(Draft) Policy Document
on
"Identity and Access Management (IAM)"

for implementation under

National e-Governance Program (NeGP)

Prepared by
Task Force on "Identity and Access Management"
(Constituted Vide Office Memorandum No. 2(10)/2006-eGovStandards
dated 31st October 2006)

VERSION 0.7

APRIL, 2007

e-Governance Standards Division
National Informatics Centre
Department of Information Technology
Ministry of Communications and Information Technology
(GOVERNMENT OF INDIA)
NEW DELHI

Policy Document

on

IDENTITY AND ACCESS MANAGEMENT (IAM)

for implementation under

National e-Governance Program (NeGP)

Document No.

Vision

Identity and Access Management (IAM) is to support common identity needs of all transactions arising out of various e-Government Programs (G2G, G2E, G2B, G2C and G2X), reduce costs of government and enhance service quality, under an obligation to preserve individual's privacy and to secure identity information.

Mission

To build a comprehensive Identity and Access Management (IAM) System that will provide secure access to resources, reduce access costs, strengthen integrity, security and comply with regulatory requirements.

Objective

This document defines the policy for "control and management" of digital identity of all users and resources for smooth operationalisation of various e-Government Programs in the country.

Preamble

Use of Internet technology and access mechanisms (i.e. Internets as well as Intranets) as a primary medium for official transactions has brought in a new set of concerns viz., security, privacy and management. Deploying an Identity and Access Management (IAM) solution entails a complex set of challenges to balance: the need for security and privacy, demand for online services, and issuance and management of digital identities, to make e-Government Programs and their services a reality. This requires, among the others, **an integrated framework** of laws, policies, operational best practices and guidelines, technology, and institutionalization.

Background

The Government of India has launched the National e-Governance Action Plan (NeGP) with the intent to support the growth of e-governance within the country. The Plan envisages creation of right environments to implement G2G, G2B, G2E and G2C services.

Keeping in view of the strategic and contemporary importance of standards for e-Governance, an Apex body has been constituted under the chairmanship of Secretary, DIT (Department of Information Technology) with senior representatives from Government, NASSCOM, Bureau of Indian Standards (BIS), etc. with a mandate to approve, notify and enforce the Standards formulated by various Working Groups and to oversee that they are in accordance with international practices in this regard. The following areas have been identified to begin with:

1. Network and Information Security
2. Metadata and Data Standards for Application Domains
3. Quality and Documentation
4. Localization and Language Technology Standards
5. Technical Standards and e-Governance Architecture

6. Legal Enablement of ICT Systems

Working Groups have been constituted for formulating the standards in all the areas mentioned above with members from DIT, Associations, Industry, Academia, representatives from Central & State Government etc. One of the important outcomes of this initiative is to herald a standards-based approach in all e-Governance application developments by multiple agencies. e-Governance Standards will have far reaching influence on the accelerated growth and spread of e-Governance across the country.

It is considered important that the standards should allow seamless access and interoperability between all kinds of e-governance applications, bridging existing legacy applications and their codes wherever applicable and possible. This effort will also support both NeGP Mission Mode Projects as well as the other projects of the Central and State Governments.

As a step towards e-Governance Standards for Identity and Access Management (IAM), a National summit was organized on July 27-28, 2006 at NIC HQrs, New Delhi. The agenda and session topics for this summit were as follows:-

- Role of IAM in eGovernance applications
- Necessity for Standards in IAM
- Supporting Technologies for achieving effective IAM
- Importance of Services oriented approach for IAM
- Key processes of IAM
- Need of PKI in IM to support assurance
- Significance of Federated Identity environment
- Strategy of implementing IAM in Government and related legal issues
- Presentation of solutions from IT industry

As a follow up of this Summit, a Task force was constituted vide Office Memorandum No. 2(10)/2006-eGovStandards dated 31st October 2006 for the preparation of a policy document on "Identity and Access Management" for implementation under the National e-Governance Programme (NeGP). The composition of the Task Force is given in Annexure – VI. A series of meetings of the Task Force were arranged to discuss the policy issues of the Identity and Access Management. This document is based on the outcomes of the National Summit and points discussed during the Task Force Meetings.

Metadata Elements

Sl. No	Metadata Element	Definition of Element
1.	Title	Policy Document on "Identity and Access Management (IAM)"
2.	Identifier	To be provided by the publisher at the time of publishing
3.	Document version	April, 2007
4.	Date Issued	To be provided by the publisher at the time of publishing
5.	Type of Standard Document	Policy
6.	Category of Standard	Recommended and emerging
7.	Brief Description	User's identities are at the core of any operation. Anyone desires to access service needs to prove his identity. When these services are offered online, digital identities come in picture. Identities are required for all users. An integrated and comprehensive Identity and Access Management approach is must for addressing identity related issues in providing e-Government services. The policy document addresses the major components and issues faced while implementing Identity and Access Management solutions.
8.	Target Audience	• Multiple agencies involved in e-Governance applications development and implementation

		• Government Departments • Business Organizations • Citizens
9.	Owner	National Informatics Centre, Department of Information Technology, Ministry of Communications and Information Technology, Govt. of India
10.	Creator	Task Force on "Identity and Access Management" (Constituted Vide Office Memorandum No. 2(10)/2006-eGovStandards dated 31st October 2006)
11.	Contributor	Members of the Task Force, Various Technology Solution Providers
12.	Publisher	a. During Standard Formulation Process - NIC
		b. After Approval by Apex Body - STQC
		c. At National Level
13.	Subject	Digital Identity and Access Management
14.	Subject. Category	Refer to the list of subjects
15.	Coverage.Spatial	India
16.	Format	Microsoft Word
17.	Language	English
18.	Source	
19.	Keywords	Identity, Access, Access Control, Identity and Access Management, Policy, E-Governance Policy, Authentication, Authorization, Single-Sign-On, Identity Federation
20.	Rights. Copyright	To be provided by the publisher at the time of

		publishing
21.	Distribution Category	Open to All / Limited to target audience only / Restricted (To be provided by the publisher at the time of publishing)

Table of Contents

1. Scope

1.1.Scope of Identity and Access Management

To establish a scalable, extensible and secure "standards" based framework for identity data acquisition, storage and its access by the stakeholders for the envisaged benefits.

1.2.Purpose for formulation of policy guidelines

Many e-Governance initiatives are done in isolation. In the absence of any standards the integration of e-Governance applications becomes difficult. Most of the e-Governance applications build their own mechanism for Identity and Access Management resulting in identity silos, duplicate efforts and disjointed collection of service points. These applications are seldom interoperable even though many have similar features and functionalities. The formulation of e-Governance standards guidelines will promote the uniform, consistent and coherent approach which in turn will help in building interoperable applications to deliver integrated services to citizens.

1.3.Description of Identity and Access Management

1.3.1.Importance of Identity and Access Management

High expectations of the citizens / customers for improved services and requirement of the government and private organizations to be efficient has resulted in the proliferation of online services. Highly sophisticated information technology based solutions and telecommunication-networked environments have made it possible for the organizations to provide the user the fastest and easiest means to avail the services online. Organizations want to deliver the online services securely without any risk of unauthorized access to their resources. As transactions are carried out invisibly there is need to know who is at the other end of the transaction. On the other hand user requires an

organization to protect integrity and confidentiality of their identity information and ensure safety of their transaction. In these circumstances identity has become a key asset to organizations.

An integrated and comprehensive Identity and Access Management approach can address all the identity related issues of the organizations as well as users. Identities need to be managed to facilitate the right access to the right resources. Identity and Access Management provides consistent, efficient and secure method to manage identities both internally and externally.

1.3.2. Envisaged Benefits

The use of the IAM system is expected to provide the following benefits:

- Elimination or significant reduction in storing duplicate identities
- A single and comprehensive view of an identity
- Interoperability of applications by enforcement of Data standardization through IAM
- Single Sign On Facility to the Users
- More Secure Access
- Reduction in the risk of unauthorized access to and modification or destruction of government information assets.
- Control, enforce and monitor access to resources through auditing
- Improved user's participation
- Improved performance
- Improved service delivery to citizen
- Improved regulatory capabilities
- Improved availability

1.3.3. Key Objectives of the IAM System

- To create federated repository of identity resources of all Identities with their entitlements.
- To provide stakeholders on-line access to various resources of their interest in a secure manner.
- To allow existing applications to use IAM within the IAM security framework.
- To reduce the Total Cost of Ownership of the IAM system.

1.3.4.Some Important Attributes

The System should be:

- Standard Based
- Scalable
- Extensible
- Secure / trustable
- Available
- Robust

Technology and Implementation Issues have been discussed In Annexure-I. It depicts Identity and Access Management Framework, Identity and Access Management Life Cycle as well as gives the roadmap for implementing various components of IAM.

2. Target Audience

- Multiple agencies involved in e-Governance applications development and implementation
- Government Departments
- Business Organizations
- Citizens

3. Type of Standards Document

The document is the policy document on "Identity and Access Management (IAM)"

3.1.Enforced Category

The policy document is the recommendations of the Task Force for implementing Identity and Access Management solutions under National e-Governance Program (NeGP) which is an emerging technology.

4. Definitions and Acronyms

4.1.Key Definitions

4.1.1.Identity

Identity is a set of attributes that uniquely identifies entity. An entity can be anything that the Government of India wishes to uniquely identify for its purposes. Identity is the presentation of the entity. Entity can be a person, group of persons, device, organization, service etc.
The same entity may have multiple identities as people perform many social, economic and political functions, for example a person can be a citizen, a trader, an employee, etc. Each role may require different set of attributes to establish the identity. Sometimes individuals are known by different names in different context. However, identity uniquely represents entity.
A digital identity is a set of claims made by one digital subject about itself or another digital subject.

4.1.2.Identity and Access Management

Identity and Access Management (IAM) comprises of set of business processes, technologies, supporting infrastructure and policies to create, maintain and use digital identities within a legal framework.

4.1.3.Authentication

Authentication is a process of checking the credentials of an identity against the values in an identity store.

4.1.4.Authorization

The process of determining the user's entitlements for accessing the resource against the permissions configured on that resource.

More definitions and Acronyms have been provided in Annexure – V.

5. Policy

*5.1.*Citizen Identities

The person accessing e-Governance services must be identified to the defined level for accessing these services. An individual may register for a government service on their own account or as a representative of an organization (natural, corporate or legal). If an individual is registering as a representative of an organisation it is necessary to verify and validate the a) Identity of the individual b) Identity of the organization c) Authority of the individual to register on behalf of the organisation.

5.2.Owner of identities

Identity Store should be maintained by issuer of credentials.

5.3.Process of Identification

The person accessing e-Governance services needs the identification. Birth Certificate, first point of interaction with the government can be taken as the starting point. Identity Schema should be decided. The minimal set of attributes required for identification of a person can be taken as level 0 identification.

*5.4.*Interoperability and Standards

5.4.1.Interoperability

Different organizations deploy various applications using different technology platforms and environments. These applications should be seamlessly interoperable with each other including the requirement of sharing the authentication and authorization information and maintaining the consistency of identity information as it flows through the processes. Interoperability requires standards on several levels. Harmonization of approaches through the use of standard protocols, guidelines and agreed best practices is necessary to ensure inter-working between different applications within organization as well as across

organizations.

5.4.2. Standards

System should be based on multiple **open standards** for portability and interoperability. The use of specialized software or proprietary vendor protocol should be avoided. In order to interlink a variety of operating platforms, platform neutral common authentication and authorization systems based on nationally, and internationally accepted standards should be selected. Infrastructure vendors should support a variety of open standards to provide flexibility and maneuverability. Standards are now available to address the issues of operability and interoperability. These standards have been listed in Annexure- II.

5.5. Identity Management

5.5.1. Identity Stores

Organization can have single or multiple identity stores. Multiple Identity Stores can exist across different organizations / departments / divisions / applications. These Identity stores can be managed centrally or in distributed environment using delegation of administration.

5.5.2. Aggregation and Synchronization

Integrity of the identities in multiple identity stores should be maintained by Aggregation and Synchronization of these identity stores. The appropriate Identity Aggregations and Synchronization should be used to integrate systems to share their identity information and create and maintain the same entitlements through common policies. It must be capable to handle naming convention challenges and also must have ability to map different identifiers of a single individual used in different context.

5.5.3.Levels of Assurance of identities

The level of assurance of identities to access resource / service depends on the sensitivity and/or intrinsic value of that resource / service. The level of assurance of identities should be determined by the risk factor involved when the identity is compromised.

5.5.4. Provisioning / de-provisioning of Identities

User registration is must for user identification and can be completed by government agency or can be delegated to trusted third party on agreed terms and conditions. Identifiers must be assigned which is unique. The mechanism for receiving a credential should be closely scrutinized. Orphaned accounts should be disabled / deleted quickly to avoid unauthorized access.

5.6.Security

Identity and Access Management should allow organizations to extend access to their information systems without compromising security. It should support an organization's total security management strategy.

For critical and sensitive applications all facets of information security should be addressed such as confidentiality, integrity, availability and non-repudiation. Organisations should have Risk Management Plan in place if identity is compromised.

5.7.Access Management

5.7.1.Authentication

Depending upon the requirement of the level of security the weak authentication or strong authentication should be implemented. The required level of security should be determined based on the sensitivity / intrinsic value of the resource. For high security environments suitable combinations of what you know (Identity Number and/ or password), what you have (a card or token) and who are you (multiple forms of biometrics) should be used to add strength in authentication process and to increase convenience.

5.7.1.1.Single Sign On

Single Sign On capabilities should be provided for the accessing the resources wherever possible. Only in case of critical application or before performing particular sensitive operation, the user may be prompted to provide authentication credential again.

5.7.2.Authorizations

Authorization can be implemented through role based access control or through Access Control Lists. A role can be defined as Administrator, Manager, Creator, Writer, Reader, etc. These roles are then mapped to application permissions such as create, delete, read record / file / table / database etc. Administrator can create the roles and assign permissions to these roles.

5.7.3.Access Control

While implementing Identity and Access Management, access policies should be in place as per the requirements of the organization. Access policies should be defined in terms of role, resource, operation and restriction. These should be defined by resource owner. The access can be role based (Manager, Administrator etc.), rule based (Membership of a group, specific rule based such as time, location etc.) or identity based.
With the help of Identity and Access Management, organisations should be able to associate access rights with a role within the organization. Identity and Access Management should dynamically assign and automatically change access rights based on changes in user role. Organisations should be able to provide the access by precisely managing entitlements and modifying or terminating access rights promptly.

5.7.4.Audit and Reporting

Organizations should detail what types of auditing are required and how audit information is captured, stored and used. Integrated Identity and Access Management systems should provide auditable proof that only appropriate access is granted to critical data. Security auditing should provide audit trail of

user activities, access violations, authentication events, authorization events and changes to directory objects. It should consolidate log and events, compile reports and trigger alarms and alerts. It should also be able to monitor activities of the Super user accounts, System administrators and system operators who can gain unrestricted access to virtually all files and commands and thus making the resources vulnerable to abuse.

Required audit records should be produced and kept for an agreed period to assist future investigations and access control monitoring.

5.8.Accessibility

While implementing Identity and Access Management system care should be taken that the authorized person should not be deprived of access due to physical disability, educational limitations, language barriers, non-availability of infrastructure like connectivity.

In addition to traditional delivery systems, the Identity and Access Management services should be made available to other delivery channels as they emerge. This enables the use of common authentication mechanism across delivery channels, wherever appropriate and within constraints of the channel.

5.9.Legal Issues

5.9.1.Regulatory Compliance

Regulatory Compliance of the Identity and Access Management System should be achieved through the implementation of comprehensive security, audit and access policies. It should ensure that organizations meet the applicable privacy, authentication, authorization and auditing requirements mandated by any and all applicable regulations, legislations and contractual clauses. Identity and Access Management should ensure that all the users must be uniquely identified, all their access to protected resources must be tightly controlled, access to these resources must be based on a defined security policy and access and security events must be easily and fully auditable.

The various agreements should be developed and implemented between end-users, application service providers and identifier and credential issuers. These

agreements will specify the various obligations and remedies for the participants in respects of liabilities, dispute solution, privacy and operational performance. These agreements should be homogenized across government.

In Governance, the access, access control, supervision and regulations are driven by statutory and constitutional empowerments, power delegations and authorizations. In this context, any e-Governance initiative necessarily demands technology compatibility with related statutes. It is therefore imperative to integrate empowerments, delegations and authorizations with technology capabilities. To enable this compliance, as and when a Government activity is electronically functionalized the related statutes need to be examined in detail for necessary change. As an alternate, the existing Information Technology Act could accommodate a broad amendment to enable all e-Governance initiatives.

5.9.2. Privacy

The Identity and Access Management system should have mechanism to protect identity data from unauthorized use and distribution. Organisations should maintain the confidentiality, integrity and privacy of the Identity data.

5.10. Acceptance

While implementing the Identity and Access Management system, all stakeholders should be consulted as their acceptance of the system is very important for successful implementation.

5.11. Identity Federation

There should be formal agreements between the participating members in federation on the policies such as authentication, authorization, privacy of identity information, confidentiality or non-disclosure agreements, legal and contractual obligations, maintenance and administration of the identities, government regulations to be followed for cross-country, cross-region federations, standards, auditing requirements, contractual security obligations and roles and responsibilities of the members.

5.12.Classification and Controls

Organization's Resources and Services must be classified in order to achieve and maintain appropriate level of protection of these resources and to control their access. Organizations should adopt a standardized approach to the classification of resources/services. The classification of resources/services can be in terms of its value, sensitivity, priority and criticality from privacy, commercial or other (national security) perspective to the organization. An information classification system should also indicate the need for special handling measures.

5.13.Procedures

All procedures for all processes of Identity and Access Management should be defined, documented, maintained and made available to users who need them. The well defined set of procedures creates the foundation for Identity policy of the organisation.

5.14.Capacity Building, Awareness Campaign

For the successful implementation of Identity and Access Management System all the stakeholders should be provided different level of training. Employees should be educated and trained on implementing IAM. The privacy role played by security services must be emphasized. Users should be educated for usage of authentication mechanism and should be made aware of how to protect their identity and privacy information.

*5.15.*Administration and Governance Framework

The governance structure should be set up for steering the implementation of comprehensive and integrated Identity and Access Management system.

6. Recommendations for Procedures/ Practice to be followed

- The rules, regulations, instructions, manuals and records of Government of India should include detailed guidelines for government agencies to implement Identity and Access Management System while providing online services. It should also help government agencies and other stakeholders to

understand potential risks involved and requirements to address them while adopting the Identity and Access Management solutions.

- Laws specific to address Identity and Access Management issues like identity theft, online fraud, authentication, authorization, integrity, non-repudiation, protection of privacy, confidentiality, etc should be formulated or necessary amendments should be made in existing laws with the help of members from law and IT fraternity
- The governance structure should be set up to oversight and manage the current and future Identity needs of various Government organisations
- The IAM architecture should be based on standard protocols, guidelines and best practices to ensure the interoperability and consistency.
- The Identity Information is stored by multiple agencies in multiple documents like Ration card, Driving License, Passport, Voter's card, Birth Certificate etc. The purpose of the Project unique ID (UID) initiated by the Planning Commission is to create a central database of resident information and assign a Unique Identification number to each such resident (Citizens and Persons of Indian Origin) in the country. The outcome of this project may act as input to the Identity and Access Management System.
- The appropriate Identity Aggregations and Synchronization should be used to integrate systems to share their identity information.
- Single sign-on should be provided to the citizens accessing e-Government services.
- Risk Assessment should be carried out to identify the impact that may result from accepting fraudulently asserted identity. Risk assessment involves identification of resources, identification of threats and identification of vulnerabilities that might be exploited by the threats.
- Organisations should have Risk Management Plan in place if identity is compromised.
- Based on authentication assurance level requirements identity authentication credential types should be selected. Basic authentication should be used for services like request for specific information on government services, online discussion groups etc. Strong authentication should be used for the services which needs signing of documents and where it is very important to know the identity of the user for e.g. submission of duly signed reports. The detail

classification is shown in Annexure – III.

- User should be provided with a consistent, comprehensive and integrated, easy-to learn user interface for presenting his identity.
- Automated provisioning and Self-service capabilities such as self-registration and changing password should be provided wherever possible to avoid administrative overhead.
- The mechanism for receiving a credential should be closely scrutinized for e.g. receiving password through an encrypted, direct channel, smart card after showing identification.
- Identity and Access Management should enforce the consistent application of policies for requesting and approving entitlements. The provisioning system should also provide audit trail that records when decisions and approvals were made and by whom.
- Orphaned accounts can be used for unauthorized access of resources. Hence these accounts should be disabled quickly in case complete deletion of these accounts is not possible. The IAM system should not just identify the orphan accounts, but must also take corrective actions automatically.
- IAM should automatically alter the privileges to access resources depending on change in job functions and authority. In order to avoid misuse, the privileges to access Government resources should be immediately revoked in case of the death of the citizen, or on expiry of the period for which privileges are granted.
- Security can be enhanced by policy enforcement such as
    - Requiring user to choose complex password which is difficult to guess but easy enough to remember eliminating the need to write it down, password of minimum length, change it frequently
    - Removing/disabling orphan accounts to avoid misuse of such accounts.
    - Session Time out – Termination of inactive session after a defined period of inactivity
    - Restriction on connection times for high-risk applications
    - Implementing strong authentication for sensitive and critical applications
    - Reducing attack surface
    - Dedicated, isolated computing environment for sensitive systems
    - Integrating and Consolidating the identity stores

  - Single Sign On to make it easier for user and avoiding the need for him to write down complex password since it becomes difficult to remember multiple passwords. Only in case of performing critical operation or accessing sensitive information user may be asked to provide credentials again.
- Privacy and integrity of the identity information should be maintained.
- To automate the processes which span various government departments, agencies, divisions the application of Identity Federation technology should be implemented.
- The policy should be reviewed at planned intervals or if significant changes occur to ensure its suitability, adequacy and effectiveness.

7. Legal and Regulatory Issues

To be provided by the publisher at the time of publishing

8. Annexures

Annexure – I: Technology and Implementation Issues

The following is a provisional description of the envisaged IAM system --
The IAM is a distributed system of servers (Secondary Identity Server – SIS) scattered across the country for storing identity data. A master server (Central Identity Server - CIS) located at the Center is used for data consolidation. Each server operates with a standard identity schema (To be identified) and corresponding database of identities. The identities are entered by the authorized users of the system through a web based interface. (The overall process describing the data acquisition procedure is to be identified and documented) The SIS servers synchronize its data with the CIS server in an incremental manner.

The IAM system offers web based Single Sign On (SSO) to the users (Standards in this connection are to be identified: Refer to IETF RFC 2109). This is achieved through an IAM Portal which also is used for providing a single point access to all registered service providers (RSP). All registered service providers will need to establish a trust relation with the IAM Portal (Additional requirement for RSP?..) . This allows the authenticated users of the IAM portal to get access to the contents stored at the RSP end without providing any additional identification information (What information is to be passed to the RSP for their auditing purpose need to be identified?).

The SIS and CIS servers also offer programming interfaces to facilitate new application developments.

I.1. Required Operations

Identity Management

- Identity Store
- Identity Synchronization
- Identity Integration

- Identity Administration
- Provisioning / de-provisioning

▪ Access Management

- Authentication
- Entitlement
- Authorization
- Trust and Federation
- Auditing

I.2. Identity and Access Management Framework

Diagram 1 below depicts a framework for Identity and Access Management

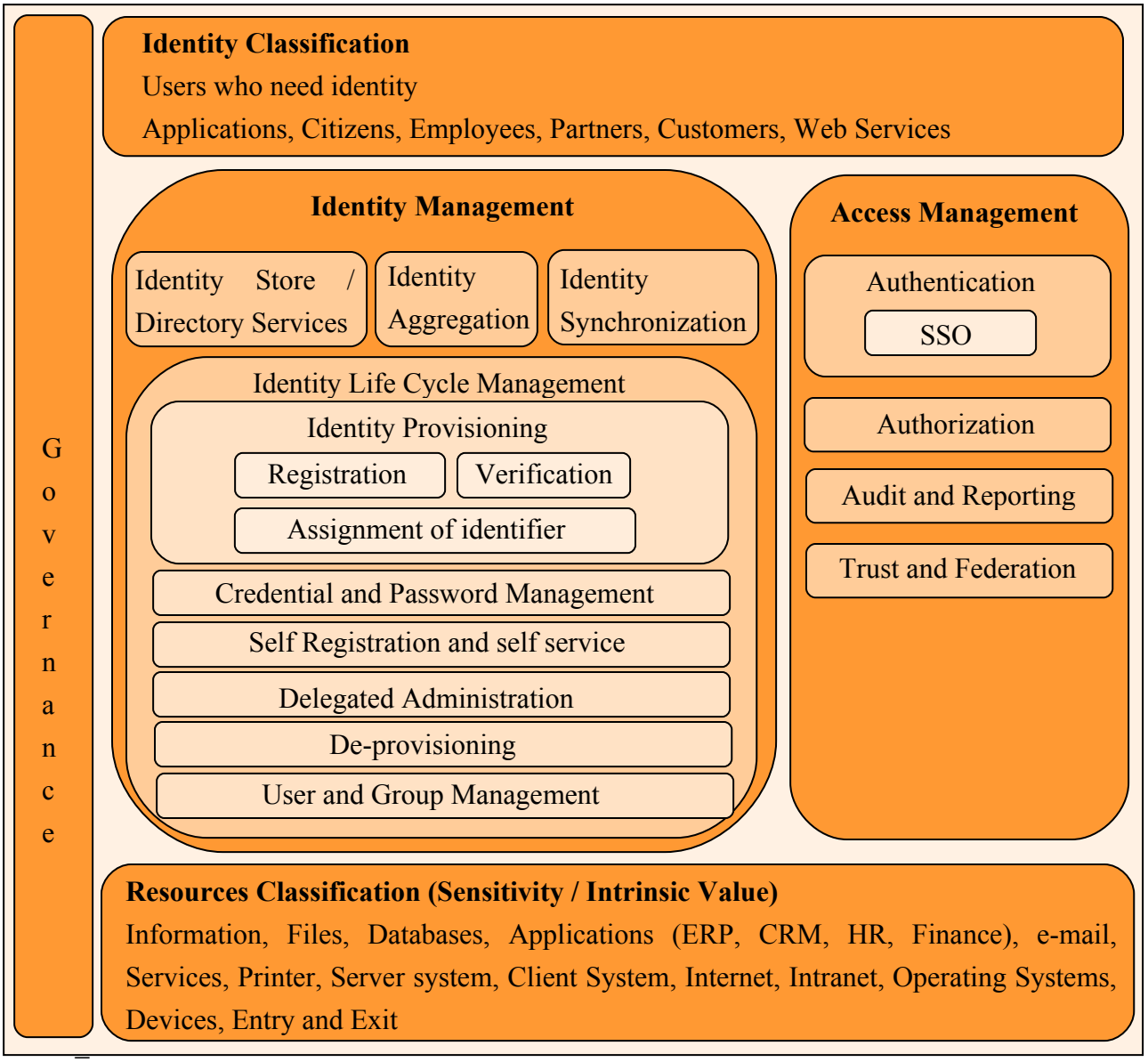

Diagram -1

I.2.1.Identity and Identity Classification

User's identities are at the core of any operation. Anyone desires to access service needs to prove his identity. When these services are offered online, digital identities come in picture. Identities are required for all users, including human users like citizens, employees, customers, divisions, departments, organizations, and technology users like applications, web services, devices etc.

The Identity Information is stored by multiple agencies in multiple documents like Ration card, Driving License, Passport, Voter's card, Birth Certificate etc.

I.2.2.Identity Management

I.2.2.1.Identity Stores / Directory Services

Identities are stored in identity stores. Organization can have single or multiple identity stores. Identity and Access Management Strategy should be to consolidate the multiple identity stores into minimum number of identity stores that collectively become the standard directory services of the organization. But it is not always possible to store all the digital identities in a single identity store because of

- regulatory requirements for information and management boundaries within organizations such as finance, personal etc.
- different levels of authentication needs for different resources
- different formats of entitlements for different resources

Using Integration and Synchronization techniques, integrity of these stores can be maintained.

I.2.2.2.Aggregation and Synchronization

It is not often feasible to store all the identities in single identity store. Same identity may exist in multiple identity stores in different ways with different set of attributes. Aggregation allows linking of digital identities from multiple identity stores. It involves discovering all the managed identity stores, choosing attributes from multiple identity stores, determining the authoritative source of various attributes, creating global view of identity information and synchronizing

identity information across different identity stores. It helps in providing the unified view of all digital identities and improved identity administration from a single identity store. The appropriate Identity Aggregations and Synchronization should be used to integrate different systems to share their identity information and create and maintain the same entitlements through common policies to reduce cost associated with management of identities, reduce the administration overhead related to linking of identity information in multiple identity stores and minimize productivity loss, limit errors introduced by human administration.

I.2.3. Identity Life Cycle Management

Identity Life Cycle Management involves Identity Provisioning, Credential and Password Management, Self Registration and self service, Delegated Administration, De-provisioning, User and Group Management.

Provisioning is the process of adding identities to an identity store. The provisioning will incorporate the following sub processes -

- User registration (Receiving User request)
- Verification (face-to-face, on seeing the original documents, physical evidence, check already completed by another agency or trusted third party)
- Assignment of identifier which is unique
- Issuance of credentials
- Creation of identity in identity store

Automated provisioning and Self-service capabilities such as self-registration and changing password should be provided wherever possible to avoid administrative overhead. The mechanism for receiving a credential should be closely scrutinized for e.g. receiving password through an encrypted, direct channel, smart card after showing identification.

Identity and Access Management should enforce the consistent application of policies for requesting and approving entitlements. The provisioning system should also provide audit trail that records when decisions and approvals were made and by whom.

De-Provisioning is the process of removing identities from an identity store. Orphaned accounts can be used for unauthorized access of resources. Hence these accounts should be disabled quickly in case complete deletion of these accounts is not possible. The IAM system should not just identify the orphan accounts, but must also take corrective actions automatically. As the employee moves in the organization his access privileges change based on his change in status and job responsibilities. IAM should automatically alter the privileges to access resources depending on his new job functions and authority. In order to avoid misuse, the privileges to access Government resources should be immediately revoked in case of the death of the citizen, or on expiry of the period for which privileges are granted.

Users having particular attribute can be assigned to specific group and entitlements to access resources then can be configured for this group. Group management includes automatic and manual assignment of user accounts to and from groups as well as removal of accounts from groups.

I.2.4.Access Management

I.2.4.1.Authentication

Various forms of authentication technologies exist today. These are user name and password (Plain text or cryptographically signed), biometrics, tokens, digital certificates, smart cards etc. For high security suitable combination of these can be used. For e.g. smart card along with digital key entry. The required level of security should be determined based on the sensitivity / intrinsic value of the resource.

I.2.4.2.Single Sign On

Single Sign On is the ability for a user to authenticate once with the system to access all servers, applications and data sources that user is authorized to use without need for providing credentials repeatedly. The end result is that the user only has to sign on once before using many applications.

Single Sign On has immediate benefits for both the users and administrators. User can gain access to multiple resources with a single login saving him from multi-password confusion. It provides greater convenience, choice and control to users. It reduces risk of Security exposure that can occur with writing down passwords. For administrators, single sign on simplifies maintenance across servers. It saves the time and resources spent administrating passwords, unlocking accounts and dealing with lost / forgotten passwords.

I.2.4.3.Authorizations

Authorization is checking of authority of user to undertake the specific process or access the resource and relates to specific access permissions / privileges granted to user by resource owner. Authorization ensures that correctly authenticated entity can access only those resources for which it has been entitled. Authorization can be implemented through role based access control or through Access Control Lists.
A role can be defined as Administrator, Manager, Creator, Writer, Reader, etc. These roles are then mapped to application permissions such as create, delete, read record / file / table / database etc. Administrator can create the roles and assign permissions to these roles.
Access Control Lists are the lists of users or groups together with permissions for each user or group.

I.2.4.4.Access Control

Access policies are usually defined in terms of role, resource, operation and restriction and are defined by resource owner. The access can be role based (Manager, Administrator etc.), rule based (Membership of a group, specific rule based such as time, location etc.) or identity based. While implementing Identity and Access Management, access policies should be in place as per the requirements of the organization.

With the help of Identity and Access Management organisations should be able to associate access rights with a role within the organisation. Identity and Access Management should dynamically assign and automatically change access rights based on changes in user role. Organisations should be able to provide the

access by precisely managing entitlements and modifying or terminating access rights promptly.

I.2.4.5.Audit and Reporting

Security auditing is typically used to monitor for the occurrence of events, problems and security breaches. It provides a means to monitor access management events and changes to directory objects. Integrated Identity and Access Management systems should provide auditable proof that only appropriate access is granted to critical data. It should keep track of user activities and access violations. Establishing a security auditing policies results in early detection of attacks, alerting mechanisms to initiate emergency procedures.

Security auditing should provide audit trail of

- Authentication events
- Authorization events
- Changes to directory objects
- Should trigger alarms and alerts

The Identity and Access Management should

- Track all changes in directory objects and access privileges
- Record all access activities and events
- Consolidate logs and events
- Compile reports and
- Trigger alerts

I.2.4.6.Trust and Federation

A federation is an association of organizations to exchange information about their users and resources in order to enable collaborations and transactions. The sharing of digital identities to enable federation is defined as "Identity Federation". It is a special kind of trust relationship between the organizations. Federation involves description of identities, protocols to exchange security tokens, preservation of privacy and methods for establishment of trust. The arrangement which enables users who can authenticate to one identity store to

authenticate to a second one, even though they have no digital identity in the second store is called a trust relationship. Trust relationships exist between separate realms, where realm defines a security boundary. It allows the identity information to flow across organizational boundaries, independent of platforms, application or security model. It enables users to work with different organizations/organizational units seamlessly as if they were part of the same security domain, while in fact the domains remain largely independent. It allows organizations to work together more efficiently, without the overhead of authenticating and authorizing each digital transaction or exchange of information.

Since different organizations have to trust a common system, same rules need to apply to everyone. When every party knows how others are using the system, only then there can be trust in the common system. Requirements for confidentiality or non-disclosure agreements reflecting the participating organizations needs for the protection of information should be identified.

In government scenario, the Identity Federation is essential while automating the processes which span various government departments, agencies, divisions to be completed.

I.2.5.Resources Classification

Every resource including information has following characteristics associated with it –

- Ownership – who is the fundamental owner of the resource
- Guardianship – who is the custodian of the resource
- Value / sensitivity – how sensitive is the resource from privacy, commercial or other (National security) perspective.

These attributes play a major role in determining who is able to access the information, to add, view, alter or delete it. Hence resources should be classified based on these attributes and controlled.

Information classification includes

- Inventory of information resources
- Classification

- Labeling

Level of sensitivity of data should be assigned when it is created, changed, enhanced, stored or transmitted. Classification of information is done as

- Public domain
- Restricted
- Confidential
- Secret
- Top secret

All information and assets associated with information processing facilities should be "owned" by a designated part of the organization and rules for the acceptable use of these should be identified.

I.2.6.Governance

The proposed framework envisages the formation of Identity Management Steering Committee. It is required for

- Consistent approach to Identity and Access Management across different agencies
- Co-ordinate Identity and Access Management activities
- Formulation of standards and best practices, policy revision whenever the need arise
- Examine the logistics and benefits associated with shared credentials, infrastructure and services
- Establishing and coordinating education, trainings and awareness in the Identity and Access Management areas

It may consist of representatives from

- Government Departments
- Business Organizations
- Multiple agencies involved in e-Governance applications development and implementation
- Law fraternity
- Citizens

Its responsibilities should include

- Development of policies
- Development or selection of standards
- Development of model processes and best practices guides
- Development and conducting of appropriate awareness programs, education and training in the areas of Identity and Access Management

I.2.7.Identity and Access Management Life Cycle

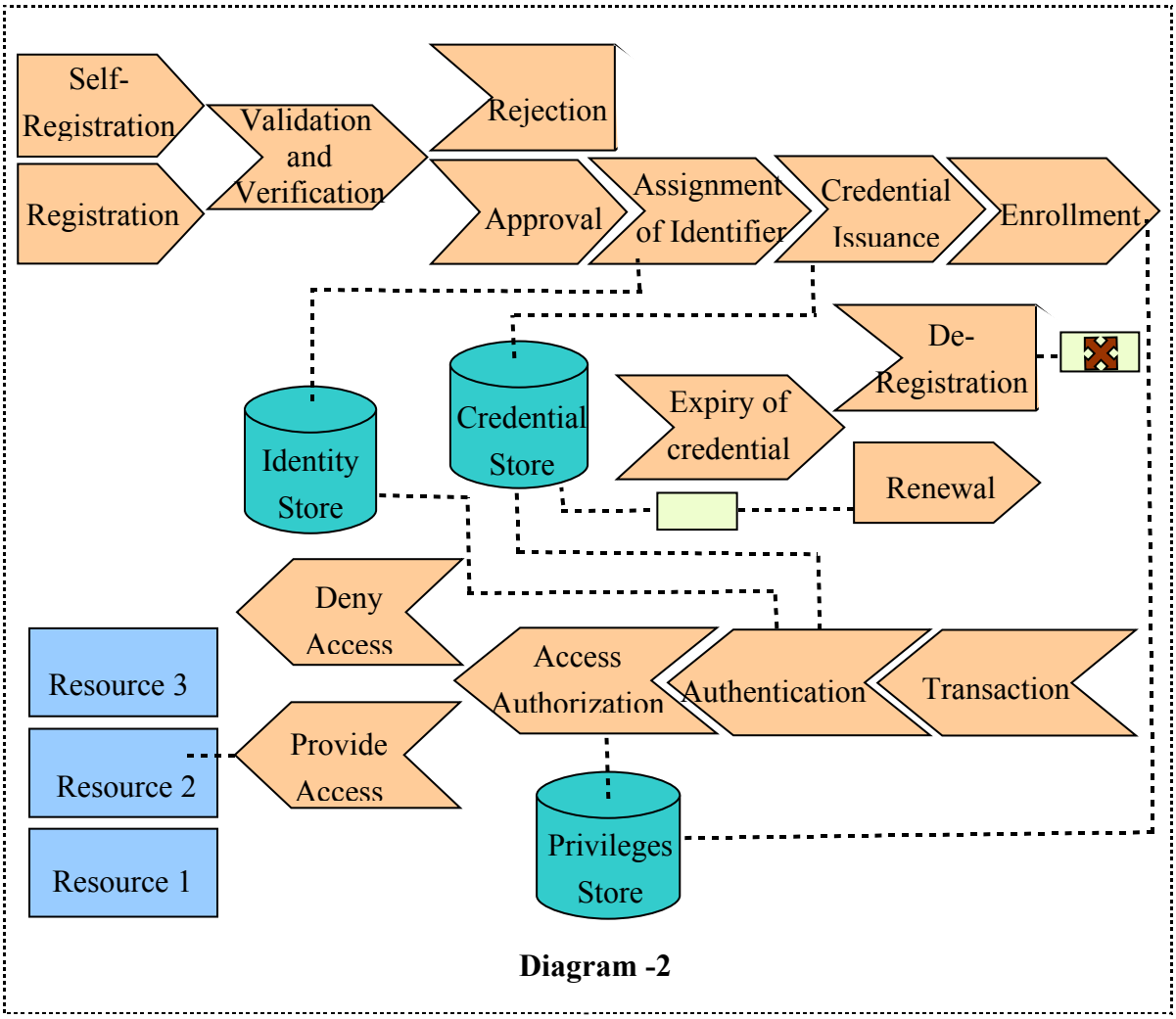

Diagram -2

I.2.8. Identity Life Cycle Management

Identity Life-Cycle Management includes the process and technologies for provisioning, de-provisioning, managing and synchronizing digital identities while complying with the governing policies in a secure manner generating complete audit trail of the transactions.

Road Map:

- Identify the data sources.
- Schema for describing "Identity" to be formulated.
- Schema for describing the rule and role based entitlements to be formulated.
- Format for digital ID to be identified. This may be used as the primary key for identifying the identities.
- Procedures governing the Identity Life Cycle covering all stages from creation of records to deletion, alteration and backup to be formulated with the constraints of providing security and generating log data for audit trails.
- Mechanism for appropriate synchronization/integration of identity servers to be evolved.
- Manner in which the ID is to be made available to different users of the system to be identified. (Smart Card/A coded number/ etc)
- Identify prospective standard based technologies for implementation of Identity Life Cycle Management
- Identify prospective legal and regulatory issues
- Identify risks and counter mechanisms

I.3. Access Management

Identity Access Management includes the processes and technologies for controlling and monitoring access to resources consistent with governing policies. Access management encompasses authentication, authorization, trust and security auditing.

Road Map:

- Identify the users (people, organizations, applications, Web Services etc.) which need access to IAM system
- Identify the environments in which the IAM system may be used.
- Identify the feasible required security level for each resource.
- Identify prospective standard based technologies to implement Trust relationships to provide Single Sign On facility to user.
- Identify Criteria to allow external entities to enter into a Trust relation with the IAM system.
- Standardize services to be made available to the trusted partners/application/Web service in a secure way.
- Identify the IAM system response to security breaches.
- Identify requirements for auditing access information.
- Identify prospective legal and regulatory issues
- Identify risks and counter mechanisms

I.4. Management Issues

Road Map:

1. Identify the IAM system management responsibilities
2. Propose the required organization structure to facilitate management and control of IAM System
3. Identify audit requirements.

Annexure – II: Standards for Identity and Access Management System

- XML-the lingua franca of information storage and sharing
- SAML-a standard developed by OASIS for exchange of authentication and authorization information across security domm,ains.
- WS-* Security Architecture, incorporating WS-Security, Ws-Policy, WS-Trust, WS-metadata exchange for secure web services.
- SAML, Liberty ID-FF, WS-Federation standards for federated identity
- SPML- citizen self-service (Federated provisioning)
- XACML - a general policy language used to protect resources as well as an access decision language
- Secure Sockets Layer or Transport Layer Security for confidentiality and when passwords are required between the client and Web or application servers
- Crypto API or Public-Key Cryptography Standard 11 for smart card interfaces to applications and external cryptographic functions.
- BioAPI based Biometric devices for enrollment, verification and identification.
- Internet Engineering Task Force's Public Key Infrastructure X.509 standards for implementing PKI. This set of specifications provides certificate profiles, operational protocols, management protocols, policy outlines, and time stamp and data certification services.

Annexure – III: Risk Classification and Authentication Mechanisms

Level 1 – Minimal Risk
When there is minimal damage if identity is compromised while accessing e-Government services.
Level 2 – Low Risk
When there is minor damage if identity is compromised while accessing e-Government services.
Level 3 – Moderate Risk
When there is moderate damage if identity is compromised while accessing e-Government services.
Level 4 – High Risk
When there is substantial damage if identity is compromised while accessing e-Government services.
Level 5 – No compromise
When there is exceptionally grave damage like threat to national security or loss of lives, if identity is compromised while accessing e-Government services. For e.g. Defense data.

Authentication Mechanisms

Authentication Mechanism	**Current Authentication Mechanism strength**
None, password (Plain Text)	Weak ■——— Strong
Passwords(Cryptographically signed), One time Password Token	Weak ——■——— Strong
PIN protected tokens, OTP Tokens Certificates, Secondary Channel (Phone, code book), Knowledge based	Weak ———■— Strong
Secondary Channel, Certificates, Smart Cards, Biometrics, etc.	Weak ———■ Strong

The effective strength of authentication mechanism will change over time as new threats emerge. Hence a periodic review of the above table is

recommended.

Annexure – IV: Identity related e-Governance applications

Indian Government Context

The Government of India has launched the National e-Governance Action Plan (NeGP) with the intent to support the growth of e-governance within the country. The Plan envisages creation of right environments to implement G2G, G2B, G2E and G2C services. Establishment of the right environment to implement these services requires that a range of security and management concerns be addressed including that of Identity and Access management. Identity and Access Management plays an important role to ensure the availability of right services and resources to right users at right time while protecting these from unauthorized access. Open yet secure access is important in Government to citizen interactions. With Identity and Access Management in place services can be made online. Identity and Access Management reduces the risk of unauthorized access to and modifications or destruction of government information assets.

At present there is no consistent approach for implementation of Identity and Access Management solutions. Different Government organizations / departments and within these different applications have their own policies / procedures, infrastructure and solutions for identification, authentication and authorization with almost nil or insufficient auditing mechanism. No standards are available; hence interoperability is an issue. This has resulted in formation of identity silos, multiplicity of identity information, duplicate efforts, potential security loopholes and increased management cost for the government organizations. This also leads to the requirement for citizen to re-establish their identity when dealing with multiple government agencies and need to maintain multiple credentials. End result is inefficiencies in delivering services to citizens, increased risk of identity theft, unauthorized access and failure to meet

regulatory compliance.

Government's goal should be to seek harmonization of Identity and Access management approaches across agencies for the purpose of achieving uniform excellence and interoperability by using common set of policies and processes. It should ensure

- Information sharing
- Optimization of resources by sharing expertise, facilities, credentials etc.
- Secure and trusted transactions and information sharing environments
- Coordinated and consistent approach rather than multi-siloed approach
- Improved service through enabling users to use the same identity and authentication credentials across services within a department and across government wherever feasible.
- Integrated service / single window solution

Identity and Access Management should be deployed and implemented as a set of common shared service components of e-Government architecture wherever possible.

There are different identity related e-Governance applications operational in different departments at Centre and State taken up as the e-Governance Mission Mode Projects under NeGP. Some of these are listed below.

(A) State Sector 11 MMPs of NeGP

1. Land Records: The Record-Of-Right (ROR) is used as identity of land owners Property Registration: Buyer/seller address is used as identity, which is verified by the Lamberdar/Patwari at villages and by Member of Municipality at urban areas
2. Transport: Driving License as citizen identity and Vehicle Registration as Vehicle Identity
3. e-Municipalities: The house number is taken as property identity
4. e-Panchayats: The Village Panchayat Address is taken as Panchayats identity. Each Below Poverty Line (BPL) Households, has a code for identity

5. Employment Exchanges: The un-employed persons registration number is used as identity
6. Commercial Taxes: The Registered Dealers registration number is used as identity
7. Agriculture: Each Mandi has been provided with an Identity number.
8. The Animals husbandry surveys provide an identity number to every animal.
9. Treasuries: Each Transaction is identified under Voucher level computing with heads/sub-heads/minor-heads/transaction code. Each DDO is identified with a DDO Code. The Departments have been provided with a unique code.
10. Police: Each Police station is provided with an identity code. Each FIR is coded. Each Police Personnel is provided with a personal ID.
11. E-District: Each District, block, village is identified through a unique code.

(B) Additional State Sector MMPs:

1. Education: The roll number or Certificate number of Matric Examination or +2 Examination Certificate of the CBSE/State Board of School Education provides identity for the students. Each school is codified to have identity.
2. Health: Each Angan Wadi Worker, Hospital/CSC, PHC, Health Sub-Centre requires a code for identity. Each Birth & Each Death (as Birth / death Certificate) can have a unique ID for providing the identity
3. Food and Civil Supplies: The Ration card is authentic and legal document, which can be used for identity of household as well as residence proof
4. Social Justice and Empowerment: The Old Age/Widows/ Physically Handicapped citizens IDE details as their Identity

[C] Central Sector MMPs

1. Central Excise and Customs: All Exporters registered with customs have a registration number as their identity
2. Income Tax: The PAN number is used as tax payers identity
3. Insurance: Every Insurance (Life/General) policy is identified with a unique policy number
4. Banking: Within a Bank, each customer is provided with a unique Account

number for identity. Now most of the banks have upgraded to these bank account numbers as unique across the country.

5. Passport: Each individual passport has a unique number for identity
6. MCA: Every registered business and its Directors have been provided with unique Identity numbers.
7. Pensions: Each government Employee has a unique PF number with respective Accountant General. Each Private Employee, PSU and other employees have a unique CPF number with Provident Fund Commissioners. Each Pensioner has been provided with a unique pension number for identity.
8. e-Posts: Each post office Location having a unique PIN, Each accountholder have a unique account number, Each Telephone have a unique Identity number.
9. National UID Project: This project has been initiated, with Voter ID Numbers and BPL households in the first instance. Each Voter has a Voter ID. A large number of voters have been provided with a Voter ID Card. Each BPL family has also been provided with a BPL card.
10. e-Courts: Each Sub-ordinate court is identified. Each registered judicial court has a unique identification number at Sub ordinate Courts, High Court and Supreme Court.

Annexure – V: Glossary

Term	Definition
Access Authorisation	The system controls and surrounding processes that provide or deny parties the capability and opportunity to gain knowledge of or to alter information or material on systems. In practice, the act of authorising access usually occurs after authentication has been successful.
Access Control	Limiting or granting access to a file system, Web site, or other digital environment, usually via some sort of authentication.
Access Management System	The collection of systems and/or services associated with specific on-line resources and/or services that together derive the decision about whether to allow a given individual to gain access to those resources or make use of those services.
ACL	Access Control List: A list of Access Control Instructions (ACI's)
Applicant	Role which initiates applications.
Approval	Within the context of management document descriptions, refers to the authorisation by the appropriate management entity to proceed with work described by a proposal or plan, or adopt a defined management process.
Assertion	A statement made that purports to be true. Categories of Assertion that may be subjected to Authentication include Agents, Attributes, Credentials, Data Integrity, Entities, Identities, Location, and/or Value.
Assertion	When an Identity Provider authenticates a user and directs them back to the referring Service Provider, it includes as part of the message an assertion to prove that the user is authenticated. See also Identity Provider, Service Provider.
Assertion	The identity information provided by a Credential Provider to a Resource Provider.
Assurance level	The degree of trust associated with the authentication credentials that are Proffered.

Assurance level	A specific level on a hierarchical scale representing successively increased confidence that a target of evaluation adequately fulfils the requirement
Attribute	A single piece of information associated with an electronic identity database record. Some attributes are general; others are personal. Some subset of all attributes defines a unique individual. Examples of an attribute are name, phone number, group affiliation, etc.
Audit	An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.
Audit Trail	A list of all recorded activity, which resources are being accessed, when and by whom and what actions are being performed. Audit trails are one of the requirements of system accountability, enabling any system action or event to be traced back to the user responsible for it. Audit trails are also used to investigate cyber crimes. They are indispensable for incident response and the follow-up aspect of digital forensics. The audit trail enables the person investigating the incident to follow the trail that was left.
Authentication	A process used by a system to uniquely identify a user. Most systems authenticate users by asking them to type a secret password. Other forms of authentication include: 1) Using hardware tokens 2) Using a PKI certificate 3) Using a smart card 4) Providing a biometric sample (fingerprint, voice print, etc.) 5) Answering personal questions. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
Authentication	Authentication in this context is the process of determining a user's identity, usually by verifying a supplied username and password combination. Single-Sign on systems provide a means where authentication information can be shared between services, preventing a user from having to

	authenticate themselves multiple times. See also Authorisation, Single Sign-On.
Authentication	Authentication is the process of establishing whether or not a real-world subject is who or what its identifier says it is. Identity can be proven by: Something you know, like a password; Something you have, as with smart-cards, challenge-response mechanisms, or public-key certificates; Something you are, as with positive photo identification, fingerprints, and biometrics. (For more on this topic, see Internet-2 Middleware Authentication website <http://middleware.internet2.edu/core/authentication.html>.) AuthN protocols such as Kerberos v5, Secure Sockets Layer (SSL), NTLM, and digest authentication protect the authN process and prevent the interception of credentials.
Authentication	Establishing the individual identity of a user, or determining that the user has certain attributes or is a member of a specified group.
Authentication	The process by which a person verifies or confirms their association with an electronic identifier. For example, entering a password that is associated with an UserID or account name. A security measure designed to establish the validity of a transmission, message, or originator, also a means of verifying an individual's authorization to receive specific categories of information.
Authentication Devices	Devices used by organizations to verify the identities of users requesting access to information and applications. Authentication devices include: Fingerprint, Face, Voice, Signature, Password/PIN, Smart Card/Swipe Card, and Token.
Authentication Mechanism	The 'technology' approach used to support the act of authentication e.g.: UserID Password, PKI, Smartcards, Biometrics. These can be single-factor (e.g UserId-Password) or Multi-factor (e.g. Password+Smartcard).
Authentication Token	A portable security device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords. These require complementary software or hardware. Smart cards, smart card readers, USB tokens, and touch memory devices

	are a few examples.
Authorisation	Authorisation in this context is the process of determining a user's right to access a resource. Authorisation almost always relies on the user having been authenticated.
Authorisation	AuthZ: based on the identity of a person, and the accompanying attributes or characteristics, allowing/denying access to resources. The determination that a request can be honoured is known as authorization. (For more on this topic, see Internet-2 Middleware Authorization website <http://middleware.internet2.edu/core/authorization.html>.) The process of evaluating whether an authenticated entity is authorised to do something to a particular resource under a defined set of circumstances. The process of resolving a user's entitlements with the permissions configured on a resource in order to control access.
Authorisation	Establishing what an individual is permitted to do.
Authorisation	The process of giving individuals access to system objects based on their confirmed Identity.
Authorisation	The process or determining a specific person's eligibility to gain access to an application or function, or to make use of a resource. A right or permission that is granted to access a system resource.
Biometric Authentication	Biometric authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some intrinsic characteristic of that user. Biometric samples include fingerprints, retina scans, face recognition, voiceprints, and even typing patterns. Biometric authentication depends on measurement of some unique attribute of the user. They presume that these user characteristics are unique, that they may not be recorded and reproductions provided later, and that the sampling device is tamper-proof.

Biometrics ▪ ▪ ▪	A measure of an Attribute of a Natural Person's physical self, or of their physical behavior. In principle at least, a Biometric can be used: to validate an entity (where the entity is a Natural Person); as an Authenticator for an Assertion involving an Entity; and as a means of restricting the use of a personalised Token to the appropriate Natural Person. Examples include: fingerprint, voiceprint, and iris-scan
Biometrics	Generally, the study of measurable biological characteristics. In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. There are several types of biometric identification schemes: Face: the analysis of facial characteristics; Fingerprint: the analysis of an individual's unique fingerprints; Hand geometry: the analysis of the shape of the hand and the length of the fingers; Retina: the analysis of the capillary vessels located at the back of the eye; Iris: the analysis of the colored ring that surrounds the eye's pupil; Signature: the analysis of the way a person signs his name; Vein: the analysis of pattern of veins in the back if the hand and the wrist; Voice: the analysis of the tone, pitch, cadence, and frequency of a person's voice.
CA - Certificate Authority	A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Confidentiality	Ensuring that a resource may only be used by its intended recipient.
CP - Credential Provider	A campus or other organization that manages and operates an identity management system and offers information about members of its community to other InCommon participants.
CPS - Certification Practice Statement	A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. http://www.ietf.org/rfc/rfc3647.txt
Credential	Information identifying a party that has physical or digital existence, and

	that assists in the process of Authentication of an Assertion.
Credential	An object that is verified when presented to the verifier in an authentication transaction. Credentials may be bound in some way to the individual to whom they were issued, or they may be bearer credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization. Electronic credentials can be digital documents used in authentication and access control that bind an identity or an attribute to a claimant's token or some other property, such as a current network address. Credentials are verified when presented to the verifier in an authentication transaction. Anonymous credentials are used to evaluate an attribute when authentication need not be associated with a known personal identity.
Credential Store	The systems-based repository that holds user credentials.
Deactivation	Deactivation is the process of disabling a user's accounts, so that the user can no longer authenticate to those systems or access their resources or functions. Deactivation does not necessarily imply that the accounts are deleted -- simply that they are made inoperative.
De-provisioning	The removal of records on systems relating to the authentication credentials and/or access permissions of users.
Delegated User Administration	As the number of accounts in a system grows, central user administration becomes impractical. Delegated user administration is a feature found in some systems to enable designated users to create new users and manage existing users in just a segment of the user directory.
Digital Certificate	In the PKI environment, the data, equivalent to an identity card, issued to a user by a CA (Certificate Authority), which he/she uses during business transactions to prove his/her identity.
Digital Signature	A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message, or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged.
Digital Signature	The number derived by performing cryptographic operations on the text to be signed. This operation, or hash function (also called hash algorithm), is performed on the binary code of the text. The result is

	known as the message digest, and always has a fixed length. A signature algorithm is applied to the message digest, resulting in the digital signature.
Digital Signature	A digital signature provides information about the source of a digital object, and allows the receiver to determine if the object has been altered in transit.
Directory	A directory is a specialized database that may contain information about an institution's membership, groups, roles, devices, systems, services, locations, and other resources.
Directory	A collection of accounts managed by a single system. Directories may be internal to a system (e.g., the SAM database in a Windows NT domain), or may be shared by multiple systems (e.g., an LDAP directory).
Directory	A directory is a specialized database that may contain information about an institution's membership, groups, roles, devices, systems, services, locations, and other resources.
Directory Services	Services that provide identity, demographic and authorization information on a user.
Directory Synchronization	A directory synchronization process compares users, user groups, and user attributes as they are defined on two or more systems. It applies business logic to detected differences, and automatically updates the users, user groups, and/or user attributes on at least one system to match those found on others.
Disabled Account	An account is disabled in the event that some administrator or user provisioning process, presumably with suitable authorization, actively set a flag to prevent further logins to that account. Most systems differentiate between locked and disabled accounts.
Encryption	The process of encoding information so it cannot be accessed without first being decrypted through the use of an encryption key.
Encryption	The scrambling of data so that it becomes difficult to unscramble or decipher. Scrambled data is called ciphertext, as opposed to unscrambled data, which is called plaintext. Unscrambling ciphertext is called decryption. Data encryption is done by the use of an algorithm and a key. The key is used by the algorithm to scramble and unscramble the data. The algorithm can be public (for inspection and analysis by the

	cryptographic community), but the key must be kept private. Encryption does not make unauthorized decryption impossible, but merely difficult. Time, and the power (ever increasing) of computers are the factors involved in the feasibility of decryption.
Enrollment	The initial process of collecting biometric data from a user and then storing it in a template for later comparison.
Enrolment	The act of setting up permissions that enable a known user to gain knowledge of or to alter information or material on systems. e.g. a known user will be enrolled into the email, HR, Financial etc systems Multiple enrolments into various systems may occur after a user has been registered. Although 'Registration' and 'Enrolment' are sometimes used as synonyms, a distinction is being drawn here between the two terms.
Entity	A real-world thing. Categories include objects, animals, artifacts, natural persons, and legal persons (such as corporations, trusts, superannuation funds, and incorporated associations).
Federated Identity	The management of identity information between members of a federation.
Federation	A Federation is a organisation composed of institutions which agree on a common set of principles in order to share information. Federations form the core of the Federated trust principle which Shibboleth is designed to use. See also Shibboleth.
Federation	A special kind of trust relationship established beyond internal network boundaries between distinct organizations.
Federation	A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions.
Identification	The process whereby data is associated with a particular Identity. It is performed through the acquisition of data that constitutes an Identifier for that identity
Identifier	One or more data-items concerning an Identity that are sufficient to

	distinguish it from other Identities, and that are used to signify that Identity. Identifiers include names. A natural person may use more than one name, and variants of each name. Identifiers also include 'id numbers' or 'id codes' issued by other Entities that the Entity interacts with. An Entity may be assigned many such numbers and codes. A legal person may have many names (e.g. associated with business units, divisions, branches, trading names, trademarks and brand names), and multiple 'id numbers' and 'id codes' assigned by other Entities that the Entity interacts with.
Identifier	Unique pointer, within a certain context (namespace) to an identity
Identity	Description of a person or organisation, e.g. by a set of characteristics or attributes. To avoid schizophrenic views, a person or organisation can only have one identity, but multiple roles. WordNet dictionary - the individual characteristics by which a thing or person is recognized or known;
Identity	Identity is the set of information associated with a specific physical person or other entity. Typically a Credential Provider will be authoritative for only a subset of a person's identity information. What identity attributes might be relevant in any situation depend on the context in which it is being questioned.
Identity	The username used to identify an individual to an application. An individual may have multiple Identities, one per application.
Identity Credential	An electronic identifier and corresponding personal secret associated with an electronic identity. An identity credential typically is issued to the person who is the subject of the information to enable that person to gain access to applications or other resources that need to control such access.
Identity Database	A structured collection of information pertaining to a given individual. Sometimes referred to as an "enterprise directory." Typically includes name, address, email address, affiliation, and electronic identifier(s). Many technologies can be used to create an identity database or set of linked relational databases.

Identity Federation	Identity federation allows users to present a single set of identity and authentication information to access applications and services across multiple domains and distributed, heterogeneous networks. A federated system allows a user's identity in one domain to be used to gain access to resources in another domain without the need for separate authentication.
Identity Management	The comprehensive management and administration of user permissions, privileges, and individual profile data. It provides a single point of administration for managing the lifecycle of accounts and profile data.
Identity Management System	A set of standards, procedures and technologies that provide electronic credentials to individuals and maintain authoritative information about the holders of those credentials.
Identity Provider	An identity provider is a service which asserts the identity of a user who is local to the institution running the provider. See also Origin.
Identity Provider	The originating location for a user. Previously called the Origin Site in the Shibboleth software implementation.
Integrity	Establishing that an object has not been altered in any way.
Integrity	The assurance that information has not been changed or corrupted by an unauthorized party.
Issuer	The CA that issues a certificate.
Knowledge Based Authentication	An authentication approach in which a user is challenged to provide one or more answers to questions/challenges provided by the party undertaking the authentication. The information sought could be 'shared secrets' provided by the user during a registration process and/or personal information (e.g. address, date of birth, mothers maiden name, etc) and/or transactional data (e.g. date, amount, reference number of last payment).
Multi factor authentication	An Authentication process in which multiple forms of Evidence are used, in order to increase the level of confidence in the Assertion.

	In the case of Identity Authentication, this involves two or more of the • an additional Identifier provided by the person • knowledge demonstrated by the person ('something you know') • an act performed by the person (something you can do) • a Credential provided by the person ('something you have') • a Biometric surrendered by the person ('something you are' or something you do).
Liberty Alliance	The Liberty Alliance Project [LibAll] consists of a diverse consortium of businesses whose common aim is to define an open standard framework, call for enabling business transactions via web services within a circle of trust or federation.
Liberty Alliance	A consortium of technology and consumer-facing organizations, formed in September 2001 to establish an open standard for federated network identity. http://www.projectliberty.org/
Non-repudiation	Proof that an action was taken (e.g. an email sent) at a particular time and by a particular person or agent.
Non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
OASIS	Organization for Advancement of Structured Information Standards
OASIS	The Organization for the Advancement of Structured Information Standards (OASIS) is a standards body involved in the creation of international standards for electronic business. OASIS particularly focuses on standards for Web Services and security. see http://www.oasis-open.org/who/. OASIS are responsible for the SAML standard. See also SAML.
Orphan Account	An orphan account is an account belonging to a user who has left the organization.
Owner	The term owner identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the resource. The term "owner" does not mean that the person actually has property rights to resource.
Password	A password is a secret string of characters that a user types when signing into a system, to prove his identity. Identity is established by virtue of the

	assumption that no other person knows the user's password. This implies that the password is difficult to guess, is not written down, and has not been shared with others.
Password Change	A password change is a routine process whereby a user, who knows his own password, selects a new, replacement password value for use on one or more systems.
Password Management	Password Management Systems automate the ability to reset lost or expired passwords and then synchronize these changes with the back-end system
Password Management	Refers to self-service password resets, password synchronization and delegated user administration.
Password Reset	A password reset is some process where a user who has either forgotten his own password, or triggered an intruder lockout on his own account, can authenticate with something other than his password, and have a new password administratively set on his account. Assisted password resets are similar to self-service password resets (self-service-reset), but with the intervention of a support analyst.
Password Synchronization	A password synchronization system is any software or process used to help users maintain a single password value on multiple password protected systems. Password synchronization may be optional or mandatory. Users may be encouraged to synchronize their passwords manually, or provided with an automated system for updating multiple
personal secret	Used in the context of this document, is synonymous with password, pass phrase or PIN. It enables the holder of an electronic identifier to confirm that s/he is the person to whom the identifier was issued
PKI - Public Key Infrastructure	Public Key Infrastructure: The PKI includes the Certificate Authority (CA), key directory, and management. Other components such as key recovery, and registration, may be included. The result is a form of cryptography in which each user has a public key and a private key. Messages are sent encrypted with the receiver's public key; the receiver decrypts them using the private key.
PKI - Public Key Infrastructure	Short for public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

	PKIs are currently evolving and there is no single PKI or even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread. A PKI is also called a trust infrastructure.
PKI - Public Key Infrastructure	The set of standards and services that facilitate the use of public-key cryptography in a networked environment.
Policies	Statements that outline the process and procedures that will be followed.
Policy-Based Access Control	Policy-based access control is a strategy for managing user access to one or more systems, where business classification of users is combined with policies to determine what access privileges a user should have. Theoretical privileges are compared to actual privileges, and differences are automatically applied. For example, a role may be defined for a territory sales manager. Specific types of accounts on the network, sales-force automation software and document management system may be attached to this role. Appropriate users are then attached to this role.
Privacy	The anonymity and secrecy of information, i.e. preventing others from obtaining information about you or the things you are doing.
Privacy Policy	A statement to users of what information is collected and what will be done with the information after it has been collected.
Privileges	A privilege is the right to do something on a system. Privileges normally relate either to the ability to access data (e.g., update a payroll record) or the ability to use some feature (e.g., surf the Internet).
Profile	Data comprising the broad set of attributes that may be maintained for an identity, and the data required to authenticate under that identity.
Protection	Protecting a work from unauthorized use.
Provisioning	The process of adding identities to an identity store and establishing initial credentials and entitlements for them. Deprovisioning works in the opposite manner, resulting in the deletion or deactivation of an identity. Provisioning and deprovisioning typically work with identity integration services to propAgate additions, deletions, and deactivations to connected identity stores.
Provisioning	The process of providing customers or clients with accounts, the appropriate access to those accounts, all the rights associated with those accounts, and all of the resources necessary to manage the accounts.

	When used in reference to a client, provisioning can be thought of as a form of customer service.
Provisioning	The process of providing users with access to data and technology resources. The term typically is used in reference to enterprise-level resource management. Provisioning can be thought of as a combination of the duties of the human resources and IT departments in an enterprise, where (1) users are given access to data repositories or granted authorization to systems, applications and databases based on a unique user identity, and (2) users are appropriated hardware resources, such as computers, mobile phones and pagers. The process implies that the access rights and privileges are monitored and tracked to ensure the security of an enterprise's resources.
Public / Private key encryption	An encryption approach whereby encryption is done using a user's public key, but decryption can only be done through the user's private key, which is never shared outside of the user's environment. Knowing the public key does not make it possible to derive the private key and decrypt the content.
Public Domain	A rights holder can place their content completely into the public domain. However, in the academic community accepted practice still dictates that attribution should occur when public domain content is used.
Registration	The process of establish a user's Authentication Credentials. This may involve e.g. requirement for production of Evidence of Identity and the issuing of one or more Credentials. Multiple enrolments may occur after a user has been registered. Although 'registration' and 'enrolment' are sometimes used as synonyms, a distinction is being drawn here between the two terms.
RBAC - Role-based Access Control	Access control that is granted based on your role within an organization (e.g. teacher, student, system administrator). Roles may be established through authentication and directory services or by other means, such as logging on through a campus IP address.
RBAC - Role-Based Access Control	In the context of a single system, role-based access control (RBAC) means a process where access privileges on a single system are grouped into roles, and users are attached to roles as a convenient mechanism to manage their privileges. Implementation of single system RBAC is simple,

	and almost every modern operating system and database supports roles or privilege groups. In the context of a user provisioning across multiple systems, RBAC means that types of accounts on multiple systems are grouped into roles, and users are attached to roles as a convenient mechanism to control user privileges across multiple systems. Implementation of multi-system RBAC is complex, since users may belong to multiple roles, which specify different or conflicting privileges on the same system. User classification, role definition and conflict resolution make multi-system RBAC a significant challenge.
Risk	A measure of the likelihood of harm arising from a threat
Risk Assessment	A process to determine the extent to which expenditure on safeguards is warranted in order to protect against identified threats.
Role	The specific right and duties and activities that a person or organisation (an identity) has/does within a certain context. A role is usually characterised by a subset of an identity's attributes. For example, being a professor at Macquarie University and a member of the E-Learning community. An identity can have multiple roles, and each role should have a unique identifier.
SAML	A security standard, created by OASIS, which is use to create a federation. SAML is defined by OASIS as a "Security Assertion Markup Language, an XML-based security specification for exchanging authentication and authorization information". See also OASIS.
SAML	Sercurity Assertion Markup Language - a standard, developed by the OASIS Security Services Technical Committee, for the exchange of authentication and authorization information across security domains.
Security	The prevention of unauthorized access and use via a combination of some or all of the other functions in this section.
Service Provider	A service provider is a web-based service which is protected by Shibboleth. See also Target.

Single factor authentication	An Authentication process in which a single form of Evidence is used to authenticate the user. In the case of Identity Authentication, this involves one of the following: • an Identifier provided by the person • knowledge demonstrated by the person ('something you know') • an act performed by the person (something you can do) • a Credential provided by the person ('something you have') • a Biometric surrendered by the person ('something you are' or something you do).
Smart Card	A small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit (IC). Smart cards containing an IC are sometimes called Integrated Circuit Cards (ICCs). Smart cards are used for a variety of purposes, including: 1) Storing a patient's medical records 2) Storing digital cash 3) Generating network IDs (similar to a token). To use a smart card, either to pull information from it or add data to it, you need a smart card reader, a small device into which you insert the smart card.
SOAP	Simple Object Access Protocol, esp. used for sending XML-based text messages across the Internet. It defines the message envelope (with a header to optionally describe security or transaction related info and a body for the data), encoding rules, RPC convention, and the binding with underlying protocols. Java API: JAXM, SAAJ, JAX-RPC (JSR 101), JMS
SP	Acronym for Service Provider.
SSO	SSO stands for 'Single Sign On'.
SSO - Single Sign-On	Single Sign-On (SSO) is a term used to describe technology which allows a user to access multiple resources, whilst only having to authenticate once. An example of a Single Sign-On technology is Pubcookie.
SSO - Single Sign-On	An authentication process in a client/server relationship where the user, or client, can enter one name and password and have access to more than one application or access to a number of resources within an enterprise. Single sign-on takes away the need for the user to enter

	further authentications when switching from one application to another. Single sign-on is also spelled single sign on or single sign-on and abbreviated as SSO.
Threat	A circumstance that could result in harm to an entity, for example, an earthquake, electricity failure, vandalism, malware (e.g. virus, trojan), software bug. A threat may be natural, accidental or intentional.
Threat assessment	A process to identify and examine the nature and implications of threats to an entity's assets.
Trust	A state that describes the agreements between different parties and systems for sharing identity information. A trust is typically used to extend access to resources in a controlled manner while eliminating the administration that would otherwise be incurred to manage the security principals of the other party.
Token	A physical thing, issued as a Credential. A Token is likely to include security features intended to render it difficult to forge, and tying it in some manner with the particular Entity. Examples include 'identity cards'(especially 'photo-id'), smartcards, one Time-password devices (e.g. RSA SecurID)
Two-Factor Authentication	Two-factor authentication is authentication using any two different methods. The most popular two-factor system is a combination of hardware tokens and passwords.
User	Any person who interacts directly with a computer system.
User ID	On most systems, accounts are uniquely identified by a short string of characters. This is called the User ID, login ID or login name.
User ID	A string of characters that is issued to an Identity, and is included within an Access Control List, and which thereby has Permissions, and is subject to Restrictions, in relation to Access to System Resources. Also referred to as LoginID and User Name. Normally used in conjunction with a Password or PIN, and possibly also a Token, in order to enable Authentication.
User Name	A unique handle assigned to each authorized user upon system registration.

validation	The process of identification of certificate applicants.
Verification (1:1, Matching, Authentication)	The process of establishing the validity of a claimed identity by comparing a verification template to an enrollment template. Verification requires that an identity be claimed, after which the individual's enrollment template is located and compared with the verification template. Verification answers the question, "Am I who I claim to be?"
Vulnerability	The susceptibility of an entity to a threat, in the form of a weakness that may permit a threatening event to give rise to harm. Safeguards are intended to reduce vulnerabilities. However, they may also increase them, or may create new vulnerabilities.
Workflow	Supports the routing of documents and content between individuals and processes. Enables features such as document approval.
WS	Web Services
WS-Federation	This specification defines mechanisms that are used to enable identity, account, attribute, authentication, and authorization federation across different trust realms. By using the XML, SOAP and WSDL extensibility models, the WS* specifications are designed to be composed with each other to provide a rich Web services environment. WS-Federation by itself does not provide a complete security solution for Web services. WS-Federation is a building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of security models.
WS-Security	Security Standard (JSR 183), Delivering a technical foundation for implementing security functions such as integrity and confidentiality in messages implementing higher-level Web services applications.
WS-Trust	The Web Services Trust Language (WS-Trust) uses the secure messaging mechanisms of WS-Security to define additional primitives and extensions for the issuance, exchange and validation of security tokens. WS-Trust also enables the issuance and dissemination of credentials within different trust domains. In order to secure a communication between two parties, the two parties must exchange security credentials (either directly or indirectly). However, each party needs to determine if they can "trust" the asserted credentials of the other party. This specification defines extensions to WS-Security for

	issuing and exchanging security tokens and ways to establish and access the presence of trust relationships. Using these extensions, applications can engage in secure communication designed to work with the general Web Services framework, including WSDL service descriptions, UDDI businessServices and bindingTemplates, and SOAP messages.
XACML	Extensible Access Control Markup Language. a policy language which allows administrators to define the access control requirements for their application resources. It was approved and became an OASIS standard in February 2003.

Annexure – VI: Task Force for preparation of Policy Document on Identity and Access Management

Chairman: Dr.S.I. Ahson, Professor of Computer Science, Department of Computer Science, Jamia Millia Islmia

Members

1. Dr. K. Subramanian, Deputy Director General, NIC
2. Mr. J. Satyanarayana, CEO, NISG
3. Mr. Gopal Krishna, J S-DIPP(E-BizProject)
4. Prof. P. Subba Reddy, Osmania University, Hyderabad
5. Prof. lndranil Sengupta, Head, School of IT, IIT Kharagpur
6. Mr. M.Badrinarayana, Sr. DGM, ECIL, Hyderabad
7. Ms. Anjana Choudhury, Senior Technical Director
8. Dr. S.C.Gupta, Senior Technical Director, NIC
9. Mr. T.M. Rao, Senior Technical Director, NIC
10. Mr. Raghunathan, State Informatics Officer, Kerala
11. Mr. Ramachandran, State Informatics Officer, Pondicherry
12. Mr. Vidya Shankar, Secretary, IIIT Law, Bangalore
13. Representative from STQC
14. Representative from CDAC
15. Representative from DARPG
16. Ms. Radha Chauhan, Principal Consultant E-Governance PMU, DIT
17. Ms. Rama Nangpal, SeniorTechnical Director, NIC
18. Ms. Debjani Nag, Scientist F, CCA, DIT
19. Mr. Pravin Chandekar, Additional Director, e-Governance, DIT
20. Mr. Golok Kumar Simli, Sr.Consultant, e-Governance PMU,DIT
21. Mr. Vikas Kanungo, CEO, SPeGov
22. Ms. Sudha Kumari, Senior Technical Director, NIC
23. Representatives from the Technology Solution Providers
    - i. IBM
    - ii. Microsoft
    - iii. Oracle
    - iv. Computer Associates
    - v. Novell
    - vi. Honeywell
    - vii. HP
    - viii. Red Hat
    - ix. ILANTUS Technologies
    - x. MPhasis
    - xi. PwC

Member Convenor: Ms. Pratibha Lokhande, Scientist-D, NIC

Annexure – VII: e-Governance Standards Division of NIC

There is a perceptible need to institutionalize the task of codifying e-governance standards and processes for the sake of ensuring interoperability of applications and solutions. Evolving standards and adoption of these for various components of e-Governance is indeed a high priority activity and is critical to the success of NeGP. National Informatics Centre (NIC) has been entrusted with the task of originating white papers on all the desired standards. To steer the process of evolving the Standards, a separate "e-Governance Standards Division" has been created by NIC under the chairmanship of Shri M. Moni, Deputy Director General. The major activities of this division are -

1. To steer and manage the standardisation activities under National e-governance program (NeGP).
2. To provide secretariat to the working groups, apex body.
3. Coordinate with the working groups, apex body and other organisations.
4. To originate white papers on all the desired standards that would serve as discussion papers for development of standards.
5. To work out timelines and resources required.
6. To form working groups as and when required.
7. To prepare terms if reference (TOR's) for the working groups.
8. To take services of experts and /or other specialized organisations.
9. To publish the draft standards on the website for obtaining feedback from external community and industry.
10. To submit draft standards to apex body for approval.
11. To coordinate with STQC for adopting of approved standards.

e- Governance Standards Division

Mr M. Moni, Deputy Director General

Ms. Suchitra Pyarelal, Technical Director and Head of Department

Member Secretaries of Working Groups

1. Ms. Aruna Chaba, Sr. Technical Director, Quality & Documentation Standards

2. Mr. T.M. Rao, Sr. Technical Director, Network & Information Security Standards
3. Dr. (Ms.) Meenakshi Mahajan, Technical Director, Meta Data & Data Standards for Application Domains
4. Mr. Kewal Krishan, Technical Director, Localisation & Language Technology Standards
5. Ms. Suchitra Pyarelal, Technical Director, Technical Standards & E-Governance Architecture
6. Mr. P.S. Bhat, Technical Director, Legal Enablement of ICT Systems

(URL: http://egovstandards.gov.in)

9. References

1. http://www.projectliberty.org/
2. http://www.oasis-open.org/who/
3. Messaoud Benantar, Access Control Systems: Security, Identity Management and Trust Models, Springer,2006
4. Rafae Bhatti, Elisa Bertino, and Arif Ghafoor, "An Integrated Approach to Federated Identity and Privilege Management in Open Systems", Communications of the ACM, February 2007,pp81-88
5. Western Australian Government Office Of e-Government, Identity & Access Management Framework, (Final Draft V2.0), 15 September 2005
6. HMG's Minimum Requirements for the Verification of the Identity of Individuals, e-Government Strategy Framework Policy and Guidelines, Version 2.0, Crown Copyright 2003
7. Laws of Identity, Kim Cameron, Microsoft Corporation
8. Microsoft's Vision for an Identity Metasystem
9. IBM Tivoli Security / Directory Standards
10. Accelerate Without Fear, Identity Management Helps Business Gear Up, White Paper, December 2005 by Sun Technologies
11. Identity Federation: Business Drivers, Use Cases and Key Business Considerations white paper by Computer Associates
12. Identity and Access Management (IAM) For E-Government in India: Issues, Challenges and an Approach, white paper by Venkata Ravipati, Oracle Corporation
13. Identity Management, white paper by HP
14. Identity Summit presentation by Novell
15. Success Factors for a PKI Based Identity Management Solution by Rajarathnam Nallusamy, Solution Architect, Red Hat India
16. Identity related e-Governance applications by Shri Ghan Shyam Bansal, Sr. Technical Director, NIC and State Informatics Officer, Haryana