other applications running in servers.

### Application Development Toolsets (IDEs)

An integrated development environment (IDE) also known as *integrated design environment* or *integrated debugging environment* is a software suite of products that provide comprehensive facilities to develop software computer programmers for software development to simplify the construction of GUI and object-oriented solutions. An IDE normally consists of:

- a source code editor
- a compiler and/or an interpreter
- build automation tools
- a debugger
- version control
- integrated tools
- test tools
- a class browser
- an object inspector
- a class hierarchy

## Application / Web Development Technical Domain

IDEs are designed to maximize programmer productivity by providing tightly-knit components with similar user interfaces. IDEs typically present a single developer workspace in which all development occurs. This developer workspace typically provides many features for authoring, modifying, compiling, deploying and debugging software. IDEs are complex environments, however, once the learning curve is mastered, the programmer has much less mode switching to do than when using discrete development programs.

IBM Rational Eclipse (incl. Java, C#, C++, and WSDL) and Microsoft Visual Studio (incl. Visual Basic, Visual C#, Visual C++, Java, and F#) are multiple-language IDEs.

JBoss Enterprise Application Platform is the market-leading platform for innovative and scalable Java applications. Integrated, simplified, and delivered by the leader in enterprise open source software, it includes leading open source technologies for building, deploying, and hosting enterprise Java applications and services.

### Standalone Testing Tools

Testing tools may be standard parts of the IDEs. You may have separate testing tools as well, for example, you may utilize tools for stress or load testing.

### Source Code Management

Source control management (SCM) is software that provides coordination and services between members of a software development team. At the most basic level, it provides file management and version control so that team members do not write over each other's changes, and only the newest versions of files are identified for use in the workspace. More enhanced SCMs also give developers the ability to work concurrently on files (in branches that may or may not converge), to merge changes with other developers' changes, to track and audit changes that were requested and made, and to track bug-fix status and to perform releases. In some cases, SCMs may include other components to assist in managing a software process throughout the entire lifecycle. SCM tools help development teams in many ways:

- **Collaboration:** SCM tools prevent one user from accidentally overwriting the changes of another, allowing many developers to work on the same code without stepping on each other's toes.
- **History:** SCM tools track the complete development history of the software, including the exact changes which have occurred between releases and who made those changes.
- **Release notes generation:** Given the tracking of each change, the SCM can be used to generate notes for their software releases that accurately capture all of the changes included in the new release.
- **Documentation and test management:** SCM tools can be used to manage not just software source code, but also test suites and documentation for their software.
- **Change notifications:** To keep interested members of the team informed when changes occur to the source code.

# Application / Web Development Technical Domain

## **Business Process Management**

Business process modeling (BPM) addresses the process aspects of business architecture and is part of the business process management (BPM) discipline. The graphical representation of business process information is of value to business stakeholders, business analysts and system developers. Effective BPM is at the heart of Service Oriented Architecture design (see below).

### **Modeling**

Business Process Modeling Notation (BPMN) — defines a standard graphical notation for specifying business processes in a business process diagram.

Unified Modeling Language (UML) — an open method used to specify, visualize, construct and document objects, components and services during system design and analysis.

### **Workflow**

A workflow application is a software application, which automates, at least to some degree, a process or processes. The processes are usually business-related, but it may be any process that requires a series of steps that can be automated via software. Some steps of the process may require human intervention, such as an approval or the development of custom text, but functions that can be automated should be handled by the application. Advanced applications allow users to introduce new components into the operation. Automated workflow tools use a programming language in conjunction with libraries and interfaces that capture abstractions for task coordination such as Microsoft Windows Workflow Foundation.

It is also possible to use languages designed for business process modeling (e.g. the Business Process Modeling Notation) to specify workflows. However, to fit the purpose of workflow specification, such notations need to be enhanced with additional constructs to capture data passing, data transformations and routing conditions and to bind tasks to their implementation. Indeed, business process modeling is about capturing business processes at a higher level of abstraction in order to enable their analysis through methods such as simulation. Meanwhile, workflow specification is about capturing processes at a level of detail that is sufficient to enable their execution.

## **Messaging and Middleware**

Middleware is software that supports communications between the functional tiers of an application, between two or more different applications, and between applications and shared services. The role of middleware is to insulate application developers from having to understand the complexities of the networking and computing environments and to minimize the use of directly interfacing to platform, network and data layers. Middleware also provides an environment in which to implement business rules (logic) and workflow rules (orchestration and choreography in SOA environments).

For the full list of standards for messaging and middleware, please refer to the [Middleware Domain document](#).

# Application / Web Development Technical Domain

## **Application Middleware and Messaging Products**

Message Oriented Middleware (MOM) is inter-application communication software that generally relies on asynchronous message passing, generally on some sort of message queuing system. An Enterprise Service Bus (ESB) performs a similar function within a Service Oriented Architecture solution. Message queuing software is considered to be a point to point model (sender and receiver know each other). The other general model is publish and subscribe in which neither the sender nor receiver know each other (a good metaphor is anonymous bulletin board).

## **Technical Standards**

Business Process Execution Language (BPEL) — BPEL is a standard executable language for specifying interactions with services or Web Services in WOA and SOA applications.

URI/URL

XML, XSLT, XPath, WS-BPEL

## **Message Queuing**

Message queuing software is considered a point-to-point model (sender and receiver know each other). Message queues provide an asynchronous communications protocol, meaning that the sender and receiver of the message do not need to interact with the message queue at the same time. Messages placed onto the queue are stored until the recipient retrieves them. Most message queues have set limits on the size of data that can be transmitted in a single message. Many implementations of message queues function internally: within an operating system or within an application. Such queues exist for the purposes of that system only. Other implementations allow the passing of messages between different computer systems, potentially connecting multiple applications and multiple operating systems. These message queuing systems typically provide enhanced resilience functionality to ensure that messages do not get "lost" in the event of a system failure.

## **Reporting**

The reporting category covers two primary types of tools: (1) tools intended for end-users for simple reporting and analysis and (2) tools designed to enable developers to easily deliver reports that are either fundamental to a system or more complex than the end-user can reasonably be expected to produce.

Tools intended for end-users are covered in the [Collaboration and Directory Services Domain](#) document under desktop standards.

## **Report Creation**

Reporting software allows report designers to create highly formatted reports, connected to virtually any data source. Features to look for in a good reporting tool include:

- Interactivity empowering business users to manipulate data
- Ad Hoc report creation
- Security

## Application / Web Development Technical Domain

- Ability to securely share, schedule and deliver reports in a variety of formats including e-mail and over the Web
- Customization
- Export capabilities to other formats such as Excel, PDF, CSV, XML, TIFF (and other image formats), MS Word, and HTML Web Archive.
- Support page styling including fields, images, graphs, tables.
- Support field definitions including extended attributes of fields populated with formulas, dynamic data, or Database derived data.
- Accept Parameters either furnished by the user or passed in from another application; and database connections and queries for pulling data into the report.

### **Report Servers**

A report server is the central component of a Reporting Services installation, consisting of a pair of core processors plus a collection of special-purpose extensions to handle authentication, data processing, rendering, and delivery operations. Processors are the hub of the report server. The processors support the integrity of the reporting system and cannot be modified or extended. Extensions are also processors, but they perform very specific functions. Reporting Services includes one or more default extensions for every type of extension that is supported. You can add custom extensions to a report server to support features such as support for single sign-on technologies, report output in application formats not handled by the default rendering extensions, and report delivery to a printer or application.

A single report server instance is defined by the complete collection of processors and extensions that provide end-to-end processing, from the handling of the initial request to the presentation of a finished report. Through its subcomponents, the report server processes report requests and makes reports available for on-demand access or scheduled distribution.

### **Online Analytical Processing (OLAP) tools**

In situations where the drill down and sorting features of Enterprise Reporting products are insufficient to meet user needs for custom reporting, Query / Analysis tools may be used to satisfy the needs of the “advanced” user. OLAP tools are required when high-end scalability and advanced ad hoc analytical queries, and multi-dimensional and cross-dimensional operations are required.

### **Miscellaneous Applications**

Technology standards in this category include Project Management tools, Help File/Facilities tools, Optical Character Recognition (OCR) tools, and Document Management tools. Other technology standards, that do not fall under the other Application Development categories, may be added to this section.

#### **Help File/Facilities**

Help authoring tools (HAT) automate and speed up the generation/creation of help files. HAT tools vary in the formats supported for import, including such formats as ASCII, HTML and Microsoft Word, and compiled Help formats such as Microsoft WinHelp and Microsoft Compressed HTML Help. The output from a HAT can be either a compiled Help

## Application / Web Development Technical Domain

file in a format such as WinHelp (\*.HLP) or Microsoft Compiled HTML (\*.CHM), or non-compiled file formats such as Adobe PDF, XML, or HTML.

Base the selection of the format you use for your help files on an evaluation of how your system will be distributed and how people will use it. Do they need a context help file in the application or will they print out the entire help file and keep the manual on their desk? How often will you update the help file? Is it relatively easy to distribute together with your program files or is it better to store it on the website? Answering these questions will help you decide which format is best. Often a combination of approaches is best, for example:

- Keep the HTML manual on your website for reference and it may attract people from search engines
- Distribute the CHM file with the application for context sensitive help
- Upload the printable version of the help file in PDF or RTF\DOC format on the public website for those who may want to print out the entire document as a reference
- Maintain a permanent version in your Document Management database

### Other

**Optical Character Recognition (OCR)** is the mechanical or electronic translation of scanned images of handwritten, typewritten or printed text into machine-encoded text that can be easily edited, searched, electronically stored, displayed, and printed free of scanning artifacts. OCR greatly reduces the storage space as required by hard copy materials and enables the use of such techniques as machine translation, text-to-speech and text mining. It is widely used to convert books and documents into electronic files, to computerize a record-keeping system in an office, or to publish the text on a website.

OCR technology requires both hardware and software. Sophisticated OCR systems may require an additional circuit board in the computer itself to complete the process. An optical scanner scans the text on a page and breaks the fonts down into a bitmap, and translates the bitmap into computer text. Currently, OCR technology supports most common fonts; however, improvements still need to be made in handwriting recognition or fonts that look similar to handwriting.

OCR is a field of research in pattern recognition, artificial intelligence and computer vision.

**Document Management** controls the life cycle of documents in your organization from how they are created, reviewed, published, and consumed to how they are ultimately disposed of or retained. Although the term "management" implies top-down control of information, an effective document management system should reflect the culture of the organization using it. The tools you use for document management should be flexible, allowing you to tightly control documents' life cycles or loosely structure the system if that better suits your enterprise. A well-designed document management system should support ease of finding and sharing information; organize content in a logical way; make it easy to standardize content creation and presentation across an enterprise; promote knowledge management and information mining; and help your organization meet its legal responsibilities. Document

## Application / Web Development Technical Domain

management systems commonly provide storage, versioning, metadata, security, as well as indexing and retrieval capabilities.

For additional information on the State's standards of Document Management please refer to the [Collaboration and Directory Services Domain](#) Document.

### **Geographic Information Systems (GIS)**

GIS software allows users to effectively capture, store, manipulate, analyze and display all forms of geographically referenced information. Such information includes any data that can be identified with a specific location on a map, whether it is tied to a specific address or aggregate information about a particular area of land such as a town, county or state.

Geographic data is logically and effectively organized so that users can take such data and turn it into information that can be communicated in an intuitive manner that enhances understanding and decision-making. GIS software allows users to present such information in a map format, or information can be generated using tools included in the software and then presented in other formats as needed.

#### **Technical Standards**

ArcGIS Desktop by ESRI is available in several licensing levels that include more or less features and cost commensurately more or less to license:

- ArcView (Basic)
- ArcEditor (Intermediate)
- ArcInfo (Advanced)

There are also many extensions to the software to perform specialized functions and analysis that may be purchased separately, including:

- ArcGIS 3D Analyst
- ArcGIS Geostatistical Analyst
- ArcGIS Network Analyst
- ArcGIS Schematics
- ArcGIS Spatial Analyst
- ArcGIS Survey Analyst
- ArcGIS Tracking Analyst

#### **Enterprise GIS**

ArcGIS Server by ESRI, , for which there are several editions that include more or less features and cost commensurately more or less to license:

- Basic
- Standard
- Advanced

Each edition can then be licensed at two different levels of capacity, including:

## Application / Web Development Technical Domain

- Workgroup (limited to running on a single machine, 4 GB of storage on a multi-user database, up to 10 simultaneous connections to a single multi-user database, and uses only SQL Server Express as the database engine.
- Enterprise (runs on multiple machines, user's choice of multi-user database, with unlimited storage and number of simultaneous connections to multi-user geodatabases.

### **Web Oriented Architecture (WOA)**

Web-Oriented Architecture (WOA) is an architecture approach that leverages characteristics and technology of the web (e.g., XML, HTTP), and that uses Asynchronous Java and XML (AJAX) for communications. Some WOA applications are in fact a flavor of SOA design. The term WOA is not synonymous with Web 2.0, which is a developmental approach to web based designs that emphasizes flexibility and user interaction.

For the full list of standards for WOA, please refer to the [Middleware Domain](#) document.

#### **Technical Standards**

WSDL, SOAP, XML, XForms, XHTML, HTML

#### **Web Browser**

The primary interface for applications is a “standard” web browser, in keeping with web based architecture design. The choice of web browser that is the target environment is based on the target audience of the application. The technology in this category is defined in conjunction with the platform domain team.

#### **HTML/XML Editing**

HTML or XML creation and editing is normally handled by the application development toolset; it can also be handled through the portal product or a stand-alone tool.

### **Web publishing and Content Management**

Web publishing consists of those topics involved with the presented images, the process for creation of websites, maintenance of the sites, and content management.

#### **Technical Standards**

Many interdependent standards and specifications, some of which govern aspects of the Internet, not just the Web, directly or indirectly affect the development and administration of websites and web services. Considerations include the interoperability, accessibility and usability of web pages and websites.

#### **Web Browsers**

Within this domain, Web Browser standards are set for development, testing, and production. These are the minimum web browser requirements that websites and web applications being created for state business should function within. Web browsers are primarily intended to

## Application / Web Development Technical Domain

access the [Internet](#). They can also be used to access information provided by Web servers in private networks or files in file systems.

### **Portals**

A Portal is a term, often used interchangeably with gateway, as the entry point for users connecting to Internet, Extranet or Intranet enterprise sites. Portals generally provide a single access point to enterprise services and a variety of standard and customizable features. A Portal does not provide web content management, enterprise content management, or identity content management.

### **Web Page Creation and Editing**

This category includes software used to develop and manage a website outside a Web Content Management System.

### **Web Content Management System (WCMS)**

A WCMS is a web application used to create, manage and control a large, dynamic collection of Web materials (HTML documents and their associated images). A WCMS facilitates content creation, content control, editing, and essential Web maintenance functions.

### **Link Checker**

Software tools to aid web content managers to locate orphans or broken links within a site.

### **Forums**

Software tools to aid web content managers to design and host moderated forums.

### **Graphic/Photo Editors**

Software with which a user may manipulate, enhance, and transform images.

### **Interactive Content Development**

Multimedia includes a combination of text, audio, still images, animation, video, and interactivity content forms.

### **On-Line Publication**

Software animation, storyboard, 2D and 3D tools to aid web content managers in designing web content, must include a comparable text page for section 508 compliance.

### **Video Editors**

Software which handles the editing of video sequences on a computer. Digital editors are typically based on a timeline interface paradigm where sections of moving image video recordings, known as clips, are laid out in sequence and played back. They offer a range of tools for trimming, splicing, cutting and arranging clips across the timeline.

# Application / Web Development Technical Domain

## Video Captioning Tools

This category includes tools to assist in making a transcript and adding closed captioning to video to meet accessibility requirements.

## Search Engines

A web search engine is designed to search for information on the WWW. The search results are usually presented in a list and are commonly called *hits*. The information may consist of web pages, images, information and other types of files.

Definitions above provided by Wikipedia at <http://en.wikipedia.org>

## eCommerce

The two major forms of eCommerce are Business-to-Consumer (B2C) and Business-to-Business (B2B). The terms “e-business” and “e-tailing” are often used synonymously with eCommerce. The terms “e-tailing” or “virtual storefronts” refer to websites with online catalogs. Security includes authenticating business transactors, controlling access to resources such as Web pages for registered or selected users, encrypting communications and, in general, ensuring the privacy and effectiveness of transactions.

## Technical Standards

- Electronic Data Interchange (EDI) is used for the business-to-business exchange of data. EDI may be replaced by one or more standard Extensible Markup Language (XML) formats, such as electronic business Extensible Markup Language (ebXML).
- Among the most widely-used security technologies is the Secure Socket Layer (SSL) which is built into Web browsers. (Refer to [Security Domain Document](#))

## Online Payment Processing

- DoIT has developed a web service called “DoIT Payment Service” to be used by State agencies when developing websites and/or applications that need to process Credit Card transactions. This payment service uses PayPal Payflow Pro API to communicate with PayPal, the secure commercial Credit Card processing tool.

# Application / Web Development Technical Domain

## *Summary of principles*

### **General Architecture Principles**

1. Product choices and solution architectures should minimize overall total cost of ownership. This can be accomplished by consistency and uniformity in making choices about standards and products.
2. Product choices and solution architectures must provide for and enhance the overall security and integrity of systems and information assets.
3. Products choice decisions must consider the availability of training and technical support.
4. Product choices and solutions should minimize short term and long term risks, this can be partially accomplished by utilizing widely supported products or those with long-term support commitments by vendors (see principle 6).
5. Solution architectures should maximize information sharing among agencies and applications.
6. Product standards will consist of vendor supported versions only; this includes open source products.
7. New products and version/release upgrades for existing products will not become standard until a minimum 6 months has passed after the manufacturer's General Availability date.

### **Application / Web Development Specific Principles**

1. Use the State's SDM for all applicable projects involving development, enhancement, procurement, deployment of applications and systems.
2. Implement IT systems in adherence with all security, confidentiality, and privacy policies and applicable statutes. Act appropriately to protect information confidentiality, integrity and availability.
3. Applications, systems, and infrastructure that support the anytime/anywhere access to information and services will be given priority over alternate solutions where practical.
4. The boundaries between application component functionality should reflect the way work is accomplished in the business unit. Interfaces between components should reflect business interfaces so there is linkage between the business and IT solutions.
5. Document the design of all application. Object models, service, WSDL, interaction diagrams and other design artifacts record the structure, behavior and interfaces of application solutions. These are important deliverables of the development process that can benefit future efforts.
6. Leverage data warehouses to facilitate the sharing of existing information to accelerate and improve decision-making at all levels.
7. Design, acquire, develop, or enhance systems allowing data and processes to be shared and integrated across the enterprise and with our partners.
8. The enterprise architecture must reduce integration complexity to the greatest extent possible.
9. Look to reuse existing applications, systems and infrastructure before investing in new solutions. Build only those applications or systems that will provide a clear business advantage and demonstrate cost savings.
10. Analyze, simplify and otherwise redesign business processes as appropriate first, then implement new information systems.

## Application / Web Development Technical Domain

11. Applications, systems and infrastructure will employ reusable components across the enterprise, using an *n-tier* model.
12. The logical design of application systems and databases should be highly partitioned. These partitions must have *logical boundaries* established and must not be violated.
13. The interfaces between separate applications requiring real-time synchronization should be message-based for both internal and external systems.
14. Deploy application systems driven by business events.
15. Applications and systems should be evolving toward an object-oriented approach.
16. Employ consistent software engineering practices and methods based on accepted industry standards.
17. Websites and Web-based systems such as eGovernment, eCommerce and Web Content Management:
  - a) Should be driven by business principles and events.
  - b) Must always be in compliance with applicable Federal and State laws and regulations.
  - c) Must be developed and implemented using the appropriate application standards and security models based on data classification (Refer to Security Domain Document)
  - d) Should always be published with and adhere to a strict and valid privacy policy (Refer to CT.gov Privacy Policy for model).

# Application / Web Development Technical Domain

## *Product/Technology Life Cycle Matrix*

### Life Cycle Definitions

The Life Cycle Matrix is based a sliding window of 12 quarters (3 Fiscal years). The date range of a fiscal year is July 1 through June 30.

Key	Definition
S	<b>Standard</b> - These are the products and standards selected by the state for NEW development or acquisition, and for the replacement of <i>obsolete</i> or <i>transitional</i> standards or products. They are supported by DOIT and have mainstream support from one or more vendors or standards bodies.
T	<b>Transitional</b> - Products are currently supported by DOIT, the agencies, or a vendor; however they have been replaced by new standard products or standards. Transitional products may have limited support from a vendor or have a defined End of Life (EOL). Neither the State nor the agencies should use these standards or products for NEW development. Existing implementations may be upgraded to a newer version to fix security or functional issues.  Agencies should develop plans to migrate from transitional to new standard products either by replacing the technologies or replacing the solution prior to the End-of Life of the product.
O	<b>Obsolete &amp; Divest</b> – Products or standards that are in use by the agencies. These products are generally End of Life and have very limited or no support from vendors, the community or DOIT.  Neither the agencies nor the State should undertake new investments or development using these products (this includes version upgrades).  Plans should be developed by to migrate from obsolete to standard products either by replacing the technologies or replacing the solution as rapidly as possible.

## Application / Web Development Technical Domain

### *Application/ Web Development Domain Products and Standards*

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
<b>Application Development</b>														
<b>Technical Standards</b>														
ASP.NET 4	.NET				S	S	S	S	S	S	S	S	S	S
ASP.NET 3	Microsoft .NET or JAVA		S	S	T	T	T	T	T	T	T	T	T	T
ASP.NET 2	Microsoft .NET		T	T	O	O	O	O	O	O	O	O	O	O
ASP.NET 1.1	Microsoft .NET	Legacy support only	O	O	O	O	O	O	O	O	O	O	O	O
<b>HTML/XML Editing Tools</b>														
MS XML Notepad		Entry Level XML Editor	S	S	S	S	S	S	S	S	S	S	S	S
Altova XML Spy			S	S	S	S	S	S	S	S	S	S	S	S
<b>Application Development Languages</b>														
Visual Basic	.Net		S	S	S	S	S	S	S	S	S	S	S	S
Visual C#	.Net		S	S	S	S	S	S	S	S	S	S	S	S
Visual Basic v6.0			O	O	O	O	O	O	O	O	O	O	O	O
ASP.NET	.NET		S	S	S	S	S	S	S	S	S	S	S	S
Java	Microsoft .NET or JAVA		S	S	S	S	S	S	S	S	S	S	S	S

Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Jscript		limited client side edits, dynamics	S	S	S	S	S	S	S	S	S	S	S	S
COBOL LE			T	T	T	T	T	T	T	T	O	O	O	O
MicroFocus Cobol			T	T	T	T	T	T	T	T	O	O	O	O
<b>Application Development Toolsets</b>														
Visual Studio 2010					S	S	S	S	S	S	S	S	S	S
Visual Studio 2008			S	S	T	T	T	T	T	T	T	T	T	T
Visual Studio 2005			T	T	O	O	O	O	O	O	O	O	O	O
Borland JBuilder Enterprise 2006	JAVA		T	T	T	T	T	T	T	T	O	O	O	O
Eclipse		JAVA Open Source IDE	S	S	S	S	S	S	S	S	S	S	S	S
IBM Rational Suite		High end diagramming tools used to document complex systems or business processes or other complex models.	S	S	S	S	S	S	S	S	S	S	S	S
Oracle JDeveloper			T	T	T	T	T	T	T	T	O	O	O	O
JBoss Development Studio	JAVA	Java Application Server	S	S	S	S	S	S	S	S	S	S	S	S

Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
<b>Standalone Testing Tools</b>		Contact Enterprise Architecture for Information												
<b>Source Code Management</b>														
HCM	Mainframe		S	S	S	S	S	S	S	S	S	S	S	S
Team Foundation Server	MS .NET				S	S	S	S	S	S	S	S	S	S
Visual SourceSafe 6.0c	MS .NET		S	S	T	T	T	T	T	T	T	T	T	T
Perforce	JAVA/.NET	Software Version / Change Management	S	S	S	S	S	S	S	S	S	S	S	S
<b>Business Process Management</b>														
<b>Modeling</b>														
MS Visio 2010					S	S	S	S	S	S	S	S	S	S
MS Visio 2007			S	S	T	T	T	T	T	T	T	T	T	T
<b>Workflow</b>														
MS Windows Workflow Foundation	MS .NET		S	S	S	S	S	S	S	S	S	S	S	S

Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
FileNet P8 Workflow.	Mainframe		S	S	S	S	S	S	S	S	S	S	S	S
Laser Fiche			T	T	T	T	T	T	T	T	O	O	O	O
<b>Messaging and Middleware</b>														
<b>Technical Standards</b>														
XML 1.0 / 1.1		Refer to <a href="#">Middleware Domain</a>												
XSD 1.1		XML Documentation	S	S	S	S	S	S	S	S	S	S	S	S
XSLT 2.0		XML Validations	S	S	S	S	S	S	S	S	S	S	S	S
XSLT 1.1	XML Validations	XML Validations	T	T	T	T	T	T	T	T	O	O	O	O
XPath 1.0		Refer to <a href="#">Middleware Domain</a>												
WS-BPEL 2.0	Oracle		S	S	S	S	S	S	S	S	S	S	S	S
<b>Message Queuing</b>														
IBM WebSphere MQ 7.0.1	All	Middleware Messaging			S	S	S	S	S	S	S	S	S	S
IBM WebSphere MQ 6.0	All	Middleware Messaging	S	S	T	T	T	T	O	O	O	O	O	O
ActiveMQ	All	Middleware	T	T	T	T	T	T	T	T	O	O	O	O

## Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
		Messaging												
JBoss Messaging 1.4	Java	JBOSS implementation of JMS	S	S	S	S	S	S	S	S	S	S	S	S
Windows Communication Foundation (.NET 4.x)	All	Part of .NET 4.x framework Uses MS Message Queuing			S	S	S	S	S	S	S	S	S	S
Windows Communication Foundation (.NET 3.x)	All	Part of .NET 3.x framework. Uses MS Message Queuing	S	S	T	T	T	T	T	T	T	T	T	T
<b>Reporting</b>														
MS SSRS 2008		SQL Server	S	S	S	S	S	S	S	S	S	S	S	S
MS SSRS 2005		SQL Server	T	T	T	T	T	T	T	T	O	O	O	O
Visual Studio 2010					S	S	S	S	S	S	S	S	S	S
Visual Studio 2008			S	S	T	T	T	T	T	T	O	O	O	O
Crystal Reports		Oracle / SQL Server	S	S	S	S	S	S	S	S	S	S	S	S
<b>Report Servers</b>														
MS SQL Server		Refer to <a href="#">Database Management Domain</a>												
Crystal Reports Server		Refer to <a href="#">Database</a>												

Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
		<a href="#">Management Domain</a>												
<b>OLAP tools</b>														
		Refer to <a href="#">Database Management Domain</a>												
<b>Miscellaneous Applications</b>														
<b>Help File/Facilities</b>														
Adobe RoboHelp (versions 5,6,7,8 –v 8 released in 2009)		Help file creation (formerly Blue Sky and Macromedia)	S	S	S	S	S	S	S	S	S	S	S	S
Snag-It		Refer to <a href="#">Collaboration and Directory Services Domain</a>												
<b>Other</b>														
OCR - Pegasus	.NET	Document Scanning and Optical Character Recognition (OCR)	S	S	S	S	S	S	S	S	S	S	S	S
Asprise (Doc management)	Java/.NET	Document	S	S	S	S	S	S	S	S	S	S	S	S

Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
		Scanning												
<b>GIS</b>														
<b>Technical Standards</b>														
ESRI ArcGIS Desktop 9.x							S	S	S	S	S	S	S	S
ESRI ArcGIS Desktop 8.x			S	S	S	S	S	T	T	T	T	T	T	T
MapInfo			T	T	T	T	T	T	T	T	O	O	O	O
<b>Enterprise GIS</b>														
ESRI ArcGIS Server 8.x			S	S	S	S	S	S	S	S	S	S	S	S
<b>Web Oriented Architecture</b>														
<b>Technical Standards</b>														
WSDL		Refer to <a href="#">Middleware Domain</a>												
SOAP 1.2		Refer to <a href="#">Middleware Domain</a>												

Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
<b>Service Oriented Architecture</b>														
<b>Technical Standards</b>		Refer to <a href="#">Middleware Domain</a>												
<b>Web publishing and Content Management</b>														
<b>Technical Standards</b>														
HTML 4.01 Transitional*		Markup Language	S	S	S	S	S	S	S	S	S	S	S	S
XHTML 1.1		Hypertext with the full benefits of XML architecture	S	S	S	S	S	S	S	S	S	S	S	S
CSS 2.1		Style Sheet Standard	S	S	S	S	S	S	S	S	S	S	S	S
XML 1.0		Markup Language	S	S	S	S	S	S	S	S	S	S	S	S
WMV		Streaming Video Standard	S	S	S	S	S	S	S	S	S	S	S	S
SWF		Non-streaming (short duration)	S	S	S	S	S	S	S	S	S	S	S	S
* HTML is based on 3 document type declarations (Strict, Transitional, and Frameset)														
<b>Web Browsers</b>		Browsers listed below are for development compliance. See Platform domain for Enterprise Desktop Standards.												

## Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Microsoft Internet Explorer 8.0		Required Standard	S	S	S	S	S	S	S	S	S	S	S	S
Microsoft Internet Explorer 7.0		Required Standard	S	S	S	S	S	S	S	S	S	S	S	S
Internet Explorer 6		Baseline for Web development only	O	O	O	O	O	O	O	O	O	O	O	O
Mozilla Firefox 3.6		Required Standard	S	S	S	S	S	S	S	S	S	S	S	S
Google Chrome 4.1		Optional	S	S	S	S	S	S	S	S	S	S	S	S
<b>Portals</b>														
Microsoft SharePoint 2010		Internet, Extranet, and Intranet Enterprise Portals			S	S	S	S	S	S	S	S	S	S
<b>Web Page Creation and Editing (HTML Editors)</b>														
MS FrontPage 2003		Website creation and support	T	T	T	T	O	O	O	O	O	O	O	O
MS Expression Web 3		Website creation and support. Better integration with Microsoft technology.	S	S	S	S	S	S	S	S	S	S	S	S
Adobe Dreamweaver CS4		Website creation and support	S	S	T	T	T	T	T	T	O	O	O	O
Adobe Dreamweaver CS5		Website creation and support. Better integration with Adobe products.			S	S	S	S	S	S	S	S	S	S

Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
<b>Web Content Management Systems</b>														
Classic DSF 2.0 (Cimbrian)			S	S	S	S	T	T	T	T	O	O	O	O
<b>Link Checker</b>														
InSpyder (OrFind, InSite)		OrFind for orphan reporting, InSite for link checking.			S	S	S	S	S	S	S	S	S	S
<b>Forums</b>														
ASPPlayground.Net		Moderated Forums			S	S	S	S	S	S	S	S	S	S
<b>Graphic/Photo Editors</b>														
Adobe Photoshop CS4		For complex photo and graphic manipulation	S	S	T	T	T	T	T	T	O	O	O	O
Adobe Photoshop CS5		For complex photo and graphic manipulation			S	S	S	S	S	S	S	S	S	S
Corel Paint Shop Photo Pro X3		For standard photo and graphic manipulation	S	S	S	S	S	S	S	S	S	S	S	S
Paint.Net		For basic photo and graphic manipulation	S	S	S	S	S	S	S	S	S	S	S	S
<b>Interactive Content Development</b>		For animated introductions and video only. Not for												

Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
		site development use.												
Adobe Flash CS4 Professional		For animated introductions and video only	S	S	T	T	T	T	T	T	O	O	O	O
Adobe Flash CS5 Professional		For animated introductions and video only			S	S	S	S	S	S	S	S	S	S
<b>On-Line Publication</b>														
DigiCel Flipbook		Animation, Storyboard, 2D, 3D, and Stop Motion Must be followed-up with comparable text page.			S	S	S	S	S	S	S	S	S	S
<b>Video Editors</b>														
Adobe Premier Pro CS4		High Performance, feature-rich video editing software.	S	S	T	T	T	T	T	T	O	O	O	O
Adobe Premier Pro CS5		High Performance, feature-rich video editing software.			S	S	S	S	S	S	S	S	S	S
Avid Pinnacle Studio Ultimate Collection 14		User friendly - entry level video editing software	S	S	S	S	S	S	S	S	S	S	S	S
<b>Video Captioning Tools</b>														
NCAM MAGpie 2.0.5		Free tool to add captions to video	S	S	S	S	S	S	S	S	S	S	S	S

Application / Web Development Technical Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
DicTran WAVpedal 7		Transcription Tool	S	S	S	S	S	S	S	S	S	S	S	S
<b>Search Engines</b>														
USASearch		External Sites Only - Free service from federal government	S	S	S	S	S	S	S	S	S	S	S	S
Ultraseek		Search engine used for internal websites (Intranets)	T	T	T	T	O	O	O	O	O	O	O	O
<b>E-Commerce</b>														
<b>Technical Standards</b>														
EDI		Electronic Data Interchange	S	S	S	S	S	S	S	S	S	S	S	S
XML/ebXML		Extensible Markup Language/ Electronic Business XML	S	S	S	S	S	S	S	S	S	S	S	S
SSL		Secure Socket Layer	S	S	S	S	S	S	S	S	S	S	S	S
<b>Online Payment Processing</b>														
DoIT Payment Service		DoIT Developed Service utilizing PayPal	S	S	S	S	S	S	S	S	S	S	S	S

## Application / Web Development Technical Domain

### *Best Practices*

- Best Practice 1.** Adopt a total cost of ownership model for applications and technologies that balances the costs of development, support, training, disaster recovery and retirement against the costs of flexibility, scalability, ease of use, and reduction of integration complexity.
- Best Practice 2.** Implement business rules as discrete components ensuring the correct enactment of policies governing the accuracy of related data and the execution of the actions to be performed. Discrete components support the ease of change to business rules and policies and verification that the information or process complies with the applicable rules.
- Best Practice 3.** Access data through business rules.
- Best Practice 4.** Make business rule components platform-neutral supporting SOA architecture.
- Best Practice 5.** Assign responsibility for defining and maintaining the integrity of business rules to business units.
- Best Practice 6.** Adopt coding standards for all languages on all platforms.
- Best Practice 7.** Design applications for future usage and added functionality. Most applications evolve to support new business requirements. Extensibility provides functional scalability.
- Best Practice 8.** Use integrated tool sets to support the use of the State's SDM.
- Best Practice 9.** Document object models, interaction diagrams, design artifacts, and record the structure, behavior and interfaces of application solutions. Document business processes, business rules, source code and user interface.
- Best Practice 10.** Design applications that are platform independent.
- Best Practice 11.** Design the code providing input and output to the user interface to support as wide a range of interfaces as needed, including other applications and other types of user interfaces such as internal user, mobile user, Internet, and Extranet.
- Best Practice 12.** Once the detailed application design is complete, concentrate on achieving a working system utilizing reusable components whenever possible, allowing the system to be tested first and optimized later.
- Best Practice 13.** Design applications so they can be managed using the enterprise's system management practices and tools.
- Best Practice 14.** Design for ease of testing; design application components so they can be tested and debugged easily.
- Best Practice 15.** Design web-facing applications to support the current minimum "code to" standards for web browsers. Recommended baseline "code to" standards optionally include Microsoft IE 6.0 and above, Mozilla Firefox 3.x and above, Google Chrome 4.x and above, Apple Safari 3.x and above, and Opera 10.x and above.
- Best Practice 16.** Implement Commercial Off-The-Shelf (COTS) solutions with little or no customizations and well defined governance procedures. Business needs requiring specific customizations should lean towards Modifiable Off-The-Shelf (MOTS) solutions or Government Off-The-Shelf (GOTS) solutions.
- Best Practice 17.** Establish and maintain shared reuse libraries.

## Application / Web Development Technical Domain

- Best Practice 18.** Develop solutions using industry standard coding practices including conventions, styles, standards, and security guidelines.
- Best Practice 19.** “DoIT Payment Service” must be used by State agencies when developing websites and/or applications that need to process Credit Card transactions. This payment service uses PayPal Payflow Pro API to communicate with PayPal, the secure commercial Credit Card processing tool.
- Best Practice 20.** The use of Adobe Flash is limited to only creating animated introductions and features on existing websites and for video. Flash cannot be used to develop interactive websites or applications. Special consideration should be given to ensure accessibility of any Flash content.
- Best Practice 21.** Within this domain, Web Browser standards are set for development, testing, and production. These are the minimum web browser requirements that websites and web applications being created for state business should function within.
- Best Practice 22.** It is the policy of the State of Connecticut to ensure that people with hearing, visual and other disabilities have equal access to public information that is available on the Internet and the Web to ensure access.
- a. Federal Rehabilitation Act Section 508 standards must be incorporated on state funded websites;
  - b. It is the direct responsibility of the agency and its web page developers to become familiar with the guidelines for achieving universal accessibility and to apply these principles in designing and creating any official State of Connecticut Website;
  - c. Testing tools should be used to validate a site’s adherence to Section 508. Recommended tools are available at <http://www.access.state.ct.us/tools.html>.
- Best Practice 23.** CT.gov “branding standards for new websites or applications is available.
- a. Agencies should review the [CT.gov Website Guidelines](#) for more details on home page content standards.
- Best Practice 24.** Data validation must be written into all online forms
- Best Practice 25.** A security assessment should be performed on all new websites and applications that collect information or were developed in a programming language. (Refer to [Security Domain Document](#))
- Best Practice 26.** All websites and applications should have a valid privacy policy that meets the requirements of the application or website where it resides. CT.gov policy can be used or modified as needed to ensure policy compliance.
- Best Practice 27.** All applicable policies should be reviewed prior to creating any new websites and applications (including social networking websites) (Refer to the [State of Connecticut Policies Relevant to this Domain](#))
- Best Practice 28.** Content on websites and applications should reviewed, at a minimum, on an annual basis. Outdated content should be removed or modified.
- Best Practice 29.** Content no longer needed should be deleted from web servers. Web servers should not be used for archive purposes. All content that needs to be saved and stored for record retention should be housed locally at the agency.
- Best Practice 30.** Websites that are no longer being used must be taken offline and the domain name should be redirected to an active website.

***State of Connecticut IT Policies Relevant to this Domain***

[Policy for the Management of State Information Technology Projects](#)

[Domain Name Registration and Usage](#)

[Implementation and Deployment of State Agency Internet Sites and Extranet Sites](#)

[Acceptable Use Policy of State Systems \(Internet and E-Mail\)](#)

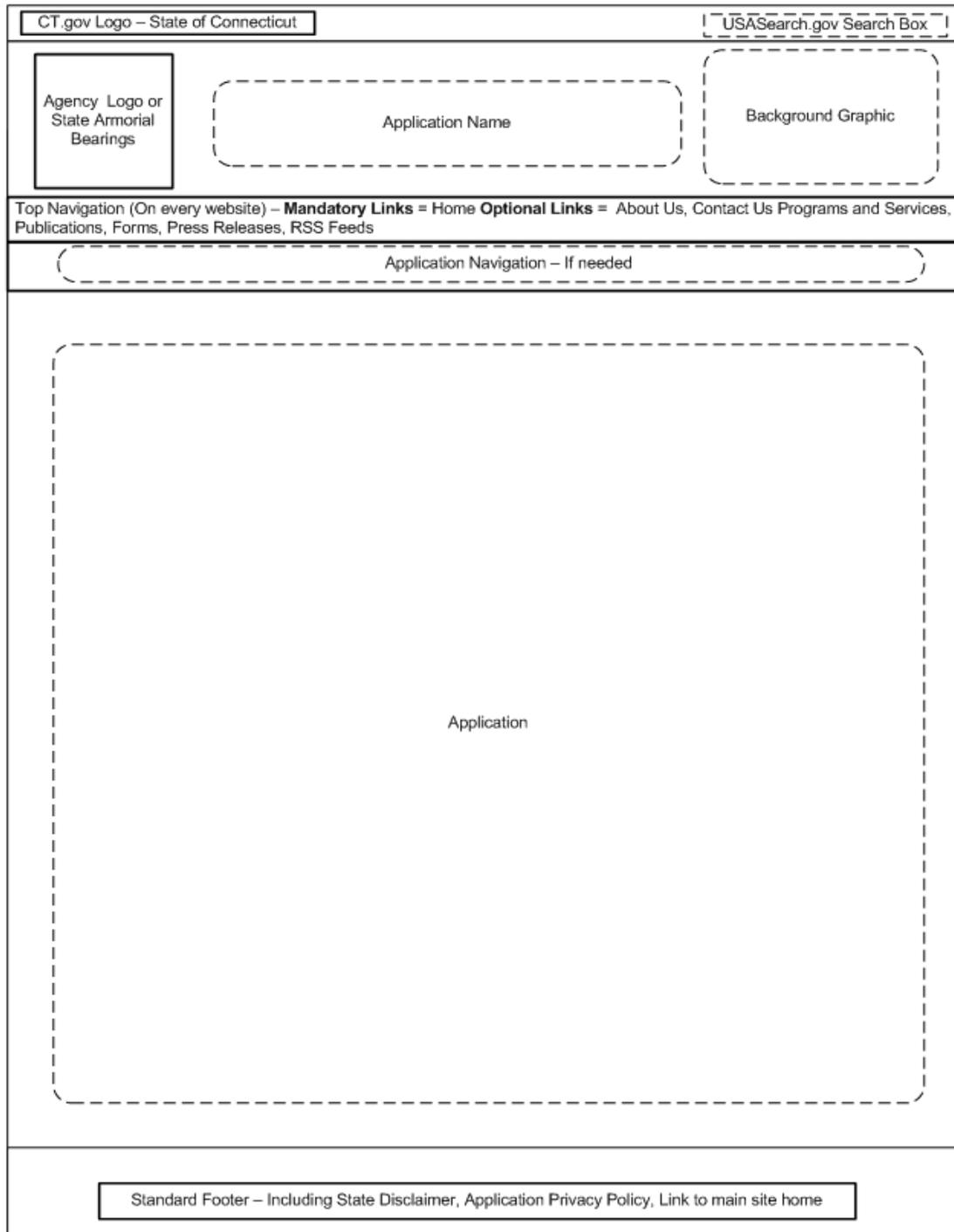
[Accessibility Policy for Connecticut State Government Websites](#)

[\*\*Management of State Information Technology Projects\*\*](#)

[\*\*Network Security and Procedures\*\*](#)

# Application / Web Development Technical Domain

## Generic CT.gov Application Template



Example of Site available at [www.ct.gov/dot](http://www.ct.gov/dot)

Revised April 2010

## Enterprise Systems Management Domain

---

### History of Changes

<b>Date</b>	<b>Modification</b>	<b>Author</b>
May 11 <sup>th</sup> 2010	Approved by Enterprise Architecture	Enterprise Architecture
June 2 <sup>th</sup> 2010	Approved by CIO	Enterprise Architecture
June 30 <sup>th</sup> 2010	Approved by the Information & Telecommunication Systems Executive Steering Committee	Enterprise Architecture
December 13 <sup>th</sup> 2010	Service Management Standard set by Enterprise Systems Management Domain	ESM Domain Team Lead
December 5, 2010	Approved by Enterprise Architecture	Enterprise Architecture
December 13, 2010	Approved by CIO/CTO	Enterprise Architecture
December 22, 2010	Approved by the Information & Telecommunication Systems Executive Steering Committee	Enterprise Architecture

# Enterprise Systems Management Domain

## Table of Contents

History of Changes .....	1
Purpose.....	3
Overview.....	3
Technology categories in this domain .....	3
Service Management.....	3
Service Desk .....	3
Incident Management.....	4
Problem Management .....	4
Change Management .....	4
Configuration Management .....	4
Network / System Management.....	4
Storage Management .....	5
Electronic Software Distribution .....	5
Packaging.....	6
Distribution .....	6
Client-Side Installation .....	6
Reporting.....	6
Summary of principles .....	7
General Architecture Principles.....	7
Enterprise Systems Management Specific Principles.....	7
Product/Technology Life Cycle Matrix .....	8
Life Cycle Definitions.....	8
Systems Management Products and Standards.....	9
Service Management.....	9
Storage Management .....	10
Electronic Software Distribution .....	10
Best Practices .....	12

# Enterprise Systems Management Domain

## **Purpose**

The purpose of this document is to set expectations of the agencies, bidders, vendors and consultants on life cycle and support for technical standards and products to be used by the agencies in acquiring, developing and deploying application and systems. This document defines the strategic standards and products for the Enterprise Architecture Standards Process (EASP) and provides technology road-maps or time frames for those standards and products. It does not address (at this time) patterns or implementation principles.

## **Overview**

The Enterprise Systems Management (ESM) Domain defines the operational aspects of IT services delivery and identifies accepted State-wide policies, practices, standards, and processes for administering, monitoring, and controlling hardware and software components of the infrastructure.

ESM activities include, but are not limited to: network monitoring, server monitoring, applications monitoring, troubleshooting tools, service desk, asset management, storage management, and event management.

## **Technology categories in this domain**

### *Service Management*

Service Management relates to managerial and procedural activities that operations must support to meet customer and business requirements. The management actions and activities associated with this core process are planning, administration, cost control, service options, and customer relations.

Service Support is the connection between the other core processes. The primary role for Service Support is to be the communication channel between the customer and the IT service organization. There are several sub-processes, such as Supporting and Changing, by which customer interactions take place. It is through these sub-processes that IT service personnel manages all customer-facing issues and problems.

The agency Help Desk provides a single point of contact for handling a wide range of user support requests and service delivery issues related to information technology. All requests and issues are tracked in a service management tool. The service management tool integrates with many support functions including service requests, incident management, problem management, change management, and configuration management.

### **Service Desk**

The Service Desk is the central point of contact between service providers and users/customers on a day-to-day basis. It provides a Single Point of Contact ("SPOC") to meet the communications needs of both users and IT and to satisfy both customer and business objectives. It is also a focal point for reporting *Incidents and Problems* (disruptions or potential disruptions in service availability or quality) and for users making *Service Requests* (routine requests for services).

# Enterprise Systems Management Domain

## **Incident Management**

An 'Incident' is any event which is not part of the standard operation of the service and which causes, or may cause, an interruption in or a reduction of the quality of the service. Incident Management processes and procedures enable restoration of normal service operation as quickly as possible and minimize the impact on business operations. Procedures shall include steps to address actions such as incident detection, recording, classification, initial support, investigation, diagnosis, resolution, recovery, closure, ownership, monitoring, tracking, and communication.

## **Problem Management**

A problem is a condition often identified as a result of multiple incidents that exhibit common symptoms. The Problem Management purpose is to minimize the impact on the organization. Problem Management plays a key role in detecting and providing solutions (work around and known errors) and prevents a reoccurrence. The Problem Management process is intended to reduce the number and severity of incidents on the business, and create documentation to be available for the first and second tier of the help desk.

## **Change Management**

A change is “an event that results in a new status of one or more configuration items (CIs).” A Change Management process institutes procedures that provide for the analysis, implementation, and follow up of all environmental changes requested, including those made due to problem resolution. This process supports change initiation and control actions, supports the ability to conduct impact assessments, handles changes in an automated manner, including emergencies, document, all changes in the configuration management database, demonstrates chain of custody for the change, and complies with release policies.

## **Configuration Management**

Configuration Management is a process that tracks all individual Configuration Items (CI) in a system. Configuration Management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. CIs are documented in a Configuration Management Database (CMDB). The CMDB has the ability to create a parts list of every CI in the system, define the relationship of CIs in the system, track the current and historical status of each CI, track all Requests for Change (RFC) to the system, and verify that the CI parts list is correct and complete.

## **Network / System Management**

Network Management refers to the activities, methods, procedures, and tools that pertain to the operation operation, administration, maintenance, and provisioning of networked systems. Network management is the top-level administration and maintenance of a computer or telecommunications network. In network management, functions such as security, monitoring, control, allocation, deployment, coordination and planning are executed. Network management

# Enterprise Systems Management Domain

is governed by a number of protocols that exist for its support and must adhere to network Domain EASP standards; please refer to *Network Domain* document.

## Storage Management

Exercising strict data management necessitates having operating processes and procedures that ensure that the data is protected, retrievable, and recovered in a timely manner to meet business continuity Requirements. Storage Management is concerned with data care and control of the environment. Storage Management operational process consists of two major focus areas: (1) Data Backup, Restore, and Recovery Operations and (2) Storage Resource Management.

### Back-up and Recovery

Agencies with Storage Management responsibilities shall ensure policies and procedures address back-up and recovery for all critical data and conduct testing of these procedures on a regular basis. Procedures shall address timing, frequency, and restore time objectives (RTO) that support the business continuity plan.

### Storage Resource Management

Storage Resource Management (SRM) refers to software that manages storage from a capacity, utilization, policy and event-management perspective. This includes monitoring, reporting and analytic capabilities that allow users to drill down for performance and availability information.

Key elements of SRM include asset management, charge back, capacity management, configuration management, data and media migration, event management, performance and availability management, policy management, quota management, and media management.

## Service Monitoring

Service Monitoring and control consists of procedures and tools for proactive notification of events that may have severe consequences on the business. In addition, to the extent performance metrics are defined, monitoring of these metrics is important for SLA management and reporting.

## Network Monitoring

Network Monitoring describes the use of a system that constantly monitors an internal network computer networks for problems and that notifies the network administrator network administrator in case of outages via email, pager or other alarms. It is a subset of the functions involved in Network Management.

## Electronic Software Distribution

Electronic software distribution (ESD), with proper planning will alleviate much of the repetitive “grunt-level” work in provisioning user equipment. In addition, third-party vendors (e.g., McAfee, Novell, Microsoft, Intel, Seagate, Attachmate) have significantly improved ESD

## Enterprise Systems Management Domain

functionality by providing: rollback capabilities, network bandwidth control, and ODBC back-end databases.

### **Packaging**

Packaging is a collection of tools to automate the process of installing, upgrading, configuring, and removing software packages from a computer. Packaging is the act of taking a software request and bundling the software to be delivered (with necessary installation routines, pre-installation checks, post-installation activities, and any backup that may be necessary) into a single deliverable unit. Organizations should establish a set of “common” packages, which are the applications used by the entire enterprise (e.g., word processors, client shells, or standard application interfaces).

### **Distribution**

Distribution is the act of creating the list of and sending packages to the recipients. This involves sending the software directly to the end users, and the stages a package must go through in delivery. Bandwidth consumption is a consideration. To minimize this, a tool should be deployed with regional distribution hubs, where a package is delivered from a central point to the hub (over a WAN) and then replicated at the hub and distributed locally over a LAN.

### **Client-Side Installation**

Client-side installation is the point where the software is actually laid down on a machine or target.

### **Reporting**

Reporting is necessary on all packages. This should be done not just through the ESD tool itself, but also through reading the inventory database, mainly after manual packages have been sent out. Reports should also be reviewed to look for ways to improve ESD processes.

# Enterprise Systems Management Domain

## *Summary of principles*

### **General Architecture Principles**

1. Product choices and solution architectures should minimize overall total cost of ownership. This can be accomplished by consistency and uniformity in making choices about standards and products.
2. Product choices and solution architectures must provide for and enhance the overall security and integrity of systems and information assets.
3. Products choice decisions must consider the availability of training and technical support.
4. Product choices and solutions should minimize short term and long term risks, this can be partially accomplished by utilizing widely supported products or those with long-term support commitments by vendors (see principle 6).
5. Solution architectures should maximize information sharing among agencies and applications.
6. Product standards will consist of vendor supported versions only; this includes open source products.
7. New products and version/release upgrades for existing products will not become standard until a minimum 6 months has passed after the manufacturers General Availability date.

### **Enterprise Systems Management Specific Principles**

1. Agencies with ESM responsibilities shall perform capacity planning and performance monitoring to ensure infrastructure resources are appropriately sized to meet current and planned workload demands.
2. Agencies with ESM responsibilities shall implement accounting processes and procedures that identify and attribute costs for IT resources used to support the business.
3. IT operational and services processes should adhere to the ITIL framework best practices methodology. [Link to ITIL webpage](#)
4. Agencies shall establish data storage and archival retention policies and procedures that meet operating business requirements, statute, and regulatory mandates.
5. Agencies shall establish an IT disaster recovery plan. In addition, there shall be procedures to test the IT disaster recovery plan periodically and update the plan based on the test outcome or environment changes.
6. IT systems shall adhere to all security, confidentiality and privacy policies, and applicable statutes.
7. Agencies shall restrict access to any IT infrastructure resources including ESM tools in conformance with security policies and procedures.
8. Systems must be designed, acquired, developed, or enhanced such that data and processes can be shared and integrated across the enterprise and with our partners.
9. Incident Management procedures should include steps to address actions such as incident detection, recording, classification, initial support, investigation, diagnosis, resolution, recovery, closure, ownership, monitoring, tracking, and communication.

# Enterprise Systems Management Domain

## *Product/Technology Life Cycle Matrix*

### **Life Cycle Definitions**

The Life Cycle Matrix is based a sliding window of 12 quarters (3 Fiscal years). The date range of a fiscal year is July 1 through June 30.

<b>Key</b>	<b>Definition</b>
<b>S</b>	<b>Standard</b> - These are the products and standards selected by the state for NEW development or acquisition, and for the replacement of <i>obsolete</i> or <i>transitional</i> standards or products. They are supported by DOIT and have mainstream support from one or more vendors or standards bodies.
<b>T</b>	<b>Transitional</b> - Products are currently supported by DOIT, the agencies, or a vendor; however they have been replaced by new standard products or standards. Transitional products may have limited support from a vendor or have a defined End of Life (EOL). Neither the State nor the agencies should use these standards or products for NEW development. Existing implementations may be upgraded to a newer version to fix security or functional issues.  Agencies should develop plans to migrate from transitional to new standard products either by replacing the technologies or replacing the solution prior to the End-of Life of the product.
<b>O</b>	<b>Obsolete &amp; Divest</b> – Products or standards that are in use by the agencies. These products are generally End of Life and have very limited or no support from vendors, the community or DOIT.  Neither the agencies nor the State should undertake new investments or development using these products (this includes version upgrades).  Plans should be developed by to migrate from obsolete to standard products either by replacing the technologies or replacing the solution as rapidly as possible.

## Enterprise Systems Management Domain

### *Systems Management Products and Standards*

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
<b>Service Management</b>														
Numara Footprints	Server	ITIL based Service Management tool to track incidents, requests, problems, changes, knowledgebase and configuration management.			S	S	S	S	S	S	S	S	S	S
Track-It	Server	Help Desk tool to track incidents, requests, problems and changes.			T	T	T	T	T	T	T	T	T	T
Automation Center 6.1.2 (formerly IMPACT)	Server	Help Desk tool to track incidents, requests, problems and changes.			T	T	T	T	T	T	T	T	T	T
<b>Network Management</b>														
Uptime 5.x	Applications server	Event Notification	S	S	S	S	S	S	S	S	S	S	S	S
IBM NetCool	Network	Event Notification	S	S	S	S	S	S	S	S	S	S	S	S
Foglight 5.5.X	Database Server	Tracks performance of			S	S	S	S	S	S	S	S	S	S

## Enterprise Systems Management Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
		database manager.												
<b>Storage Management</b>														
EMC Control Center 6.2			S	S	S	S	S	S	S	S	S	S	S	S
<b>Electronic Software Distribution</b>														
<b>Packaging / Distribution / Reporting/ Client-Side Installation</b>														
Altiris Deployment Solution from Symantec 6.9	Windows, Linux	Create/Push Packages, Programs and Images	S	S	S	S	S	S	S	S	S	S	S	S
Altiris Deployment Solution from Symantec 6.9	Windows, Linux	Agent	S	S	S	S	S	S	S	S	S	S	S	S
Altiris Deployment Solution from Symantec 6.9	Windows, Linux	Reports	S	S	S	S	S	S	S	S	S	S	S	S
PatchLink 6.4	Windows, Linux	Windows security patches & updates	S	S	S	S	S	S	S	S	S	S	S	S
PatchLink 6.4	Windows, Linux	Agent	S	S	S	S	S	S	S	S	S	S	S	S
PatchLink 6.4	Windows, Linux	Reports	S	S	S	S	S	S	S	S	S	S	S	S
Desktop Authority 8.0	Windows	Create/Push Packages	T	T	T	T	O	O	O	O	O	O	O	O

## Enterprise Systems Management Domain

Tool/Technology	Platform	Usage/Type	FY 2011				FY 2012				FY 2013			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Desktop Authority 8.0	Windows	Agent	T	T	T	T	O	O	O	O	O	O	O	O

## Enterprise Systems Management Domain

### *Best Practices*

- Best Practice 1.** Agencies should establish an Incident Management process and procedures; the process and procedures shall enable restoration of normal service operation as quickly as possible and minimize the impact on business operations.
- Best Practice 2.** Agencies should establish a system event monitoring console and institute systems performance alert thresholds ensure systems faults are averted and corrective measures are taken to limit the chance of total systems failure.
- Best Practice 3.** Agencies should utilize a Service Desk facility that is staffed with properly trained personnel who can minimally respond to level 1- type problems, incidents, and events. The Service Desk shall utilize an automated contact management tool and is the single point of contact for all IT service requests and services communications.
- Best Practice 4.** Agencies should establish an IT disaster recovery plan. This risk-based plan shall incorporate the operating constraints of the business continuity plan. In addition, there shall be procedures to test the IT disaster recovery plan periodically and update the plan.
- Best Practice 5.** Agencies with ESM responsibilities should institute procedures for problem handling. These procedures shall include steps for performing root cause analysis of incidents and correction of the error to the satisfaction of the customer.
- Best Practice 6.** Agencies should establish a release management process. Process activities shall include procedures for hardware, license/version control across the infrastructure, rollout planning, communication protocols, and quality control of the process
- Best Practice 7.** Agencies should ensure critical back-up data files are rotated to an Off-Site location on a scheduled basis as defined in the back-up and recovery procedures. In addition, Off-Site locations shall comply with data security requirements such as encryption; as defined in the security domain.
- Best Practice 8.** ESM systems should be implemented in adherence with all security, confidentiality and privacy policies and applicable statutes.

# Security Domain Technical Architecture

---

## History of Changes

<b>Date</b>	<b>Modification</b>	<b>Author</b>
May 11 <sup>th</sup> 2010	Approved by Enterprise Architecture	Enterprise Architecture
June 11 <sup>th</sup> 2010	Approved by CIO	Enterprise Architecture
June 30 <sup>th</sup> 2010	Approved by the Information & Telecommunication Systems Executive Steering Committee	Enterprise Architecture
December 5, 2010	Approved by Enterprise Architecture	Enterprise Architecture
December 13, 2010	Approved by CIO/CTO	Enterprise Architecture
December 22, 2010	Approved by the Information & Telecommunication Systems Executive Steering Committee	Enterprise Architecture

# Security Domain Technical Architecture

## Table of Contents

Purpose.....	3
Overview.....	3
Technology Categories in This Domain .....	3
Access Control .....	3
Firewalls.....	3
Specialized application firewalls .....	3
Web Application Firewalls .....	3
Database Application Firewalls .....	4
Filtering appliances.....	4
Administration Tools .....	4
Protocol Analysis Software.....	4
Centralized LAN/WAN Management Console .....	5
Real-Time Risk Management and Remediation Tools .....	5
Intrusion Detection Systems .....	5
Email Content Filtering and Virus Scanning Systems.....	5
Vulnerability, Scanning, and Penetration Testing Tools .....	5
Encrypted Transport.....	5
Authentication.....	5
Mainframe.....	6
Remote Access.....	6
Proprietary Token-based Authentication .....	6
Biometrics .....	6
Cryptography .....	6
Public Key / Private Key technology.....	6
Digital Signature .....	7
Secret Key Cryptography.....	7
Content Encryption .....	7
Network Security .....	8
Security Protocols .....	8
Remote Access.....	8
Virtual Private Networks (VPNs) .....	9
Summary of Principles.....	10
General Architecture Principles.....	10
Security Specific Principles .....	10
Product/Technology Life Cycle Matrix .....	11
Life Cycle Definitions.....	11
Security Domain Products and Standards.....	12
Administration Tools .....	13
Vulnerability, Scanning and Penetration Testing Tool.....	13
Real-Time Tools .....	13
Encrypted Transport.....	14
Authentication.....	14
Cryptography .....	15
Network Security .....	18
Best Practices .....	20

# Security Domain Technical Architecture

## ***Purpose***

The purpose of this document is to set expectations of the agencies, bidders, vendors and consultants on life cycle and support for technical standards and products to be used by the agencies in acquiring, developing and deploying application and systems. This document defines the strategic standards and products for the Enterprise Architecture Standards Process (EASP) and provides technology road-maps or time frames for these standards and products. It does not address (at this time) patterns or implementation principles.

## ***Overview***

The purpose of security is to protect and secure the state's information resources in order to provide an environment in which the state's business can be safely transacted. A directory is a natural place to centralize management of security. It is the vault that contains the most trusted and critical components of an enterprise security strategy. This will require authorization and authentication services and a common enterprise repository of digital certificates that secures and supports E-commerce applications.

## ***Technology Categories in This Domain***

### **Access Control**

Firewall technology is rapidly evolving. There are two basic types, packet filtering and application gateways (proxy servers). The network architecture and location of firewalls relative to internal networks is an important consideration in securing internal networks.

#### **Firewalls**

Firewalls are a common term for physical devices, software and network architectures designed to block or filter access between a private network and a public network such as the Internet. They can also be used to provide access control between separate internal networks. Firewalls enforce the enterprise's security policy at determined perimeters, e.g., access point to the public Internet. To be effective, each must provide the single point of access to and from an un-trusted network.

#### **Specialized application firewalls**

Specialized application firewalls offer a rich feature-set in protecting and controlling a specific application. Most specialized network appliance application firewalls are for web applications.

##### **Web Application Firewalls**

Standard firewalls are designed to restrict access to certain ports, or services that an administrator doesn't want unauthorized people to access. Web Application Firewalls are often called 'Deep Packet Inspection Firewalls' because they look at every request and response within the HTTP/HTTPS/SOAP/XML-RPC/Web Service layers. Some Web Application Firewalls look for certain 'attack signatures' to try to identify a specific attack that an intruder may be sending, while others look for abnormal behavior that doesn't fit the websites normal traffic patterns. Web Application Firewalls can be either software, or hardware appliance based and are installed in front of a web server in an effort to try and shield it from incoming attacks.

# Security Domain Technical Architecture

## **Database Application Firewalls**

A database firewall is an application firewall which protects databases from application attacks- for example, SQL injection, database rootkits, and unauthorized information disclosure. A database firewall is a computer application firewall operating at the database application layer of a protocol stack. Also known as a proxy-based firewall, it may be implemented as a piece of software running on a single computer, or a stand-alone piece of hardware. Often, it is a host using various forms of reverse proxy services to proxy traffic before passing it to a gateway router. Because it acts on the database application layer, it may inspect the contents of the traffic, blocking specified content, such as certain websites, viruses, attempts to exploit known logical flaws in client software. Most often, database firewalls work on the SQL application level atop the TCP/IP stack, all applications' connection to the database or SQL management interfaces, and may intercept and enforce all packets traveling to or from a database network or application interface. Some database firewalls include automated SQL learning capabilities, which assist in policy configuration. The learning capabilities will list queries directed to a specific Database.

## **Filtering appliances**

Application level firewalls or proxy servers protect internal networks by not permitting direct access from the internal network to un-trusted networks such as the public Internet. Internal users connect to the 'proxy' which then acts on their behalf, completing the connection to the requested external service. Proxy firewalls are specific to the applications they proxy. Not all applications can be proxied. For those that can't be proxied, proxy-like gateways shuttle data between internal and external networks. They maintain the characteristic of preventing direct connections between the internal and external networks. Current technology allows these products to "filter" invisibly the type of traffic and its destination.

## **Administration Tools**

The security architecture must provide the capability to track and monitor successful and unsuccessful interactions with the information infrastructure. Accountability for interactions must be tied to specific users. The architecture should be able to audit all significant security events including authentication, accessing of services and security administration.

Technical analysis includes administrative procedures, cryptographic procedures, inspection of hosts and network devices, physical site inspection, external network scans, and design or code review of critical applications.

## **Protocol Analysis Software**

Protocol Analysis Software is a powerful network visibility tool that enables the security administrator to monitor network traffic in real time, collect detailed utilization and error statistics for individual stations, and save historical utilization and error information for baseline analysis. These systems can generate visible and audible real-time alarms, and notify security administrators when troubles are detected.

# Security Domain Technical Architecture

## **Centralized LAN/WAN Management Console**

In order to maintain specific uptime requirements of a large enterprise network, a centralized LAN/WAN Management Console is needed. This hardware/software component provides:

- Network Security management, which assists in keeping network devices up and running.

## **Real-Time Risk Management and Remediation Tools**

### **Intrusion Detection Systems**

Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) technology is an important component of a comprehensive enterprise security strategy. IDS / IPS products alert security administrators of suspicious activity that may be occurring on their systems and networks in real time.

### **Email Content Filtering and Virus Scanning Systems**

An Email content filtering and virus scanning system can allow the security administrator to easily manage, filter and if necessary block unauthorized company communications made through e-mail, newsgroups and FTP sites. This component is more than a simple filtering product since it can determine the content and context of e-mails, FTP downloads, newsgroup postings and "spam" that's going into, out of, or through the state's network.

## **Vulnerability, Scanning, and Penetration Testing Tools**

Vulnerability Assessment products complement IDS / IPS very well. They help determine the overall security posture of a system or network, and allow security administrators to identify and fix vulnerabilities before an attacker can exploit them. .

## **Encrypted Transport**

Encrypted transportation of content (e.g., documents, e-mail) via FTP, e-mail, file sharing. Compliance with privacy and data protection regulations such as U.S.-based HIPAA, PCI, and GLBA requirements.

## **Authentication**

Authentication is the act of verifying the identity of a user or process. Authentication answers the question: "Are you who you say you are?" The most common method used to authenticate a user is a password. A password is a secret series of characters and numbers associated with an individual user id by the owner/user. A sign-on process to authenticate the user accepts a password and a user-id. The sign-on process matches the password given, with a stored password for that user. If they match, the system has verified the user's identity. Electronic business transactions have stricter requirements on uniquely identifying and authenticating the sender or recipient of electronic information. These can be satisfied with a 'digital signature,' which is the equivalent of a handwritten signature. Authentication techniques such as Public Key Certificates have been developed to address the strict authentication requirements of electronic business processes.

# Security Domain Technical Architecture

## **Mainframe**

Mainframe Security protects and secures state resources. System administrators control access to the State's computers, network, and databases in order to protect the data maintained.

## **Remote Access**

Remote Access is defined as a user outside the normal boundaries of the state's network connected through external means, such as a cellular or other Internet connection. This mode of access is increasing due to the mobility of employees, and the increasing requirement of providing access to state systems for vendors and business partners. There must be assurance that these methods of access are secure and cannot be compromised.

## **Proprietary Token-based Authentication**

Tokens are physical cards similar to credit cards that work in conjunction with a user id to identify a user to the system. They combine something a person knows, such as a password or PIN, with something they possess, a token card. Token cards commonly generate either dynamic passwords or a response in a challenge-response communication between the user and the system. These tokens work together with server based systems to match a token holder to a user profile, normally referred to as Authentication Servers.

## **Biometrics**

A biometrics is a unique, measurable physical or behavioral characteristic of a human being for automatically recognizing or verifying identity. Biometrics characteristics can include fingerprints, iris data, hand and face geometry, signature, voice and DNA. Each of these methods has different degrees of accuracy, cost, social acceptability and intrusiveness. An extreme example of an intrusive technique would be a DNA sample. Voice identification would be an example of a non-intrusive and socially acceptable technique.

Biometrics systems are not 100% accurate. Accuracy in biometrics is measured by false acceptances versus false rejects. The accuracy of biometrics can also be improved by combining two techniques such as fingerprint identification and face recognition. An intersection of the matches from two biometrics techniques typically results in an acceptable identification.

## **Cryptography**

Documents, communications and data travel inside and outside the enterprise in electronic form. Electronic information is easy to read, modify or replace without detection. However, in many situations, the confidentiality of the information in transit must be maintained. Information transported across the state's TCP/IP networks and across the public Internet is passed in clear text. As described in the authentication section above, cryptography is a means to scramble information such that only authorized entities (people or processes) have access to the information. A combination of public key cryptography and secret key cryptography can be used to implement authenticated and protected communication for secure access control. Most bulk encryption of information involves the use of secret key cryptography.

### **Public Key / Private Key technology**

Authentication which requires the unique identification of a user is often based on Public / Private Key cryptography. This form of cryptography uses two related keys. Information encrypted with one key can only be decrypted with the other key.

## Security Domain Technical Architecture

- The 'Public' Key is made openly available in a repository to anyone who wants to communicate with the user in a secure manner.
- The 'Private' Key is kept only by the owner and is never divulged. Since only the owner has the private key, its use is considered sufficient to uniquely authenticate the owner. A digital signature is an example of a private key being used to verify that the sender (originator of the information) is really who they say they are.

A user's public key is distributed using an electronic document called a Public Key Certificate. This certificate contains the user's name, public key, an expiration date and other information. It is considered reliable when a trusted authority digitally signs it. Trusted authorities that issue certificates are known as Certificate Authorities.

### **Digital Signature**

Digital signatures are the equivalent of a handwritten signature in that they tie an individual to a document. The first step in digitally signing an electronic document is to generate a message digest of the document. The signer encrypts this message digest using the signer's unique private key.

The document and encrypted message digest are sent to one or more recipients. Verifying a digital signature is the reverse process. The recipient generates a message digest from the document. By using the signer's public key, the recipient can recover the original message digest from the encrypted one. This proves it must have come from the signer since only they have the private key.

If the recovered and the generated message digests are equal, the document has not been modified and the sender cannot deny their digital signature. The digital signature, therefore, provides non-repudiation, which means that the sender cannot falsely deny having sent the message.

### **Secret Key Cryptography**

Secret key technology is a form of cryptography where encryption and decryption use the same key, a 'secret' key. Pairs of users or processes share the same secret key. Data encrypted with a secret key is decrypted using the same secret key. Secret key technology is used to do most encryption because it is much faster than other techniques. Examples of commonly used secret key algorithms include AES-256, 3-DES, RC2, RC4, IDEA and CAST.

### **Content Encryption**

This subcategory deals with persistent encryption of files and folders, disk drives and removable media using public/private key encryption. This is required by Connecticut State IT Policy and by Executive Order.

It is suggested that encryption modules meet the requirements found in *45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information*, section B. *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*. Of special note is *FIPS 140-2 validation* for encryption processes.

# Security Domain Technical Architecture

## Network Security

### Security Protocols

Protocols are well-defined message formats used for communicating in networked systems. Security protocols provide security functions. When considering products, it is useful to check present and future planned compliance to standards. Important security protocols are described below:

- 802.1X provides port-based authentication, which involves communications between a supplicant, authenticator, and authentication server. Port refers to a single point of attachment to the LAN infrastructure. The supplicant is often software on a client device, such as a laptop; the authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.
- Secure Sockets Layer— SSL is a widely used means for securely communicating between a Web browser and Web server. SSL creates an encrypted link between a client and server that need to communicate securely. Both client and server authentication is possible. SSL can also be used with other applications such as ftp, telnet, etc.
- Simple Key Management for Internet Protocols — SKIP is a "secret key exchange protocol" that operates below the IP layer in a TCP/IP communications protocol. This method can be used to provide transparent security between entities.
- Security Multi-parts for MIME — S/MIME is an application security protocol. It is implemented for email but it has wider implications for store-and-forward messaging.
- Internet Protocol Security Extensions — IPsec is a security protocol defined for IP networks which operates at the network layer in TCP/IP communications protocol. IPsec adds header extensions to the IP communications protocol, designed to provide end-to-end security for packets traveling over the Internet. IPsec defines two forms: sender authentication and integrity, but not confidentiality, using an Authenticating Header (AH), and sender authentication, integrity and confidentiality using an Encapsulating Payload (ESP).
- Internet Key Exchange — IKE provides secure management and exchange of cryptographic keys between distant devices. It is the standard key exchange mechanism for IPsec.

### Remote Access

Remote Access is defined as a user outside the normal boundaries of the state's network connected through external means, such as a cellular or other Internet connection. There must be assurance that these methods of access are secure and cannot be compromised.

# Security Domain Technical Architecture

## **Virtual Private Networks (VPNs)**

Virtual private networks (VPN) are ways of connecting two networks or trading partners that must communicate over insecure networks such as the public Internet. A VPN establishes a secure link by using a version of the IPSec security protocol. These links are typically implemented between firewalls. VPNs today often use proprietary record structures and have inter-operability problems. A secure communications link between the networks does not ensure that communications beyond that link are secure.

Some VPNs use a variety of non-IPSec protocols. These include PPTP, L2TP, L2F, and proprietary protocols. These protocols offer similar services but are better suited to remote-access applications and non-IP traffic across the public Internet.

## *Summary of Principles*

### **General Architecture Principles**

1. Product choices and solution architectures should minimize overall total cost of ownership. This can be accomplished by consistency and uniformity in making choices about standards and products.
2. Product choices and solution architectures must provide for and enhance the overall security and integrity of systems and information assets.
3. Product choice decisions must consider the availability of training and technical support.
4. Product choices and solutions should minimize short term and long term risks. This can be partially accomplished by utilizing widely supported products or those with long-term support commitments by vendors (see Principle 6).
5. Solution architectures should maximize information sharing among agencies and applications.
6. Product standards will consist of vendor-supported versions only; this includes open source products.
7. New products and version/release upgrades for existing products will not become standard until a minimum 6 months has passed after the manufacturer's General Availability date.

### **Security Specific Principles**

1. Product choices and solution architectures must provide for and enhance security, confidentiality and privacy.
2. Base application security on open standards where possible, industry standards when practical.
3. Use existing services consistent with open standards where possible, industry standards when practical.

## Product/Technology Life Cycle Matrix

### Life Cycle Definitions

The Life Cycle Matrix is based a sliding window of 12 quarters (3 Fiscal years). The date range of a fiscal year is July 1 through June 30.

Key	Definition
S	<p><b>Standard</b> - These are the products and standards selected by the state for NEW development or acquisition, and for the replacement of <i>obsolete</i> or <i>transitional</i> standards or products. They are supported by DOIT and have mainstream support from one or more vendors or standards bodies.</p>
T	<p><b>Transitional</b> - Products are currently supported by DOIT, the agencies, or a vendor; however they have been replaced by new standard products or standards. Transitional products may have limited support from a vendor or have a defined End of Life (EOL). Neither the State nor the agencies should use these standards or products for NEW development. Existing implementations may be upgraded to a newer version to fix security or functional issues.</p> <p>Agencies should develop plans to migrate from transitional to new standard products either by replacing the technologies or replacing the solution prior to the End-of Life of the product.</p>
O	<p><b>Obsolete &amp; Divest</b>– Products or standards that are in use by the agencies. These products are generally End of Life and have very limited or no support from vendors, the community or DOIT.</p> <p>Neither the agencies nor the State should undertake new investments or development using these products (this includes version upgrades).</p> <p>Plans should be developed by to migrate from obsolete to standard products either by replacing the technologies or replacing the solution as rapidly as possible.</p>

**Security Domain Products and Standards**

Tool/Technology	Platform	Usage/Type	FY2010				FY2011				FY2012			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
<b>Firewalls Software</b>														
Checkpoint 4.x			O	O	O	O	O	O	O	O	O	O	O	
Checkpoint R55			O	O	O	O	O	O	O	O	O	O	O	
Checkpoint R62			T	T	T	T	T	T	O	O	O	O	O	
Checkpoint R65			T	T	T	T	T	T	O	O	O	O	O	
Checkpoint R70	Nokia / Dell		S	S	S	S	S	S	S	S	S	S	S	
IPSO 4.1			T	T	T	O	O	O	O	O	O	O	O	
IPSO 4.2			S	S	S	O	O	O	O	O	O	O	O	
IPSO 6.2						S	S	S	S	S	S	S	S	
<b>Firewalls Hardware</b>														
Nokia Appliances			S	S	S	S	S	S	S	S	S	S	S	
Cisco Pix			T	T	T	T	T	T	T	O	O	O	O	
<b>Internet Content Filters</b>														
WebTrack SMARTFILTER DA			T	T	T	T	O	O	O	O	O	O	O	
N2H2			T	T	T	T	O	O	O	O	O	O	O	
8E6		Enterprise	S	S	S	S	S	S	S	S	S	S	S	

<b>Administration Tools</b>														
<b>Protocol Analysis Software</b>														
Infinistream		Enterprise	S	S	S	S	S	S	S	S	S	S	S	S
WireShark		Local use Desktop and Networking	S	S	S	S	S	S	S	S	S	S	S	S
<b>Vulnerability, Scanning and Penetration Testing Tools</b>														
DBMS AppDetective		Database testing and analysis	S	S	S	S	S	S	S	S	S	S	S	S
Application AppDetective		Application testing and analysis	S	S	S	S	S	S	S	S	S	S	S	S
NESSUS		Hardware and OS configuration testing. (remote)	S	S	S	S	S	S	S	S	S	S	S	S
DISA disk (MS)		Microsoft configuration testing and analysis	S	S	S	S	S	S	S	S	S	S	S	S
<b>Real-Time Tools</b>														
<b>Email Content Filtering and Virus Scanning Systems</b>														

McAfee 3300 (WebShield A/V and Anti Spam)		Anti-Spam, Anti-Virus email scanning	S	S	S	S	S	S	S	S	S	S	S	S
<b>Intrusion Detection Systems</b>														
ISS Proventia		Anomaly detection and prevention at the network layer.	S	S	S	S	S	S	S	S	S	S	S	S
<b>Encrypted Transport</b>														
Tumbleweed MailGate Now AXWAY		Used for secure FTP	S	S	S	S	S	S	S	S	S	S	S	S
Tumbleweed MailGate Now AXWAY		Used for secure e- mail	S	S	S	S	S	S	S	S	S	S	S	S
WinZip	Windows	Desktop/Server	S	S	S	S	S	S	S	S	S	S	S	S
<b>Authentication</b>														
Radius with ACE Software	Server	<i>Contact Enterprise Architecture for Information</i>												
Enterasys Trusted End-System (TES)		<i>Contact Enterprise Architecture for Information</i>												

Network Access Control (NAC)		<i>Contact Enterprise Architecture for Information</i>												
Novell Access Gateway		External Authentication and reverse proxy	S	S	S	S	S	S	S	S	S	S	S	S
Novell Identity Manager		Novell's Identity Application Layer	S	S	S	S	S	S	S	S	S	S	S	S
Novell eDirectory ver. 8.9		Novell's LDAPv3	S	S	S	S	S	S	S	S	S	S	S	S
Active Directory 2008		Novell's LDAPv3			S	S	S	S	S	S	S	S	S	S
Active Directory 2003		for file and print services; for Exchange authentication. Internal authentication.	S	S	T	T	T	T	T	T	T	T	O	O
<b>Mainframe</b>														
ACF-2		Authentication	S	S	S	S	S	S	S	S	S	S	S	S
<b>Proprietary Token-based Authentication</b>														
RAS-Secure ID			S	S	S	S	S	S	S	S	S	S	S	S
<b>Cryptography</b>														

<b>Mainframe Encryption</b>														
IBM DS8700	IBM ZOS	Contact Enterprise Architecture for Information												
<b>Oracle</b>														
Oracle Advanced Security Transparent Data Encryption (TDE) (Oracle 10g & 11g @ FIPS 140-2 and higher) which uses .... Oracle Cryptographic Libraries for SSL Software Version: 10g (10.1.0.5)	Server	Encryption of Sun server data. Tested as meeting Level 2 with Sun Solaris 8.0 with Admin Suite 3.0.1 on Sun Ultra 60	T	T	T	T	T	T	T	T	O	O	O	O
Oracle Cryptographic Libraries for SSL 10g (9.0.4) software	Workstation	Encryption of Sun server data Tested as meeting Level 2 with Sun Solaris Version 8 running on a Sun Ultra 60 UltraSparc	T	T	T	T	T	T	T	T	O	O	O	O
Oracle on Sun/Solaris		Encryption of Sun server data	T	T	T	T	T	T	T	T	O	O	O	O
Oracle 11GR-2	Windows		S	S	S	S	S	S	S	S	S	S	S	S

<b>MS SQL</b>														
Windows	Windows	Database encryption	S	S	S	S	S	S	S	S	S	S	S	S
<b>Public Key / Private Key Technology</b>														
VeriSign		External Certificates of 048 bit or greater	S	S	S	S	S	S	S	S	S	S	S	S
VeriSign		External Certificates of 1024 bit or greater	T	T	T	T	T	T	T	T	T	T	T	T
RSA		VPN Keyfob	S	S	S	S	S	S	S	S	S	S	S	S
Microsoft		Self-signed signatures for internal use	S	S	S	S	S	S	S	S	S	S	S	S
<b>Secret Key Cryptography</b>														
Kerberos	Windows	Windows / Network encryption and authentication	S	S	S	S	S	S	S	S	S	S	S	S
AES 256 bit encryption		Federal standard for file encryption	S	S	S	S	S	S	S	S	S	S	S	S
<b>Content Encryption</b>														
McAfee Endpoint Encryption for PC	Windows PCs	Device encryption	S	S	S	S	S	S	S	S	S	S	S	S

McAfee Endpoint Encryption for Files and Folders	Windows PCs, Servers	Device encryption	S	S	S	S	S	S	S	S	S	S	S	S
McAfee Endpoint Encryption for Removable Media	Removable media	Device encryption	S	S	S	S	S	S	S	S	S	S	S	S
<b>Network Security</b>														
<b>Security Protocols</b>														
SSLv3	SSL VPN		S	S	S	S	S	S	S	S	S	S	S	S
802.1x	Network	Authentication	S	S	S	S	S	S	S	S	S	S	S	S
IPSec	Nortel VPN, Cisco Routers	VPN Users, VPN Branch to Branch, Routers with encryption	S	S	S	S	S	S	S	S	S	S	S	S
X.509		<i>Contact Enterprise Architecture for information</i>												
WS Security		<i>Contact Enterprise Architecture for information</i>												
XML Encryption		<i>Contact Enterprise Architecture for information</i>												
XML Signature		<i>Contact Enterprise Architecture for information</i>												

LDIF 1	Server	<i>Contact Enterprise Architecture for Information</i>													
LDAPv3	Novell/Linux	SSO	S	S	S	S	S	S	S	S	S	S	S	S	S
<b>Virtual Private Networks (VPNs)</b>															
Nortel Contivity VPN		IPSec VPN Users, IPSec Branch to Branch, SSL VPN	S	S	S	S	S	S	S	S	S	S	S	S	S

## ***Best Practices***

**Best Practice 1.** Resetting security assurance levels should not require modification of the architecture.

**Best Practice 2.** Provide infrastructure security services to enable the enterprise to conduct business electronically.

**Best Practice 3.** An accurate system date and time are essential to all security functions and accountability and must be maintained.

**Best Practice 4.** Perform a business-driven risk assessment for all automated systems.

**Best Practice 5.** When designing collaborative systems (e.g. document management, workflow), the content that will move through the system must be classified according to applicable statutes, policies and regulations pertaining to availability, retention

A privacy policy should be published on every government web site, even if the site does not create records of the information collected. Because state agency web sites have many different purposes, the privacy policies found on these sites should also be diverse and specific to the visited site. A policy should have an *introductory statement* that identifies the agency and includes a short overview of privacy practices and how they apply to the site. In the course of operating a web site, certain information may be collected automatically in logs or by cookies. Agencies may have the technical ability to collect information and later take additional steps to identify people, such as looking up static Internet Protocol addresses that can be linked to specific individuals. The privacy statement must clearly denote the policy. It is imperative to ensure these policies are consistent with the State's **Freedom of Information laws.**

**Best Practice 6.** Utilize Defense in Depth practices to create a multi-level, multi-layer construct to protect State of Connecticut assets. (Example: harden servers, use a multi-tier firewalls, host and network based intrusion prevention appliances, router access control lists, encryption, anti-virus, anti-malware etc.)

**Best Practice 7.** Apply a level of security to resources commensurate to its value to the organization and sufficient to contain risk to an acceptable level.

**Best Practice 8.** Treat security architecture as a continuous process.

**Best Practice 9.** Locate security in the appropriate layer of a communications protocol to ensure maximum usability with minimum future modification.

**Best Practice 10.** Use commercially generated certificates when encryption is needed and where there will be a direct interaction with a user's browser or client software. The browser or client software will accept this as a valid certificate without question. Use non-commercial or self generated certificates between machines to ensure the data stream is encrypted, but the certificate will not be verified or questioned by a certificate authority. This reduces TCO of using certificates while providing confidence to the user that the connection is a verifiable certificate and the encryption level.