Document No: e-Pramaan: 01
Version: 1.0
October, 2012

e-Pramaan: Framework for e-Authentication

Government of India
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
New Delhi – 110 003

Metadata of Document Framework for e-Authentication

S. No.	Data elements	Values
1.	**Title**	e-Pramaan: Framework for e-Authentication
2.	**Title Alternative**	ePramaan
3.	**Document Identifier** *(To be allocated at the time of release of final document)*	ePramaan:01
4.	**Document Version, month, year of release** *(To be allocated at the time of release of final document)*	Version 01, October 2012
5.	**Present Status**	Approved by Ministry of Communication & IT for Notification through THE GAZETTE OF INDIA and for publishing on http://egovstandards.gov.in and http://www.mit.gov.in
6.	**Publisher**	Department of Electronics and Information Technology (DeitY), Ministry of Communications & Information Technology, Government of India (GoI)
7.	**Date of Publishing**	26/11/2012
8.	**Type of Standard Document** *(Policy / Technical Specification/ Best Practice /Guideline/ Process)*	Framework
9.	**Enforcement Category** *(Mandatory/ Recommended)*	Mandatory
10.	**Creator** ***(**An entity primarily responsible for making the resource)*	Department of Electronics and Information Technology (DeitY)
11.	**Contributor** ***(**An entity responsible for making contributions to the resource)*	DeitY, Ministry of Communications & IT, New Delhi National e-Governance Division(NeGD), New Delhi
12.	**Brief Description**	The online and mobile based service delivery mechanisms of Government of India have generated the need for electronically authenticating the identity of the users so that each service or benefit reaches its intended recipient in a secured manner. It has also necessitated electronic authentication of Government Web sites in order to build trust

S. No.	Data elements	Values
		among the users. The Framework for e-Authentication (e-Pramaan) aims at making public services available to the residents of the country in a secured way through electronic authentication of users on Government Web sites. The Framework also aims at creating a common infrastructure to be used by all Central Ministries and State Governments for their electronic services which will avoid duplication of authentication infrastructure, reduce cost and efforts, and ensure faster delivery of services.
13.	**Target Audience** *(Who would be referring / using the document)*	All Central and State Government Departments and Agencies providing public services electronically
14.	**Owner of approved standard**	Department of Electronics and Information Technology, Ministry of Communications & Information Technology, New Delhi
15.	**Subject** *(Major Area of Standardization)*	Framework for e-Authentication
16.	**Subject. Category** *(Sub Area within major area)*	Policy guidelines and implementation framework for e-Authentication
17.	**Coverage. Spatial**	INDIA
18.	**Format** *(PDF /A at the time of release of final document)*	PDF
19.	**Language** *(To be translated in other Indian languages later)*	English
20.	**Rights. Copyrights**	DeitY
21.	**Source** **(***Reference to the resource from which present resource is derived)*	NIL
22.	**Relation** *(Related resources)*	N/A

Contents

1. Preamble

The National e-Governance Plan (NeGP) of Government of India takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is being developed, and large-scale digitization of records is taking place to enable easy and reliable access over the internet. As part of this larger initiative, several public services are being provided to the users through electronic means. To ensure easier and quicker access to public services in rural areas of the country, the government has established Common Services Centres (CSCs) as common service delivery outlets where the users can access all public services over the internet. The government has also launched a new initiative on mobile governance to provide all these services through mobile devices as well. The online and mobile based service delivery mechanisms have generated the need for electronically authenticating the identity of the users so that each service or benefit reaches its intended recipient in a secured manner. It has also necessitated electronic authentication of government websites in order to build trust among the users.

2. Background

The online transactions require that each party has confidence in the identity and, in some cases, the authority of the other party. This assurance ensures that unauthorised transactions are not executed and sensitive information is protected from being released to unauthorised entities. It also helps in preventing fraudulent activity by web sites impersonating as legitimate government entities.

Due to isolated project implementations of the individual e-governance initiatives of various ministries/departments, the present authentication mechanisms are inadequate and disparate across various applications. As a result, there is not only a lack of uniformity in the authentication methods of various departments, but citizens also have to provide different kinds of identity proofs for accessing public services which are fairly similar in many cases in terms of their sensitivity. This scenario has led to sub-optimal end user experiences.

Against this backdrop, the Department of Electronics and Information Technology (DeitY), Government of India has conceptualized the “e-Pramaan: Framework for e-Authentication” that is intended to serve as the guiding document for all central and state ministries, departments and government agencies for implementing an appropriate authentication model for online and mobile based delivery of their services while maintaining uniformity and consistency across various authentication mechanisms.

3. Objectives

The e-Pramaan framework enables various government departments and agencies to address the access management and authorisation requirements associated with the deployment of e-governance applications and services. The objectives of its creation are as follows:

1. To provide a guiding framework to all government ministries, departments and agencies at both central and state levels for implementation of appropriate authentication processes and mechanisms as part of their service delivery strategy;
2. To define various types of authentication mechanisms and their usability in different scenarios that can be utilized by all government ministries, departments and agencies for electronically authenticating the users of government services;
3. To enable government ministries, departments and agencies to incorporate Aadhaar based authentication in their e-authentication mechanisms;
4. To enable consistency in the processes and procedures towards e-authentication of user identity;
5. To enable government ministries, departments and agencies to incorporate appropriate mechanisms for authentication of their websites to generate trust among the users;
6. To avoid duplication of authentication infrastructure and reduce the cost and efforts of the government ministries, departments and agencies in this regard;
7. To increase efficiency and maximize the ease of use in the e-authentication processes and mechanisms for all the stakeholders involved; and
8. To provide an implementation approach to assist the government ministries, departments and agencies in implementing e-authentication in the most appropriate manner.

4. Overview

4.1 e-Authentication

Electronic Authentication (or “e-Authentication”) is the process of electronic verification of the identity of an entity. The entity may be a person using a computer/mobile, a computer/mobile itself or a computer/mobile program. Authentication is a way to ensure that the user who attempts to perform functions in a system is in fact the user who is authorised to do so. 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 departments and agencies to assess the authenticity of the users.

An authenticated identity is linked to the online services delivered by government departments and agencies through the process of “Authorisation”. Authorisation deals with the permissions or privileges granted to a user to access particular services provided by an application.

4.2 Benefits of e-Authentication

Electronic authentication helps to build 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, there is a need to set up suitable e-authentication processes based on an assessment of the risks associated with these transactions.

4.3 Overview of e-Authentication Mechanisms

Electronic authentication is accomplished based on the following factors:

- **Knowledge -** something the user knows (e.g. user name, password, PIN, secret questions and answers, etc.);
- **Possession -** something the user has (e.g. digital signature, smart card, etc.);
- **Be -** something the user is (e.g. biometric fingerprint, iris pattern, etc.); or
- A combination of the above.

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 an application).
ii. **Two Factor Authentication:** An authentication mechanism where a combination of two factors is used (e.g., a user using username and password as first factor and One Time Password (OTP) as the second factor).
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 her Aadhaar number (first factor – "Knowledge") and her biometrics (third factor – "Be") to authenticate herself).

Associated level of risk shall determine the appropriate authentication mechanism to be adopted. The systems, applications and information with high-level of associated risk require a stronger authentication mechanism that confirms the user's digital identity.

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 mechanism 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.

5. Policy Statement

Government of India shall adopt and deploy uniform electronic authentication mechanisms in a time-bound manner to ensure delivery of public services to the intended recipients.

The e-Pramaan Framework for e-Authentication lays down the following main policy measures:

i. Uniform electronic authentication mechanisms and processes shall be established to ensure electronic authentication of online and mobile users to facilitate access to and delivery of public services. The electronic authentication mechanisms shall incorporate Aadhaar based authentication.

ii. All government departments and agencies shall deploy e-Authentication processes as part of their service delivery strategy.

iii. All government Web sites shall be electronically authenticated in order to build trust among the users.

6. Key Components of e-Pramaan Framework

6.1 Identity Management

Identity management is a significant component of e-Pramaan Framework to ensure trusted and reliable online delivery of government services to the authenticated users. Authentication and authorisation should be considered within the context of identity management.

Identity management can be described as "…the management of individual identifiers, their authentication, authorization, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks. ….Identity management (IdM) is a term related to how users are authenticated (identified) and their actions authorized across computer networks. It covers issues such as how users are given an identity, the protection of that identity, and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords, etc.)."[1] This includes single sign-on and password management functionality and a single point of administration for accounts hosted over one or multiple user stores.

6.2 e-Authentication

e-Authentication is the process of verifying the identity of an entity as explained earlier in section 4.1.

6.3 Authorisation

Authorisation is the process of verifying that a known person has the permissions and rights to perform a certain operation in an application. Authentication, therefore, must precede authorisation. An effective access management system incorporates one or more methods of authentication to verify the identity of the user, including passwords, digital certificates, hardware or software tokens, and biometrics. 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.

6.4 Credential Registration

Credential registration is the process which results in issuance of an e-authentication credential, using which an identity can be electronically verified. The credential can be of different strengths, e.g. a password, a token, a digital certificate, or a biometric parameter. The strength of the credential required will be determined by the sensitivity level requirements of the

[1] Source: http://en.wikipedia.org/wiki/Identity_management, accessed 16 October 2012.

application or transaction. Credential registration process may consist of a combination of the following elements:

1. **Online/Offline process to allow users to register with the required identity and associated information**
2. **Creating user entries in an identity directory**
   The database includes users' identities 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.

6.5 Permission Assignment

In order to provide the user access to online services, appropriate permissions need to be assigned to the user as part of the permission assignment process after issuance of the 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 departments and agencies as part of the credential registration process.
- **As a separate activity performed at some time after registration.**
  Access permissions may be assigned to the user based on a credential issued by some other agency at a later point of time.

6.6 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.

6.7 Single Sign-On

Single sign-on is a specialized form of e-authentication that enables a user to authenticate once and gain access to the resources of multiple applications. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them.[2]

However, the user may be prompted to provide an additional authentication credential, such as an OTP, a token, a digital certificate, a biometric parameter, etc. in the subsequent applications depending upon the sensitivity level of that application or transaction. Figure 1 shows a schematic diagram for single sign-on.

[2] Source: http://en.wikipedia.org/wiki/Single sign-on, accessed 16 October 2012

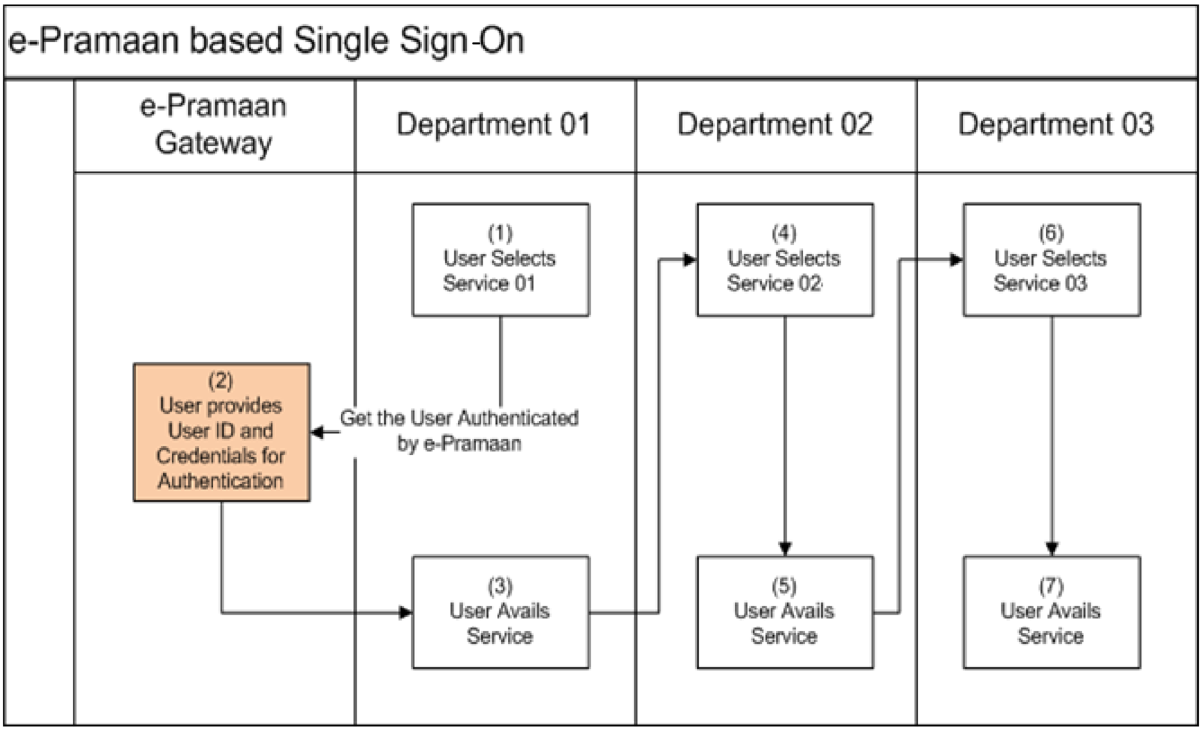

e-Pramaan based Single Sign-On
e-Pramaan Gateway
Department 01
Department 02
Department 03
(1) User Selects Service 01
(2) User provides User ID and Credentials for Authentication
Get the User Authenticated by e-Pramaan
(3) User Avails Service
(4) User Selects Service 02
(5) User Avails Service
(6) User Selects Service 03
(7) User Avails Service

Figure 1: e-Pramaan based single sign-on

7. Methodology

7.1 Implementation Approach

The implementation approach for the e-Pramaan framework can be defined as a four-step process. It primarily addresses identity related solutions that include identity authentication, step-up authentication, and single sign-on across various government Web sites.

The steps of the e-Pramaan implementation approach are as follows:

1) Determine the business requirements
    a) Identify the services to be provided online
    b) Assess the risk associated with each online service
    c) Define the sensitivity level for each online service
    d) Identify the appropriate authentication mechanism
2) Select the registration approach with e-Pramaan
3) Incorporate e-Pramaan at the application Level
4) Review the e-Authentication solution

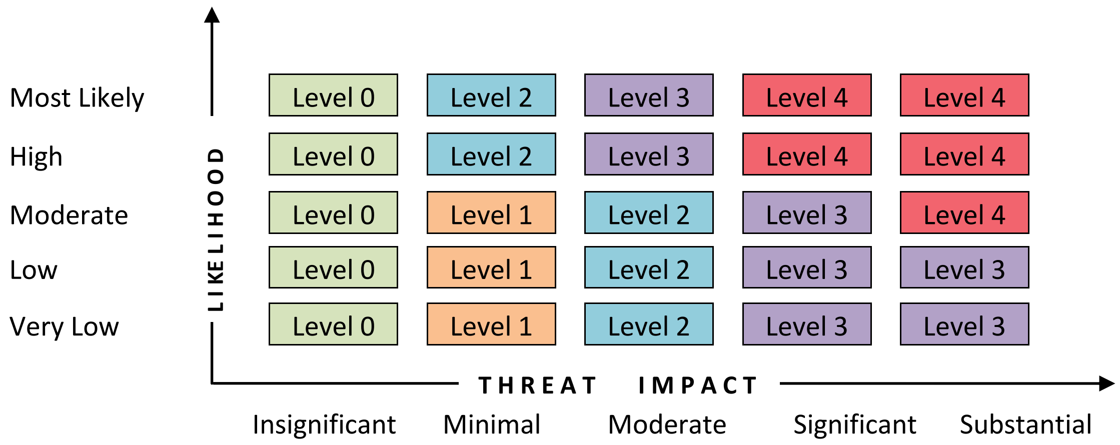
7.2 Sensitivity Levels and Risk Assessments

Sensitivity levels are used to describe the level of assurance of identity of users required for an application and the resultant level of robustness of the required solution. Table 1 describes the various sensitivity levels for assurance of identity.

Table 1: Levels of authentication assurance

Level 0	**No** assurance of identity
Level 1	**Minimal** level of assurance of identity
Level 2	**Moderate** level of assurance of identity
Level 3	**Strong** level of assurance of identity
Level 4	**Very Strong** level of assurance of identity

The e-Pramaan Framework helps in determining the sensitivity levels based on an assessment of the risk associated with getting e-Authentication of users wrong for an application. 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 Figure 2 below.



	Insignificant	Minimal	Moderate	Significant	Substantial
Most Likely	Level 0	Level 2	Level 3	Level 4	Level 4
High	Level 0	Level 2	Level 3	Level 4	Level 4
Moderate	Level 0	Level 1	Level 2	Level 3	Level 4
Low	Level 0	Level 1	Level 2	Level 3	Level 3
Very Low	Level 0	Level 1	Level 2	Level 3	Level 3

Figure 2: Indicative application sensitivity level based on likelihood and impact of threats

Once the application sensitivity level has been decided using the above approach, the appropriate authentication mechanism can then be chosen based on the "Application Sensitivity Matrix" as presented in Table 2 in section 7.3.3.

7.3 e-Authentication Assurance Levels

7.3.1 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 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 mechanism at the right time. Application sensitivity level will determine the calling of a suitable authentication mechanism from Level 1 through Level 4 at the appropriate stage.

A summary of the five levels is provided below:

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

Level 1: This is the basic authentication mechanism using username and password. The user could be provided the capability of self-registration by which she can generate a username/password. A self-service identity management mechanism will be used by the user if she forgets her password. It will avoid unnecessary calls to the helpdesk for resetting the user password. Aadhaar based verification involving matching of demographic information and Aadhaar numbers can also be used appropriately for verifying the identity of the users.

Level 2: At Level 2, a user will be able to prove her identity using OTP token along with her Level 1 credentials (i.e., username and password or Aadhaar number and demographic information).

Level 3: At Level 3, the user would need to prove her identity through a hardware or software token (along with PIN) and username and password (i.e. through a two factor authentication process). For this purpose, token would be a digital certificate/digital signature or a smart card that would be required from the user end. Biometrics based verification using the Aadhaar authentication process may also be used at this level.

Level 4: At Level 4, the user will prove her identity using two factor authentication which will necessarily include biometrics as one of the factors while the other factor could be either a token (hardware or software based) or a username/password. This is the highest level of authentication security that would be available to a user. Biometrics based verification would be done in accordance with the Aadhaar authentication process.

7.3.2 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. Level 0 applications accessed through mobile 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 level will determine the calling of a suitable authentication mechanism from Level 1 through Level 4 at the appropriate stage.

A summary of the five levels is provided below:

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

Level 1: This is the basic authentication mechanism using username and password. The user would receive the username & password after successful enrolment in e-Pramaan. The user will receive the password through SMS or print mailer. Aadhaar based authentication involving matching of Aadhaar number with demographics can also be used appropriately for verifying the identity of the users at this level.

Level 2: At this level, a user will prove her identity using username, password and OTP. At the time of accessing a government service, the user will first provide her username and password or Aadhaar number with demographics and will then be prompted to enter the OTP.

Alternate option (only for smart phones): In this case, the user would need to prove her identity through username and password (or Aadhaar number with demographics) plus the random OTP generated through the OTP Generator (i.e., two factor authentication). 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).

Level 3: At Level 3, the user would need to prove her identity through username and password plus a hard/soft token on a modified SIM or SD/microSD card/other medium containing the user's digital certificate along with PIN (i.e., through a two factor authentication). Biometrics based verification using the Aadhaar authentication process may also be used at this level.

Level 4 (for biometric enabled phones/devices): At Level 4, the user will prove her identity using a two factor authentication which will necessarily include biometrics as one of the factors while the other factor could either be a hard/soft token (as mentioned in Level 3 above) or a username/password. This is the highest level of authentication security that would be available to a user. For this purpose, the user should have a biometric enabled phone/device. Biometrics based verification would be done in accordance with the Aadhaar authentication process.

7.3.3 "Fraud Management" Layer for Applications

Considering that the need for assurance of identity of users for applications falling under sensitivity levels 2 to 4 varies from moderate to very strong, 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. This layer will evaluate the fraud potential of online/mobile access attempts and assess the risk based on a broad set of variables. The "Fraud Management" layer will perform this task transparently without inconveniencing the legitimate users.

A reference "Application Sensitivity Matrix" for identifying the right level of authentication is provided in Table 2 below.

Table 2: Application sensitivity matrix for identifying the right authentication level

Application Sensitivity Matrix					
Sensitivity level	Level 0	Level 1	Level 2	Level 3	Level 4
User experience	No inconvenience	Minimal inconvenience	Moderate inconvenience	Significant inconvenience	Substantial inconvenience
Scenario	Public information	Information having minimal impact in case of breach	Information having moderate impact in case of breach	Information having high impact in case of breach	Information having very high impact in case of breach
Suggested authentication method	No authentication required	Username and password /Aadhaar number with Demographics	Two factor authentication: username/password (or Aadhaar number with Demographics) and OTP	Two factor authentication: soft/hard token with username and password, biometrics based verification using Aadhaar authentication process	Two factor authentication: biometrics based verification using Aadhaar authentication process plus soft/hard token or username and password
Indicative examples	Election Results	Examination Results	Personally Identifiable Information (birth, death, marriage certificates, land records, etc.)	Statutory returns for taxation, statutory documents, etc.	Applications having security implications (Passport, Visa, etc.)
Fraud Mgmt. layer	No	No	Yes	Yes	Yes

The government department or agency will identify the services that will be provided by it over the web and mobile platforms as well as the information that will be accessed by the users. It will then determine the appropriate authentication level based on the guidelines specified in this framework and in compliance with the applicable statutory requirements.

7.4 Web site Authentication

During the delivery of online public services, it is not only important to authenticate the user for her identity, but it is also important to authenticate the Web site that the user is accessing for availing various public services. Considering the number of phishing[3] attacks that take place over the web every day, the user must be able to correctly identify that the Web site that she has accessed is actually the right Web site that it is claiming to be.

Lack of appropriate security measures in ensuring the authenticity of Web sites may lead to the user revealing her personal credentials over a fake Web site, which can result in severe financial and social losses not only to the user but also to the concerned department whose web interface was imitated for this purpose.

For prevention of phishing attacks through Web sites, the following techniques can be employed by various government departments and agencies:

- User education and awareness
- Web site design to avoid phishing:
    - Watermark/Customized logo,
    - Last login details, last transaction details, etc.
- Digital certificates for Web sites
- Programming solutions to prevent superimposition by fake Web sites

There are multiple ways of ensuring Web site authentication, e.g., watermark/customized logo, using hardware or software tokens, biometrics, public key infrastructure (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. A government department or agency shall determine the appropriate method for Web site authentication based on these factors and implement the same for its Web site.

8. e-Pramaan Gateway

Under the National e-Governance Plan (NeGP), National and State e-Governance Service Delivery Gateways (NSDG/SSDG) have been created to ensure interoperability among autonomous and heterogeneous entities of the government at both central and state levels. NSDG and SSDG infrastructure acts as a standards-based messaging middleware between service access providers and government departments acting as service providers. Additionally, for mobile governance services, Mobile Service Delivery Gateway (MSDG) has been created that provides a government-wide shared infrastructure.

[3] 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

e-Pramaan Gateway shall 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 departments and agencies to assess the authenticity of the users. The e-Pramaan Gateway shall be integrated with NSDG, SSDG and MSDG and shall act as a standard e-authentication mechanism between service access providers and the corresponding messaging middleware (NSDG, SSDG or MSDG). Figure 3 depicts how this integration shall be achieved.

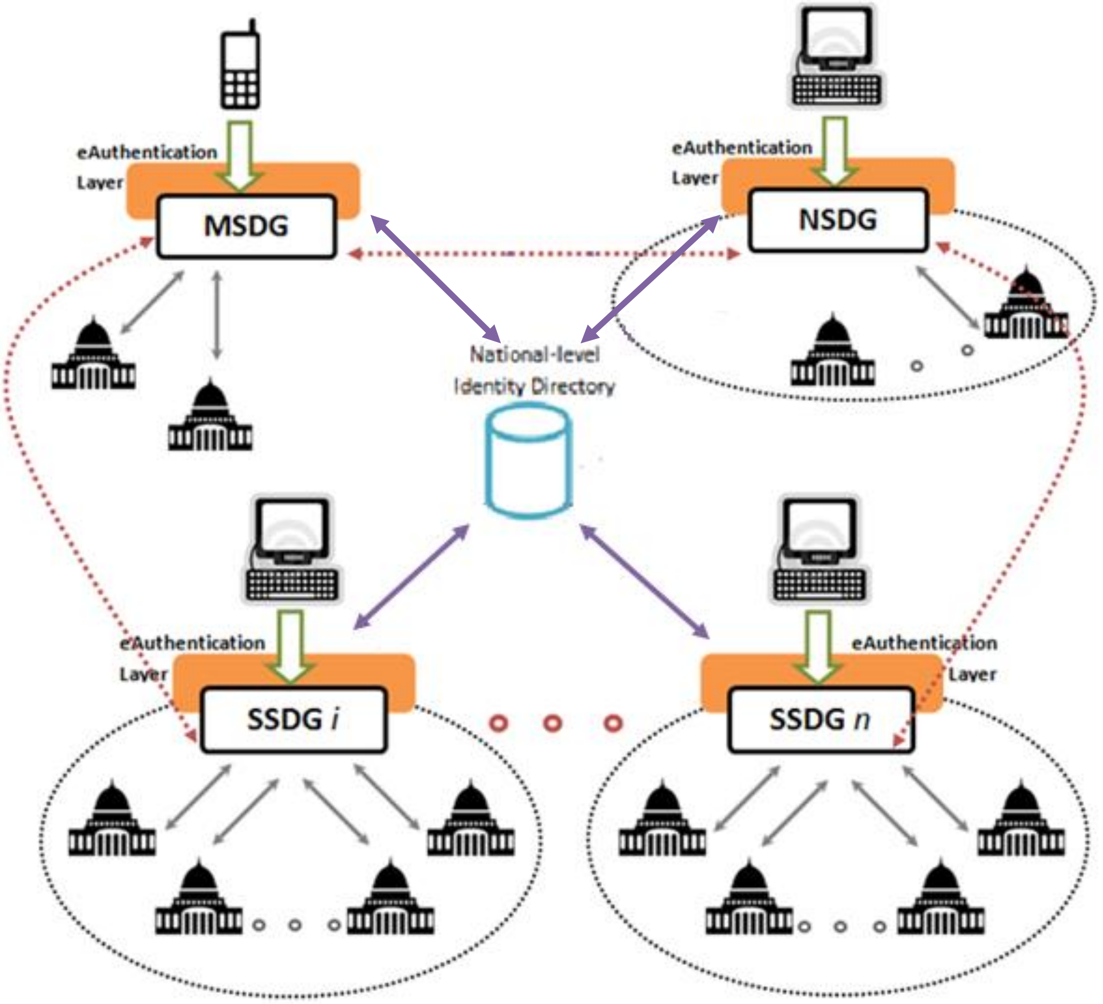


Figure 3: The e-Pramaan Gateway

In order to leverage the NSDG, SSDG and MSDG infrastructure, the e-Pramaan Gateway will establish a centralised identity directory. e-Pramaan Gateway may incorporate new technologies, processes and authentication mechanisms in future.

9. Privacy Implications

It will be the responsibility of the concerned government department or agency that aims to deploy online/mobile based applications to identify the privacy implications inherent in the proposed transactions and appropriately address the same.

10. Addressing the Digital Divide

It is important to address the issue of digital divide in the context of implementation of the e-Pramaan Framework. This framework aims to widen the access of common users to online and mobile based electronic services through suitable e-authentication mechanisms. This shall be achieved in the following ways:

- As penetration of mobile phones in India has increased manifold recently and is currently much greater than the same for internet and computers, especially in rural areas, the e-Pramaan Framework has made specific provisions for mobile phone based authentication of users.

- To ensure easier and quicker access to public services in rural areas of the country, the government has established Common Services Centers (CSCs) as common service delivery outlets where the users can access various public services over the internet. The e-Pramaan Framework proposes to use these CSCs for registering users and generating their e-Pramaan credentials.

- Unique Identification Authority of India (UIDAI) has a mandate of enrolling 60 crore residents by 2014. The e-Pramaan Framework incorporates authentication of users based on the Aadhaar authentication process as this will help users who are not conversant with generation and usage of user ID/password or digital certificate based authentication mechanisms.

- The Registrar General & Census Commissioner of India has also proposed to issue Resident Identity Cards (Smart cards) to all usual residents of 18 years of age and above in the National Population Register (NPR). These smart cards will have the Aadhaar based details of the residents and will facilitate the electronic authentication of users. They will thus greatly help in widening the access to electronic services for the common people.

11. Review of the e-Pramaan Framework

The Government of India reserves the right to review and revise the e-Pramaan Framework as and when necessary.

12. Point of Contact

Queries or comments related to the e-Pramaan Framework may be sent to the Additional Secretary (e-Governance) or Joint Secretary (e-Governance), Department of Electronics and Information Technology (DeitY), Electronics Niketan, 6 CGO Complex, Lodhi Road, New Delhi – 110003. They can also be sent through e-mail to asegov@mit.gov.in, jsegov@mit.gov.in, or neaf@negp.gov.in.

ANNEXURE I: Implementation Strategy

To ensure the implementation of the e-Pramaan Framework in a time-bound manner, following actions will be taken.

1. **Formulation of e-Pramaan Guidelines:**
   DeitY shall formulate detailed guidelines on the e-Pramaan Framework to enable the government departments and agencies to select the right authentication mechanisms for e-authentication of users for delivery of their public services. It will also formulate detailed guidelines for authentication of government Web sites.

   The e-Pramaan guidelines shall help in ensuring security and confidentiality of data. The guidelines shall also help the government departments and agencies in applying a consistent approach in selecting the appropriate e-authentication mechanisms.

2. **Creation of an e-Pramaan Gateway:**
   The e-Pramaan Gateway is the core infrastructure to enable electronic authentication of users for delivery of public services electronically to the intended recipients as well as to build trust of the users in the online and mobile environments. The e-Pramaan Gateway will be used as a shared infrastructure by the central and state government departments and agencies. It shall incorporate the Aadhaar based authentication mechanisms provided by the UIDAI.

3. **Creation of an Identity Directory:**
   The e-Pramaan framework shall create identity directory(ies) to maintain the identity database. These identity directory(ies) may be built using the data collected, including the identity document numbers such as Ration Card Number, Voter Card Number, Driving License Number, etc., during the creation of the National Population Register (NPR) or by other government departments and agencies at central and state levels.

   e-Pramaan Gateway shall use the identity directory(ies), Aadhaar based authentication mechanisms and other suitable mechanisms such as those based on One Time Passwords (OTPs), digital certificates, etc. for authenticating users for delivering public services to the intended recipients through internet/mobile. e-Pramaan Gateway may incorporate new technologies and processes for authentication in future.

4. **Creation of a Facilitating Mechanism:**
   DeitY shall establish and manage an appropriate facilitating mechanism to ensure implementation of the e-Pramaan Framework by all government departments and agencies.