3. State Portal Reference Architecture

State Portal reference architecture would serve as a repository of architectural best practices for implementation of State Portals. It provides architecture and technology related standards, guidelines and best practices. It would be used as reference architecture while implementing State Portals. Along with the specific requirements, it should be used for deriving and defining the architecture of State Portals.

From the point of view of functionality, implementation technologies and architecture, the present state of State Portals varies significantly from state to state. Some of the states are in the process of conceptualizing where as some states have a website up and running and few states offer transactional government service on their State Portals. State Portal reference architecture would help to achieve some amount of uniformity and consistency among the State Portals. It would enable state's which are conceptualizing State Portal projects to adopt already implemented best practices as well as prevent errors. It would serve the need of sharing best practices and learning from past mistakes. It needs to ensure that the State Portal's architecture is flexible, extensible, scalable, vendor independent and able to accommodate state specific functional and technology variances.

Following are the design goals of State Portal reference architecture:

a. Adopt service oriented architecture
b. Develop and expose business functionality as services
c. Provide web based user interface
d. Support multiple access devices such as desktop computer, cell phones, and PDA.
e. Ensure confidentiality of citizen's data
f. Achieve interoperability between State Portals and National Portal.
g. Enable easy discovery of information
h. Integrate with departmental applications to make services accessible
i. Integrate with websites of government departments and organization for content

3.1. Principles of State Portal

Principles guide the definition of State Portal Framework. This section explains the principles of State Portal framework.

3.1.1. Summary of Principles

	Principles
	Business principles
1	Principles are supreme and universally applicable
2	Maximize Benefits to the State
3	All State Organizations and Departments are responsible for Information Management
4	Provide Common use Services
5	Comply with Law and Policies defined for the State
6	IT organization takes Responsibility of IT systems
7	Continuous Improvement through Feedback Collection and Statistical Analysis
	Application principles
1	Portal should be Scalable
2	Portal should be highly available

3	Portal should be Extensible
4	Portal should be Secure
5	Maximize Portability
6	Minimize Technology Dependence
7	Portal should be Easy to Use
	Data Principles
1	Data is an Asset
2	Data is shared
3	Data is Accessible
4	Data is secured
	Technology principles
1	Changes should be Driven by Business Requirements
2	Control Technical Diversity
3	Promote Interoperability

3.1.2. Business Principles

Principle 1: Principles are supreme and universally applicable

Statement
These principles apply to all state government departments and organizations at all levels such as Department, District, Block etc. who would be offering services through the State Portal.

Rationale
The only way we can provide a consistent and measurable level of quality information and services to citizens is when all concerned departments and organizations abide by the principles.

Implications
a. Absence of defined principle may lead to exclusions, favouritism, and inconsistency would rapidly undermine the management of information across the State at each level.
b. Information management initiatives will not begin until they are examined for compliance with the principles.
c. A conflict with a principle will be resolved by changing the framework of the initiative.

Principle 2: Maximize Benefits to the State

Statement
Information management decisions are made to provide maximum benefit to the State as a whole.

Rationale
Decisions made from a state-wide perspective have greater long-term value to citizens than decisions made from the perspective of any particular department.

Implications

a. Achieving maximum state-wide benefit will require changes in the way we plan and manage information. Technology alone will not bring about this change.
b. State level departments and organizations may have to concede their own preferences for the greater benefit of the entire state.
c. Application development priorities must be established by the state for the state which should be reflected in the implementation model.
d. Applications components should be shared across departmental boundaries and it should come out clearly in the implementation model.
e. Information management initiatives should be conducted in accordance with the defined plan. Individual departments should pursue information management initiatives, which conform to the priorities established by the State.

Principle 3: All State Organizations and Departments are responsible for Information Management

Statement
All organizations and departments in the State participate in information management decisions needed to accomplish State Portal's objectives.

Rationale
In order to ensure that information management is aligned with the State Portal's objectives, all organizations in the state must be involved in all aspects of the information management. The domain experts across the State and the technical staff responsible for developing and sustaining the information environment need to come together and jointly work as a team.

Implications
a. To operate as a team, every stakeholder at Centre, State, District, Block and other entities such as Universities and Partners, will need to accept responsibility for information management.
b. Commitment of resources will be required.

Principle 4: Provide Common Use Services

Statement
Development of services used across the state is preferred over the development of similar or duplicative services.

Rationale
Duplicative capability is expensive and may result in conflicting data.

Implications
a. Departments which depend on a capability which does not serve the entire state must change over to the replacement State-wide capability.
b. Departments and Organizations of State are suggested not to develop capabilities for their own use which are similar/ duplicative of State-wide capabilities. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.

Principle 5: Comply with Law and Policies defined for the State

Statement
State Portal should comply with all relevant laws, policies, and regulations of the state.

Rationale
State Portal policies should abide by laws, policies, and regulations of the State. However this should not prevent business process improvements that lead to changes in policies and regulations.

Implications
All departments and organizations must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data. Changes in the law and changes in regulations may drive changes in processes or applications.

Principle 6: IT Organization takes Responsibility of IT Systems

Statement
The IT organization is responsible for owning and implementing IT processes and infrastructure that enable solutions to meet user-defined requirements for functionality, service levels, cost, and delivery timing.

Rationale
Effectively align expectations with capabilities and costs so State Portal would operate in a cost-effective manner. Efficient and effective solutions have reasonable costs and clear benefits.

Implications
A well defined process for State Portal must be created to prioritize changes. The IT function must define processes to manage expectations. Data, application, and technology models must be created to enable integrated quality solutions and to maximize results.

Principle 7: Continuous Improvement through Feedback Collection and Statistical Analysis

Statement
The state portal should be capable of collecting and measuring data against set benchmarks.

Rationale
Use data to improve performance and user experience.

Implications
Implementing set statistical goals and techniques to measure goal achievement.
A well defined process for State Portal must be created to prioritize changes. The IT function must define processes to manage expectations. Data, application, and technology models must be created to enable integrated quality solutions and to maximize results.

3.1.3. Application Principles

Principle 1: Portal should be Scalable

Statement
State Portal should be scalable enough to accommodate new services offered for the citizens. It should also provide scalability in terms of providing services to additional number of citizens with time.

Rationale

a. With time growing number of citizens should be supported by State Portal.
b. The hardware, network related resources like more bandwidth etc. may need to be increased with growing user load.

Implications

a. State Portals will be required to have flexibility to add more memory, more bandwidth to support growing users.
b. Scalability requirements must be addressed clearly.
c. Scalability should be addressed at each and every component level.

Principle 2: Portal should be highly available

Statement

State Portal operations are maintained in spite of system interruptions.

Rationale

In order provide reliable service through State Portal, suitable steps should be taken from design to use. State Portal must be provided with the capability to continue their functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop State Portal activities. The State Portal functions must be capable of operating on alternative information delivery mechanisms. The backup plan must be in place to overcome hardware or software failures.

Implications

a. Dependency on shared system applications mandates that the risks of interruption of operations of State Portal must be established in advance and managed. Management includes but is not limited to periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to assure continuous availability through redundant or alternative capabilities.
b. Recoverability, redundancy, and maintainability should be addressed right from design time.
c. Techniques of Clustering, load balancing should be built in the architecture
d. State Portal will be required to have well defined version and change management plan

Principle 3: Portal should be Extensible

Statement

State Portals must be extensible in the sense that new features can be easily added or plugged-in without any significant changes to existing system.

Rationale

a. The State Portal would have to support new new features and services in future.
b. It is very much possible that new services and functions can also be derived; accordingly State Portal must be able to incorporate them.

Implications

a. State Portal will be able to add new information, features and services.
b. It will be extensible for newer features straightforwardly in future.

Principle 4: Portal should be Secure

Statement
State Portal must be secure in terms of authorization, authentication etc.

Rationale
a. The Portal being web based system usually incurs security issues typically through Cross-Site Scripting, SQL Injection, OS Commands, and a few other weaknesses.
b. The portal may involve the citizen's identity, online payment, inter department transactions, which is critical with respect to security.

Implications
a. State Portal is required to have protection against cross-site Scripting, SQL injection etc.
b. The portal may involve citizen's personal identity and financial data; any leak in confidentiality, authentication & authorization may lead to compromising confidential information.

Principle 5: Maximize Portability

Statement
State Portal should ensure portability of data & content on any platform as per the discretion of the state. Portal must be built using Open standards & provide interoperability with other platforms.

Rationale
a. The state portal shall be an integrated system working across state, district & block where different platforms are already in use delivering different government services.
b. Interoperability with different platforms shall save the cost & effort of redevelopment of e-gov solutions from time to time.
c. It shall also help in maintaining the technology competitiveness.

Implications
a. State Portal will be used in heterogeneous environment and it gives the flexibility in maintaining the system.
b. State Portal should avoid the situation of Vendor Lock-in.

Principle 6: Minimize Technology Dependence

Statement
The proposed State Portal should be able to interoperate and integrate with various technologies.

Rationale
This shall enable the states to choose different technology platforms. Otherwise rather than the user requirements, technology (which is nearing obsolescence and vendor dependence) becomes the driver.

Implications
a. This principle will require adopting standards to facilitate interoperability.
b. For Off-The-Shelf software tools and products, there will be provision to choose the technology platform.

Principle 7: Portal Should be Easy to Use

Statement
State Portal should be easy to use. The underlying technology should be transparent to users, so they can concentrate on tasks at hand.

Rationale
a. Compromising user friendliness would lead to loss of productivity.
b. Ease-of-use is a positive incentive for using State Portal.
c. Training is kept to a minimum, and the risk of using a system improperly is low.

Implications
a. State Portals will be required to have a common ‘‘look and feel’’ and support ergonomic requirements. Hence, the common look and feel standard must be designed and usability test criteria must be developed.
b. Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. Factors such as linguistics, regional language support such as Hindi for UP State, and proficiency in the use of technology have broad ramifications in determining the ease-of-use.

3.1.4. Data Principles

Principle 1: Data is an Asset

Statement
Data pertaining to State Portal is an asset that has value to the state and is managed accordingly.

Rationale
a. Data is a valuable resource; it has real, measurable value.
b. Accurate, timely data is critical to quality of service.
c. Most assets are carefully managed, and data is no exception.
d. Data must be carefully managed to ensure that we know where it is, can rely upon its accuracy, and can obtain it as and when it is needed.

Implications
a. All stake holders of State Portal should be trained to ensure that they understand the value of data, sharing of data, and accessibility to data.
b. Data quality will need to be measured and steps taken to improve data quality — it is probable that policy and procedures will need to be developed for this as well.
c. Since data is an asset of value, accountability for data must be defined.

Principle 2: Data is shared

Statement
State portal should allow sharing of data as necessary

Rationale
a. Timely access to accurate data is essential for improving the quality and efficiency of services. It is less costly to maintain timely, accurate data in a single service, and then share it, than it is to maintain duplicative data in multiple applications.
b. Shared data will result in improved quality of service we will rely on fewer (ultimately one virtual) sources. Electronically sharing data will result in increased efficiency when existing data entities can be used, without re-keying.

Implications
To enable data sharing common set of policies, procedures, and standards governing data management and access.

Principle 3: Data is Accessible

Statement
Data is accessible for State Portal users to perform their functions

Rationale
Wide access to data leads to efficient delivery of information and services, and affords timely response to information requests and service delivery. Using information must be considered from an State perspective to allow access by a wide variety of users.

Implications
a. Accessibility involves the ease with which users obtain information.
b. The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of users and their corresponding methods of access.
c. Access to data does not constitute understanding of the data. Personnel should take caution not to misinterpret information.
d. Access to data does not necessarily grant the user access rights to modify or disclose the data.

Principle 4: Data is secured

Statement
Data specific to State Portal is protected from unauthorized use and disclosure.

Rationale
a. Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information.
b. Existing laws and regulations require the safeguarding the privacy of data, while permitting free and open access.
c. Work-in-progress or not yet authorized for release, information must be protected to avoid unwarranted speculation, mis-interpretation, and inappropriate use.

Implications
a. Access to information should be based on a need-to-know policy.
b. In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level.
c. Data security safeguards can be put in place to restrict access to ‘‘view only’’, or ‘‘never see’’ basis.
d. Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorized access and manipulation.

3.1.5. Technology Principles

Principle 1: Changes should be driven by Business Requirements

Statement
Changes to functionality and technology should be made only in response to State Portal related needs.

Rationale

This principle will foster an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to IT changes. This is to ensure that the purpose of the information support (the transaction of business) is the basis for any proposed change. Unintended effects on business due to IT changes will be minimized. A change in technology may provide an opportunity to improve the business process and, hence, change business needs.

Implications

a. Changes in implementation will follow full examination of the proposed changes using the State IT architecture.
b. Change management processes conforming to this principle will be developed and implemented.

Principle 2: Control Technical Diversity

Statement

Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

Rationale

a. There is a real, non-trivial cost of infrastructure required to support alternative technologies.
b. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained. Limiting the use of diversified technologies will simplify maintainability and reduce costs.
c. The advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements.
d. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

Implications

a. Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.
b. Technology choices will be constrained by the choices available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and emplaced.

Principle 3: Promote Interoperability

Statement

Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology

Rationale

a. Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs.

b. Standards for interoperability additionally help ensure support from multiple vendors for their products.

Implications

a. Interoperability standards and industry standards will be followed unless there is a compelling reason to implement a non-standard solution.
b. A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.

3.2. Layered View

Architecture of State Portal would be based on the layered architecture pattern, where in each layer will be allocated defined set of functionality. Components of any layer shall only communicate with components of neighbouring layers. Layered view provides clear demarcation between various types of functionality required by State Portals. Following diagram depicts the various layers of State Portal.

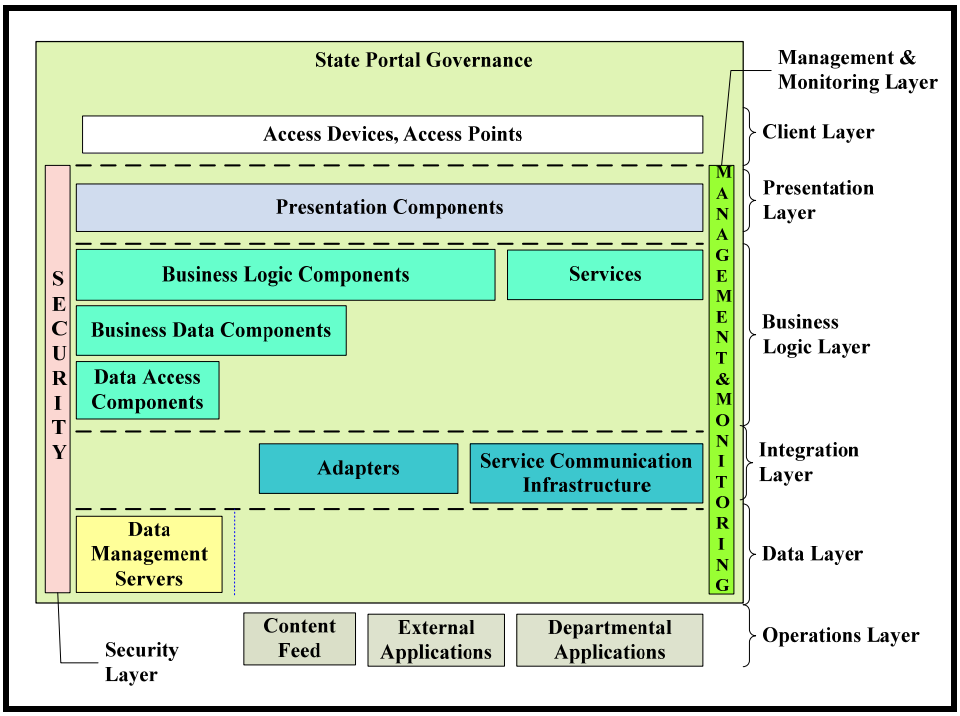

Figure 4. Layered View

State Portal functionality would be realized using commercial off the shelf software components as well as custom developing some of the components. COTS components would package various components belonging to different layers in the form of single packaged software. Therefore, information about, whether they are making use of layered architecture or not may not be available and it should not be a matter of concern. For example content management system will consist of presentation components, business logic components, business data components, and data access components and may use external data management server, security components etc.

In case of custom developed components, every component must belong to one and only one layer and should include one component only. This would help in achieving functional independence, low level of coupling and high level of cohesion between functional components

3.2.1. Client Layer

This layer depicts class of users, access points and access devices through which State Portals would be accessed. Following figures depicts the same pictorially.

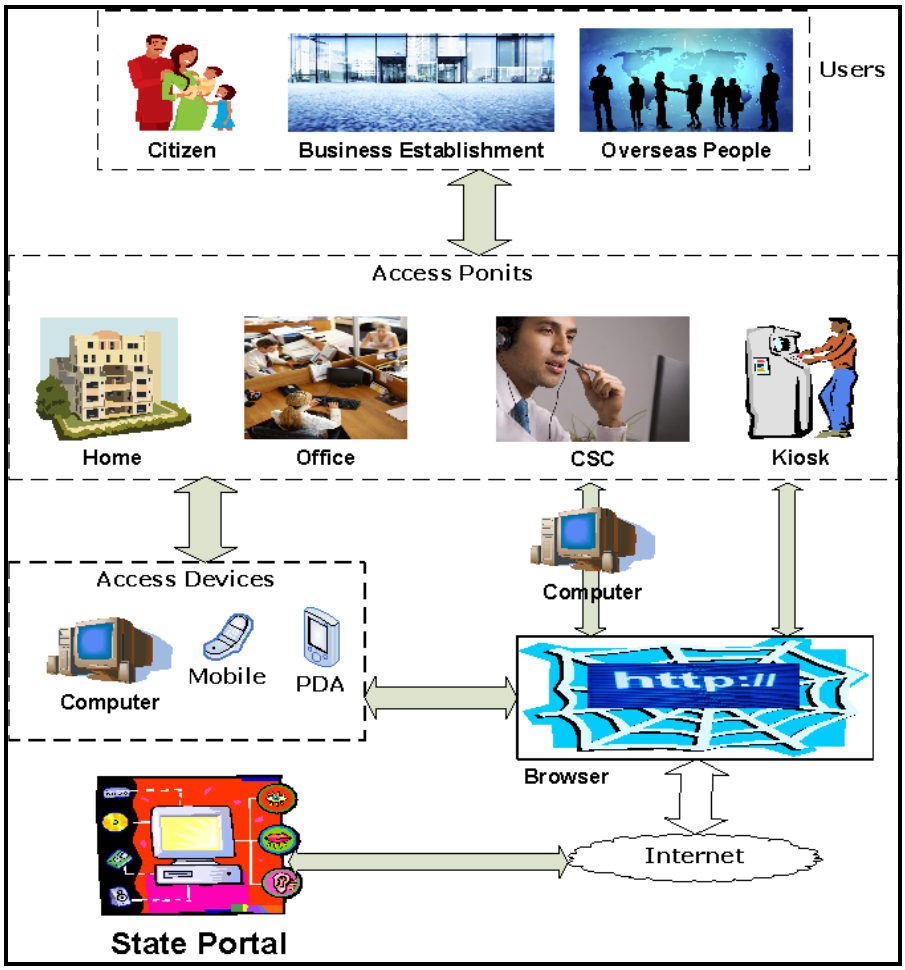

Figure 5. Access Points and Access Devices

State Portals would be accessed by citizens, businesses and overseas people using a web browser or mobile browser from above mentioned access devices or kiosks. Specific browsers versions, access points and access devices required to be supported would be finalized during the RFP process by states in accordance with the guidelines provided in "Suggested requirements for State Portal" section of this document.

3.2.2. Presentation Layer

Presentation layer will be responsible for receiving requests from the client layer, preparing response suitable to access devices and sending it. For handling dynamic content State Portal should use model view controller (MVC) design pattern , which provides loose coupling between content display format and request processing logic. Model component will be implemented as part of business logic layer. Controller and view components belong to the presentation layer. For static page requests, desired view of requested page is prepared after applying presentation rules.

3.2.3. Business Logic Layer

This layer contains all business logic related functionality of State Portal. Business logic layer consists of services, business logic components, business data components and data access components.

3.2.3.1. Services

Coarse grained business functionality, which maps to core business functions or activities, should be developed as services. Services should be implemented using multiple business logic components. Wrapper services use “service communication infrastructure” to communicate with COTS applications and departmental applications Loose coupling should be maintained between services and rest of the State Portal so that other government websites and applications can reuse them.

3.2.3.2. Business Logic Components

Business logic components should be used for implementing relatively fine grained business functionality. They would be responsible for processing business data. They access data using business data components and apply business rules.

3.2.3.3. Business Data Components

Business data components encapsulate business data, typically providing **C**reate, **R**ead, **U**pdate and **D**elete (CRUD) type of functionality. They access data from data layer using data access components. They use adapters for interacting with COTS software applications or products.

3.2.3.4. Data Access Components

Data access components are responsible for encapsulating access to data stores, database servers, connection management and data persistence. They should be implemented using Data Access Object (DAO) design pattern. These components help the State Portal to migrate to different database servers with ease.

3.2.4. Integration Layer

This layer contains components that are required to integrate with external bespoke or **C**ommercial **O**ff **T**he **S**helf (COTS) applications or products. It consists of adapters and service communication infrastructure. Adapter should be used for integrating with external bespoke or COTS applications in a scenario where service based integration is not appropriate or feasible. Service communication infrastructure should be used to integrate with departmental applications using services.

3.2.5. Data Layer

Data layer contains all data servers for managing structured data (RDBMS, OODBMS, XML DBMS etc.), unstructured data, data files, documents, images, and audio video files. Products like RDBMS, document management system, web content management system, content repository, directory server etc. belongs to this layer.

3.2.6. Operations Layer

Operations layer represents all external applications, including departmental applications, with which State Portal would be exchanging information. External applications includes COTS applications such as customer relationship management system, video stream server etc. which may be required in future to implement part of the State Portal functionality.

3.2.7. Management & Monitoring Layer

This layer contains administration, management and monitoring related functionality for network, links to internet, hardware nodes, system software and applications. Hardware nodes include all server class of computers. This layer cuts across all other layers. It should automate processes such as performance monitoring, network monitoring, incident management, patch deployment, data backup, disaster management etc.

3.2.8. Security Layer

This layer provides all security related functionality such as authentication, authorization, and single sign-on etc. It runs across all other layers i.e. components from all other layers may interact with security layer components. It should make available public content to all users without authentication. It authenticates users and allows them access only to those parts of the portal for which they are authorized. It should serve as one of the identified class of content in a secured manner using HTTPS protocol.

3.2.9. State Portal Governance Layer

State Portal governance layer is an all encompassing functionality, which acts as a base for all other layers. It provides governance and compliance for State Portal covering the entire life cycle of State Portal that involves conceptualization, development, pre-release, maintenance and sustenance phases. This layer is responsible to enforce design and run-time polices that the services should implement and confirm to. Refer to Governance and Compliance Framework document for more details.

3.3. Logical View

The State Portal Logical Architecture depicts the typical functional components and interaction among them. State Portal shall adopt service oriented architecture. Government departments would be exposing the functionality of departmental applications and citizens related functionality in the form of services. State Portal would be consuming these transactional government services to make them accessible on State Portal. Some of the functionality of State Portal such as search and web-form based services would also be exposed as services. Following diagram depicts the logical view.

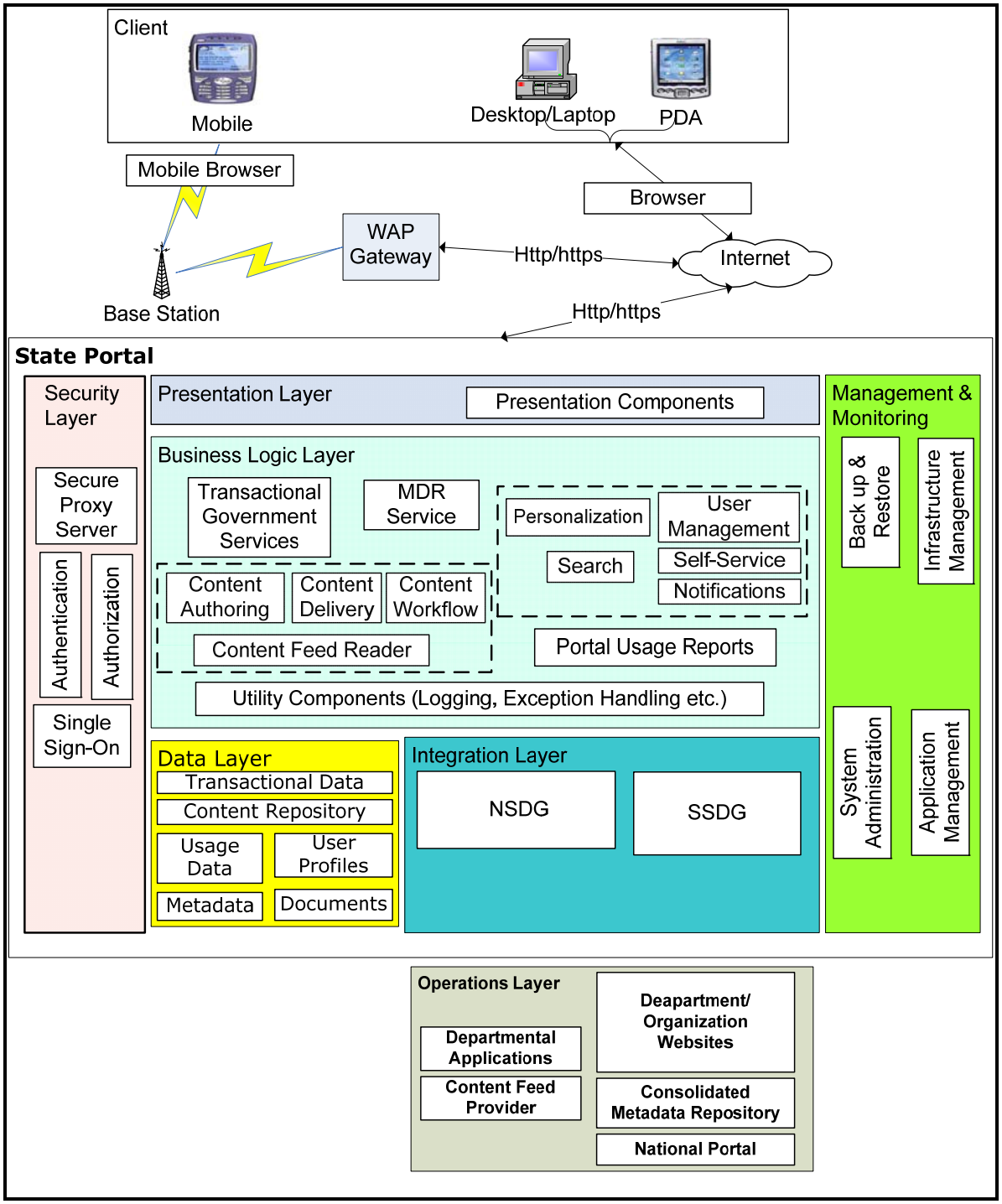

Figure 6. Logical View

3.3.1. Client Layer Entities

Client layer entities present the information provided by State Portal to users and handles the interaction between users and State Portal, including transactional government services. Client layer entities depend on type of access devices and access point. Standard web browser would be used on desktop and laptop computers, where as mobile or WAP browser will be used on cell phones and PDAs. Web browser will make use of technologies like HTML/XHTML, and Javascript, where as mobile browsers will make use of WML. WAP Gateways act as a bridge between the mobile world and the Internet and offers WAP services like encoding of WML pages, end-user authentication system, WML script compiling and converting WAP requests to HTTP requests and HTTP responses to WAP responses.

3.3.2. Presentation Layer Entities

3.3.2.1. Presentation Layer Components

Presentation layer contain user interface components, such as JSP, Servelet, JSP tags, HTML forms, CSS etc. These components typically contain code to perform functions such as configuring the visual appearance of content; accepting and validating user input; and acquiring and rendering data from business components. Every functional module would have some presentation components catering to user interface of the functional module.

3.3.2.2. Personalization

Personalization component of State Portal provide users to customize their preferences for better user experience. Increasingly, portals themselves offer users the ability to tailor the function available to best suit their needs. That part of personalization that is relevant for presentation is of direct concern to authors when creating web content that support multiple delivery contexts. State Portal should have template based user preferences.

3.3.3. Business Logic Layer Entities

Business logic layer modules will be implemented using services, business logic components, business data components and data access components. Following are the suggested scenarios for implementing functional modules.

3.3.3.1. Service Module

This functional module consists of services. Services should be developed using business logic components, business data components and data access components. External application would access these services through service communication infrastructure. Business logic components should use adapters and service communication infrastructure to communicate with external application and services respectively.

Typical communication flow would be:
Service operations -> Business logic components -> Business data components -> Data access components -> Data layer entities

3.3.3.1.1. Transactional Government Services

The Government services will provide required services for its citizens. These services will be provided by various departmental applications and consumed by State Portals using service communication components & SSDG.

3.3.3.1.2. Web-Form Services

Web-form service is a quick and simple approach for making available transactional government services on the State Portal. This approach may be used in a scenario, where state departments are yet to adopt computers and automate their processes, Refer “Integration and Management of Transactional Government Services” section for further details as well as Appendix C.

3.3.3.1.3. Metadata Replication Service (MDR Service)

MDR service would be -service responsible for replicating metadata from State Portal to “consolidated metadata repository” using Metadata Consolidation Server. Further details are provided in the “Content Integration” section.

3.3.3.2. Portal Functionality Module

This functional module implements portal related functionality, which is not required to be exposed as services. These functional modules would be developed using business logic components, business data components and data access components. Business logic components should use adapters and service communication infrastructure to communicate with external application and services respectively.

Typical communication flow would be:
Business logic components -> Business data components -> data access components -> Data layer entities

3.3.3.2.1. User Management

The user management function should address how identities and users are created, maintained, or revoked on termination.

3.3.3.2.2. Self-Service

Self-Service component will provide interface to let citizens manage their own profile information like user registration, reset passwords, update contact information, request for accessing government services if required, etc. During user registration process State Portal must provide CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part) where users should enter those details to register themselves with State Portal.

3.3.3.2.3. Reporting

State Portal Reporting component will be used to generate reports for following requirements but not limited to

1. Generate web analysis report to business users
2. Provide audit trail, i.e. author, date created, modifier, date modified, for each program.
3. Generate report for general application statistics, such as availability and average response time etc.

3.3.3.2.4. Search

State Portal will have search component to provide quick access to information, which includes documents, HTML pages, images, audio files, video files etc.

3.3.3.2.5. Notifications

State Portal should have facility to send notifications to its registered users. Users should be able to subscribe for some of the services like News Letters, Journals etc. On updates in these services, subscribed users of State Portal will get notifications by email.

3.3.3.3. Content Management Module

This functional module provides content management related functionality. This module should be realized by customizing off the shelf web content management system.

3.3.3.3.1. Content Delivery

State Portals will have large number of content objects and documents. It must manage complete life cycle of all content objects, for this purpose, It must use a content management system. Content management system include content aggregation/deployment tools, which make use of content objects from content management system's content repository for delivery of relevant content to State Portal users. For more information refer to "Content Management Framework" section.

3.3.3.3.2. Content Authoring

Content authoring component is for building web content that can be accessed by citizens via a wide variety of different devices with different capabilities. For more information refer to "Content Management Framework" section.

3.3.3.3.3. Content Workflow

Content workflow component of State Portal are content creation, reviews, submission, Metadata creation etc. For more information refer to "Content Management Framework" section.

3.3.3.3.4. Approach for Consuming Content Feeds

Content feeds are a type of electronically sourced content over internet using standard protocols and content formats such as RSS. RSS (Really Simple Syndication) is a XML file format, used for distributing news headlines on the Web (web syndication). It is used for frequently modified content such as news blogs etc. Following guidelines should be followed for receiving or consuming content feeds:

a. Design and develop a "feed reader" component to receive content feeds
b. Use job schedulers to download content feeds at defined time intervals and save into content repository as content object.
c. Always display original source, while displaying content received by means of feeds.
d. Content feeds must be received only from pre-approved sources.

3.3.3.4. Utility Components

State Portal would contain following list (but not limited to) of utility components to provide certain common functionality to other components.

a. Application level logging
b. Validations
c. Exception handling
d. Application level caching
e. Localization
f. Application configuration
g. Master data management
h. Session management

3.3.4. Integration Layer Entities

3.3.4.1. Service Communication Infrastructure (SSDG)

To access departmental services, State Portal would use service communication infrastructure component, which encapsulates

- Provide container environment for services
- Service interface

- Protocol translation
- Message routing
- Data transformation.

This component will be used by State Portal to access services provided by various government departments. It may be SSDG compliant or web services compliant or both. In some cases it may happen that some of the services would be developed and deployed as SSDG services where as few other services would be developed and deployed and web-services. As far as E-Form application under this project is concerned, it has to use the SSDG as the middleware. The application architecture will be as per the appendix C.

3.3.4.2. Adapters

In some cases some of the functionality of State Portal may be implemented using a COTS (**C**ommercial **O**ff **T**he **S**helf) software like CRM, SAP etc. In such a case availability of adapter should be ensured before finalizing the COTS software. State Portal should use the adapters for integrating with COTS software products or applications.

3.3.5. Data Layer Entities

3.3.5.1. Database Server

State Portal application will use Relational Database Management System (RDBMS) for persistent store of structured data.

3.3.5.2. Document Repository

Static content of State Portal such as documents, PDF files, images, audio/video files etc would be stored in document repository. These files should not be stored in database.

3.3.5.3. Content Repository

Content repository is an integral part of content management system. It is a database in which electronic documents and other web content are stored. A content repository may also contain pointers to files stored on a file server. However it is not necessary that content is stored in some database. Web content, stored in a common or single repository, can easily be accessed as and when necessary, reused in a variety of ways. It can facilitate creation, modification and approval of content from any location by authorized users. It can facilitate scheduled publication of content to a web-site in a controlled manner using a defined process. Refer “Content Management Framework” for further details.

3.3.5.4. Directory Server

A directory is a specialized database that is optimized for lookups. Unlike a traditional RDBMS, LDAP is not designed to show complex relationships. It is designed to efficiently process simple "selects" from anyone, anywhere over the Internet. It should be used for storing infrequently modified but frequently queried data such as application settings, user profiles, group data, policies, access control information etc. It should conform to LDAP standard.

3.3.5.5. Portal Usage Data

State Portal will capture the user experience information like how many hops a citizen is performing to reach a certain business service, usage of services, time spending on each service, State Portal hits/visits etc. Based on these inputs States will do the business processes optimization to provide better experience to its citizens. This data would be stored in relational database management system.

3.3.5.6. Security Data

Security data includes user passwords, roles, access control lists etc. This may be stored in directory server or in database tables. State portal implementation should facilitate using “access control server” products.

3.3.6. Operations Layer Entities

3.3.6.1. Service Registry and Repository

The service registry will provide a way for a consumer to find a departmental service. This will involve publishing a service’s description (in WSDL format) in a registry. A consumer iterates through a registry and obtains service's description.

Although much of the required information is already part of the service contract, the service repository will provide additional information, such as physical location, information about the provider, contact persons, usage fees, technical constraints, security issues, and available service levels.

3.3.6.2. State Department Applications

Department applications will provide required business services to state citizens channelling through State Portal using services. Various integration techniques are detailed out in “Integration and Management of Transactional Government Services” section.

3.3.6.3. Other State Departmental Applications

A State Portal will integrate with other states departmental applications using services. Integration techniques are detailed out in “Integration and Management of Transactional Government Services” section.

3.3.6.4. National Portal

State Portals integrate with National Portal to provide state services to citizens if users want to access required information using National Portal.

3.3.6.5. Content Feed Provider

Content feed providers provide content to State Portal. Following guidelines should be followed for content feeds

a. All feeds must be received only in electronic form
b. RSS standard should be used for live feeds
c. Wherever possible feeds should be received online

3.3.7. Management and Monitoring Layer Entities

Following table provides the brief description of various entities of management and monitoring layer.

	Entity	Description
1	Network Monitoring and Management	Network Monitoring and Management provides the ability to monitor and control network interconnect devices. Monitoring includes the collection and storage of key device parameters. Controlling includes the ability to affect the configuration of the device. The data that is collected will support the analysis of network traffic (availability, utilization, capacity, errors, and throughput) and the generation of associated network performance profiles.
2	Host / Node Monitoring and Management	Host Monitoring and Management provides the capability to monitor, display, detect, set, and report information about computer hosts and peripheral devices. Host parameters include accessibility, CPU usage, memory usage, swap usage, and disk usage etc. Device Management provides the capability to monitor and control other SNMP and non-SNMP devices.
3	Application Monitoring and Management	Application Monitoring and Management provides the capability to monitor and control software application processes on monitored computer hosts. In addition, to the collection and display of application parameters (performance, space, resource conditions, availability), application management allows for the initiation and termination of application software directly from the management console.
4	Security Management	Security Management provides the capability to manage user and network security across a distributed environment. User security includes the management of available authorization and authentication controls. Network security includes the ability to protect the managed environment from specific external accesses, intruder detection, virus protection, etc
5	Data Backup & Restore	Automated backup & restore components of State Portal will take backup of required content like application code/executables, data, content etc and restore as per defined policy or as and when required.
6	Disaster Management	State Portal should support business continuity. Therefore data should be replicated to DR site as per policy defined by the State so that DR site take over State Portal within defined time lines.
7	Host Administration	It is likely that production environment of State Portal would have number hosts or servers, possibly of multiple type in terms of hardware architecture, operating system and other infrastructure software. It is desirable that all servers could be administered from a single system using unified interface.
8	Application administration	User friendly web based interface should be provided for State Portal's administration related functionality.

3.4. Integration View

Integration Architecture specifies how various automated applications operating on different platforms can effectively work together. Integration techniques should be used when new application systems need to access existing application systems, while maximizing the investment in existing systems and platforms. State Portal will integrate with following external interfaces to provide services to citizens:

a. National Portal
b. State government departments (Departmental Applications)
c. Websites of government departments and organizations
d. National level service registry
e. National level service repository
f. State level service registry
g. State level service repository
h. Consolidated Metadata Repository

Following diagram depicts the high level overview of external interfaces.

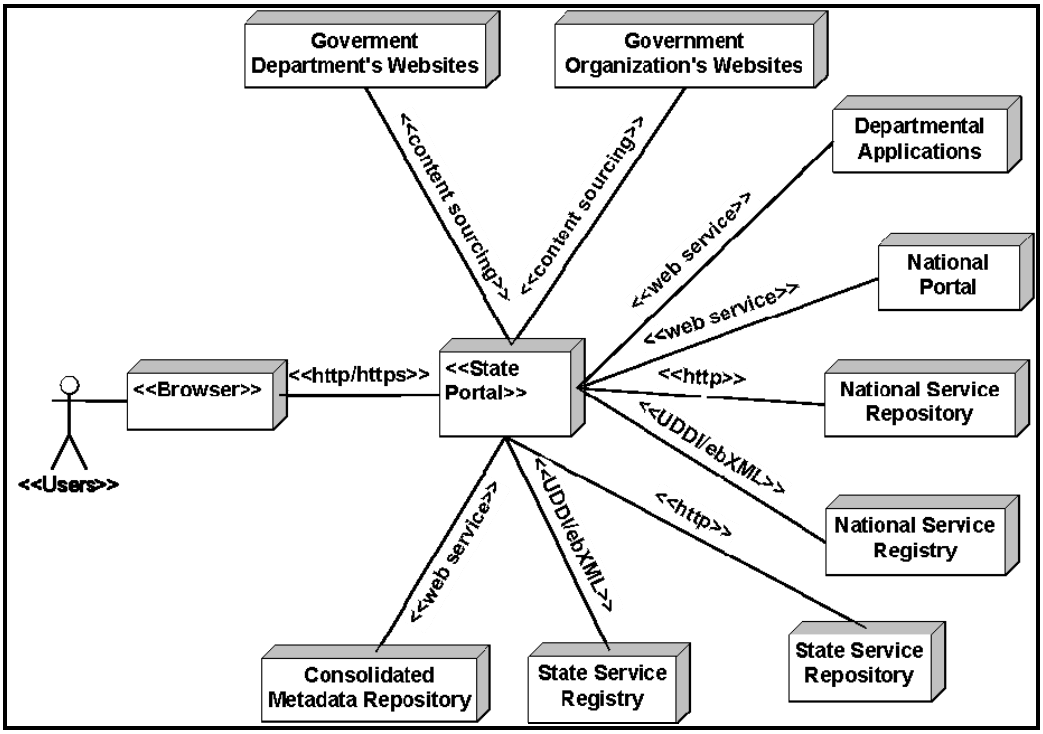

Figure 7. Application Integration View

3.4.1. Integration with Departmental Applications

"Integration and management of transactional government services" section explains the approach for integrating departmental applications with State Portal. During the implementation of transactional government services, adopted integration approach and rationale behind the chosen approach must be documented as part of architecture document. It is possible that transactional government services development may be combined with the development of State Portal for some or all of the services. As far as E-Form application under this project is concerned, it has to use the SSDG as the middleware. The application architecture will be as per the appendix C.

3.4.2. Content Integration

One of the major objectives of State Portal would be to integrate content from government department and organization's websites onto State Portal and provide interoperability with National Portal by means of keeping consolidated metadata repository updated with metadata of State Portal's content. "Content Integration" section explains

a. Various content sourcing scenarios, which would be adopted for sourcing content from various websites of departments and organizations
b. Approach for consolidating metadata from all state portals and
c. Approach for metadata based search within all State Portals, using "consolidated metadata repository"

3.5. Data View

Data and information are extremely valuable assets of the state. Data view establishes an infrastructure for providing access to high quality, consistent data wherever and whenever it is needed. This infrastructure is a prerequisite for fulfilling the requirement for data to be easily accessible and understandable by authorized end users and applications state wide. Following are the suggested best practices that state should follow managing data.

	Guideline	Description
	Data modeling	
1	**Design a flexible data model**	Design data models such that any future changes in business requirements can be accommodated.
2	**Minimize manual entry of data**	a. Use look-up tables where ever appropriate b. In the design phase, consider the values that may be input into a field.
3	**Use normalize and de-normalize patterns accordingly for performance**	a. The third normal form is the most commonly recommended form for the ER model. b. To increase the performance, a de-normalized database can be used as there can be fewer joins, or reduced access to multiple tables.
4	**Setup indexes and relationships**	a. Limit the number of indexes on databases that will be experiencing significant insert and update activity. When an insert is performed, not only is the record updated, but all the indexes are updated as well. b. Increase the number of indexes on databases where importance lies in retrieval time. c. Indexes can increase performance on retrieval time. d. Before creating a database, indexes, or data access programs, verify that all relationships have been documented.
5	**Archive and protect the data model**	Data models along with data must be archived and stored in a secured position to minimize the loss of data
	Metadata management	
6	**Keep consolidated metadata repository up-to-date**	The repository must be actively maintained (e.g., changes to metadata occur in the repository whenever new content is published at

		portals).
7	**Communicate and share metadata definition**	Information about standard metadata model should be easily available and communicated too all concerned parties.
8	**Define review process for metadata**	Design reviews are essential to ensure that shared content data is defined consistently across all portals. Design reviews also determine whether data that already exists is consistently defined and not redundantly stored
9	**Define metadata standard taking into consideration in use models**	Review the existing standard and proposed data elements in the consolidated metadata repository before implementing a new database to ensure data elements are defined according to standards.
10	**Govern metadata**	Follow a well defined process to govern all changes to metadata
	Data Accessibility	
11	**Use industry standard database connectivity**	Use industry standard tools like JDBC, ODBC, Hibernate etc to access database instead of vendor specific accessing tools. These standards are highly adaptive for changes in database without much effort and cost.
12	**Avoid usage of vendor specific extensions**	Database vendors have its own proprietary extensions to perform certain functionality on databases. Use ANSI-SQL standards rather than using these extensions otherwise there would be vendor lock-in.

3.6. Guidelines for Realizing Architectural Requirements

This section explains guiding architectural requirements. Specific architectural requirements would vary from state to state based on the factors like portal functionality, budgeted expenditure, usage frequency etc.

3.6.1. Performance

Following guidelines should be followed for achieving high performance:

a. Design such that deployment can be easily partitioned in terms or layers.
b. Use clustering and web-farms for deployment
c. Use proper load balancing algorithms such load gets distributed uniformly on all available nodes within a layer.
d. Use proper caching mechanism for master data and mostly read data like user profile information, configuration parameters etc
e. Perform time consuming tasks asynchronously
f. Most of the application level logging should be disabled in production code.
g. Code should be optimized using performance analysis tools before deploying in production environment.
h. SQL statements should be optimized using database server provided tools.

3.6.2. Scalability

Following are few guiding principles that a State Portal must adhere to in order to achieve the Scalability:

a. The solution should be developed using layered architecture with components spread across different architectural layers including hardware such as servers, storage, routers, physical networks , system software, as well as custom software/ application.
b. In the web server layer, provision should be there to add another instance of web server parallel to the existing web servers. The requests to all these servers may be balanced by a Load Balancer.
c. The application server instances will be clustered for high availability and scalability.
d. In the data layer, to serve the data requests in parallel, multiple instances of database must be deployed. Based on the load and other parameters, one can plan the clustering of underlying data sources.
e. The data archival and purging based on the requirement will also improves the scalability of the application.

3.6.3. High Availability

Following guidelines should be followed for achieving high availability

a. Network level
    i. Failover capable network elements such as routers, gateways etc.
    ii. Failover capable firewalls
    iii. Failover capable load balancers/dispatchers
    iv. Define clusters in combination with load balancing and failover to enhance the level of system availability and system response time.
b. Hardware level
    i. Use load balancing across web servers
    ii. Use application server cluster
    iii. Use data server cluster
    iv. Use RAID enabled data storage
c. COTS software level
    i. COTS entities deployed as a part of solution should be capable of high availability configuration
    ii. COTS software should support techniques of clustering, load balancing for achieving desired performance levels

d. Application software level
    i. All file names should be relative
    ii. Do not hardcode IP addresses
    iii. Do not bind anything with ‘local host’
    iv. Minimize amount of data saved in ‘http session object’
    v. Do not use static variables
    vi. Do not perform write operations on external files
    vii. Client applications that connect to the server application must retry and recover from temporary network failures

e. General guidelines
    i. Redundancy: Each element of an application must have a backup that can take over if the primary one fails.

    ii. Recoverable design: Any individual element is more available if it is stateless, but the application as a whole typically is stateful, and state must be preserved across potential failures.
    iii. Failure detection: To be recoverable, application may have to fail gracefully by saving transaction information, notifying a user or administrator, and performing appropriate application cleanup.
    iv. Application must be monitored in real time to ensure it is still running and triggering automatic failover if it isn't.

v. Operations management integration: Applications may incorporate management APIs to raise alerts, enable full monitoring and management, and write error logs that may also be monitored.
vi. Connection management: The client part of the application should be designed to handle connection failures and automatically establish connections to alternate providers.
vii. Transaction-aware design. Application design must explicitly anticipate handling of and recovery from transaction failures.

3.6.4. Portability

Following guidelines should be followed:

a. State Portal should ensure portability of Data & Content on any Platform as per the discretion of the state. Portal must be built using Open standards & provide interoperability with other platforms.

b. COTS products if used , should provide tools for exporting and importing data using open standards

3.6.5. Extensibility

Following are few guiding principles that a State Portal must adhere in order to achieve the extensibility:

a. Solution MUST be developed using Layered architecture
b. Solution MUST follow Object oriented methodology, which inherits extensibility
c. User defined attributes
d. Business rules
e. Configurable parameters

3.6.6. Multi Lingual User Interface

Following guidelines should be followed:

a. Unicode should be used for character encoding
b. Data server and content management system should support Unicode
c. All user interface elements such as strings, constants, UI labels, images, error messages etc. should be externalized and application should use language dependent mapping using a platform defined standard.
d. Launch the application in the default user interface language, and offer the option to change to other languages
e. Position language option at “sweet spot” on home page
f. Provide language option in respective language
g. Maintain consistency between pages of multiple languages

3.6.7. Interoperability

Interoperability should be achieved primarily by means of using an open standard based interface or a defined standard based interface. Following guidelines should be followed:

a. Use a service to integrate with “consolidated meta data repository”
b. Use services to integrate with departmental applications
c. COTS products used for implementing state portal must support import and export of data using either open standards or XML format.
d. Browser based interface to content repository should be based on XML.

3.6.8. Universal Accessibility

Detailed guidelines are provided in the document "Guidelines for Indian Government Websites" of Data Centre and Web Services Division of NIC. This document is available at http://web.guidelines.gov.in. State Portal should comply with these guidelines.

3.6.9. Security

The security layer will provide various security services to State Portal across multiple layers. The security layer should be implemented using Identity and Access management tools to manage user identities, roles, security policies, organizations/businesses, authentication, authorization, access control and other additional services like data encryption and SSL. The State Portal Security Services are primarily authentication, authorization, Portal Access Control, Services Access Control, Secured Pages, Single-Sign on, security event logging and Audit trailing.

3.6.9.1. 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. Following guidelines should be followed for authenticating users:

a. Authenticate users prior to accessing services.
    i. Allowing only authenticated users to access system resources protects those resources from inappropriate access.
    ii. Authenticating users are the basis for providing accountability.
b. Use Public Key / Private Key technology for authentication when digital signatures are required.
    i. Public Key / Private key technology is the most widely accepted form of digital signatures.
    ii. Digital signatures are central for most electronic business.
c. Use token-based or strong password based authentication where public key certificates are not feasible.
    i. Token-based systems are an improvement over passwords.
    ii. Where token-based identification and authentication is not possible, a password policy based on best practices can provide an acceptable level of security.
d. Use a State-wide public key infrastructure.
    i. Collaboration and co-operation will be required to support security services across the states and departments.
    ii. A unified approach to a Public Key infrastructure enables the state to respond to changing requirements and conditions.
    iii. A fragmented approach to a public key infrastructure will complicate administration and management of security across the state.
e. CAPTCHA technique should be used for protecting automated form submission during important user input forms.

3.6.9.2. Authorization

Authorization answers the question: "Are you allowed to do what you are asking or trying to do?" Access to applications, the data they process and database modifications must be carefully controlled. Authorization is the permission to use a computer resource. Access is the ability to do something with a computer resource. Access controls are the technical means to enforce permissions. They allow control over what information a user can use, the applications they can run and the modifications they can make. Access controls may be built into the operating system, may be incorporated into application programs or major utilities, or may be implemented in add-on security packages that are installed into an operating system. Access controls may also be present in components that control communications between computers.

Authorization component should make sure that users must be able to access whatever information they have got access to. An authorized system user should be allowed to define the various available roles in the system. Each user should be mapped to the respective role. Based on this the user should be provided access to various available functionalities of State Portal. State Portal should provide role based access control at the page level.

3.6.9.3. Portal Access Control

State Portal ACL (Access Control List) should contain list of authorizations such as read, write, and delete that is given to a subject who may be attached to objects. An ACL lists the type of access to an object that each user or a group of users is allowed or denied. In order to make ACLs shorter and more manageable, users with the same access rights are often put into security groups.

3.6.9.4. Service Access Control

Securing Services is one of the key challenges in services based environment. The immediate security level that can be provided on Services is securing the transport protocol used to transmit the SOAP requests and responses. Service should be made available through HTTP, SSL will be a good way to fulfil security requirements. SSL provides integrity and confidentiality for the communication between the service provider and service consumer.

3.6.9.5. Secured Pages

State Portal will have public and protected pages based on the secure information of the functionality. This secure information should be transferred using secured protocol like HTTPS. Pages like User Login, Transactional pages where credit card information etc will be considered as secured pages.

3.6.9.6. Secure Proxy Server

The secure proxy server intercepts users whenever they request to access the secured information. URL will be routed to this component, whereas it will challenge (User Id and Password) the user for authentication if user accesses the secured information.

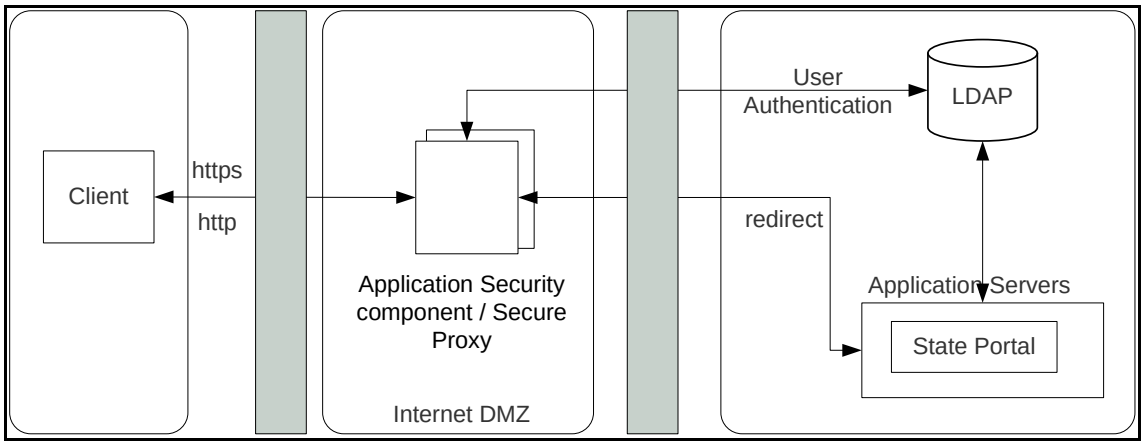

Figure 8. Access Security View

3.6.9.7. Single Sign-on

Within the State Portal, the citizen interacts with State Portal and in turn interact with multiple back-end applications/departments/portals such as RTI, Pension, land records etc. SSO facilitates seamless user navigation across multiple departmental

applications/portals and avoids multiple logins. In case of unsupported applications customised mechanisms will be used to achieve the single sign-on.

3.6.9.8. Activity Logging

The State Portal should be able to log and react to (such as storing the event for reporting later, or generating an alert) events generated from various source components and takes specific actions based on the business requirement. A centralized Event Logging framework will be used by most of the software components/providers in the State Portal. The information logged using this Event Logging framework, will be stored at a central location via messaging channels. Typical consumption of this information could involve "business transaction reporting", or "audit trail of a system configuration changes (business rule change, security policy change etc.)".

3.6.9.9. Audit Trail

The State Portal should have a mechanism that captures all changes (add, update, delete) to citizens data. These include changes to data that may have occurred outside the application functionality.

3.6.9.10. Data Security

The state's data is a very valuable resource, and establishing a secure data environment is a key component of the State's Technical Architecture, particularly since more and more applications use the Internet to access data. It is critical that the state's data be protected against any unauthorized access. Data security should be designed to protect data against the following threats:

1. Unauthorized use of the database or application.
2. Accidental modifications and deletions.
3. Confidentiality and integrity breeches for data in data transport and physical storage.
4. Disasters.

Following guidelines should be followed for securing the data.

	Guideline	Description
1	**Use generic, protected user accounts for direct database access to streamline administration, ensure scalability, and protect against non-application data access.**	a. Access to the database should be provided only through application and no direct access to users b. The user accounts must be defined only at one directory repository with standard protocol to access it.
2	**Manage sensitive data**	a. Sensitive data must be secured on a database server with proper policies and procedures in place. b. Ensure that passwords are encrypted both inside application executables and across the transport layer. c. A backup and recovery plan for databases must be in place.
3	**Record information about users and their updates to data for audit trail purposes**	The information that can be captured by the application includes: a. The user account the user logged in with. b. The TCP/IP addresses the connected user's

	Guideline	Description
		workstation. c. The certificate information (if using certificates) about that user. d. The old values that was stored in the record(s) before the modification. e. The new values that were input to the record(s).
4	**Implement transaction logging so recovery of original data is possible and protect the transaction log.**	a. Transaction logging records activity on the database and can be used to roll back a transaction. b. Protect the transaction log through access control and backup. Only the database should be writing to the transaction log. All other access should be read only. c. The transaction log should be located on a separate physical disk if possible. If not possible, use RAID to protect the integrity of the log file.
5	**Implement security scanning and intrusion detection.**	a. Scan the database and database server for potential weaknesses before they become a problem. b. Monitor the database for possible intrusions. For example, monitor and alert when multiple invalid login attempts occur. Intrusion detection protects the database server from attacks from both sides of the firewall (e.g., internal network, WAN, or Internet). c. Audit logins, user account creation, and failed login attempts.
6	**Ensure data integrity by securing data movement or data transport.**	a. When high impact, sensitive data is transported through the LAN, WAN, or Internet, ensure that the data is encrypted and protected from alterations. This can be accomplished through Secured Socket Layers (SSL) or Virtual Private Network (VPN). b. Other types of data must be encrypted and protected if there is a risk of the data being altered.
7	**Protect source code in data access rules, particularly if it contains password information.**	a. On the back end, an application needs to store account and password information in order to authenticate to a database or other application service. Protect the source code from unauthorized viewing. b. Store passwords in an encrypted format when possible.
8	**Protect and encrypt data for sensitive applications**	When it is absolutely necessary to store sensitive data, it should be stored in encrypted form..
9	**Change all default database**	System administrator accounts have full access

	Guideline	Description
	passwords	to all databases in a database server. Hackers often attempt a login to a system administrator account using a default password. As soon as a database is set up, change all default passwords.

3.7. Standard Architectural Components

Following is the list of minimum suggested architectural components for realizing the State Portal:

Layer	Entities
Client layer	• Access devices: Desktop / Laptop, Mobile, PDA • Browser: Internet Explorer, Mozilla Firefox
Security layer	• Secure Proxy Server • Authentication • Single Sign-On • Authorization
Presentation layer	• Page layouts • UI templates • Style sheets • Client side validation libraries
Business Logic layer	• Transactional Government Services • Metadata Replication Service • User Management • Personalization • Self-Service • Content Authoring • Content Workflow • Content Delivery • Portal Usage Reports • Search • Application Logging • Exception Handling
Management & Monitoring layer	• Application Management • Infrastructure Management • Backup and Restore • System Administration tools
Data layer	• Database Server • Directory Server • Documents Repository • Portal Usage Database • Content Repository
Operations layer	• Service Registry • Service Repository • Content feed providers