State of New Jersey
Shared
IT Architecture

March 2004
Version 2.0

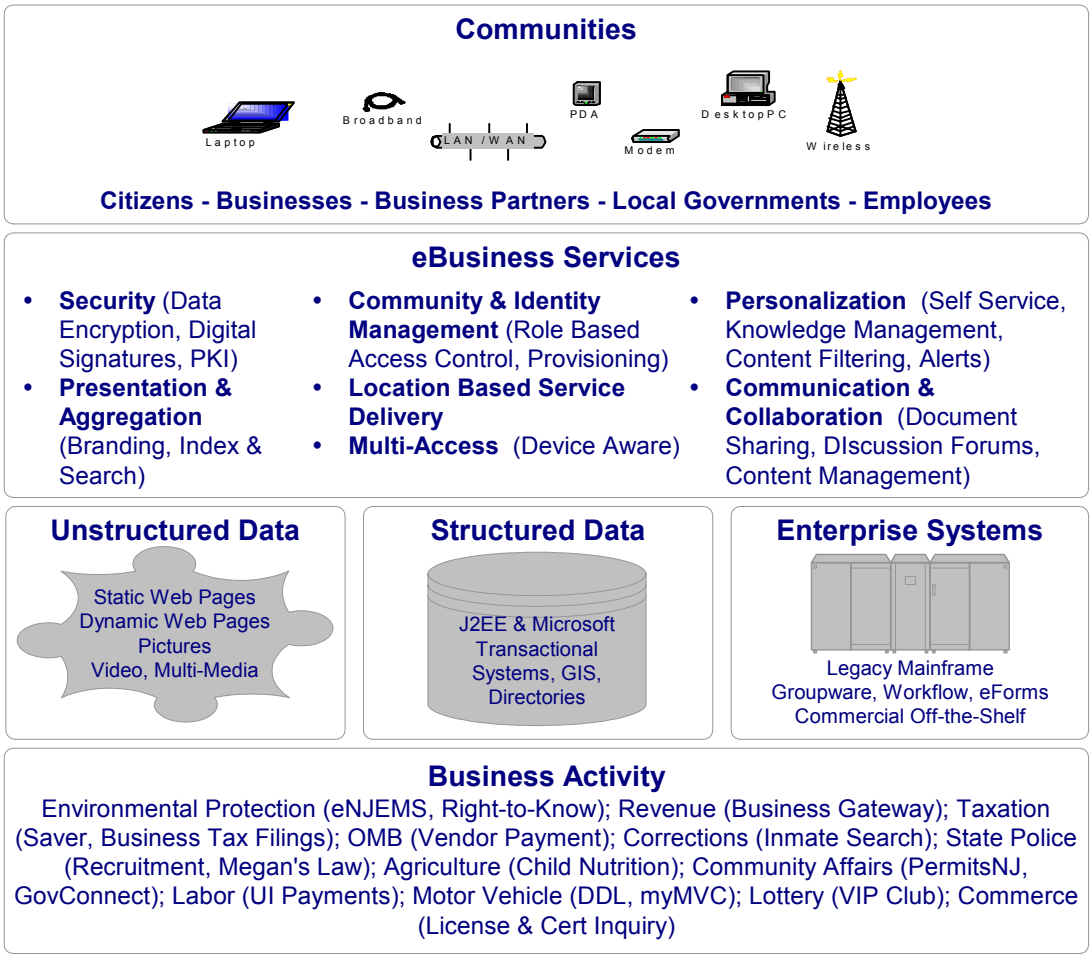
Executive Summary

The purpose of this document is to guide Executive Branch Agencies toward leveraging existing shared IT infrastructure, processes and support staff in order to minimize risk and lower the overall cost of IT projects.

This document focuses on existing shared infrastructure and resources used across multiple State agencies and is not a complete listing of every product used by every State agency.

The ability to rapidly develop and reliably deploy scalable, highly available business systems based on Internet technology is a major focus for the State of New Jersey. Today the Web has emerged as a versatile platform for delivering high-value solutions on virtually any device, including cellular phones, PDAs and desktop computers. The traditional geography of State government service delivery – employees at their desks, residents and business partners in lines or on the phone - no longer exists. We expect information and services to be available anywhere, anytime, on any device, for any user community.

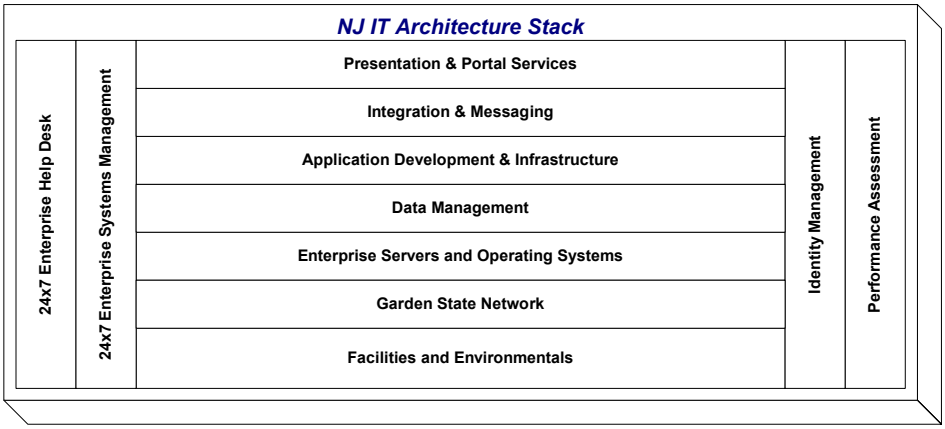
This new eBusiness paradigm is depicted below:



The State's Shared IT Architecture has been designed and implemented to facilitate this new business paradigm. While continually evolving, it is based on industry standard open system solutions that provide a high degree of vendor neutrality, maximum flexibility, and the agility needed to meet the ever-growing service delivery needs of the State's Executive Branch.

Most new applications must be available across the State's diverse community of users – including residents, businesses, business partners, employees and all levels of government. For most of these applications, integration with legacy applications and data is essential.

This document is intended to provide sufficient technical detail regarding the various components of the State's Shared IT Architecture and, in Appendix 3, denotes which technologies and products are generally preferred by the State of New Jersey. The organization of this document is based on the IT Architecture Stack depicted below, where each layer represents a set of technologies put in place to enable certain business/technology processes.

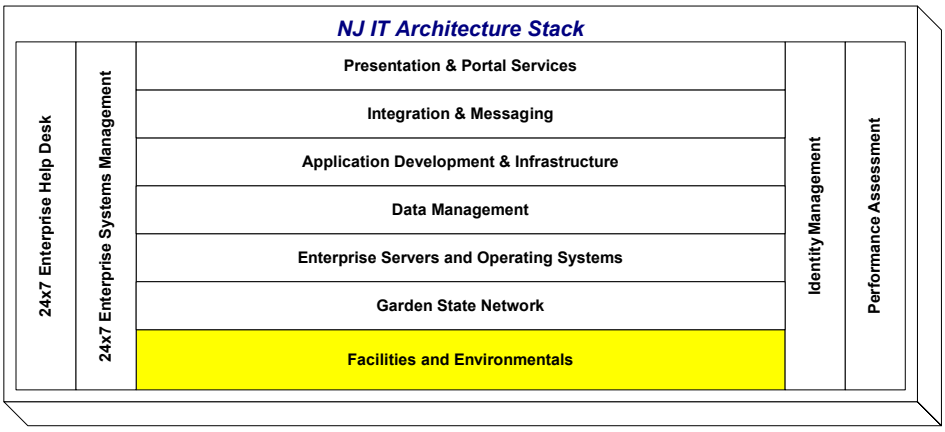


At every layer, the products and technologies implemented were selected to maximize investment dollars and to ensure architectural integrity (i.e., Product A works with Product B). This architecture stack is currently used to deliver information and services to every major user community in State government. State agencies leveraging this architecture maximize taxpayer investments in technology. They are free to focus on the development and delivery of critical business services without the added burden and expense of redundant hardware, software and support.

Specific benefits of the architecture include:

- *Reduced costs for new applications*
- *Improved access to legacy data*
- *Centralized help desk, backup and recovery services*
- *Faster delivery of applications across a multitude of devices and networks*
- *Minimized data redundancy through data sharing*
- *Reduced dependency on proprietary components*
- *Reduced risk in reliable operations, security and change management*
- *Expert staff specially trained on enterprise platforms*

Facilities and Environmentals



The State maintains two Data Center Facilities located within the secured campus setting at State Police Division Headquarters in West Trenton, New Jersey. These facilities are known as the Hub and River Road data centers. They are housed within separate, highly secure buildings on the campus.

The facilities maintain a symmetrical design in that the key infrastructure, system, and networking technologies have been duplicated in both facilities. This common symmetry allows each facility to operate independently while providing back up services for its counterpart. High-speed fiber links both facilities allowing clients to freely deploy servers at either facility. Both offer 24x7 complete operational and production services under the protection of the New Jersey State Police and New Jersey Office of Information Technology (OIT).

Plans are now underway for a third data center facility to provide back up and recovery services and also provide agencies with a secondary geographic location where their mission critical applications can be hosted in the event of a disaster scenario at the primary facilities in West Trenton.

Physical Security

In addition to the secure campus location of the data center facilities, OIT also employs additional layers of physical security to ensure that client assets are safe, secure, and protected against outside intrusion and unauthorized access.

Campus Security

To gain access to State Police Division Headquarters campus, all persons must enter at one of two guard station checkpoints. Visitors are screened and directed to their destination.

Building Security

Uniformed and civilian personnel control the movement of all persons within the campus facilities. Security measures include registration of all visitors, viewable credentials worn by employees and visitors, access key controlled door locks, camera surveillance systems and random patrolling of facilities by security personnel.

Access to secured areas is permitted via an authorized badge access system that is maintained by the OIT Facilities Group. The access badge system database is audited to ensure that only authorized personnel are permitted access to secure areas within the data center facilities. All previously authorized personnel that are no longer working with or for the State of New Jersey are purged from the access badge system database.

Security Cameras are placed strategically throughout the data center facilities to prevent against unauthorized access or tampering activity. Security guards have the ability to pan security cameras in the event of a suspected security breach or intrusion. Video records are maintained, and all video surveillance tapes are labeled and properly archived to prevent loss or theft of video surveillance sequences that may contain evidence of illegal access or attempted access.

Unlocked Cabinet Systems

The majority of the servers are housed within standard unlocked SMC Premier LAN Module cabinet systems that are open and available to authorized system administrators (and vendors under system administrator supervision) to perform standard software, hardware, and diagnostic services.

Logical access to all servers within the server condos is protected via the logical security access system provided by the Avocent KVM (Keyboard, Video, and Mouse) backbone server access system. Once logged onto this KVM access system, the system administrator is presented with a list of servers that (s)he is permitted to access. Selection of a server from this list provides the administrator with the required server access logon menu.

Locked Smart Cabinet Systems

For more sensitive servers that require more stringent security measures as mandated by state and federal guidelines, another type of cabinet system is utilized to secure access to sensitive servers and the information they contain. Access to servers in these cabinets is protected via smart cabinet systems that are physically locked. Authorized system administration personnel are issued keys to access the cabinet systems that house servers that fall within their jurisdiction. In the event of forced illegal entry, these cabinets are equipped with smart cabinet technology that captures a picture of the perpetrator during illegal entry, logs the entry, and sends out an alert that the cabinet has been compromised. Control Center personnel proactively monitor these alerts, investigate these incidents and notify the security staff.

Control Center

Operation of each data center is managed by a Control Center housed within each facility. This control center is manned by a highly trained group of support professionals twenty-four hours a day, three hundred and sixty-five days a year. The responsibility of Control Center personnel is to ensure the availability, reliability and operational status of all production servers, the network, the environmental systems, and security systems within the facility. Facility Management, Capacity/Performance and Network Management systems and software are utilized by Control Center personnel to proactively monitor and display the status of these systems within the facility.

Alarms

Alarms are strategically placed throughout each data center facility and within the server rooms to alert personnel in the event of an unauthorized intrusion, environmental system failure, or fire. All support systems within these facilities are tested on a regularly scheduled basis to ensure that the alarm systems properly operate.

Commercial Power

Each data center is fed commercial power by the PSE&G West Trenton Power Generation Station via different power grids to multiple onsite transformers.

Power Distribution

Each data center contains redundant power systems to achieve maximum availability and reliability of all systems. Control Center personnel closely monitor external and internal power distribution systems to maximize system uptime.

A network of Power Distribution Units (PDUs) and Panels that distribute and supply redundant power to all critical servers and associated equipment is housed in each respective facility. Servers equipped with redundant power supplies are cross-connected to PDUs and panels that are connected to different power grids within the facility. This arrangement provides sufficient power redundancy to enable critical servers and other equipment with dual power supplies to remain up and operational in the event of a PDU or panel failure.

Uninterruptible Power Sources

Each data center maintains multiple Uninterruptible Power Sources (UPS) that allow all critical systems and associated equipment to remain powered up and operational in the event of a power failure. All critical equipment at each facility is connected to a two phase UPS Backup System which engages automatically when primary and secondary commercial power feeds fail. These systems include both battery and diesel generated backup power.

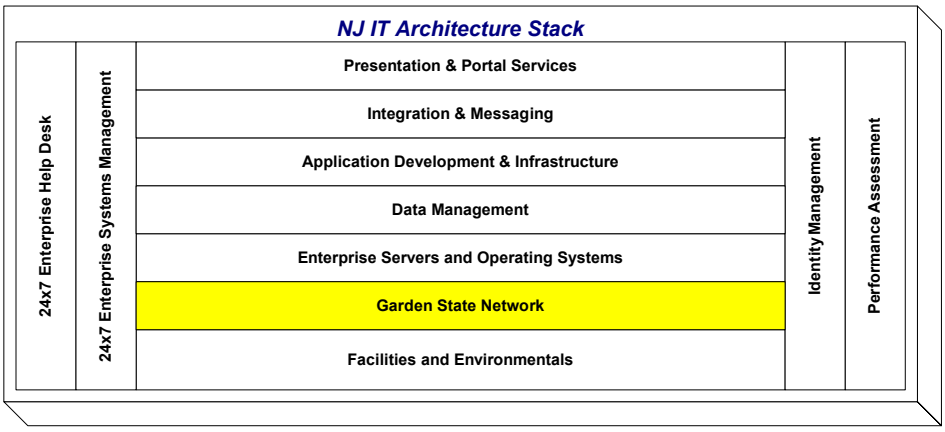
Environmental Climate Control

Each data center is equipped with a complete environmental system to guarantee optimal heating, cooling, and humidity levels in order to facilitate the availability, reliability, and continued operation of all systems. Control Center personnel monitor these environmental system controls. Each facility has N + 1 Redundant Liebert units ducted together to provide the environmental climate control to keep all systems and associated equipment operational and within the prescribed temperature and humidity limit boundaries. Any abnormal environmental climate conditions are immediately logged and reported to the OIT Facilities Group for resolution.

Fire Detection and Suppression Systems

Each data center has a complete fire detection and suppression system equipped with an annunciator panel that shows the current status of the fire detection and suppression system. The Control Center personnel proactively monitor these panels. Each facility is equipped with redundant fire suppression systems. The primary fire suppression system dispenses a fire retardant gas that extinguishes fire immediately upon detection. Additionally, each site is equipped with a secondary dry pipe sprinkler system that serves as backup to the primary system.

Garden State Network



Network Internet Architecture

The State of NJ has implemented a three-tier network architecture to provide state-of-the-art security for the State's core Garden State Network resources. This architecture consists of three firewalls protecting our core network from the Internet world (i.e., a 'double DMZ' model). See Appendix diagrams.

According to our security policy, an Internet user can only communicate with servers on the public tier. A public tier server can only communicate with a secure tier server, and only a secure tier server can communicate with core network. A server or workstation can communicate with any device on a higher layer, and the response can come back to only that originating device.

Therefore, in communicating downward in the model from the Internet, at each tier there must be a process that takes a request and hands it down to the next layer. Typically, this model fits well with distributed application design, where tier 1 handles presentation, tier 2 handles business logic, and tier 3 houses the data (web servers, application servers, and data servers).

In some instances, two-tier applications are accommodated by placing the data on the second tier. The practice of placing all components on the first tier (one-tier applications) is not acceptable.

Tunneling, simple pass-through proxy, 'double tier hops', and other techniques that do not apply policy or process to an inbound communication at each tier, are not allowed - to do so would compromise the integrity of all remaining applications that follow the security policy.

Network Protocols

The State uses the TCP/IP family of protocols as the standard network protocol to ensure technical compatibility and efficient use of the available data transport resources. Other protocols are in use, but their use is being phased out in favor of TCP/IP.

Garden State Network Architecture

The Office of Information Technology builds and manages a multi-agency, multi-protocol network (Garden State Network, GSN) across New Jersey. This network supports State agencies through dedicated and switched services in support of centralized and distributed data processing applications resident in mainframe, mini-computer, local area network (LAN), and personal computer environments. The GSN also provides Internet and email services. The GSN's reach, features and capacities are constantly being expanded to meet these needs.

The GSN is comprised of six main node facilities. These nodes are interconnected to form the statewide backbone network. The backbone is designed with multiple paths to increase service reliability and availability in the event of a failure (see Appendix 4 – Garden State Network). Primary transport technologies in use include frame relay, Integrated Services Digital Network (ISDN), Asynchronous Transfer Mode (ATM), T-1, T-3, OC3, OC12 and SONET. The major contracted carrier service providers at this time are AT&T and Verizon. The individual agency locations connect to their central node primarily with T-1, ATM, frame relay, or point-to-point services. The Inter-LATA circuits connect the main nodes via T-3 and OC3 technologies.

The GSN currently serves over 45,000 IP-addressable devices. Included in this device count are over 1000 routers and over 1000 application servers. Individual agencies administer their own local infrastructures.

The State employs Domain Naming Service (DNS) for enterprise wide name resolution. An initiative to convert to Dynamic Domain Naming Service (DDNS) is currently in the planning phase.

For Internet connectivity, New Jersey currently utilizes two 45 mbps Point-to-Point circuits with gigabit switched segments to ISP - AT&T. The two circuits are located in SAC (State Police Systems and Communications Center) and the Hub in West Trenton. They connect into different AT&T Service Node Routing Complexes (SNRCs) located in Washington, D.C., and Philadelphia, Pennsylvania.

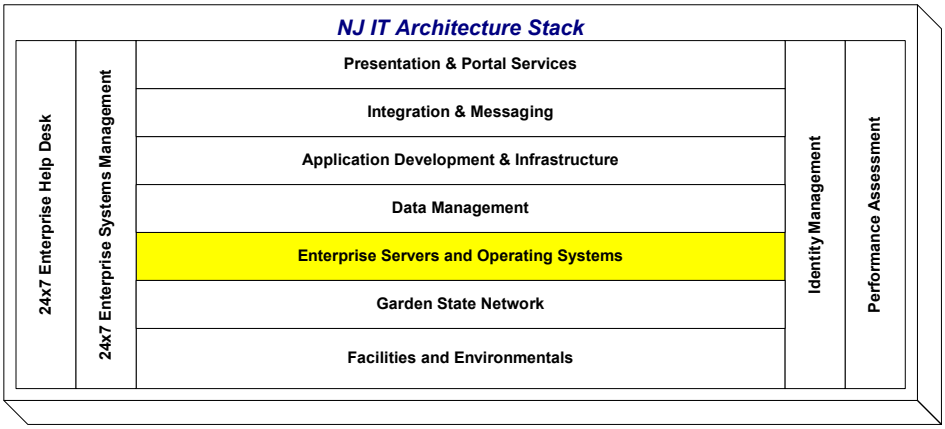
Currently there exists one entry and one exit point between the GSN and the Internet, that being through a firewall that uses IP protocol. Additional firewalls have been implemented to separate the three tiers. The firewalls have been configured such that a higher secure host (i.e. core) can initiate a connection to a less secure host (i.e., secure or public) but a less secure host cannot initiate a connection to a higher secure area without a proper firewall rule. Policy prohibits advancing inbound more than one tier at a time without a process to supervise communications with the next tier. Firewall rules are created to allow specific connection defined by specific ports. The typical public access is by port 80 (http) and 443 (https).

Dialup services are provided to limited users through Cisco 5200's. It provides 56K asynchronous capabilities for remote access.

Extranet connections require point-to-point connections from the extranet partner to the secure layer of the firewall infrastructure. The cost of these connections varies based on the circuit ordered.

Unsolicited inbound file transfers (FTPs) to the State are not allowed. FTP is only allowed within core or as a ‘pull’ back to core. See section on Data Transfers for details.

Enterprise Servers & Operating Systems



Shared Server Infrastructure

The Share Server Infrastructure (SSI) is located at the Hub and River Road Data Centers. It is an area in each computer room where mainframes and servers are being centralized to offer a common location to manage the distributed environment. Cabinets are provided to "rack" servers and eliminate excess footprint. Implementation of a standard KVM (Keyboard, Video, Mouse) matrix switching backbone solution at both facilities has improved floor space utilization, cable management and server access as well as reduced equipment requirements and power consumption. Optimizing key server resources through common logical and physical environments positions the State to properly plan, manage and control a growing server infrastructure.

Based on the best-supported environments by the IT community, the SSI supports the following operating system platforms:

- Bull GCOS
- IBM OS/390
- IBM AIX
- Sun Solaris
- Microsoft Windows

Storage Area Network

The State manages two Storage Area Networks (SAN), one at River Road and one at the Hub. A SAN is a network whose primary purpose is the transfer of data between computer systems and storage elements. The SAN consists of a communication infrastructure that provides physical connections, and a management layer that organizes the connections, storage elements and computer systems so that data transfer is secure and robust. The SAN attaches storage devices to servers in a networked fashion, using hubs, switches, bridges, and directors to build the topology. In this case, instead of the normal Ethernet communications network, the SAN is done with fibre (see Appendix 5).

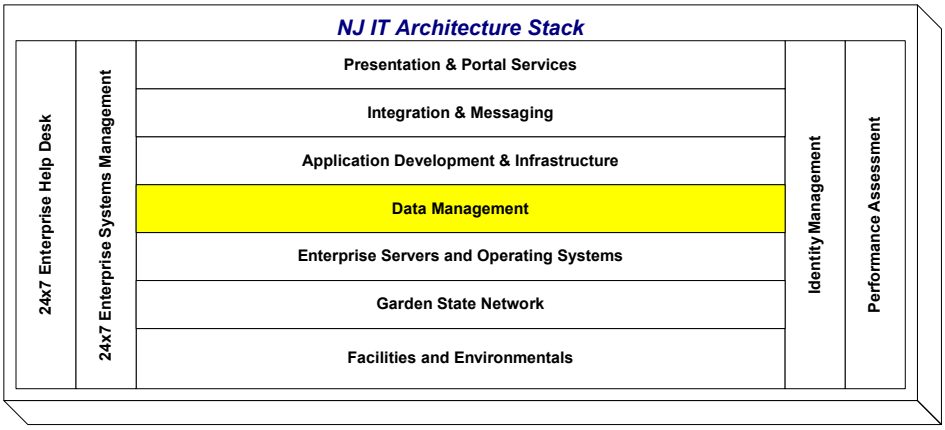
Installing two fibre adapter cards in a server and connecting the server to switches with fibre cables establishes a link to the SAN. Two cards are needed to provide redundant paths to the SAN to eliminate a single point of failure. Once connected, disk space can be "carved" from the storage array(s) and dedicated to a server. SAN technology presents many benefits to server data storage:

- Centralized storage management
- Easy to add disk capacity dynamically
- Easy to replace a deficient server without loss of data
- Faster response time than internal SCSI disks
- Potential for improved backup and disaster recovery techniques
- Better storage attributes – hardware RAID, dynamic sparing, remote data copy, mirroring and more

Backup and Recovery

The strategic direction of the State is to use Tivoli Systems Management to coordinate, manage and execute backups. Tivoli backup is capable of managing a variety of flat files and major databases through Tivoli and DBMS aware agents.

Data Management



The State has created a Common Data Architecture, including an Enterprise Logical Data Model, to guide management of data within the State. This strategy has enabled the State to use relational technologies to collect, disseminate and maintain the integrity of critical data elements across multiple State programs in an equitable, efficient manner.

The Office of Information Technology developed the New Jersey Common Data Architecture (NJCDA) to address data management issues in a consistent manner. The architecture is a collection of related tools and technologies, along with standards and policies and the methodology and the expertise to employ them. The architecture enables data retrieval from operational databases; cross-referencing of that data against data in other systems; the ability to cleanse, standardize and spatially-enable the integrated data; and the caching of data for reuse as needed. Most importantly, the architecture enables the delivery of the cached data to different audiences in the format that each requires, and allows the information consumers to ask questions of the data in their own terms.

Using a Common Data Architecture (CDA), State agencies have access to more useful information as they:

- Collect data once and use it often, improving data accuracy
- Store data more effectively for a timelier and more complete information picture
- Reduce or eliminate costs associated with data collection, storage and error correction
- Improve access to information while better protecting the privacy of individuals

The creation of a CDA is a major and essential commitment to a long-term strategic initiative to support data reusability. This architecture will form the foundation for collecting, storing, managing and controlling privacy of and access to data on an enterprise basis.

Below is a description of the concepts and tools used to accomplish this mission.

New Jersey Enterprise Logical Data Model

A data model is a tool used to provide a pictorial view of data, groupings of data, relationships between data groupings, and the organization of data groupings by dependencies. There are several types of data models – such as conceptual, logical and physical. Where a conceptual data model does not include all of the detailed attributes of an entity, a logical data model is a fully attributed view that documents both relationships and unique identifiers. A logical data model, however, does not reference the characteristics of a DBMS or the physical storage of data.

The New Jersey Enterprise Logical Data Model (NJELDM) specifically provides a definition and standardization for data used to conduct business operations, a schematic showing the natural relationship between different groups of data and a conceptual blueprint for a database.

The State of New Jersey's LDM gives a pictorial view of the Universal, Enterprise and Affinity Data Tiers – information that is common to all state agencies or shared between one or more agencies. The intent is to manage the overall data assets to achieve optimal integration, sharing, access, and utilization of technology resources and infrastructure.

Operational Data Store

This is a central repository of current operational data that is initially gathered from a variety of existing transactional systems to present a single rational view of operational data. As legacy systems are re-written, new systems write directly to the Operational Data Store (ODS). The Operational Data Store serves as a transitional facility while an organization's systems undergo a systematic re-write, as it insulates reports and interfaces from changes in the underlying transactional systems. History should not be stored in the ODS. Some reporting can occur directly against an ODS, but data can also be replicated into operational reporting areas called Operational Data Marts (Opera Marts).

Enterprise Data Warehouse

This is a central repository of historical data that is gathered from a variety of sources to support data integration efforts. An Enterprise Data Warehouse (EDW) is the single version of the truth that supplies historical data to partners, and to analysis areas called Data Marts. It is not a single database, but a consistent data integration environment that consists of multiple subject areas, staging, archiving and persistent storage and multiple physical databases. It is never directly accessed by end-users. The State's EDW does not support the development of independent data marts directly sourced from outside of the EDW environment.

Data Mart

A data mart is a pre-defined and pre-formatted subset of data from an Enterprise Data Warehouse or an Operational Data Store that has been identified based on the questions that need to be answered by the report community. Data Marts are built for the needs of the specific report community, so the same data may exist in many ways and many combinations in different data marts. Data Marts always receive data from a consistent, integrated source – never directly from individual operational systems – so the answer to the same question from any data mart is always the same. The NJCDA supports the development of dependent data marts (sourced from the EDW or the ODS) using conforming dimensions (common reference data used by multiple data marts).

Business Intelligence Tools

These query and reporting tools provide rapid development of reports that can be produced by most business people due to a friendly, graphical interface and a semantic layer that hides the complexity of data relationships from report consumers. The State's Business Intelligence Platform is BusinessObjects Enterprise, which provides a complete range of both full and thin client business intelligence solutions. For formatted reporting embedded within applications, the State supports BusinessObjects' Crystal Reports.

Extract, Transform and Load (ETL) Tools

ETL tools are used to move and transform thousands of records in a bulk fashion using a graphical interface. These tools learn about data and systems and enable reuse of knowledge on subsequent projects. The State's ETL Platform is Ascential's DataStage, which is web services-capable, XML-aware enterprise integration platform that supports both high volume batch integration and individual transaction integration in real-time.

Enterprise Application Integration (EAI) Tools

EAI tools are used to integrate common data across multiple systems at the transaction level, reusing information quality data (meta data). At the data integration layer, the State's EAI platform is Ascential's DataStage with RealTime Services and MQSeries. See Enterprise Application Integration (EAI) for more information on EAI platforms.

Meta Data Management

The NJCDA provides for common management of meta data, or information quality data, which can include such diverse categories as data dictionaries, data models, process rules, data lineage, system documentation, transformation rules and security information. These tools share definitions of data between each other and the systems that they help to connect. When possible, a common data name and definition is created and shared between systems. The State's Meta Data Management platform is Ascential's MetaStage.

Data Modeling

Data modeling tools are used to document, locate and reuse data as well as to describe the relationships between data and systems. The State's Data Modeling platform is Oracle Designer.

Data Quality and Cleansing Tools

These tools are used to analyze data values, ensure that data elements are captured and stored in a way to best comply with their business rules and intended application, find patterns of poor quality, standardize addresses, add geographic coding information to records, and perform sophisticated matching of free-form data to find exact or like matches. The State's Data Quality platform is Ascential's Integrity (QualityStage) suite.

Data Mining

Data mining is a sophisticated statistical analysis of data for patterns and clusters. It is not the ability to perform ad hoc queries against data, which is provided by business intelligence tools. Data mining tools can learn from earlier analyses and can look for patterns without guidance. The State's Data Mining platform is SAS's Data Miner suite.

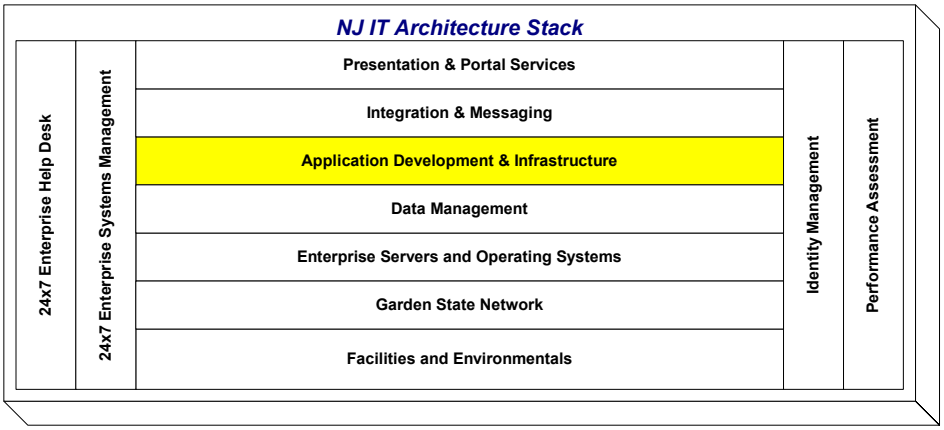
Database Management Systems (DBMS) Platforms and Knowledge Base

The strategic relational database for the State is Oracle. The State also supports IBM's DB2 UDB and Microsoft's SQL Server.

The State maintains the following mainframe legacy databases: IMS, Datacom, Adabas, Bull DM4, but has a stated objective to migrate from IMS.

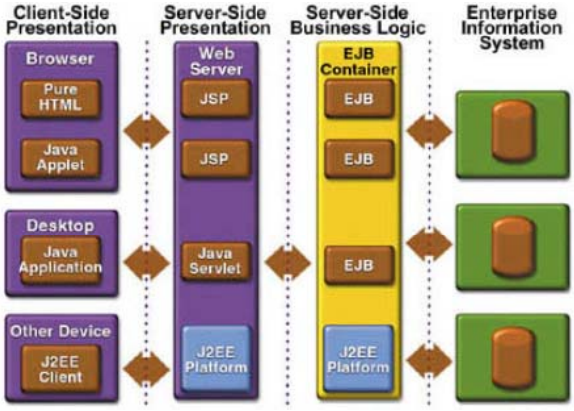
The State maintains a variety of flat files with a strong emphasis on IBM VSAM for non-DBMS legacy applications, as well as a legacy environment of Focus files. The State is migrating its Focus solution to a data-warehousing environment built with Oracle and BusinessObjects.

Application Development and Infrastructure



The strategic application environment for new applications is object-oriented design using Java J2EE components running primarily on Sun ONE application servers. Programs should be developed utilizing HTML, Java Server Pages, Java Script, Servlets, Java Beans and Enterprise Java Beans, with the goal of developing reusable components. Authentication and authorization should be provided by the myNewJersey Portal, which leverages pre-defined communities of users and applies role-based policy against those communities.

J2EE application design, dependent upon security requirements, usually conforms to a multi-tier architecture as depicted below:



A Microsoft hosting environment is supported for Commercial Off the Shelf Software and certain custom development.

J2EE Application Hosting Environment

The State's primary J2EE hosting environment is based on the Sun ONE Application Server 7, Enterprise Edition, which has been implemented in standalone as well as clustered configurations. Among the key architectural elements are:

Core Functionality

- Certified compliance with J2EE 1.3 (J2SE 1.4, EJB 2.0, JDBC 2.0, Java Servlet 2.3, JSP 1.2, JMS 1.0, Java Naming and Directory Interface (JNDI) 1.2, Java Transaction API (JTA) 1.0, JavaMail 1.2, Java Activation Framework (JAF) 1.0, JAXP 1.1, J2EE Connector Architecture 1.0, Java Authentication and Authorization Service (JAAS) 1.0)
- An integrated Java Web Services Pack, including JAXM, JAXP, JAXR, and JAX-RPC
- Enabling existing applications to become new Web services through integrated support of SOAP and WSDL

- J2EE Connector Architecture service provider interfaces
- High-performance Java Message Service (JMS) provider
- Java Transaction Service (JTS) with two-phase commit for managing database services from the leading RDBMS vendors
- Database connectivity to Oracle, DB2, and Microsoft SQL Server
- High-performance HTTP Server with SSL security, delivering high performance through an advanced multiprocessing, multithreaded architecture; efficient use of kernel threads; and sophisticated memory management
- Server-side HTML (SHTML) and chunked encoding which enhance performance of dynamic content
- Various security standards: SSLv2, SSLv3, Transport Layer Security (TLS) 1.0, X.509 certificates, PKCS #11, FIPS-140, 168-bit step-up certificates
- High-performance container-managed persistence (CMP) engine that supports object-to-relational (O/R) mapping

High Availability

- Separate Business Logic and Persistence Tiers. This enables greater scalability across both the business logic and persistence tier while allowing for integrated installation and administration.
- Distributed, Replicated State Information. Application session state data is automatically replicated and distributed across multiple servers. Any individual component can fail without affecting an application's ability to retrieve the session state.
- Inherent Data Availability. The inherent high-availability features delivered with the integrated HADB (high availability database) offers near-continuous availability for application session state data without the management and hardware. Application session state data is synchronously replicated.
- Horizontal Scalability. As the load and throughput requirements grow, additional servers for application support and session state maintenance can be easily added without downtime - yielding near linear horizontal scaling.
- Self-Repair. High-availability technology identifies failed servers and can automatically repair to alternative servers, raising overall system availability.
- Shared-Nothing Architecture. The underlying architecture used by Sun's high-availability technology is inherently distributed, eliminating bottlenecks and facilitating high throughput across multiple servers.
- “Five 9s” availability for Application Server session state persistence.
- Uninterrupted services by providing online upgrades of both software and hardware for better serviceability.

eForms

The State has implemented an eForms platform based on the Accelio product suite composed of the Adobe Accelio Capture Enterprise Server with the Capture Web module, and the Adobe Accelio Integrate InTempo workflow solution.

This eForms solution will provide forms to New Jersey’s internal and external users quickly and efficiently with no download or plug-in. The Capture Web module allows delivery from a single-XML design template, intelligent forms to any browser running on any device, from powerful desktop computers to handheld and wireless devices.

Legacy and Mainframe Services

The State has Bull and IBM enterprise servers which host applications for the law enforcement community, driver licensing, vehicle registration, unemployment insurance, the tax systems, and human services among many others. Over one million batch jobs and over one billion online transactions are run on these processors each year. The mainframes are geared toward high volume activity and have excellent response time and availability track records. The applications on the enterprise servers can be web enabled.

There is one Bull mainframe and two IBM mainframes. The operating systems are GCOS8 for Bull and OS/390 (soon to be z/OS) for IBM. The Bull environment runs an internally developed security system while the IBM systems use eTrust CA-ACF2 security software. Both Bull and IBM mainframes use TCP/IP for their network architecture protocol. Our teleprocessing monitors are TP8 for Bull and CICS for IBM. Data is stored in Oracle, DB2, Adabas, Datacom, IMS, IDS-II and VSAM data management systems. Mature application development and testing platforms exist for both the Bull and IBM systems. The Bull system has a disaster recovery site in

Phoenix, Arizona, and the IBM systems have their disaster recovery location at SunGard's data center in Philadelphia. Both disaster recovery sites are linked.

Geographic Information System (GIS) Services

The State has a goal of spatially enabling any application that would benefit from geo-awareness. The State definition of spatially enabled means that the system is:

- capable of integrating spatial data (e.g., data with a location component) with other business data across multiple, heterogeneous data sources; and
- capable of supporting abstract data types (e.g., images, text, and spatial data), spatial operators and functions, and spatial locator indexes.

Managing and accessing spatial data across the State's IT enterprise is facilitated through a gateway which utilizes a combination of technologies including Environmental Systems Research Institute (ESRI) Arc Spatial Data Engine (ArcSDE). Spatial data is served-up in a format that can be accessed by a variety of desktop GIS clients, served out to the Internet using ESRI's ArcIMS technology or by other applications using standard SQL queries. Spatial data is hosted on an Oracle and IBM AIX platform providing for high-availability and scalability.

Internet Map Server (IMS) technology provides the foundation for distributing high-end geographic information systems (GIS) and mapping services via the Internet. This technology also enables users to integrate local data sources with Internet data sources for display, query, and analysis in a Web browser. Our IMS platform is ESRI's Arc Internet Map Server (ArcIMS). ArcIMS is a powerful, scalable, standards-based tool used to quickly design and manage Internet mapping services (web services). IMS technology is currently integrated in the State's Shared Server Infrastructure (SSI) using a three-tier application architecture.

Any proposed solution that includes a GIS component and/or incorporates spatial data is evaluated, planned, designed, and implemented in concert with the OIT Office of GIS. Applications that are geo-enabled are in compliance with the OpenGIS Consortium specifications for spatial data (http://www.opengis.org/). The State of New Jersey's preferred GIS software platform is the ESRI set of products and tools (http://www.esri.com/).

Data Transfers

The State has implemented two methods of secure file transfer (SFT) to send and receive files utilizing advanced data encryption technologies. The first method is a manual interface through the myNewJersey portal Secure File Transfer Channel. After connecting through an Internet Browser and authenticating to the portal, the user will select the file they need to send, receive or browse and select the source or destination of that file. The transfer will occur using a secure socket layer (SSL) connection and the user will be advised of the success of that transfer. The second method is a client-side Java application that automates the transfer through a host scheduler. This method requires a State-issued NJ State Government Digital Certificate and allows the transfer to occur off-peak without human intervention. Both methods of SFT support 128-bit encryption.

Connect:Direct is used to transfer data over dedicated lines within the Garden State Network (GSN) or to private entities.

ePayment

OIT maintains an enterprise ePayment component that provides Internet based payment processing to State agency applications. The ePayment module allows custom developed Web based applications to either process:

- Credit card transactions by interfacing with a payment gateway provider; or
- eCheck transactions by allowing governmental entities to accept electronic checks via the Internet

This module is used with Java compliant applications. Developers of non-Java compliant applications should discuss their requirements with the OIT Application Infrastructure Services office.

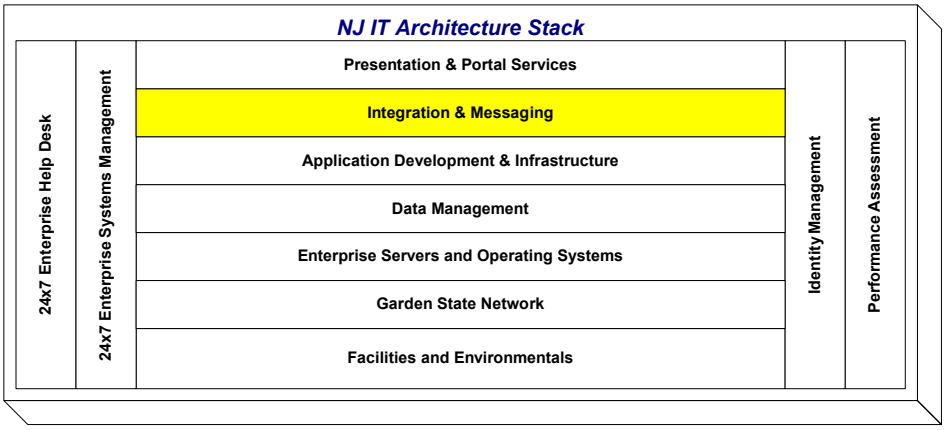
Single Sign-On

See section on Identity Management, Authentication & Authorization Services.

Messaging and Groupware

Throughout the state most agencies use MS Exchange, SunONE, Groupwise or Lotus Notes for messaging and calendar services. In addition to its own user population, OIT provides Messaging and Calendaring services to a certain number of external clients on the SunONE platform.

Integration & Messaging



Message Oriented Middleware

The State has implemented IBM Websphere MQ (formerly MQ Series) in many mission critical application environments for enterprise messaging between systems. Websphere MQ is currently in production on the Sun ONE Application Server platforms for connectivity to the J2EE application environment.

Enterprise Application Integration (EAI)

An EAI solution enables real-time data and workflow integration from one system to another. The State's Enterprise Data Integration platform, DataStage, when used with the State's message transport standard, MQ Series, provides cost-effective real-time application integration to meet many business requirements. Additionally, the State has recently evaluated several Enterprise Application Integration (EAI) products and, as of this writing, considers IBM Websphere Integrator as a leading candidate for a high-transaction-volume/high-availability workflow integration platform.

Host to Web

The State is in the process of procuring a Host to Web platform from IBM. Specifically, IBM's Host Integrator suite will provide for rapid development of HTML web based applications using existing CICS applications and native JDBC database connections for data and business logic.

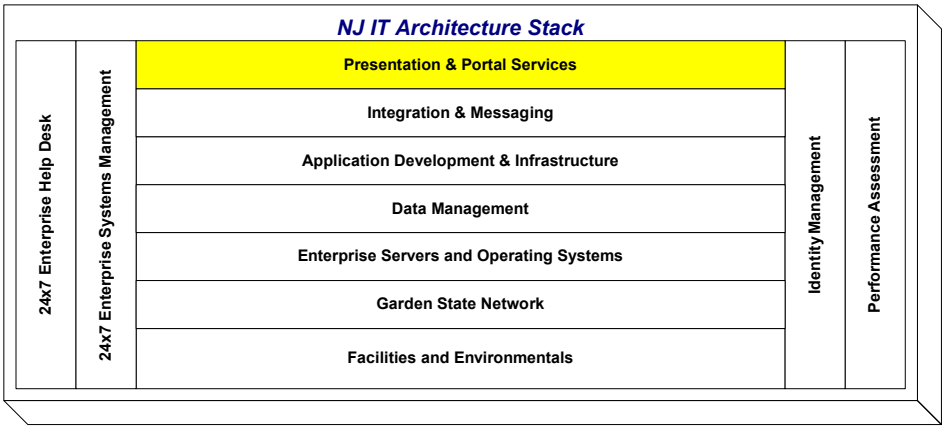
CICS Transaction Gateway

Connectivity to CICS from J2EE applications can be accomplished via the IBM Transaction Gateway. Each instance of the Gateway requires the installation and configuration of a client on the J2EE Application Server platform. On the CICS side, ACF2 Security and CICS Transactions must be established for the appropriate application(s).

DB2 Connect

Connectivity to DB2 is accomplished via a DB2 Runtime Client, which is installed and configured on the J2EE Application Server platform.

Presentation & Portal Services



State Portal Overview

The State's Internet Portal provides an identity-enabled array of services including security, user management, single sign-on, personalization, content aggregation, application integration and search capabilities. In addition, the Portal infrastructure provides a secure Application Virtual Private Network (VPN) for remote access to core computing resources. All Portal services – including the Application VPN – are provided via an ultra-thin client architecture, the only client side requirement being a standard web browser.

The Portal supports more than forty-five thousand registered members across a diverse range of communities – general public, State employees, New Jersey businesses, and local government officials.

The Portal infrastructure is based on the Sun ONE Portal Server platform with its internal LDAP directory supplemented by an external Oracle database and custom administration code.

Access to the LDAP directory and Oracle database service is managed by a custom Enterprise Java Bean (EJB) framework served from the State's J2EE hosting environment.

Key features of the Portal infrastructure include:

- Multiple load balanced Web Servers
- SSL encryption of all traffic over the Internet
- On-demand user community creation and management with delegated administration of user policy and access control through an integrated management console
- Dynamic user personalization and customization
- Role based access control (RBAC) with multi-role support, user provisioning, and self-registration
- Delivery of integrated content, applications, and services through customizable portlets
- Single sign-on for aggregated applications to the portal
- Integration with existing legacy applications through standard APIs
- Integral lightweight Application VPN
- Integral Geographic Information Systems engine for location based services
- Rapid deployment of multiple portals for many communities from a single platform architecture

Key collaboration services of the Portal infrastructure include:

- Secure role-based document library that facilitates end-user publishing of materials with email notification to user community
- Secure role-based threaded discussion forum for online collaboration
- Delegated role management with role based email distribution
- End-User content publishing (via Interwoven Teamsite)

User services of the Portal infrastructure include:

- Personalized Weather / Air Quality
- Personalized Events Calendar
- End-user self-service

Portal User Management

The State Portal provides Role Based Access Control (RBAC) to content and services. It provides single/reduced sign-on capabilities, aggregated content delivery and delegated user management services for online State services. The authentication methodology currently used with Portal is logon id and password. Access control is managed through the assignment of roles via delegated user administration.

Users can "self-register" for access to public web content only. Additional access to secure services requires the issuance of an authentication code by a designated role manager in conjunction with the business owner of the service. The authentication code process includes formal out-of-band communication between the business process owner and the user.

Additional layers of authentication, such as digital certificates or hardware tokens, may be layered on top of the Portal logon to accommodate stronger authentication requirements.

The State Portal currently uses a combination of LDAP compliant directory services and an Oracle based datastore to manage user authentication, demographic and role assignment data.

The State maintains an Application Programming Interface (API) to the Portal user management services allowing custom application developers to leverage these authentication and authorization processes.

Member services and content management are based on the concepts of User, Role, Entity, Category and Channel.

User

- Any person, public or private, who is registered with the Portal. A person may self-register with the Portal via the Internet by supplying as little information as a name and email address.

Role

- A role defines a group of users who share sufficient common interests to warrant the creation of a Portal-based user group with access to content and/or transactional systems specifically tailored to those interests.
- Each Portal user is assigned the default role of member. Users may also be assigned one or more additional roles. Roles provide for a centrally managed user environment and each role has a role manager.

Entity

- Groups of users who share a common organizational interest belong to the same entity. Each time a user is assigned a role, that user/role is associated with an entity. Entities allow for decentralized user management, as there is always a manager for each entity in the Portal.

Category

- A grouping of roles into a broad service delivery category. Examples may include the Government, Business or Employee category.

Channel

- A content provider designed to be delivered through the myNewJersey Portal page. Channels are associated with one or more roles.

Web Servers

Anonymous access to the State's static public information is provided through the public access Web servers (www.nj.gov). From there, links are provided to individual agency Web servers.

Currently there are a number of production Web servers. One cluster hosts the State's home page and related flat file information (www.state.nj.us). One cluster supports Microsoft IIS web serving, application serving and data serving through SQL Server. One cluster provides a conduit for the business logic for Java applications bound for the public web server.

The primary web server platform is the Sun ONE Enterprise Web Server. It provides the following capabilities to State Agency developers:

Web Application Development

- Full compliance for Java Servlet 2.3 and JavaServer Pages (JSP) 1.2 specifications
- Support for NSAPI, CGI, CFML, and PHP
- Built-in Java runtime environment with support for the Java Development Kit (JDK) 1.4x release, object serialization, and the JDBC 3.0 specification, including connection pooling, the Java Naming and Directory Interface 1.1 API, and JavaBeans technology
- Session management service to track information for specific users
- Java technology-based application development across JSP and Java Servlet technologies
- WAR file deployment both from command-line and GUI-based interfaces
- JSP component precompilation for faster loading
- Reuse of applications and components that are developed separately
- Standard tag library support, enhancing the user customization of JSP tags
- Fast, in-process, pluggable Java virtual machine (JVM) implementation
- Server-side preprocessing of content using SHTML
- Integration with Java optimization tools
- Web Distributed Authoring and Versioning (WebDAV)
- Netscape Application Program Interface (NSAPI) filter

Reliability and Availability

- High server uptime through multi-processing mode and process monitors
- Unique, shared-session objects to provide failover protection and enable multiprocessing support for Java Servlet extensions on UNIX systems
- Reduced server downtime by rotating logs dynamically
- Intelligent load balancing configuration with Cisco Smart Switch for high availability

Management and Administration

- Dynamic reconfiguration of Web server - without restart
- Integration with Lightweight Directory Access Protocol (LDAP)-based directory servers
- Sun ONE Directory Server management of password policies and user groups down to the site level
- Policy agent integration with the Sun ONE Identity Server
- Command-line interface for HTTP server administration, certificate and key management, and Web application deployment

Performance and Scalability

- High performance through an advanced multiprocessing, multithreaded architecture; efficient use of kernel threads; and sophisticated memory management, Server-side HTML (SHTML) and chunked encoding to enhance the performance of dynamic content
- Multiprocessing mode to increase scalability on multiple CPU machines
- HTTP 1.1 and HTTP compression
- Scalable, keep-alive handling

Security

- Support for SSLv2, SSLv3, TLS 1.0, and X.509 digital certificates
- Support for security-based standards such as PKCS #11, FIPS-140, and 168-bit, step-up certificates
- Centralized, certificate-based security with certificate-to-LDAP mapping
- Administrator setting of SSL parameters for each virtual server
- CGIs to be run as different user IDs
- Single sign-on (SSO) across multiple Web applications (or Java Servlet contexts)

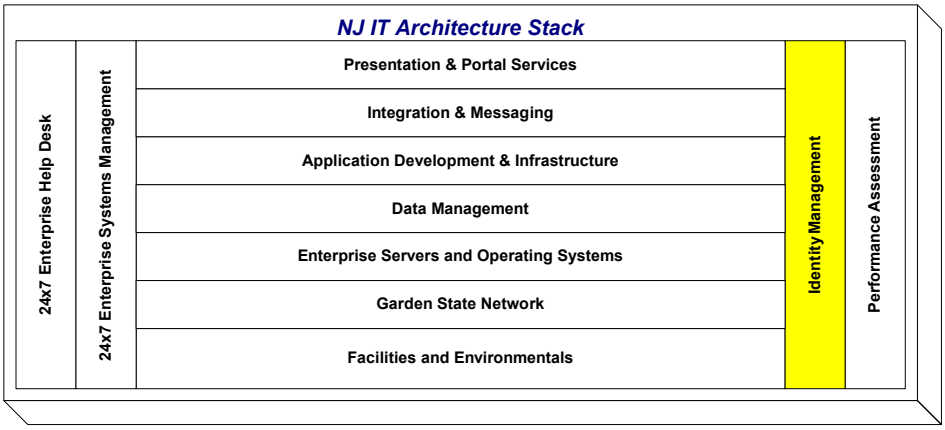
Content Management Services

- Full text and attribute searching of documents through built-in search engine

Web Content Management

Interwoven Team Site provides enterprise web content management services to State agencies.

Identity Management



Authentication & Authorization Services

State Internet / Intranet / Extranet Portal

Enterprise Authentication and Authorization services for Internet, Extranet and Intranet applications are provided by the State Portal infrastructure. See Presentation & Portal Services for details.

Agent Based Identity Management Infrastructure (Future)

Within the next year the State will implement a new Enterprise Identity Management infrastructure to provide a broader array of authentication and access control services. Portal authentication and access control will migrate to this infrastructure, with the Portal becoming a consumer of identity services - as opposed to its current role as provider of identity services.

This infrastructure will be based on the Sun ONE Identity Server and will feature a more comprehensive user provisioning toolset, helping agencies to manage authentication, authorization and access control for the State's business partners, citizens and employees.

Identity Server will provide enhanced delegated user administration for business owners of applications. Multi-factor authentication (id/password; tokens, PKI, etc.) will be supported and will be available for both Portal applications as well as non-portal applications.

The State's Enterprise Identity Management Infrastructure will support the following industry standards:

- LDAP version 2 and version 3
- X.509 digital certificates
- eXtensible Markup Language (XML)
- Simple Object Access Protocol (SOAP)
- Liberty Alliance version 1 specification
- Security Assertions Markup Language version 1 (SAML)
- Online Certificate Status Protocol (OCSP)
- Java Authentication and Authorization Service

Public Key Infrastructure

The State's Enterprise Public Key Infrastructure issues digital certificates that may be used for electronic credentialing and authentication purposes. The certificate that contains the user's public key is stored in a directory. Through key management services, certificates can be revoked or recreated or reissued.

A digital certificate contains information about an individual that can be used to provide a strong authentication credential when accessing online services. The same information can also be parsed to the application to provide access control.

The State of New Jersey issues certificates for integration into State applications where strong authentication is a requirement. Users must provide identity verification prior to issuance. These certificates can be installed on a desktop browser, a smart card or key fob.

Application Specific

User authentication and access to applications can also be controlled directly by an application using a custom authentication module and/or access controls embedded in program code or stored at the data layer.

Mainframe

OIT uses Computer Associates' ACF2 to enable security on an OS/390 mainframe. ACF2 is designed to authenticate users and to protect a variety of OS/390 resources. ACF2 prevents accidental or deliberate modification, corruption, mutilation, deletion, or viral infection of files. With ACF2, access to a system is denied to unauthorized personnel. Any authorized or unauthorized attempt to gain access is logged. System status can be monitored on a continuous basis, and a permanent usage log can be created. The logging feature, besides helping to identify potential intruders, makes it possible to identify and analyze changes and trends in the use of the system. Settings can be changed on a moment's notice, according to current or anticipated changes in the security or business requirements of the organization using the system. Users must have a valid ACF2 Logon ID and must know the current password in order to enter a ACF2 protected OS/390 system.

Enterprise Directory Services

The State maintains a Lightweight Directory Access Protocol (LDAP) compliant enterprise directory service for all State employees (NJ Direct). It is currently in use supporting PKI deployments as well as agency-based extranet user management. The directory is based on Sun ONE Directory Server Software and supports the following industry standards:

- cDSML v2
- LDAP version 2 and 3 RFCs, including RFC 1274, 1558, 1777, 1778, 1959, 2195, 2222, 2247, 2251, 2252, 2253, 2254, 2255, 2256, 2279, 2307, 2377, 2829, 2830, and 3377
- LDAP search filters, including presence, equality, inequality, substring, approximate ("sounds like"), and the Boolean operators and (&), or (|), and not (!)
- LDAP version 3 intelligent referral, which lets a directory refer a query to another directory

State personnel names, locations, telephone system data, and e-mail addresses have been integrated into the directory. Approximately 80,000 entries, one for each State employee, now reside in the directory.

Synchronization with other State agency directories is accomplished through data feeds. The State is currently piloting a meta-directory effort to automate the synchronization process. In the future, the enterprise directory will provide directory services for county and municipal employees as well as citizens and businesses.

Enterprise Public Key Infrastructure

The State has implemented and is hosting a private certificate authority using products and services from VeriSign to implement an enterprise Public Key Infrastructure.

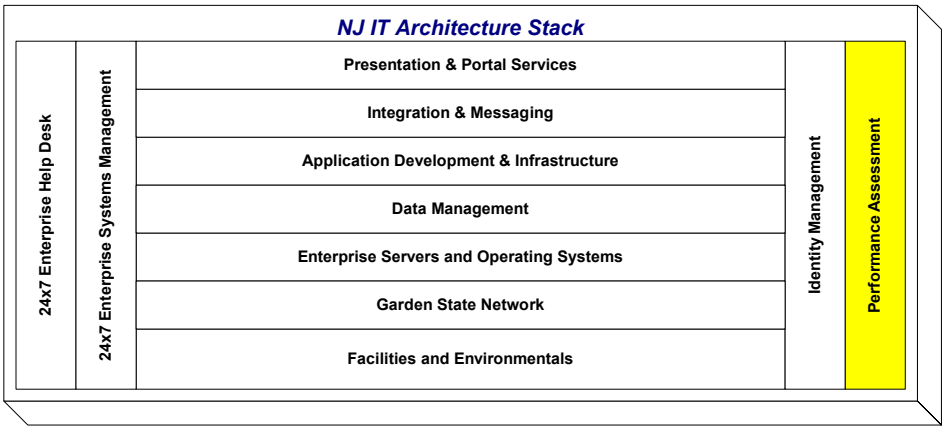
OIT technical staff have implemented the following components for enterprise PKI:

- Registration
- Certificate Issuance
- Revocation of Certificates
- Storing and Retrieving Certificates
- Certificate Revocation Lists
- Key Lifecycle Management

The Enterprise Certification Authority Model includes State of New Jersey Green, Blue and Orange certificates denoting increasing levels of trust/registration requirements.

This infrastructure is designed to meet the majority of PKI business requirements for Internet, Intranet and Extranet users. A distributed administration model gives agencies control over registration and issuance of certificates. OIT maintains the Certificate Revocation function, Certificate Revocation Lists, and Key Lifecycle Management. A statewide Certificate Policy (https://pkice.state.nj.us/njcp.pdf), Certification Practices Statement (https://pkice.state.nj.us/njcp.pdf), Subscriber Agreement (https://pkice.state.nj.us/njsubagr.pdf) and Relying Party Agreement (https://pkice.state.nj.us/relying_party.pdf) govern certificate issuance and usage.

Performance Assessment



Application Instrumentation and Performance Testing

Wiley Technology Introscope

Introscope's low overhead technology provides monitoring of production Java applications with no degradation of performance. It allows component-level views of the entire Java application environment. It can isolate bottlenecks in applications all the way down to individual Servlets, EJBs, Classes, and Methods. It can monitor applications both proactively and reactively by wrapping them in non-intrusive instrumentation code. Real-time events and historical trends are available for analysis by administrative staff.

Empirix eLOAD

eLoad is a robust load testing solution that accurately tests the scalability and performance of Web applications. The State has implemented eLoad as an automated software load testing solution to predict how well Web applications will handle user load. It is used both during application development and post-deployment to conduct stress testing. Use of this tool has dramatically improved the quality and performance of web based applications.

Bull Mainframe Tools

The Bull environment uses four tools for performance analysis: Video provides information on the jobs that are executing, response times, idle time, and disk and tape usage. Pursue8 displays tape and disk channel usage. Concurrency Monitor displays database conflicts, and Workstation Monitor provides an overview of the workstations that are running and highlights problems.

IBM Mainframe Tools

Omegamon products are used to monitor the operating system, CICS teleprocessing monitor and DB2 database. Trim is used to monitor AG's Adabas database, and Sysview is used to monitor CA's Datacom database.

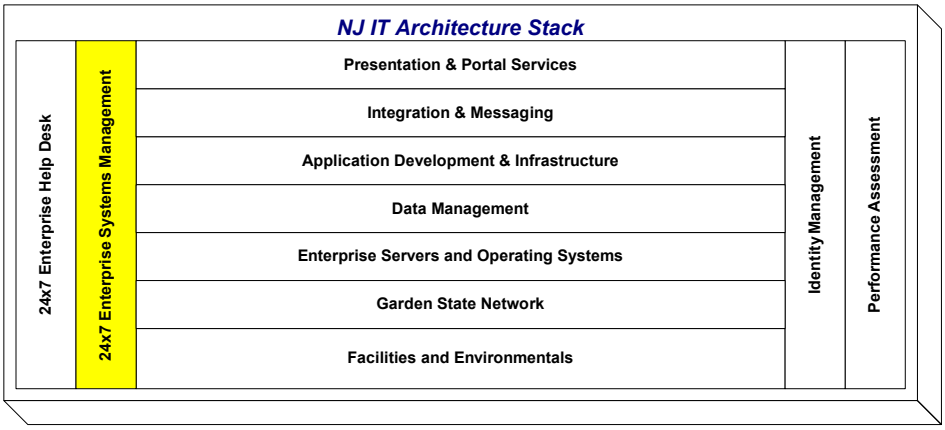
Network Performance

Compuware's Network Vantage, LAN and WAN probes are used to perform baseline analysis of the existing network environment prior to deploying new applications. The existing application protocols and their respective volumes traversing the local (LAN) and wide area network (WAN) are identified and their bandwidth consumption, average response times and traffic volumes measured. This analysis can be used as a benchmark comparison against future performance. In instances where a wide area network connection employs Frame Relay technologies, the circuit utilization can be obtained.

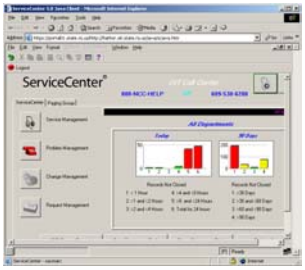
Compuware's Application Expert is used to assess applications before they are deployed in a production environment. The results will analyze host/server and network utilization as well as the efficiency and performance of the integrated application functions and will provide response time expectations.

Compuware's Application Vantage and Network Associates "Sniffer Pro" tools are also used to monitor production applications to resolve performance degradations and determine the root cause(s) of poor application performance. These tools help to determine whether poor application response times are the result of underpowered client workstations, the network infrastructure, the application code or an inefficient host server platform/OS or database.

24 x 7 Enterprise Systems Management



Enterprise Systems Management (ESM) includes the end-to-end management of the evolving, heterogeneous, multi-platform, distributed computing environment. ESM tools are used to detect, correlate, escalate and prioritize events; manage responses to those events; and report on those incidents in a pro-active, real-time event management environment in order to provide a secure, highly available, robust, multi-platform enterprise infrastructure that meets or exceeds system requirements.



The State has implemented various monitors, distributed storage management, and event management components that are integrated with problem management for the automatic generation of trouble tickets for critical events.

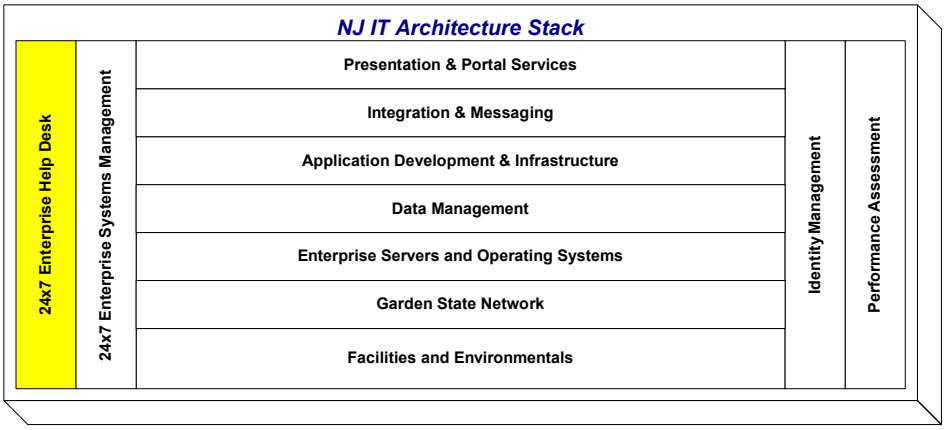
Event management via the Tivoli Enterprise Console (TEC), along with the software products that 'report to it', detect, record, and correlate all enterprise significant events. It is in many ways the central nervous system for this complicated multi-platform computing environment, gathering information on hardware, software and network devices, and, in some cases, curing problems before they occur.

Peregrine Systems Service Center (SC) is used for call management, problem management and change management. This product improves client application availability through the automatic notification and escalation of problems via pager and email and the integration of problem and change management.

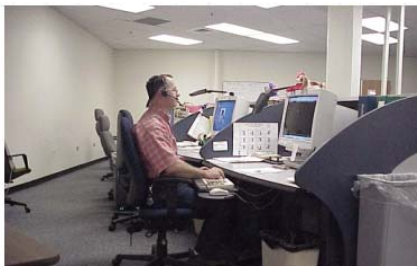
The integration of the SC with TEC further improves this process by the automatic generation of problem tickets based upon critical events forwarded to the TEC by various monitors (e.g. Netview and Oracle). In some cases problem tickets are generated and the appropriate technical staff notified via email and/or pager before a client is aware of the problem.

The State will also implement Tivoli's Configuration Manager (a robust inventory system), Remote Control, and Monitoring for Transaction Performance (to monitor the performance and availability of eBusiness and enterprise transactions).

24 x 7 Enterprise Help Desk

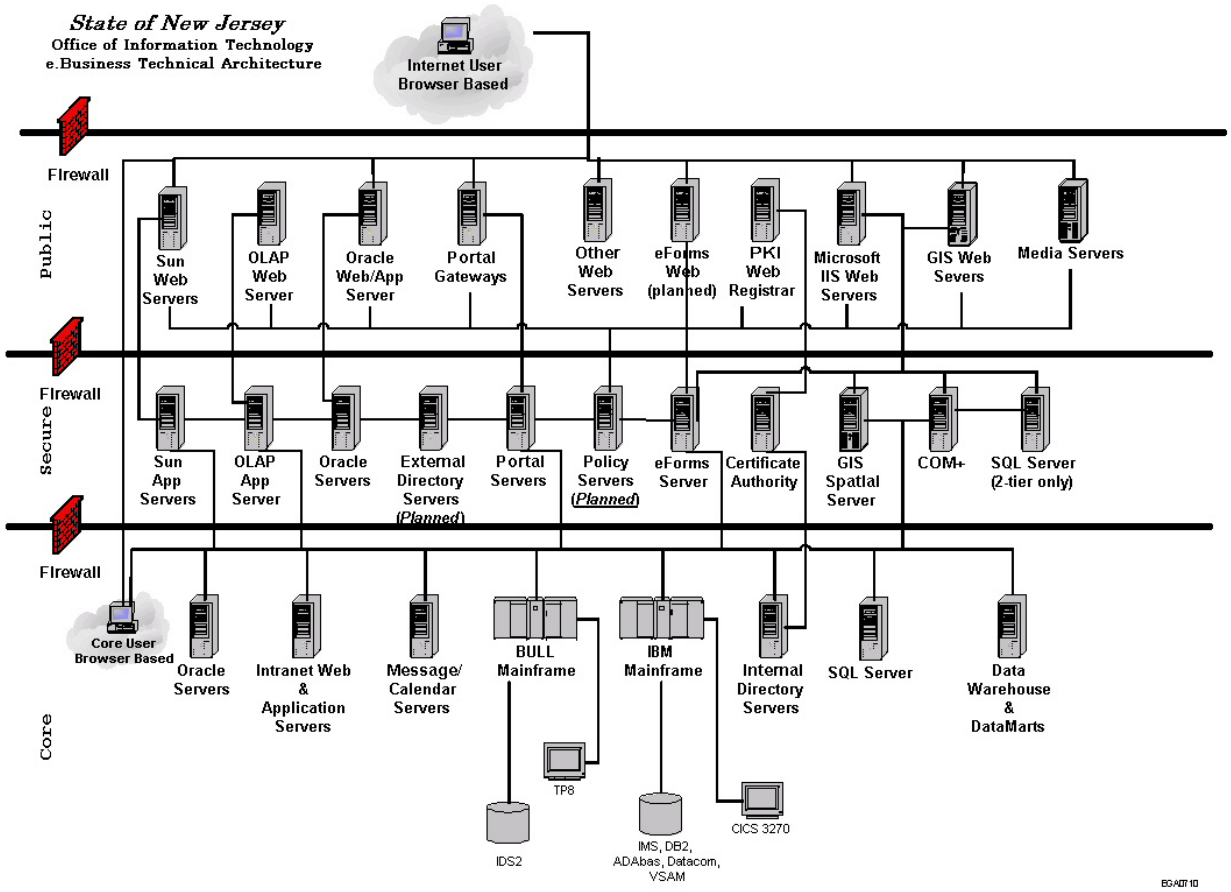


The Enterprise Help Desk / Network Call Center is staffed 24 hours a day, 365 days a year to resolve system outages. All calls made to NCC are recorded in the Service Center Problem Management System. The system simultaneously e-mails and pages resources that have been identified to resolve the problem. Resources typically include a primary contact, a back-up contact and a supervisor. Resources begin the problem resolution process and update the problem ticket with status information until it is resolved. System users can access this system via a web browser to monitor the resolution status of their problem.

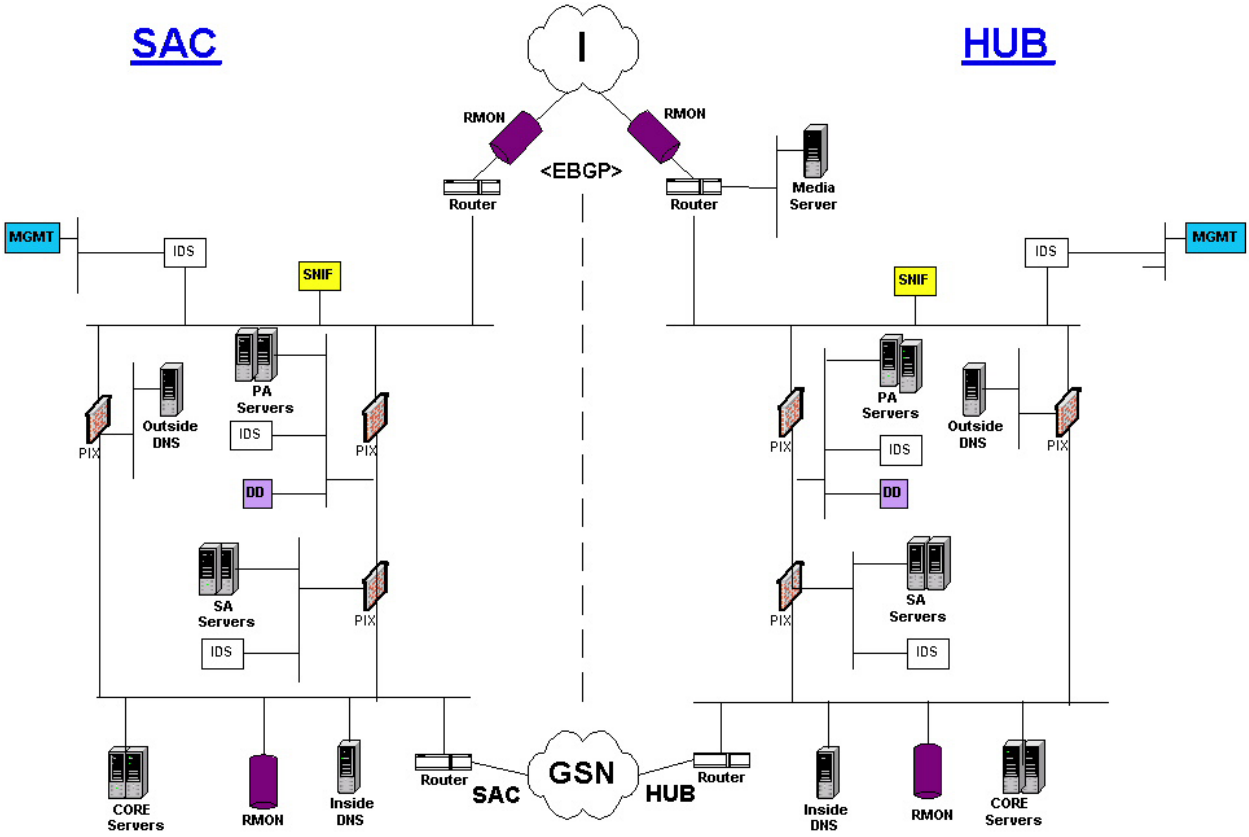


The NCC serves over 20 State agencies on both legacy and new systems. All problems and resolutions are analyzed for performance statistics and problem cause.

Appendix 1 - Logical Network Diagram



Appendix 2 - Physical Network Diagram



Appendix 3 - Products and Technologies

Category	Product	Direction *
Operating Systems		
	AIX	P
	GCOS8 (Bull)	S
	LINUX	A
	OS390	A
	Solaris	P
	Windows 2000	A
	Windows NT	S
	Z/OS	A
Database Platforms		
	Adabas	S
	Datacom	S
	DB2 UDB	A
	IDS2	S
	IMS	S
	Oracle	P
	SQLServer	A
	VSAM	S
Transaction Management		
	CICS	A
	TP8 (Bull)	S
Languages		
	COBOL	A
	J2EE Java	P
	Natural	S
	Perl	A
	HTML	P
	JavaScript	A
	SQL	P
	Visual Basic	S
	.ASP	A
	Oracle Forms/Reports	A
	XML	P
Portal Services		
	Sun ONE Portal Server	P
Identity Management / Policy Services		
	Sun ONE Identity Server	P
Directory Services		
	Active Directory	A
	Sun ONE LDAP	P
Data Transfer		
	Secure File Transfer	P
	Connect:Direct	A

Legacy Data Access		
	CICS Transaction Gateway	A
	Entire X	A
	Host to Web – IBM Host Integrator	A
EAI (Enterprise Application Integration)		
	IBM WebSphere MQSI (not yet implemented)	P
eForms		
	Adobe Accelio Capture Enterprise Server w/Capture Web module	P
	Adobe Accelio Integrate InTempo workflow solution	P
GIS Technology		
	ESRI: ArcSDE – Spatial Data Hosting	P
	ArcIMS/ArcMap Server – Internet Map Server	P
	RouteServer – Routing and Driving Directions	P
	Metadata Server – Spatial Data Catalog	P
Application Servers		
	Oracle	A
	Sun ONE	P
Web Servers		
	IIS	A
	Sun ONE	P
	Oracle	A
Messaging Technology		
	IBM Websphere MQ	P
Application Developer Desktop		
	Windows 2000	P
	Windows 98	S
	Windows 95	S
	Windows NT4	S
Security Tools		
	ACF2	A
	VeriSign PKI	A
	SSL	A
Network Management		
	Tivoli Suite	P
Imaging		
	FileNet	A
Mail		
	Sun ONE (OIT), also integrate to Exchange, Notes, GroupWise	Not Rated
Calendar		
	Sun ONE (OIT), also integrate to Exchange, Notes, GroupWise	Not Rated

Content Publishing		
	Interwoven Teamsite	P
Audio / Video		
	Real Media	A
	Microsoft	A
	Avid Xpress	A
OLAP (Online Analytical Processing)		
	Business Objects	P
Software Administration		
	SourceSafe	A
	CVS	P
	CA Librarian	A
Data Management Tools		
	DataStage (ETL Platform)	P
	Integrity (Data Quality Platform)	P
	MetaStage (Meta Data Repository)	P
	PowerDesigner (Data and Process Modeling)	A
	Oracle Designer (Data Modeling)	A
Data Mining & Statistical Analysis		
	SAS Data Miner	P
Reporting Tools		
	Oracle Reports	A
	Crystal Reports	A
	Business Objects	P
	Focus	S
	Magna8	S
Development Tools		
	Macromedia DreamWeaver (HTML)	A
	Sun ONE Studio	P
	Adobe	A
	Quark	A
	Macromedia Flash	A
	Macromedia Fireworks	A
	Pagemaker	A
Print Services		
	IBM Advanced Function Printing	P
Performance Assessment Tools		
	Java Instrumentation: Wiley Technology Introscope	P
	Load Testing: Empirex eLoad	P
	LAN/WAN: Compuware Network Vantage, Application Expert	P
	Bull: Video, Pursue8, Concurrency Monitor, Workstation Monitor	S
	IBM: Omegamon, Trim, Sysview	A

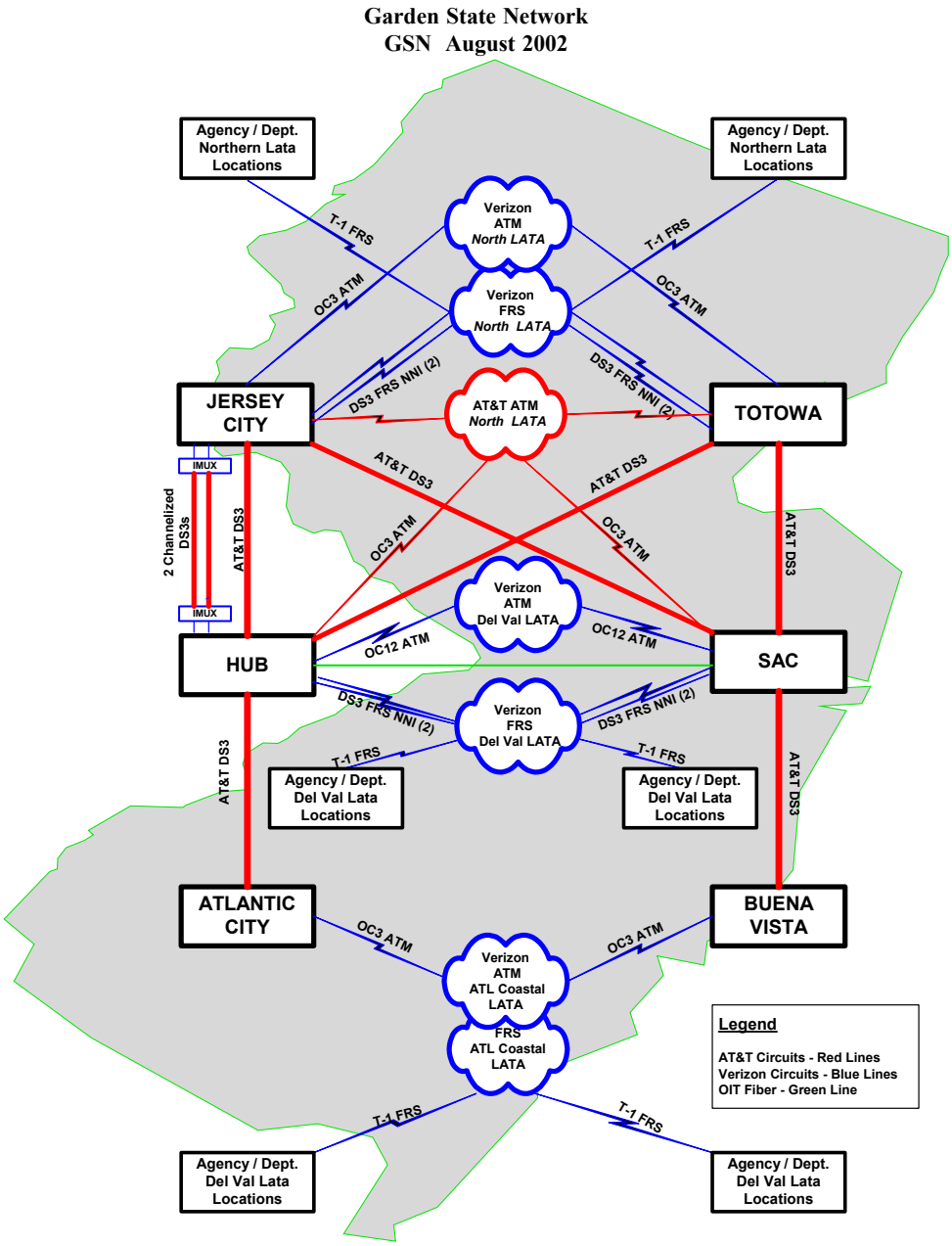
* Direction Key:

P = Preferred
This represents our strategic direction.
The State will give priority to this technology.

A = Acceptable
This represents our minimum requirements.
The State considers this technology adequate/satisfactory.

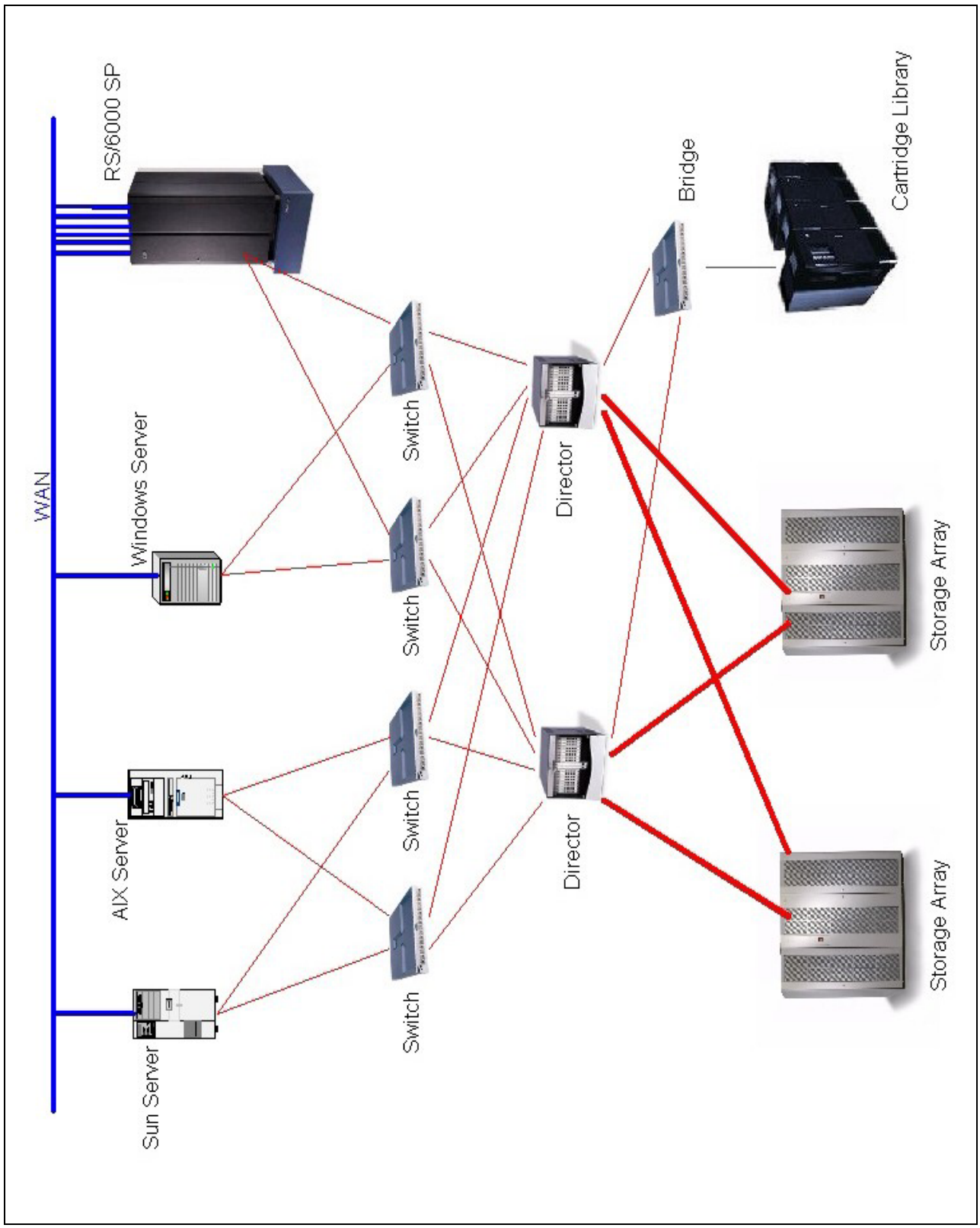
S = Sunset
The State deems this technology undesirable/unacceptable.

Appendix 4 – Garden State Network



Garden State Network Layout Figure 1

Appendix 5 – Storage Area Network (OIT)



Appendix 6 – NJ Common Data Architecture Conceptual Model