Draft National e-Authentication Framework (NeAF)

Version: 1.0
Date: 01-09-2011

National e-Governance Division
Department of Information Technology
Ministry of Communications and Information Technology
Government of India
Electronics Niketan, Lodhi Road
New Delhi – 110003

e-mail: neaf@negp.gov.in

Questionnaire

"National e-Authentication Framework for e-Governance"

Department of Information Technology (DIT), Government of India has taken up the initiative of formulating a comprehensive framework on Electronic Authentication to deliver Government services in a seamless and paperless manner to the residents of the country through both internet and mobile platforms. In this regard, a Draft Consultation Paper on National e-Authentication Framework has been prepared by the National e-Governance Division (NeGD) within DIT, and is available on the DIT's website at the following URL:

www.mit.gov.in/whatsnew

DIT invites feedback and comments on the proposed policy framework on e-Authentication from all the interested stakeholders and citizens to refine the framework towards streamlining electronic authentication in e-Governance applications in the country. We request you to go through the Draft Consultation Paper and provide your inputs/comments on the specific questions mentioned in the table below:

S. No.	Consultation Questions
1	Which, according to you, are the most relevant areas in e-Governance and m-Governance where electronic authentication can prove to be the most effective?
2	Does the proposed e-Authentication Framework present any challenges for any specific e-Governance/m-Governance services as far as citizens or other stakeholders are concerned?
3	Do the layered approach and sensitivity levels adequately cover the various scenarios envisaged in the context of e-Governance/m-governance services? Are there scenarios where the Framework may prove to be inadequate?
4	Are all the objectives, as defined in the section 1.2 of the document, met satisfactorily by the Draft National e-Authentication Framework?
5	What, according to you, could be the issues that may arise in implementing the e-Authentication Framework in case of mobile based services?
6	What would be the most appropriate mechanisms to enhance cooperation among the central and state Government departments and agencies for adopting the e-Authentication Framework in all e-Governance and m-Governance applications?
7	Would you like to provide any suggestions with regard to the conceptual framework and the implementation methodology for e-Authentication in e-Governance/m-Governance applications in the country?
8	Any other suggestions or comments that you would like to provide with regard to the Draft National e-Authentication Framework?

You can send your valuable comments and suggestions to NeGD/DIT through email at neaf@negp.gov.in. Based upon your feedback, we may contact you for further inputs or invite you to participate in face to face consultations hosted by NeGD/DIT. The Nodal Officer in NeGD/DIT for this project is Dr. Rajendra Kumar, IAS, Director (Projects), NeGD, DIT. He can be contacted at rajendra@negp.gov.in.

Table of Contents

List of Figures

List of Tables

Executive Summary

The National e-Governance Plan (NeGP) of Government of India aims to create the right governance and institutional mechanisms, the core infrastructure and the policies in order to develop a citizen-centric eco-system for governance. As part of this larger initiative, several government services are being provided to the citizens through electronic means. To ensure easier and quicker access to government services in rural areas of the country, the Government has established Common Services Centres (CSCs) as common service delivery outlets where the citizens can access all government services over the internet. The online service delivery mechanism has generated the need for electronically authenticating the identity of the users so that each service or benefit scheme reaches its intended recipient in a secure manner. It has also necessitated electronic authentication of the government websites in order to build trust among the users. Moreover, an electronic authentication mechanism is required to create confidence and trust in the online environment which is always prone to identity thefts and other associated risks.

Therefore, in an endeavor to increase citizen’s trust in the online environment and to enable the various government agencies to choose appropriate authentication mechanisms, the Department of Information Technology, Government of India has conceptualized the National e-Authentication Framework (NeAF) to provide a uniform approach to managing identity authentications of all citizens for the delivery of various public services over internet and mobile platforms. The objective of NeAF is to provide a guiding framework to all central ministries, state departments and other government agencies for implementation of appropriate authentication processes and mechanisms as part of their service delivery strategy. The overall objective is to provide a trusted electronic environment where the users can transact easily and securely with the government.

The framework first defines the principles of e-Authentication along with its various components such as Identity Management, Authentication, Authorisation, Credential Registration, Permission Assignment, Deregistration and Single Sign on. The framework then defines a layered approach towards e-Authentication along with a six step methodology to determine the business and assurance requirements of government applications, the user registration process, the implementation model and the assessment of the chosen authentication model. The framework suggests a methodology for defining the application sensitivity level and selection of authentication mechanism for both internet and mobile based applications. This is followed by the technical architecture of “e-Authentication” as well as the roles and responsibilities of various stakeholders towards adoption and implementation of this framework. In the end, the document provides the proposed architecture of National e-Authentication Gateway leveraging the National Service Delivery Gateway (NSDG), State Service Delivery Gateway (SSDG) and Mobile Service Delivery Gateway (MSDG).

The adoption of the NeAF by all central and state government departments will help mitigate identity related frauds, reduce duplication of efforts and achieve consistency of authentication approaches across several disparate project implementations.

Abbreviations

i. CAP – Chip Authentication Program
ii. CSC – Common Services Centre
iii. DIT – Department of Information Technology, Government of India
iv. DPA – Dynamic Password Authentication
v. EMV - Europay, MasterCard and Visa
vi. IAM – Identity and Access Management
vii. IVR – Interactive Voice Response
viii. MCA – Ministry of Corporate Affairs
ix. MGNREGA – Mahatma Gandhi National Rural Employment Guarantee Act
x. MSDG – Mobile Service Delivery Gateway
xi. NeAF – National e-Authentication Framework
xii. NeGP – National e-Governance Plan
xiii. NSDG – National Service Delivery Gateway
xiv. OATH – Open Authentication
xv. OTP – One Time Password
xvi. PDS – Public Distribution System
xvii. PII – Personally Identifiable Information
xviii. PIN – Personal Identification Number
xix. SSDG – State Service Delivery Gateway
xx. SSO – Single Sign-on
xxi. UID – Unique Identification Project
xxii. USSD – Unstructured Supplementary Service Data

1 Introduction

1.1 Background

Government of India launched the National e-Governance Programme (NeGP) in the year 2006 with a vision "to make all government services accessible to the common man in his locality through common service delivery outlets and ensure efficiency, transparency and reliability of such services at affordable costs to realize the basic needs of the common man". As part of NeGP, a number of central and state e-governance projects such as Passports, MCA21, CSC, e-District, Commercial Taxes etc. have been launched. At the same time, several central ministries and state departments initiated their own e-governance projects such as PDS, MGNREGA etc. in order to provide better public services to the citizens.

Considering the huge potential of internet and their wide accessibility in both urban and rural areas (through CSCs and other channels), majority of e-governance projects have aimed to utilize the internet as their primary service delivery mechanism. Recently, there have been attempts to provide services through mobile devices as well. These web/mobile applications require the user to authenticate himself/herself so as to receive the service/benefit intended for him/her. However, due to decentralized implementation approach of NeGP and isolated project implementations of the individual e-Governance initiatives of various ministries/departments, the present authentication mechanisms are rudimentary and disparate across various applications. As a result, there is not only a lack of uniformity in the authentication methods of various departments but the citizen also has to provide different kinds of identity proofs for accessing public services which are fairly similar in many cases in terms of their criticality. This scenario has led to a sub-optimal end user experience as well as high maintenance costs as the users tend to forget passwords while trying to remember multiple passwords.

Against this backdrop, the Department of Information Technology (DIT), Government of India has conceptualized the National e-Authentication Framework (NeAF) that is intended to serve as the guiding document for all central and state ministries and departments for implementing appropriate authentication model for delivery of their services while maintaining uniformity across these authentication mechanisms.

1.2 Objectives

This document provides a framework to enable the government agencies to examine and address the authorisation and access management requirements associated with the deployment of e-Governance services. The objectives of creation of National e-Authentication Framework are as follows:

1. To provide a guiding framework to all central ministries and state departments for implementation of appropriate authentication processes and mechanisms as part of their service delivery strategy;

2. To define the various kinds of authentication mechanisms, and their usability in different scenarios, that can be utilized by all government agencies for authenticating citizens;
3. To enable consistency in government processes and procedures towards e-Authentication of user identity;
4. To increase efficiency and maximize ease-of-use for all stakeholders involved;
5. To suggest an indicative implementation model for the e-Authentication Framework in order to assist the government agencies in determining the most appropriate approach towards e-Authetnication;
6. To define the roles and responsibilities of all stakeholders as part of the e-authentication process.

1.3 Scope

The scope of National e-Authentication Framework is limited to the delivery of all government services through internet/mobile. The intention of National e-Authentication Framework is to assist all government departments/agencies at both central and state levels in the selection and implementation of appropriate authentication mechanisms for delivery of government services through internet/mobile.

2 Overview

2.1 What is e-Authentication?

Electronic Authentication (or "e-Authentication") is the process of electronic verification of the identity of a user. e-Authentication provides a simple, convenient and secure way for the users to access government services via internet/mobile as well as for the government to assess the authenticity of the users.

An authenticated identity is linked to the online services delivered by government agencies through the process of "Authorisation". Authorisation deals with the permissions or privileges granted to a user to access particular services provided by a system.

2.2 Why e-Authentication?

e-Authentication helps to build up confidence and trust in online transactions and encourages the use of the electronic environment as a channel for service delivery. In online transactions, data is communicated electronically through internet and mobile applications.

With the increased prevalence of online transactions, the government needs to set up suitable e-authentication processes and solutions after assessing the risks associated with these transactions.

2.3 What is National e-Authentication Framework (NeAF)?

The National e-Authentication Framework (NeAF) is a guiding framework for providing a mechanism to the government for electronic authentication and authorisation of the identity of the citizens to a desired level of assurance and confidence. The NeAF is a generic framework that can be utilized by any central or state government department or agency for implementing appropriate citizen authentication mechanisms.

e-Authentication is accomplished based on the following factors:

- *Knowledge* - something the user knows (e.g. user name, password, PIN, secret questions and answers),
- *Possession* - something the user has (e.g. security token, access card, ATM card) or
- *Be* - something the user is (e.g. biometric fingerprint, retina pattern, face pattern), or a combination of these.

Utilising one or more of these factors, there may be three kinds of authentication mechanisms:

i. **Single Factor Authentication:** An authentication mechanism that utilizes only one of the various factors (e.g.: a user using username and password for accessing a government application).

ii. **Two Factor Authentication:** An authentication mechanism where a combination of two factors is used (e.g.: a user using an ATM card (first factor) and his PIN (second factor) to withdraw money from his bank account).

iii. **Multi-factor Authentication:** An authentication mechanism where two or more factors are used with one of the factors necessarily being the "Third Factor – 'Be'" which is something the user is (e.g.: a user providing his UID number (first factor – "Knowledge") and his biometrics (third factor – "Be") at a ration shop to authenticate himself/herself).

Acceptable level of risk determines the appropriate authentication mechanism. The systems, applications and information with high-level of associated risk require a stronger authentication mechanism that confirms the user's digital identity. However, the applications with low level of associated risk do not require such strong authentication mechanisms.

Authorisation of authenticated identities to access applications, services and information is accomplished based on various assigned roles. The process of authorisation assumes that the identity has been successfully authenticated. However, the authorisation process needs to verify that the sensitivity level of the e-authentication fulfils the minimum requirements of the application. If the minimum requirements are not met, a higher level of e-authentication is requested. Then, permissions assigned to the identity are verified before permitting or refusing access to the service.

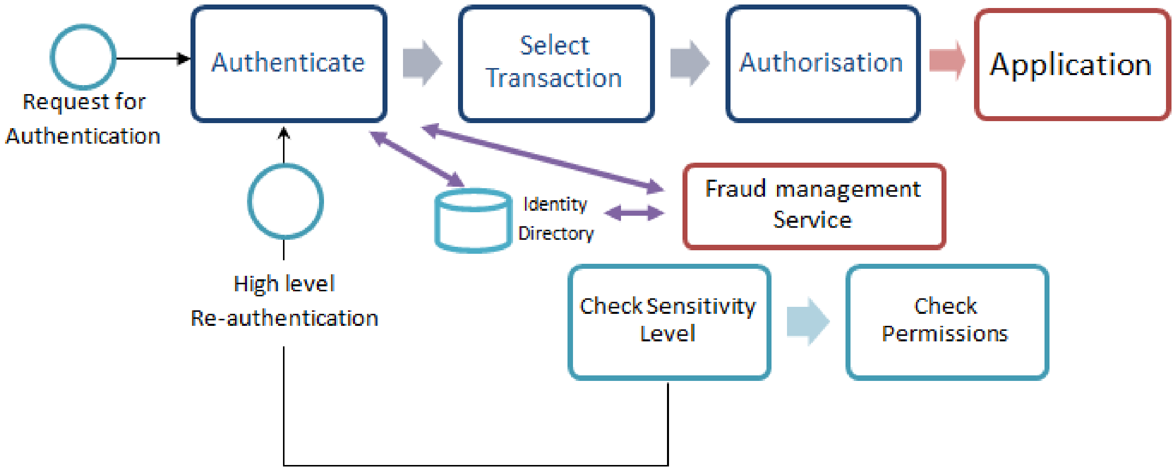

Figure 2-1 Process Flow

2.4 Why NeAF?

NeAF provides a guiding framework to all central and state ministries and departments for implementation of appropriate authentication processes and mechanisms as part of their service delivery strategy. NeAF provides guidelines that will help in the selection and implementation of the appropriate e-authentication approaches. Having a standardised e-authentication framework has the following benefits:

- Transparency – E-authentication decisions will be made in an open and transparent manner
- Cost-effectiveness – Government departments and agencies will not have to implement cumbersome and expensive e-authentication processes for simple or low-risk transactions
- Risk management – The selection of e-authentication mechanisms will be guided by the likelihood and impact of identified risks
- Consistency – Government departments and agencies will apply a consistent approach to selecting the appropriate e-authentication mechanism
- Trust – The mechanisms used will support online and mobile based services and enhance security, safety, and trust in such transactions
- Improved privacy – Personally identifiable information will be collected only where necessary as per the sensitivity level of the application or service
- Efficiency – The time to deploy an e-Authentication capability for any government application will be greatly reduced

3 Key Components

3.1 Identity Management

Identity management is a significant component to provide trusted and reliable online delivery of government services. Authentication and Authorisation should be considered within the context of identity management.

Identity management is an integrated system of business processes, policies and technologies that can enable the government to facilitate and control the citizens' access to critical online applications and resources - while protecting confidential personal and business information from unauthorised access. This includes the creation of the user entity (functionality typically found in a human resource application), authorisation and permissions (single sign-on and password management functionality), and a single point of administration for accounts hosted over one or multiple user stores.

3.2 Authentication

Authentication is the process of verifying the digital identity of the sender of a communication, such as a request to log in. The sender may be a person using a computer/mobile, a computer/mobile itself or a computer/mobile program. In a web of trust, authentication is a way to ensure users are who they say they are — that the user who attempts to perform functions in a system is in fact the user who is authorised to do so. An effective access management system incorporates one or more methods of authentication to verify the user, including passwords, digital certificates or hardware or software tokens.

3.3 Authorisation

Authorisation is the process of verifying that a known person has the authority to perform a certain operation on a given resource. Authentication, therefore, must precede authorisation. Authorisation governs what a user can access or do within an application. It lets the right users manage the content they have access to and the actions they can perform.

3.4 Credential Registration

Credential Registration is the process which results in issuance of an e-authentication credential, using which an identity can be electronically verified.

Credential Registration process may consist of a combination of the following elements:

1. **Checking identity documentation in order to verify the identity of a user**
2. **Creating user entries in a user directory**
   The database includes users' identity and associated information.
3. **Issuing a credential to a user**
   This credential will be used in the e-authentication process. The directory keeps the details regarding the credentials.

As the credential mechanism can be of different strengths, the credential may include a password, a token or a digital certificate.

The strength of the credential required will be determined by the sensitivity level requirements of the application or transaction.

3.5 Permission Assignment

In order to provide user access to online services, appropriate permissions need to be assigned to the user as part of the Permission Assignment process after issuance of credentials.
Permission Assignment may be implemented in one of the following ways –

- **As an extension of the credential registration process.**
  Access permissions may be assigned to the user for services delivered by the government agencies as part of the credential registration process.
- **As a separate activity performed at some time after the registration.**
  Access permissions may be assigned to the user based on a credential issued by some other agency, at a later point of time.

3.6 Deregistration

Deregistration is the process of de-provisioning a user from a system. As the authority of individuals may change over time, a comprehensive deregistration process helps to manage these relationships accurately.

3.7 Single Sign On

Single Sign-On is a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple applications. With this capability, a user logs in once and gains access to all systems without being prompted to log in again at each of them.

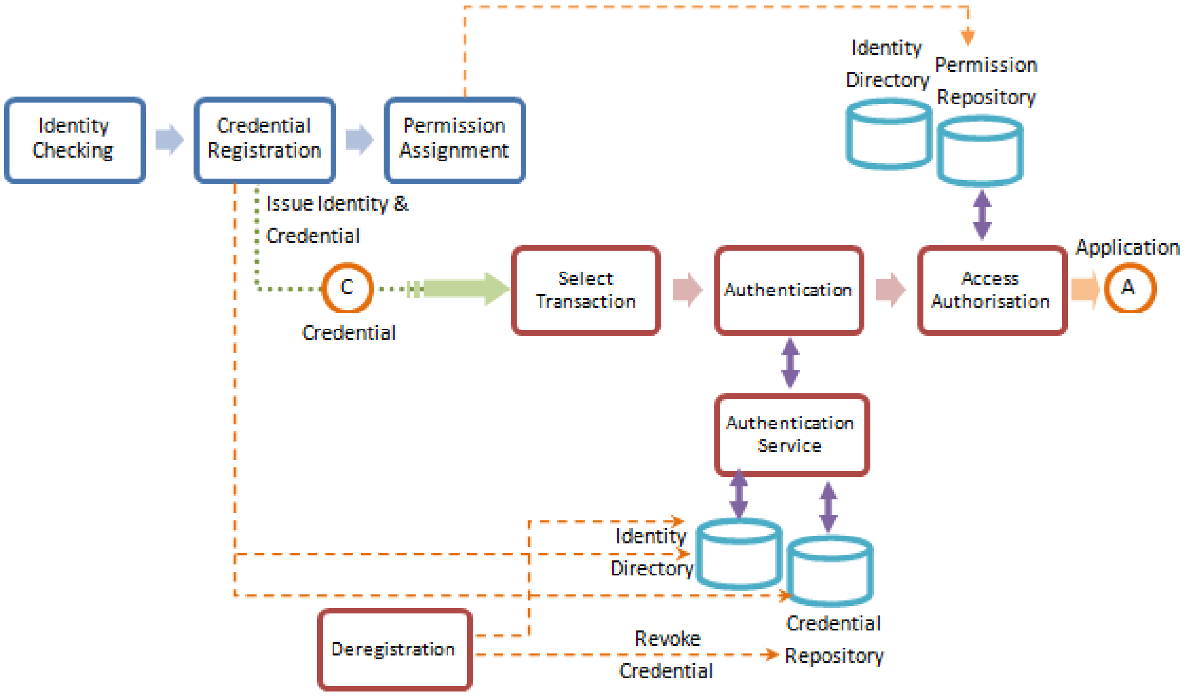

Figure 3-1 - Identity and Access Management

4 Layered Approach towards e-Authentication Implementation

Authentication and Authorisation are complementary and sequential processes in online transaction processing models and deal with the preliminaries to processing transactions. In simple terms, Authentication checks '*is this the person he/she claims to be*', and authorisation checks '*what is this person allowed to do*'.

Controlling what system resources users access and what they are authorised to do thereafter can be implemented at three levels within a system's architecture:

- Authentication layer
- Permission Management (Coarse Grained Authorisation) layer, and
- Business Logic (Fine Grained Authorisation) layer

Controls and rules of Authentication and Authorisation are abstracted from the Business Logic layer and placed in Authentication and Permission Management layers, respectively.

- Authentication layer verifies the digital identity of a user and provides a secure way for the users to access the government services via electronic media (mobile/internet).
- Permission Management layer controls access to individual application or class of applications.
- Business Logic layer implements the fine-grained Authorisation within the applications. This layer defines what activities a user can perform within an application or a class of applications. Examples of fine-grained access controls include rules relating to individual data fields in a record that may be viewed or changed.

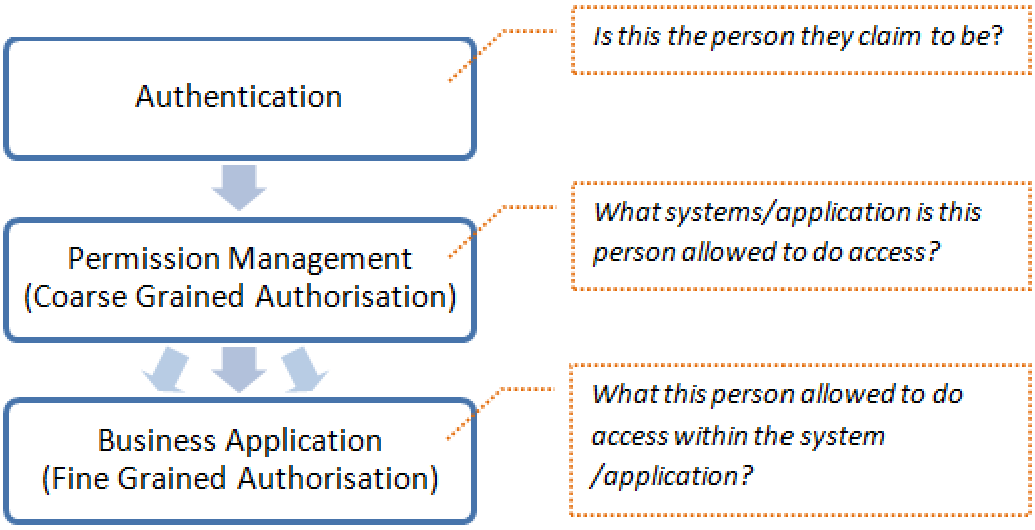
Authentication
Is this the person they claim to be?
Permission Management
(Coarse Grained Authorisation)
What systems/application is this person allowed to do access?
Business Application
(Fine Grained Authorisation)
What this person allowed to do access within the system /application?

Figure 4-1 Three layer Architecture

4.1 Links between Authentication and Permission Management Layer

A layered approach towards e-Authentication implementation requires separating the Permission Management activity from Authentication. Permission management layer is primarily concerned with the sensitivity level associated with an authenticated identity. Therefore this layer needs to access the sensitivity level associated with the e-authentication credential. It may request a higher level of e-Authentication if required. This includes situations where permission management is implemented within a business logic layer.

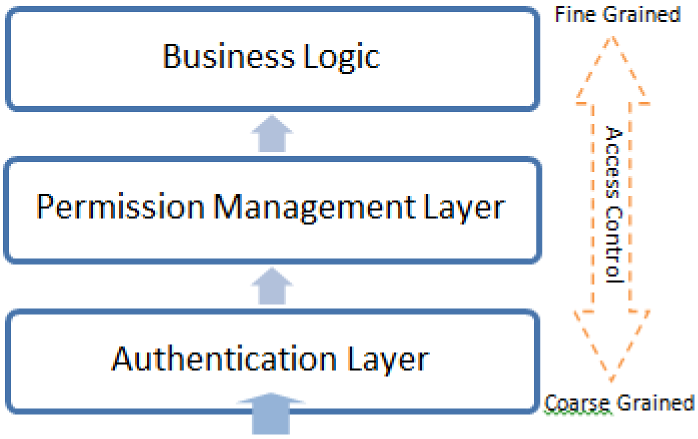

Figure 4-2 Access Control Layers

5 Methodology

5.1 Website Authentication

During the delivery of online public services, it is not only important to authenticate the user for her/his identity, but it is also important to authenticate the website that the user is accessing for availing various public services. Considering the number of phishing[1] attacks that take place over the web every day, the user must be able to correctly identify that the website that she/he has opened is actually the right website that it is claiming to be. Lack of appropriate security measures in ensuring the authenticity of websites may lead to the user revealing her/his personal credentials over a fake website, which can amount to severe financial and social losses to not only the user but also to the concerned department whose web interface was imitated for this purpose.

There are various web-based authentication techniques available today which are intended to enhance user security and/or thwart phishing scams. This is especially common in the banking world, where most applications are starting to use strong two-factor authentication. Unfortunately, for most of the large consumer web applications, implementing strong multi-factor authentication (i.e. smart cards or hardware tokens) is just not cost effective or practical because of the sheer size of the user population which needs to be dealt with that can often be upwards of several million. As a result, these applications must resort to other creative ways to strengthen their authentication.

An increasingly popular practice to ensure website authentication is the use of security images (known as "watermarks") to thwart phishing scams. This concept (generically known as site-to-user authentication) works as follows:

- During the registration process, the user selects (or is assigned) a specific image and also some user defined text (optional) with user defined font and colour. The image is one of the potentially hundreds of available images and is intended to help the user distinguish the real web-site from an impostor. The actual process of authenticating the website is split into the following three steps:
    - Step 1: The user submits her/his username (only) to the website
    - Step 2: The website shows the user with the personal "watermark" image (with text if supplied), allowing her/him to verify that she/he is at the correct site.
    - Step 3: If the watermark image is correct, the user should enter her/his password to complete the login process. If the watermark image is not correct (or not shown), the user should not proceed as she/he is likely to be at a wrong/phishing website.

The general concept is simple and is being used for many years now. Banks and other websites over the years have introduced such site authentication images to help users distinguish a

[1] Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Source: http://en.wikipedia.org/wiki/Phishing

bank's real website from the impostor sites. These sites repeatedly instruct their customers to verify their site-authentication images before entering their passwords. The absence of a site-authentication image is a clue that might reveal a man in-the-middle attack against the bank's web address. Alternatively, this clue might also alert participants that the page has been loaded from the address of a 'phishing' web site.

Organizations that wish to use strong authentication have a variety of methods from which to choose. These range from simple, traditional username/password mechanisms that exist in every operating system, to hardware based one-time password (OTP) tokens, biometric, smart card, and PKI based systems. However, all these solutions confirm that a higher level of security is a trade-off between cost and convenience. In the past, authentication solutions were either i) easy-to-use, inexpensive but insecure (such as username/password), or ii) very secure but expensive or difficult to implement (such as OTP tokens and smart cards). However, with the advances in technology, today there is a third option: a software only, two-factor authentication solution. A soft token delivers the right balance of cost, convenience, and strength for a lower cost of ownership than alternative solutions.

A soft token technology can protect citizens from sophisticated Internet threats like man-in-the-middle, brute force, phishing, pharming, password cracking, and other attacks. For example, the soft token can verify that the user is signing into the domain that issued it before prompting the user for his password, preventing the man-in-the-middle and other phishing attacks from succeeding where OTP tokens and Grid Pads cannot.

On the whole, there are multiple ways of ensuring website authentication with the help of hardware tokens, software tokens, biometrics, PKI etc. However, the need for a particular mechanism can be derived based on the level of criticality of a website as well as the profile of its user base in terms of their capabilities to use such mechanisms.

5.2 Implementation Approach

The NeAF methodology can be defined as a six-step process (in no particular sequence). It should be undertaken in the context of the wider information security risk management processes. The NeAF primarily addresses identity related solutions that include identity authentication, step-up authentication, single sign-on across various government websites & identity management. NeAF can enable authentication credential to any government website to authenticate citizens.

The six steps of NeAF methodology are as follows:

1. Determine the business requirements
2. Determine the application sensitivity level
3. Select the registration approach
4. Implementation model
5. Assess the business case and feasibility of the implementation model

6. Review the e-Authentication solution.

5.2.1 Step 1: Determine the business requirements

This step is usually undertaken as part of the "requirements gathering" phase of an e-Governance project that aims to build online/mobile services for government ministry/department.

The key business requirements that need to be determined in this step are as follows:

i. Identify the services that will be provided by the government over website/mobile as well as the information that will be accessed by the citizens;
ii. Identify the various kinds of user interactions required with the website/portal/mobile interface;
iii. Determine the authentication level based on application sensitivity matrix defined in step 2. In addition, transaction confidence such as data integrity, non- repudiation, confidentiality, etc. needs to be addressed to boost the citizen confidence in using online/mobile services.
iv. For single sign-on, it would be important to determine the assertions required for authentication. Also, it would be required to check if the user has access to the identified web/portal/mobile application.
v. Identify the privacy implications inherent in the proposed transaction, and/or the privacy issues that need to be satisfied in the determination of the need and the type of e-Authentication approach.

5.2.2 Step 2: Determine the Sensitivity Level

Sensitivity levels are used to describe the level of importance of getting e-Authentication right and the resultant level of robustness of the required solution.

Level 0	Level 1	Level 2	Level 3	Level 4
No assurance of identity is required	Minimal level of assurance of identity is required	Minor level of assurance of identity is required	Significant level of assurance of identity is required	Substantial level of assurance of identity is required

Table 5-1: Sensitivity Levels

The NeAF determines sensitivity levels based upon the assessment of the threats to agencies and/or end-users of getting e-Authentication wrong. The sensitivity level is determined by mapping the impact versus likelihood of occurrence of the threat. An indicative mapping of impact versus likelihood is illustrated in the Table 5-2 below:

	Threat Impact				
Likelihood	Insignificant	Minimal	Minor	Significant	Substantial
Almost Certain	Level 0	Level 2	Level 3	Level 4	Level 4
Likely	Level 0	Level 2	Level 3	Level 4	Level 4
Possible	Level 0	Level 1	Level 2	Level 3	Level 4
Unlikely	Level 0	Level 1	Level 2	Level 3	Level 3
Rare	Level 0	Level 1	Level 2	Level 3	Level 3

Table 5-2: Indicative Application Sensitivity level based on likelihood and impact of threats

Once the application sensitivity level has been identified using the above table, the appropriate authentication mechanism can then be chosen based on the "Application Sensitivity Matrix" as defined under section 5.2.2.1 for Internet based applications or section 5.2.2.2 for Mobile based applications.

5.2.2.1 Internet Based Applications

There are five levels of application sensitivity for web based applications ranging from Level 0 to Level 4. The Level 0 is the lowest application sensitivity level whereas Level 4 is the highest. Level 0 will not require any form of authentication and will be used for providing public information over the web. All applications will therefore authenticate users using Level 1 authentication by default. Sensitivity of the application, including URLs, should be defined during application development cycle. This would enable the application to call proper authentication scheme at the right time. Application sensitivity will call in from Level 1 through Level 4 authentication mechanisms at the appropriate stage.

A summary of the technical requirements for each of the five levels is provided below:

Level 0: This level implies no authentication. The user can go to the government website and access all information that is made available for public use.

Level 1: This is the basic authentication mechanism provided using Directory authentication. The user would receive username and password after successful enrollment which may be done either directly by the government or by an authorised agency. During the first log-on of a user to the portal or designated website, the user would be prompted to change her/his password. This password should not be transmitted in plain text format. Alternatively, the user could be provided the capability of self-registration by which she/he can generate a username/password by herself/himself. A self-service identity management mechanism will be used by the user if she/he forgets her/his password. It will avoid unnecessary calls to helpdesk for resetting the user passwords.

Level 2: At Level 2, a user will prove her/his identity using X.509 digital certificate along with his Level 1 credentials (i.e. username and password). This would enable building a trust between the user and the government website/portal. It would enable the users to upload sensitive documents that are signed using citizen's digital certificate. Information exchange between two parties would be securely processed and the transaction will be denied in case the certificate is compromised or lost.

Level 3: At Level 3, the user would need to prove her/his identity through a token plus username and password (i.e. two factor authentication). For this purpose, three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens and "one-time password" device tokens. However, the recommended kind of token to be used is a soft token due to the sheer size of the user population and the high manageability and cost implications associated with hardware tokens. The authentication mechanism would require the user to prove through a secure authentication protocol that she/he controls the token and must first unlock the token with a password or must also use a password in a secure authentication protocol to establish two factor authentication.

Level 4: At Level 4, the user will prove her/his identity using two factor authentication which will necessarily include biometrics as one of the factors while the other factor could be either a soft token or a username/password. This is the highest level of authentication security that would be provided to a citizen/internal privilege user (e.g. a department user). Bio-metric authentication should be done in accordance with biometric authentication mechanism as defined by the Unique Identification Authority of India (UIDAI) so as to avoid the duplication of citizen information.

"Fraud Management" Layer for Applications with Level 3 and Level 4 Sensitivity:

Considering that the sensitivity of applications falling under Level 3 and Level 4 is very high, there is a need for an additional layer of defence to prevent any kind of fraud. A "Fraud Management" layer will provide real-time protection against identity theft and online fraud via risk–based, adaptive authentication. It will evaluate the fraud potential of online access attempts and calculate the risk score based on a broad set of variables. The "Fraud Management" layer will perform this task transparently without inconveniencing legitimate, low-risk users. For example:

- Scenario 1: In case a user has been successfully authenticated into a critical government application and a similar authentication request is received from the same user but from a different geographical location within a very short span of time, then such a transaction would be declined.
- Scenario 2: The government may decide to block access to certain critical information if the request has been received from a specific country(ies). In such a scenario, the "Fraud Management System" can detect/stop such a request and alert the management.

A reference "Sensitivity Matrix" for identifying the right level of authentication is provided in the Table 5-3 below:

	Application Sensitivity				
Sensitivity Level	Level 0	Level 1	Level 2	Level 3	Level 4
User Experience	No inconvenience	Minimal inconvenience	Minor inconvenience	Significant inconvenience	Substantial inconvenience
Scenarios	Public information	Information with minimal impact in case of theft	Information having social impact but no financial/security impact	Information having financial/security impact	Information having very high financial/security Impact
Examples	Election Results	Examination Results	Personally Identifiable Information (birth certificate, death certificate, land records etc.)	Financial Information (Bank Accounts), Service Impairment (such as IRCTC website being brought down)	National Security Information (CCTNS, RAW, CBI Cases, etc.)
Suggested Authentication Method	No Authentication required	Username-Password	Digital certificate/soft token	Two factor authentication: Soft/hardware token along with Username and Password	Two factor authentication: Biometric + Token / Username and Password
Fraud Management Layer Required	No	No	No	Yes	Yes

Table 5-3: Sensitivity matrix for identifying the right authentication level for web-based apps

5.2.2.2 Mobile Based Applications

For mobile based applications too, there are five levels of application sensitivity ranging from Level 0 to Level 4. The Level 0 is the lowest level of application sensitivity whereas Level 4 is the highest. A Level 0 mobile application will not require any form of authentication and will be used for providing public information over a mobile device. All applications will therefore authenticate users using Level 1 authentication by default. Sensitivity of the application should be defined during application development cycle. This would enable the application to call proper authentication scheme at the right time. Application sensitivity will call in from Level 1 through Level 4 authentication mechanisms at the appropriate stage.

A summary of the technical requirements for each of the five levels is provided below:

Level 0 (for both non-smart phones and smart phones): This level implies no authentication. The user can avail the government service through various mechanisms such as SMS, USSD (Unstructured Supplementary Service Data), IVR (Interactive Voice Response) etc. using her/his mobile phone and can access all information that is made available for public use.

Level 1 (for both non-smart phones and smart phones): This is the basic authentication mechanism for accessing a personalized government service. The user would receive a username & password after successful enrolment which may be done either directly by the government or by an authorised agency. The agency may send password using SMS or print mailer. Alternatively, the user could be provided the capability of self-registration by which she/he can generate a username/password by herself/himself through SMS/USSD/IVR/Mobile Browser, etc. The user can change her/his password periodically through SMS/USSD/IVR/Mobile Browser, etc. The user can then request for a service by providing her/his username and password along with other service defined parameters to a pre-defined number.

Level 2 (for both non-smart phones and smart phones): At Level 2, a user will prove her/his identity using username, password and Q&A (Question and Answer). The user would receive the username & password after successful enrolment by the government or by an authorised agency. The user would also have to choose a few questions and answers at the time of registration, which will be asked later during authentication. At the time of accessing a government service, the user will first provide her/his username and password through SMS/USSD/IVR/Mobile browser, etc. to a service and will then be prompted with a random question (such as “what is your mother’s maiden name?” chosen out of the questions selected by the user at the time of registration). The user will have to correctly respond to this question in order to access the service. The user might be prompted for more than one question as well depending upon the criticality of the service.

Level 3 (for both non-smart phones and smart phones): At Level 3, a user has the following two choices depending upon the type of phone that she/he carries:

i. Option 1 (for both non-smart phones and smart phones): In this scenario, the user needs to prove her/his identity through username and password plus a modified SIM containing the user’s digital certificate (i.e. two factor authentication). The modified SIM will be issued to the user by her/his mobile service provider. This will ensure that all transactions performed by the user are secure not only at the end points but also through the network over which the data travels.

ii. Option 2 (for only smart phones): In this case, the user needs to prove her/his identity through username and password plus a taken based OTP (i.e. two factor authentication). This level of authentication will be available only in case of smart phones due to the requirement of data transaction over HTTP protocol. The user will be required to download and install an "OTP Generator" from a trusted website (either provided by the government or by an authorised agency). While accessing a government service, the user will have to provide his/her username, password and the random OTP generated through the OTP Generator. To generate an OTP, the user would be required to first unlock the "OTP Generator" with a separate password. This will ensure that even if a user's mobile phone is stolen and his application username/password has been accessed, the attacker will have to find out the OTP Generator's password to generate the OTP thus preventing any possibility of identity theft. The "OTP Generator" application will also need to have the capability to self-protect from various attacks such as brute force and dictionary attacks. This will ensure that the "OTP Generator" will not reveal the true password to the attacker who is using brute force or dictionary kind of attacks in order to try all possible passwords to generate an OTP. The OTP should be a standard based solution supporting open standards such as EMV – Europay, MasterCard and Visa (including CAP - Chip Authentication Program/DPA - Dynamic Password Authentication), OATH – Open Authentication and RFC 2289.

Level 4 (for biometric enabled phones): At Level 4, the citizen will prove her/his identity using two factor authentication which will necessarily include biometrics as one of the factors while the other factor could either be a soft token (OTP) or a username/password. This is the highest level of authentication security that would be provided to a citizen/internal privilege user (e.g. a department user). For this purpose, the mobile phone of the user should be equipped with a biometric reader in order to capture the fingerprint or iris (as defined by the UIDAI).

"Fraud Management" Layer for Applications with Level 3 Sensitivity:

Considering that the sensitivity of applications falling under Level 3 and Level 4 is very high, there is a need for an additional layer of defence to prevent any kind of fraud. A "Fraud Management" layer will provide real-time protection against identity theft and online/mobile fraud via risk–based, adaptive authentication. It will evaluate the fraud potential of online/mobile access attempts and calculates the risk score based on a broad set of variables. The "Fraud Management" layer will perform this task transparently without inconveniencing legitimate, low-risk users. For example:

- Scenario 1: In case a user has been successfully authenticated into a critical government application using her/his mobile and a similar authentication request is received from a different mobile phone with the same credentials (or from a different geographical location within a very short span of time), then such a transaction would be declined.

- Scenario 2: The government may decide to block access to certain critical information if the request has been received from a specific country(ies). In such a scenario, the "Fraud Management" layer can detect/stop such a request and alert the management.

A reference "Application Sensitivity Matrix" for identifying the right level of authentication for mobile based applications is provided in the Table 4 below:

	Mobile Application Sensitivity				
Sensitivity Level	Level 0	Level 1	Level 2	Level 3	Level 4
User Experience	No inconvenience	Minimal Inconvenience	Minor Inconvenience	Significant Inconvenience	Substancial Inconvenience
Scenarios	Public information	Information with minimal impact in case of theft	Information having social impact but no financial/life threatening impact	Information having financial impact	Information having very high financial / life threatening Impact
Examples	Election Results	Examination Results	Personally Identifiable Information (birth certificate, death certificate, land records etc.)	Financial Information (Bank Accounts), Service Impairment (such as IRCTC website being brought down)	National Security Information (CCTNS, RAW, CBI Cases etc.)
Suggested Authentication Method	No Authentication required	Username-Password	Username – Password + Q&A	Username – Password + OTP	Two Factor Authentication: Biometric + Soft Token (OTP) / Username – Password
Fraud Management Layer Required	No	No	No	Yes	Yes

Table 5-4: Sensitivity matrix for identifying the right authentication level for mobile based apps

5.2.3 Step 3: Select the registration approach

The registration approach will be determined by the following:

- The "Application Sensitivity Level" (level 1 through 4) desired by the government for the particular application
- Whether the user is already a known entity to the registering agency. In such a case, two variations may emerge:
  - The user has no pre-existing e-Authentication credential
  - The user has a pre-existing e-Authentication credential and requires step-up authentication or additional application access

The registration process will verify the citizen's identity or other attributes to determine the appropriate "Application Sensitivity Level" prior to creating an e-Authentication credential.

The approach to registration will depend upon the nature of the application to be accessed and the accessing party. The most common instances are:

- Registration of users (as themselves)
- Registration of users as representatives of businesses; and
- Registration of users as representatives of other individuals.

E-Authentication Framework will have following stages for registration of new users:

- Stage A – Enrolment of a user
- Stage B – Generation of authentication credentials for the user
- Stage C – Provisioning the user identity in directory and assigning appropriate access permissions to the user based on her/his profile using Identity Management System.

E-Authentication Framework will have following stages for an existing user who needs additional access permissions or step-up authentication:

- Stage A – Fill-in requisite forms through a government department or an authorised Enrolment Agency

OR

- Stage A – Upload requisite forms to India Portal/State Portal/Designated Government Website
- Stage B – Perform authorisation check in the background
- Stage C – Assign additional access to the user through Identity Management System
- Stage D – Define step-up authentication for the user and provide new credentials to her/him as per the application sensitivity matrix defined in step 2.

E-Authentication Framework will have following stages to de-provision user from the authentication server:

- Stage A – User visits the government department or the authorised Enrolment Agency for de-provisioning from the authentication server.

OR

- Stage A – User makes an online request for de-provisioning if she/he no longer requires access to the service.

5.2.4 Step 4: Implementation model

In step 3, a user would follow the registration process to obtain her/his unique User ID. An algorithm therefore needs to be developed to generate a unique User ID of each user that should be easy to remember.

As an illustration, the government can use UID or the user's mobile number as her/his "User ID" as it is unique & there is no need for providing another ID to the user.

Pre-requisites:

a. Any existing authentication process within the individual applications should be terminated and all authentication requests should be redirected to the dedicated central authentication server.

b. A common login page (such as India portal or State Portal) should be used for all user logins. All government websites/portals should redirect the login request to the common login page.

c. Fine grained access control should be maintained within the respective applications only.

d. The need for step-up authentication needs to be defined. Also, the application would determine where step-up authentication is required and send the appropriate request to the authentication server.

e. "As-Is" & "To-Be" study should be done for the existing applications from the single sign-on & authentication requirements perspective.

5.2.5 Step 5: Assess the business case and feasibility of the e-Authentication model

This step involves the tools to model costs and benefits to financially justify the implementation of the e-Authentication framework. A three-step approach to perform this cost and benefit analysis is as follows:

Step 1: Review the environment and identify business needs
Step 2: Carry out a high-level options analysis
Step 3: Carry out a detailed options analysis

5.2.6 Step 6: Review the e-Authentication solution

Once an e-Authentication framework has been selected, it is necessary to validate it. E-Authentication framework solution includes the use of a pre-existing credential. It will also be necessary to analyze the legal processes, technology and cost issues associated with the necessary implementation and operational model. Also, it should be considered whether the selected registration approach and authentication mechanism that have been decided using the "application sensitivity matrix" require any further enhancement.

5.3 Checklist

The following checklist can serve as a guideline for government departments and agencies when implementing the NeAF.

→ Identify and analyse the service or cluster of services to be provided online.
   - Service description: A full description of the service, including the number and frequency of service requests (transactions) across user groups.

→ Determine the service sensitivity level.
   - Identify the user base the services will target.
   - Review any existing approaches to e-authentication for services provided by the government (or any other government agency) to the planned user base.
   - Plan the process that will determine the service risks, sensitivity levels and e-authentication approaches.

→ Decide what information needs to be authenticated
   - Consider the nature of the service and the surrounding business processes.
   - Decide what information needs to be authenticated.
   - Assess what aspects of that information are important.
   - Decide whether identity e-authentication is necessary.

→ Assess the risks
   - Identify the types of threats that apply to online services.
   - Determine the likelihood of the threats occurring and their consequences in order to identify the level of risk.
   - Identify risk management strategies.
   - Identify the level of assurance needed from e-authentication approaches to mitigate the risk.

→ Assess the various e-authentication mechanisms
   - Identify possible e-authentication approaches.
   - Shortlist e-authentication approaches for consideration.
   - Select a default e-authentication approach.
   - Decide whether any impact assessment needs to be undertaken.
   - Decide whether the proposed approach to e-authentication is feasible from both government and business perspectives.
   - Identify the preferred e-authentication mechanism.

6 Technical Architecture

A high-level view of possible technology architecture for implementing Identity and Access Management is shown below:

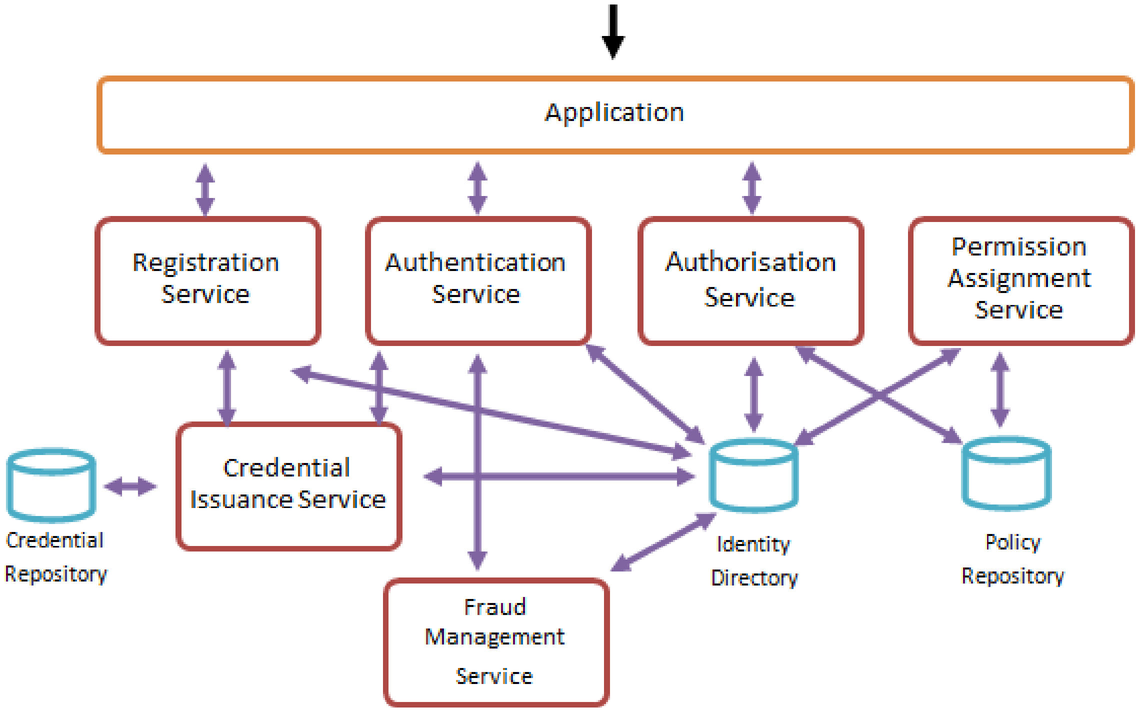

Figure 6-1 Indicative Technology Architecture

6.1 Registration and credential issuing services

Credentials are selected based on the sensitivity level of the application. At the time of registration, information about credentials is obtained from authoritative sources.

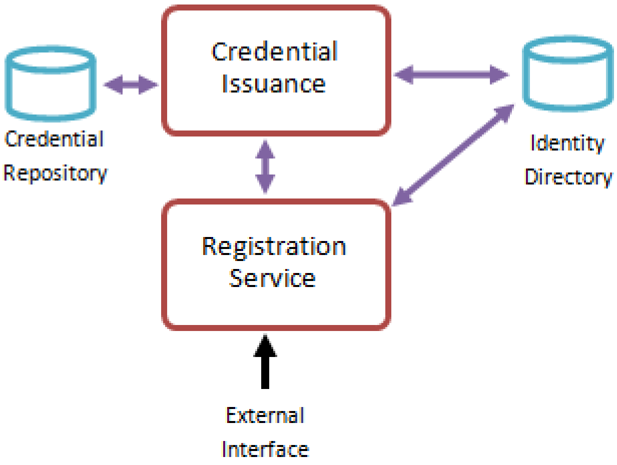

Figure 6-2 Credential issuance and registration services

6.2 Permission assignment service

Permission assignment service provides the ability to set access permissions for users.

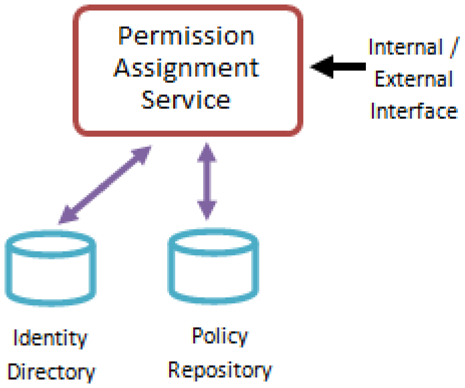

Figure 6-3 Permission Assignment Service

The policy repository stores the details of currently established permissions. This permissions information will include required e-authentication sensitivity levels. However, user details are held in the directory.

To enforce access control, Permissions enforcement services act on the permissions information in the policy repository.

6.3 Authentication services

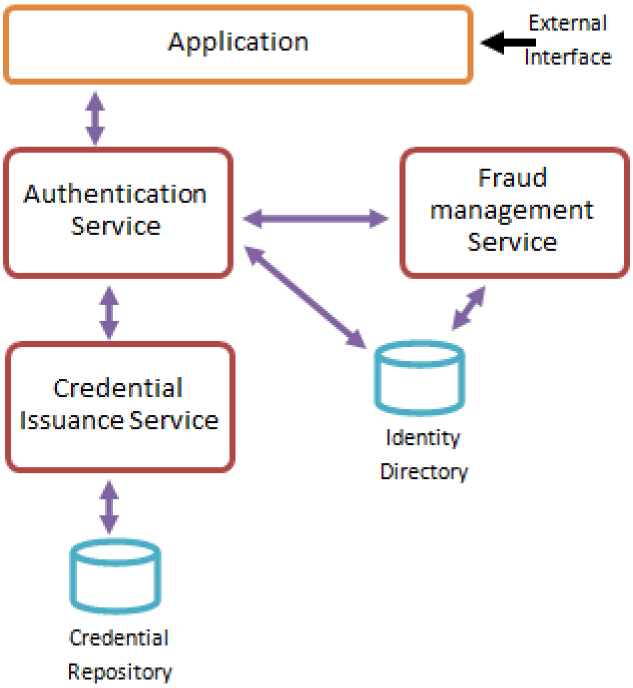

Figure 6-4 Authentication Service

The e-authentication service authenticates credentials to verify an identity. It resolves identity of the issuer of the credential by referring to the user directory and requesting e-authentication from the relevant issuer, which is the authoritative processor of e-authentication requests.

6.4 Access Authorisation services

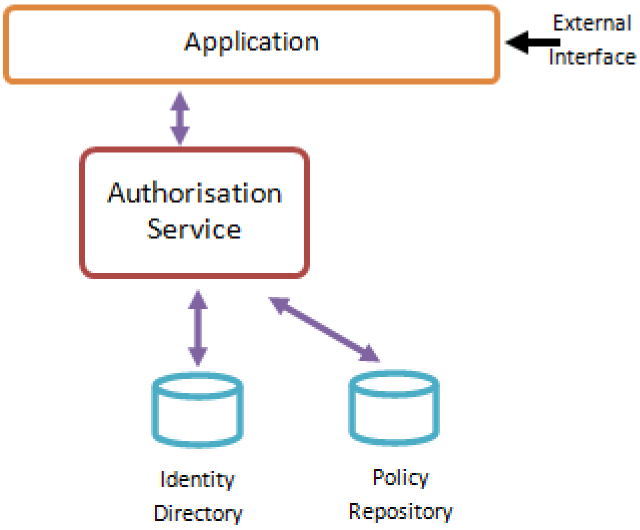

Figure 6-5 Authorisation Service

Roles and specific permissions associated with an identity are established during permission assignment and stored in the user directory and policy repository.

Access authorisation services can be called from any authenticated application requesting the current permissions of a previously authenticated identity. The authorisation services provide the necessary information to the calling application to enable it to allow or disallow access. This is based on:

- the policy for particular applications (established by the application administrators), and
- the roles of the identity held within the user directory (established during the permission assignment process) and subsequent updates to permissions and roles.

7 Components of Identity and Access Management

7.1 Identity and Access Management (IAM)

e-Authentication is part of the broader identity and access management systems. IAM comprises of people, processes and products to manage identities and access to resources of a government enterprise. Additionally, the government enterprise shall have to ensure the correctness of data in order for the IAM Framework to function properly. The ultimate goal of the IAM Framework is to provide the *right access* to the *right people* at the *right time.*

IAM components can be classified into four major categories:

(i) Authentication
- Single Sign-On
- LDAP v3 – Directory
- Step-up authentication/Strong authentication
- X.509 certificate
- Hardware/Software Token
- OTP
- Biometric Authentication

(ii) Authorisation
- Role/Rule based
- Attribute based
- Remote Authorisation

(iii) Identity Management
- User management (includes creation/deletion/modification in the end application as per the role defined in Identity Management)
- User self-service
- User request for additional application access

(iv) Central User Repository & User Activity Reporting
- Directory
- User Activity Reporting

7.2 Components of Authentication Process

The various components of the authentication process are as follows:

7.2.1 Identity Management System

Identity Management System (IMS) provides the platform that automates the creation, modification and deletion of user identities and their access to resources with an enterprise (a government department). Identity Management System's main aim is to create user in the X.500 based Directory & defining her/his role as per her/his profile. The IMS has a 3-tier architecture consisting of web tier, application tier and data tier.

Role Management is an integral part of the IMS. The success of the IMS depends on defining proper roles within Identity Management. Managing user entitlements on an individual basis is simply not a cost effective option and hence most identity management deployments are founded on a role-based approach. Role for the application may include a different provisioning policy which modifies the account (e.g., places user within an application role or group).

Identity Management provides the following capabilities:

- Automated provisioning & de-provisioning of user accounts and access permissions
- Centralized audit & reporting of user entitlements
- Delegated user administration
- Integrated workflow
- Password management
- Registration services
- User self-service
- Extensive open interfaces, including an identity management web service
- Automated input with Universal Feed Support, Web Services, and SPML

7.2.2 Directory Management

A Directory server acts as the backbone of the e-Authentication framework. Directory provides superior experience and security for web applications/portals. It is therefore important that the Directory server is scalable & tested for millions of users and hundreds of servers in distributed environments. Directory server holds the user information such as user id/password, attribute, general user information, etc. for all users that are enrolled. Directory Management provides the following capabilities:

- Unlimited scalability (a solution tested for a minimum of 100 million users)
- Built-in high availability
- Large flat-namespaces splitting across many servers using horizontal portioning
- Intelligent and transparent chaining of queries to distributed servers
- Seamless failover and failback capabilities
- Strong security

7.2.3 Single Sign-On

Users are expected to use a number of government applications for availing different services. Therefore, a user might switch from one application to another depending upon her/his need for the service. Accordingly, the user should have the capability to seamlessly access multiple applications without the need for providing username & password multiple times.

"Single Sign-On" helps achieve this objective using federation capabilities provided by Security Assertion Markup Language (SAML) protocol. SAML is an XML framework for exchanging authentication and authorisation information. Although SAML also covers authorisation to some extent, its primary focus is on passing e-authentication information. SAML based identity federation provides the users of one application the capability to securely access the data and applications of another application. This can be done without the need for redundant user stores for each application.

The various components of Single Sign-on are:
Federation: An agreement between an *identity provider* and one or more *service providers* about the data used to describe users (e.g., e-mail address, role, membership in a group, or unique (opaque) identifier known only to the *identity provider* and *service provider*).

Identity Provider (IdP): A SAML authority (e.g., an enterprise) that produces SAML assertions for p*rincipals (a system entity whose identity can be authenticated - often a user)*. These SAML assertions are used as “session tickets” to establish *federation*. *Identity provider* is synonymous with SAML producer or “asserting party”.

Service Provider (SP): An entity (e.g., an enterprise) that provides services and/or goods to *principals*. A *service provider* consumes SAML assertions produced by an *identity provider*. *Service provider* is synonymous with SAML consumer or “relying party”.

As an illustration, if India Portal is used to authenticate users through a Directory server then the India Portal will act as an “identity provider” and all applications being accessed through the India Portal will act as “service providers”.

The process flow of the Web Browser SAML Artifact Profile is as follows:

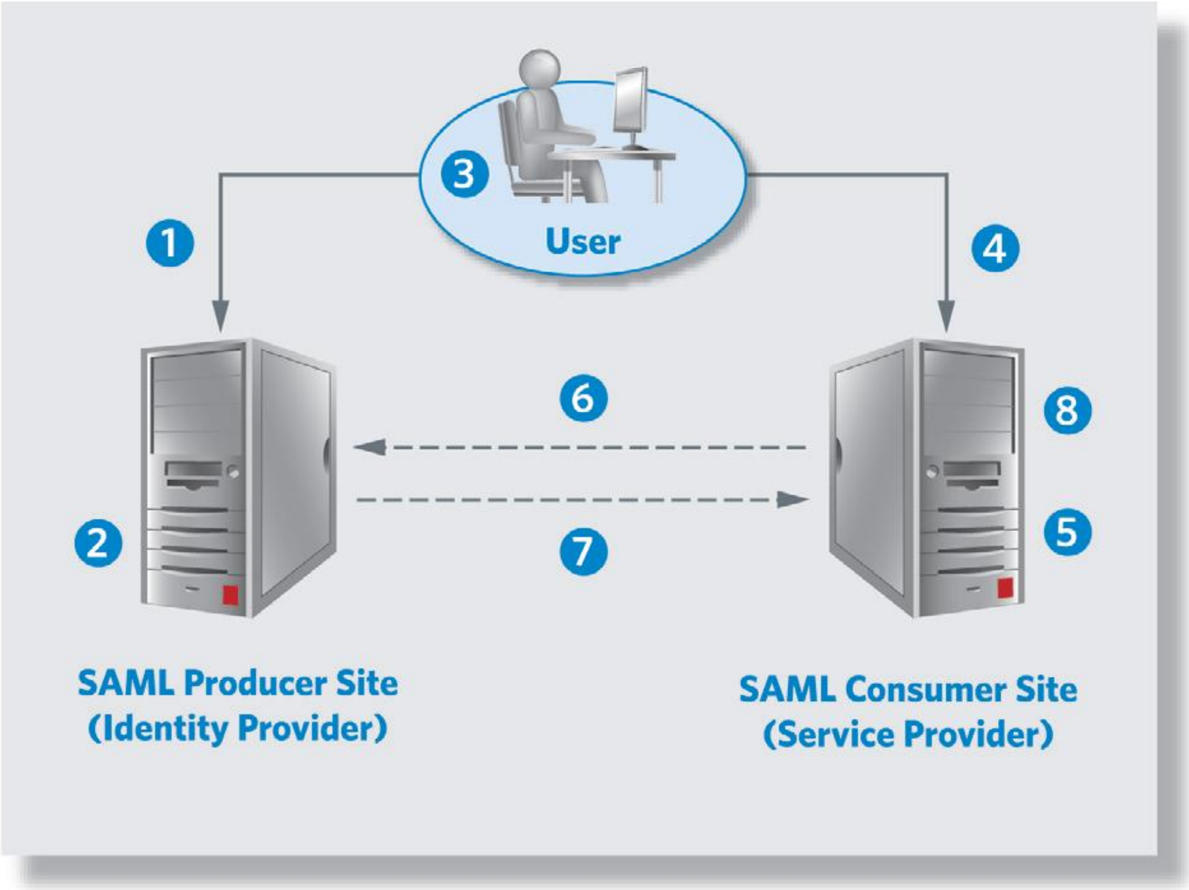

Figure 7-1 SAML Process Flow

i. The user visits a SAML producer site and is challenged to present credentials.
ii. Upon successful authentication, the SAML producer site generates a SAML assertion and a reference to the SAML assertion (SAML artifact).
iii. The user clicks on a link to a service provider at a SAML consumer site.
iv. The user is redirected to the SAML consumer site with SAML artifact and target URL query parameters.
v. The SAML consumer site processes the SAML artifact and determines who the SAML producer site is.
vi. The SAML consumer site makes a back-channel SOAP request to the SAML producer site for the full assertion describing the user.
vii. The SAML producer site returns the SAML assertion to the SAML consumer site in a SOAP message.
viii. The SAML consumer site authenticates the user by validating the SAML assertion.

7.3 Authentication Server Architecture

The Authentication Server (a server that provides authentication services to the users or other systems) will provide a single platform on which to build a cohesive, comprehensive authentication strategy. Authentication Server would act as the heart of the e-Authentication framework. Authentication Server would authenticate users with a wide range of authentication methods, giving the flexibility to choose the Authentication methods that would be determined on application sensitivity matrix level. It also helps to manage competing compliance demands by creating a central point for authentication policy creation and enforcement.

It can provide the capability to add standards-based hardware and software authentication methods and it can also be easily extended via Authentication Server callouts to proprietary authentication methods. It would provide the ability to transition to new authentication technologies quickly while avoiding vendor lock-in.

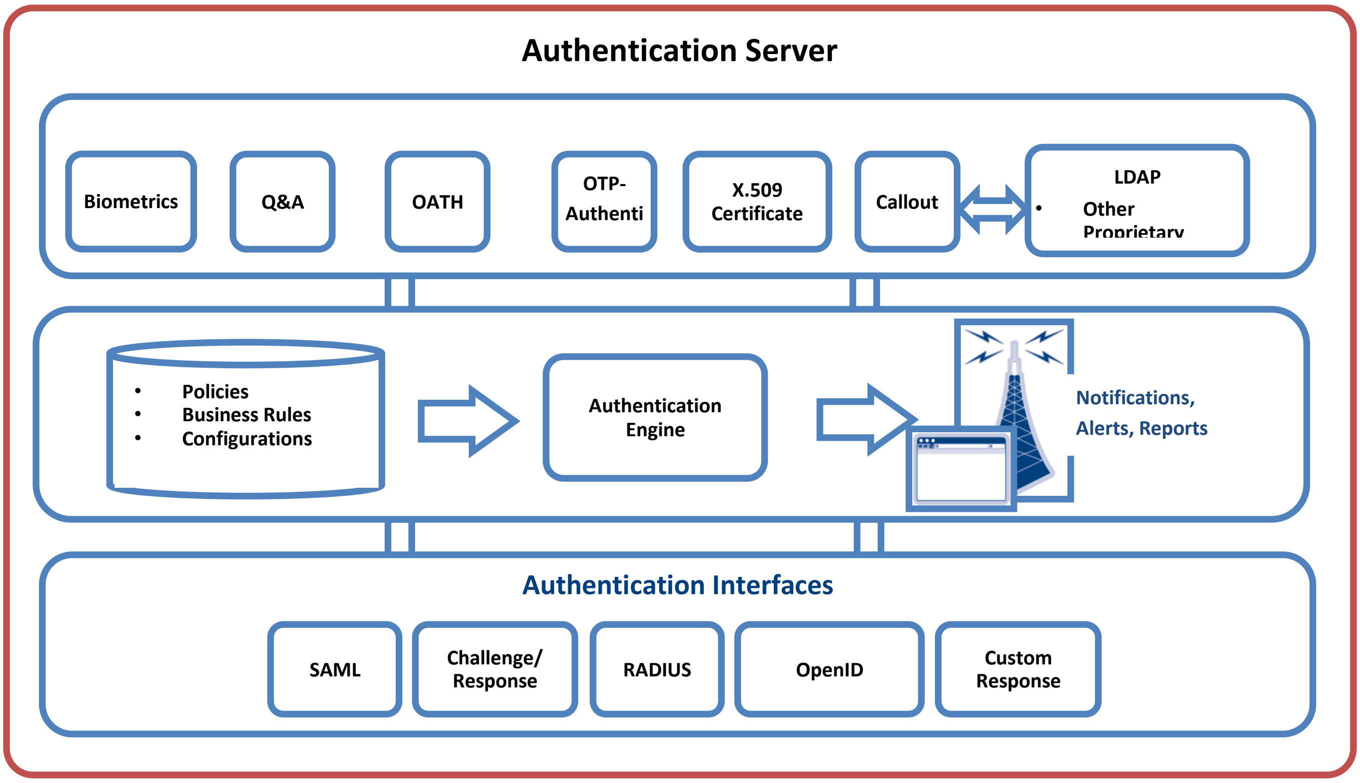

Figure 7-2 High-level Authentication Server Architecture

e-Authentication framework would provide the foundation for upgrading to the applications like secure delivery of eBills and eDocuments or digital signing of forms and documents, as and when the applications get ready.

8 Applicable Standards

8.1 Need for Open Standards

Using open standards of implementation of NeAF has the following advantages:

- Security flaws are unlikely in reputable, well-scrutinised protocols, but highly likely in home-grown protocols
- Interoperability is generally simpler
- Unnecessary re-invention is avoided
- Extensibility is easier, without the need for fundamental redesign, and
- Documentation is reduced by referencing published standards.

A strategy for protecting against security flaws in development of an e-Authentication solution should include:

- Using reputable standards-based cryptographic algorithms (these are generally defined by the security protocol standards)
- Using appropriate security standard as per the e-Governance Guidelines for Information Security (available at: http://egovstandards.gov.in/)
- Using the latest formally released version of each standard that is well supported in available products
- Avoiding custom extensions to standard protocols, but using them if needed rather than re-inventing new protocols
- Using reputable, well-tested security subsystems and components rather than local implementation, and
- Having best practice development strategies, including good system architecture design, a defensive security-aware stance, code review, and thorough testing.

8.2 Standards for Access Management

The following list of standards is only an indicative list. Other standards not listed here may be more suitable in some environments. Choice of standards will be influenced by support in available products, fitment with requirements and new and evolving standards.

- TLS (SSL, HTTPS): Transport Layer Security (the successor to Secure Sockets Layer (SSL) and the S (secure) in HTTPS when used with HTTP)
- XML signature: Extensible Markup Language signature provides integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.
- XML encryption: Extensible Markup Language encryption specifies a process for encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document), an XML element or XML element content. The result of encrypting data is an XML encryption element that contains or references the cipher data.

- S/MIME: Secure MIME (Multipurpose Internet Mail Extensions) is the most commonly supported secure email standard. It provides for digital signing and/or encryption of data based on the MIME standards.
- SAML: Security Assertion Markup Language is an XML framework for exchanging authentication and authorisation information.
- WS-Federation
- SPML: Secure Provisioning Markup Language
- X.509
- X.500 - LDAP
- XACML: Extensible Access Control Markup Language allows permissions policy enforcement points to query permissions policy decision points, which can in turn query other policy decision points. This allows for centralised permissions enforcement, and centralised, collaborative or devolved permissions management.
- WSS (WS Security): Web Services Security specifies message integrity and confidentiality for server-to-server messaging using SOAP (Simple Object Access Protocol). It allows for a variety of e-authentication approaches including username and password, digital certificates, etc. E-authentication information can be exchanged using either Kerberos or SAML.

8.2.1 Applicability

Table 5 below specifies the applicable security standards for the different layers in the e-Authentication architecture.

Layer	Applicable Security Standards
Business application systems	Applicable standards will depend on the application
Authorisation	XACML SAML WSS Liberty Alliance
e-Authentication	SAML TLS with client certificates (X.509) S/MIME XML signatures

Table 8-1: Applicable security standards for e-Authentication architecture

9 National e-Authentication Gateway

Under the National e-Governance Plan (NeGP) of Government of India, to achieve high-order of cooperation, collaboration and interoperability among autonomous and heterogeneous entities of the Government (at the central and state levels), infrastructure of National e-Governance Service Delivery Gateway (NSDG) at the national level and State e-Governance Service Delivery Gateway (SSDG) at the state-level has been created. NSDG and SSDG infrastructure acts as a standard-based messaging middleware between service access providers and government departments acting as Service Providers. Additionally, for mobile governance services, Mobile Service Delivery Gateway (MSDG) provides a government-wide shared infrastructure.

National e-Authentication Gateway (NeAG) may leverage the middleware messaging infrastructure of NSDG, SSDG and MSDG to provide a convenient and secure way for the users to access government services via Internet/mobile as well as for the government to assess the authenticity of the users. The National e-Authentication Gateway may be integrated with NSDG, SSDG and MSDG and may act as a standard e-Authentication mechanism between service access providers and the corresponding messaging middleware (NSDG, SSDG or MSDG).

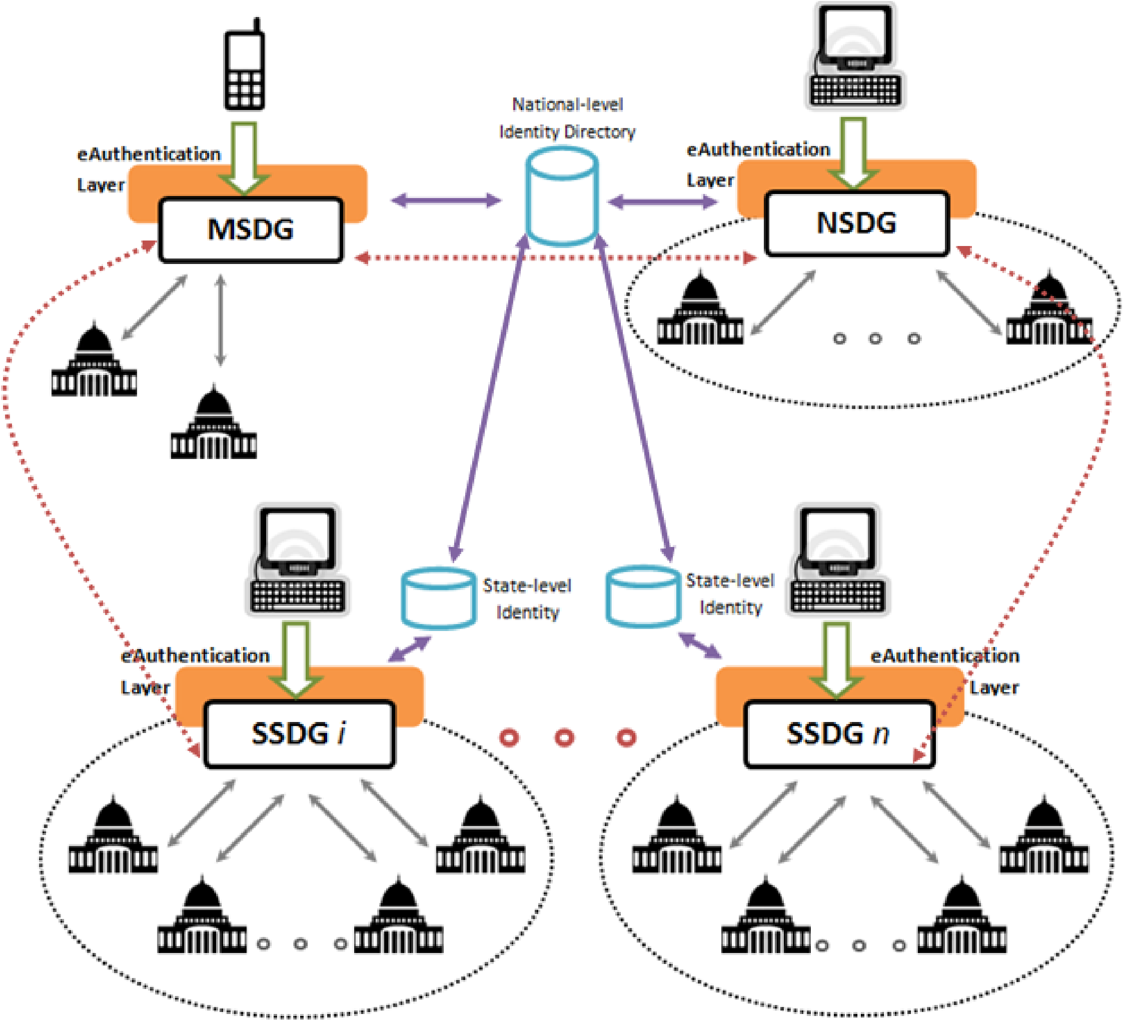

Figure 9-1 National e-Authentication Gateway

In order to leverage the NSDG, SSDG and MSDG infrastructure, NeAG will need to setup a centralised identity directory complimented by distributed state-level identity directories. Each integration of NeAG with SSDG will be supported by corresponding state-level identity directory, which will maintain the identity database for that particular state. The centralised national level identity directory is a super-set of all the distributed identity directories, with real-time copies of different directories.

To authenticate a request for a service registered with an SSDG, NeAG which will perform a lookup into the corresponding state level identity directory. In case the identity is not found in the state level identity directory, the national level identity directory shall be looked up for the identity. However, the integration of NeAG with MSDG and NSDG will perform direct lookups into the national identity directory.

10 Roles and Responsibilities

10.1 Government Roles and responsibilities

The roles and responsibilities of various government entities involved in the creation and implementation of National e-Authentication Framework are as follows:

10.1.1 Department of Information Technology (DIT), Government of India

DIT is the central IT department of Government of India having the vision of "e-Development of India as the engine for transition into a developed nation and an empowered society". DIT has successfully implemented several core IT initiatives across the country. DIT also assists all central ministries and state departments in effective execution of their respective e-Governance programmes. DIT has initiated the process of creation of the National e-Authentication Framework and to ensure its successful adoption and implementation across various e-Governance applications both within and outside NeGP. DIT has already created the core common infrastructure in the form of State Data Centers (SDCs), State Wide Area Networks (SWANs), State e-Services Delivery Gateways (SSDGs) etc. across all states/UTs in the country through which a large number of public services are expected to be delivered. The National e-Authentication Framework is also expected to leverage this core common infrastructure and provide a unified authentication mechanism to all the user departments both at central and state levels.

10.1.2 Central Ministries of Government of India

The central ministries are already executing a number of e-Governance projects such as Passports, Income Tax, MCA21 etc. where they have either already implemented a citizen authentication mechanism or are planning to build one. The central ministries are therefore expected to leverage the NeAF in order to streamline the already existing citizen authentication mechanisms with NeAF and to ensure the adherence to NeAF during any new application development. Further, a number of state level projects are also monitored and supervised by the respective central ministries. Therefore, they are also expected to provide necessary guidance to their state departments towards effective adoption and implementation of NeAF.

10.1.3 State Governments

The state governments are executing a large number of e-governance projects such as PDS, Panchayats, Commercial Taxes, etc. Considering the large geographical area of the country, the National e-Authentication Framework can play a great role in bringing in the necessary synergies among the implementation of same/similar projects across various states as well as implementation of different projects within the same state. Therefore, state governments are expected to lead the implementation of NeAF in all state projects and seek necessary guidance from the respective central ministry or DIT as and when required.

10.2 Citizens and Businesses

The roles and responsibilities of citizens and businesses which access various government services are as follows:

10.2.1 Citizens

The citizens access public services through various mechanisms such as CSCs, local government offices and directly over internet/mobile from their homes/offices. The citizens are thus expected to participate in the process for generation of their electronic identity and subsequently adhere to the authentication mechanisms as specified by the various government departments or agencies during implementation of the NeAF.

10.2.2 Businesses

Several government services such as sales tax, company registrations etc. are accessed by various businesses across the country. Therefore, all businesses are expected to adhere to the provisions of the specified authentication mechanisms as specified by various government departments or agencies during implementation of the NeAF.