Standards and Specifications

For

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

Scope of the Document

This document describes a broad level specifications for developing the e-Pramaan authentication system. This will enable the reader to understand the rationale, use cases and process flows that will be used for detailed design. It also elucidates the standards that will be used to develop the components, APIs as well as the protocols for the framework. Particulars of the communication protocols between the entities and implementation are NOT a part of this document. This document is also subject to change in future.

Intended Audience

The intended audience for this document includes Security Architects, Technical Consultants and Application Developers. The audience is expected to have knowledge of Cryptography, Information Security Principles, e-Authentication, Security Protocols, Web based Application Design and Development.

Comments and Suggestions

For comments, suggestions and feedback on this document, kindly e-mail to epramaan@cdac.in.

Normative References and Keywords

Normative References and keywords used in this section are referred from RFC 2119 [5].

- MUST - This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT - This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- SHOULD - This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT - This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

Document Structure covers the objectives of e-Pramaan, levels of authentication, standards to be adhered to for the development of authentication components etc.

Chapter 1. Provides Information on e-Pramaan

Chapter 2. Covers User Provisioning and De-Provisioning as well as Credentials handling

Chapter 3. Covers Identity Attributes

Chapter 4. Covers Session Policy Management

Chapter 5.Covers Communication and Security

Chapter 6. Covers Service Agreements

Chapter 7. Covers Audit Requirements

Table of Contents

Metadata of Document e-Pramaan Standards and Specifications

Title	**e-Pramaan Standards and Specifications**
Subject	Standards and Specifications for Implementation of e-Pramaan
Keywords	Authentication, Identity Management, IAM, IdM, Single Sign-On (SSO), SAML, Service Provider, Identity Provider, IdP, XML Signature, OTP, DSC, Digital Signature, Biometrics, Aadhaar, e-Pramaan, e-Authentication, Digital Signature Certificate, Single Sign-out, Authentication service, Authentication Framework
Source	Department of Electronics & Information Technology, Government of India
Description	This document describes broad level specifications for developing the e-Pramaan authentication system. This will enable the reader to understand the rationale, use cases and process flows that will be used for detailed design. It also elucidates the standards that will be used to develop the components, APIs as well as the protocols for the framework. Particulars of the communication protocols between the entities and implementation are NOT a part of this document. This document is also subject to change in future.
Coverage	e-Gov services
Type	e-Authentication and SSO Standards
Relation	e-Pramaan: Framework for e-Authentication
Creator	Department of Electronics & Information Technology, Government of India
Publisher	Department of Electronics & Information Technology, Government of India
Copyrights	DeitY, MCIT, New Delhi
Enforcement Category	Recommended
Rights	Only for Registered Users
Language	English
Format	PDF
Date	08-Sep-2014
Status	Draft

Abbreviations

Terms	Description
AES	Advanced Encryption Standards
ASA	Authentication Service Agency
CA	Certifying Authority.
CCA	Controller of Certifying Authorities
CIDR	Central Identities Data Repository
CP	Certificate Practise
CPS	Certificate Practise Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVC	Card Verifiable Certificates
DOB	Date of Birth
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
HSM	Hardware Security Mechanism
IPSec	Internet Protocol Security
JKS	Java Key Store
MITM	Man in the Middle Attack
NICCA	National Informatics Center- Certification Authority
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OTP	One Time Password

PAN	**Permanent Account Number**
PC	**Personal Computer**
PEM	**Privacy-enhanced Electronic Mail**
PIN	**Personal Identification Number**
PKI	**Public Key Cryptography**
RCAI	**Root Certifying Authority of India**
RP	**Relying Party**
RSA Algorithm	**Rivest-Shamir-Adleman Algorithm**
SAML	**Security Assertion Mark-up Language**
SHA	**Secure Hash Algorithm**
SP	**Service Provider / e-Gov Service**
SSL	**Secured Socket Layer**
SSO	**Single Sign On**
UIDAI	**Unique Identification Authority of India**
XML	**Extensible Mark-up Language**

Terms Used

Terms	Description
Authentication Token	**The token generated on successful authentication of the citizen**
Correlation	**Mapping of Existing user of SP with e-PramaanID**
De-Provisioning	**Terminating the user account**
e-Pramaan Transaction ID	**Transaction-ID used by e-Pramaan for communicating with SP**
Enlistment	**SP registers on e-Pramaan**
Enrolment	**User registered to SP services through e-Pramaan**
Registration	**User registers on e-Pramaan**
Service ID	**ID of a particular SP service enrolled on e-Pramaan**
SP User-ID	**User ID/Username of a user on SP**
Suspension	**Temporary blocking**

1 e-Pramaan

In an endeavour to enhance the trust of users amidst the online environment, the Department of Electronics and Information Technology (DeitY), Government of India has conceptualized "e-Pramaan: Framework for e-Authentication". This document aims at providing guidelines for all central and state ministries, departments and government agencies towards adopting an appropriate authentication model for online and mobile based delivery of public services.

DeitY along with its implementing agency C-DAC, a scientific society, has initiated the national rollout of the e-Pramaan project. The scope of the project is to formulate the authentication standards, develop pluggable authentication components and subsequently provide e-Authentication as a service to government departments so as to provide a convenient and secure way for users to access government services via internet/mobile as well as for the government to assess the authenticity of the users.

1.1 e-Pramaan Authentication Levels

e-Pramaan offers secure authentication with various levels of assurances by verifying the credentials of e-Pramaan users accessing different e-Governance services through internet or mobile devices. Users of e-Pramaan will be termed as end-users while users of e-Gov services will be termed as SP (Service Provider) users.

e-Pramaan Framework mentions different levels of authentication which are described below.

Level 1 (Password based Authentication): This is the basic authentication mechanism that uses username and password. End-user will avail the self-registration mechanism to generate a username–password pair. Additionally, the end-user may also provide her Aadhaar number in the self-registration form. Subsequently, she can login to e-Pramaan using either the chosen username and password pair or Aadhaar Number (as username) and password. End-user will be able to reset her password through e-Pramaan portal in case of a forgotten password. This will avoid unnecessary calls to the helpdesk for resetting the user password.

Level 2 (OTP based Authentication): At Level 2, the end-user will prove her identity using an OTP (One Time Password) received either on email or mobile. This authentication will be in conjunction with any one of the single factor credentials. OTP can also be generated using mobile application offered through e-Pramaan.

Level 3 (Digital Certificate based Authentication): At Level 3, end-user will establish her identity through hardware or software token (along with PIN). This shall be accomplished using tokens in the form of digital certificates/digital signatures or smart cards that would be required from the user end. Both software and hardware tokens will be supported. Interoperability will be maintained by supporting the X.509 format. Hardware tokens could be in the form of SIM extensions, SD cards, USB crypto and

SHOULD comply to CCA guidelines. Interoperability guidelines as issued by CCA will be adopted for validating the certificates.

Level 4 (Biometric based Authentication): At Level 4, end-user will prove her identity using biometrics. This is a strong authentication mechanism provided to an end-users. Biometric authentication would be conducted in accordance with the Aadhaar authentication process and the end-user must possess a valid Aadhaar number in order to avail the Biometric based authentication. For Aadhaar based authentication, e-Pramaan will receive the end-user's Personal Identity Data (PID) block from the service provider. This data will be packaged within the authentication request before transmitting to CIDR via C-DAC's ASA.

These authentication levels represents factors used for authentication. Hence e-Pramaan implementation uses them in single/ multi factor authentications described ahead. The choice of factor(s) for authentication will depend on the requirements as deemed fit by SPs. Use of additional factors will provide higher level of assurance for a safe and secure e-service experience. Multi factor is stronger than two factor which is stronger than single factor. The government departments have an option of choosing any one or a combination of factors along with Username as per the combinations described below:

i. Single Factor - Any one of the following factors: Password/Digital Signature Certificate (DSC)/Biometrics.
ii. Two Factor- Combination of any two of the following factors: Password/One Time Password (OTP) /Digital Signature Certificate (DSC)/Biometrics.
iii. Multi Factor- Combination of any two and more of the following factors: Password/ Digital Signature Certificate (DSC) /One Time Password (OTP) along with Biometrics.

e-Pramaan shall also provide mobile based authentication mechanism for level 1, 2 and 3, apart from the standard PC based access. For level 3 authentication requiring digital certificates, the use of Proxy SIM/ Crypto SIM Card / External SD Card/Software based certificates shall be considered.

Note:
Level 0 assumes the public information available to users without providing any credentials. Hence such information will be inherently available to all the users irrespective of registration on e-Pramaan.

2 User Provisioning and De-Provisioning

For an end-user to use e-Pramaan, she MUST register on e-Pramaan. The process flow for registration as well as enrolment to SP services is discussed in section 2.1, while SP registration i.e. Govt. department enlistment with e-Pramaan is discussed in section 2.4.

Different mechanisms will be facilitated by e-Pramaan for end-user registration. In all the three mechanisms, the end-user should fill up the registration form on e-Pramaan portal.

1) Identity Credentials - In this type of registration the end-user, provides her PAN Card number and/or Passport Number and/or Ration Card Number and/or Voter ID Card Number. The card numbers provided by the end-user are verified for her demographics using the back-end services. The end-user is registered on e-Pramaan only after verification of at-least one of the identity documents.

2) e-KYC based - The end-users with valid Aadhaar Number should provide their Aadhaar number which will be validated through Aadhaar based e-KYC.

3) Digital Signature Certificate based - The end-user may provide her Digital Signature Certificate from a valid CA. e-Pramaan confirms its validity.

The end-user registration process will be completed on e-Pramaan only after the successful completion of one of the above mentioned procedures and email/mobile verification i.e. user will not be allowed to access the services offered through e-Pramaan.

2.1 Provisioning of Users and Profile Creation

An end-user availing e-Pramaan service may or may not have enrolled to SP's e-Gov service. It is significant to note how e-Pramaan links the SP services to end-users. Using the concept of correlation, e-Pramaan links or relates end- users to their corresponding credentials at SP. Correlation ensures that end-users are not required to authenticate themselves distinctly on different SPs, and can rather avail seamless access to all services using e-Pramaan's unique credentials and Single Sign-On (SSO) facility. Correlation of end-users at SP and e-Pramaan will be supported through Aadhaar Number or seeding of SP User-ID at e-Pramaan. Various scenarios, taking into account both kinds of correlation, are described in section 2.1.1 and 2.1.2. The departments, in order to use e-Pramaan as an authentication system, MUST first integrate with e-Pramaan. These departments shall also provide 'Login using e-Pramaan' link on their home page. Thereon, whenever an end-user wishes to avail services through the department's login, she MUST be redirected to e-Pramaan.

2.1.1 Correlation Using SP User-ID at e-Pramaan

Through correlation, username on SP is linked to the e-PramaanID (unique ID assigned to every registered user of e-Pramaan). Correlation information will be stored at

e-Pramaan only. Table 1 describes the various scenarios for user registration using SP User-ID for correlation.

Table 1: Registration Scenarios with SP User-ID Mapping at e-Pramaan

Registered user of e-Pramaan?	Existing User on SP?	Steps to follow
NO	**NO**	Refer Section 2.1.1.1 for details
NO	**YES**	Refer Section 2.1.1.2 for details
YES	**NO**	Refer Section 2.1.1.3 for details
YES	**YES**	Refer Section 2.1.1.4 for details

2.1.1.1 Scenario I: Users Not Registered to e-Pramaan and Not Enrolled on SP

2.1.1.1.1 Self-Registration of User

Step 1: End-user fills in the username and password of her choice as well as her demographics including DOB, given name, e-mail, or mobile number. Optionally, the end-user may also upload her latest passport size photograph. However, providing username at the time of registration is mandatory. End-user will have an option to use either e-KYC verified Aadhaar Number or username along with password for login into e-Pramaan. This e-KYC will be carried out using the service provided by UIDAI. One of the user credential as mentioned in section 2 need to be mandatorily verified for completing the registration process and if Aadhaar is being verified during identity credential verification then Aadhaar can also be used as a username.

Step 2: End-user email is verified using email verification link, while her mobile number is verified using an OTP sent through an SMS. End-user has an option to provide either an email, mobile or both during registration. An email verification link or an OTP will be sent to the end-user's email or mobile as may be the case for verification.

Step 3: On successful verification of mobile or email in Step 2, end-user account is created in e-Pramaan and she can now avail e-Pramaan services.

2.1.1.1.2 User Enrolment to SP Service(s)

Step 1: A user wants to enrol to a service on SP site. SP redirects her to e-Pramaan if user chooses so. The registered end-user logs into e-Pramaan and upon successful authentication e-Pramaan redirects her to the SP's enrolment page with e-Pramaan Transaction-ID. SP can opt for a prefilled enrolment form based on e-Pramaan data shared as per the predefined XML schema agreed upon during SP integration with e-Pramaan. End-user consent is required for sharing e information between e-Pramaan and SP.

Step 2: On successful enrolment of the end-user at SP, SP communicates the SP User-ID, e-Pramaan Transaction-ID and SP-ID to e-Pramaan for correlation.

Step 3: e-Pramaan uses the SP User-ID to map it to the end-user's e-PramaanID for correlation at e-Pramaan.

2.1.1.2 Scenario II: Users Not Registered to e-Pramaan, but Enrolled on SP

Step 1: When an SP user accesses the SP's login page, user will be provided with an option "Login using e-Pramaan". If the SP user wishes to exercise this option, SP redirects her to e-Pramaan for registration.

Step 2: The SP user follows the registration process described in section 2.1.1.1.1.

Step 3: When the end-user is successfully registered, e-Pramaan will send a one-time SP user verification request to the SP for correlation purpose. Once the SP user is verified with SP credentials at SP end, SP will send the SP User-ID, e-Pramaan Transaction-ID and SP-ID to e-Pramaan for correlation. This correlation will be done by e-Pramaan on a one-time basis.

2.1.1.3 Scenario III: Users Registered to e-Pramaan, but Not Enrolled on SP

A first time user to SP will be, if chosen, redirected to e-Pramaan for authentication. User enrolment process to SP Service(s) outlined in Section 2.1.1.1.2 shall be followed here.

2.1.1.4 Scenario IV: Users Registered to e-Pramaan and Enrolled on SP

Correlation of e-PramaanID and SP User-ID will be done as outlined in Step 3 of section 2.1.1.1.2.

2.1.2 Correlation Using Aadhaar Number

e-Pramaan uses Aadhaar Number correlation to communicate with SP using SAML 2.0 (Aadhaar Number SHOULD already be seeded at SP). Table 2 describes the various scenarios for user registration using Aadhaar Number as a correlation identity.

Table 2: Registration Scenarios with Aadhaar Number at e-Pramaan

Registered user of e-Pramaan?	Existing User on SP?	Steps to follow
NO	**NO**	Refer Section 2.1.2.1 for details
NO	**YES**	Refer Section 2.1.2.2 for details
YES	**NO**	Refer Section 2.1.2.3 for details
YES	**YES**	Refer Section 2.1.2.4 for details

2.1.2.1 Scenario I: Users Not Registered to e-Pramaan and Not Enrolled on SP

2.1.2.1.1 Self-Registration of User

User should be registered on e-Pramaan as per section 2.1.1.1.1.

2.1.2.1.2 User Enrolment to SP Service(s)

Step 1: User should be registered on e-Pramaan as per section 2.1.1.1.1 and MUST have e-KYC verified Aadhaar Number at e-Pramaan.

Step 2: A user wants to enrol to a service on SP site. SP redirects her to e-Pramaan if user chooses so. The registered end-user logs into e-Pramaan and upon successful authentication, e-Pramaan redirects her to the SP's enrolment page with e-Pramaan Transaction-ID and Aadhaar Number where SP can opt for a prefilled enrolment form based on e-Pramaan data as per the predefined XML schema agreed upon during SP integration with e-Pramaan. End-user consent is required for sharing information between e-Pramaan and SP.

Step 3: On successful enrolment of the user at SP, end-user will be logged in to SP.

2.1.2.2 Scenario II: Users Not Registered to e-Pramaan, but Enrolled on SP

Step 1: When an SP user accesses the SP's login page, SP provides her with an option to login using e-Pramaan. If the SP user wishes to exercise this option, SP redirects her to e-Pramaan for registration.

Step 2: The SP user follows the registration process described in section 2.1.1.1.1.

Step 3: User Aadhaar Number should be verified at e-Pramaan through e-KYC.

Step 4: After successful registration at e-Pramaan, user can access the service from the service link provided at e-Pramaan or she may access the same service by accessing the SP portal.

2.1.2.3 Scenario III: Users Registered to e-Pramaan, but Not Enrolled on SP

A first time user to SP will be, if chosen, redirected to e-Pramaan for authentication. User enrolment process to SP Service(s) outlined in section 2.1.1.1.2 shall be followed here.

2.1.2.4 Scenario IV: Users Registered to e-Pramaan and Enrolled on SP

Aadhaar Number will be used to correlate end-users with SP. In this scenario Aadhaar Number at e-Pramaan will be verified using e-KYC service of UIDAI. This verified Aadhaar Number will be communicated to SP. Aadhaar seeding process should be completed by SP at its end.

2.2 Updation of End-User Profile

Initially, when an end-user completes her registration, her profile is created with verified email and/or mobile. User also has an option to provide Aadhaar number which can be used as login on e-Pramaan. However, using Aadhaar number for login will require e-KYC. This e-KYC will be done using service provided by UIDAI. User may also update her demographic information.

For availing services requiring Digital Signature based authentication, user needs to update her profile using Digital Signature Certificate (DSC). Pre-registration of DSC is must before using it for authentication purposes (Existing e-Gov service such as Income Tax, Land Registration etc. uses this practice). On updation of any profile information, user will be notified through email/sms.

2.3 User Suspension and De-Provisioning

e-Pramaan MUST have a process in place for suspending or de-provisioning of an end-user (who may be an end-user or SP) from using e-Pramaan authentication. If an end-user is suspended, her credential verification MUST be blocked until reinstated on e-Pramaan whereas if the end-user is de-provisioned, her credentials MUST be revoked such that they can no longer be used for authentication purpose. e-Pramaan end-user account or level shall be suspended or de-provisioned if:

i. *De-provisioning initiated by e-Pramaan end-user*

   On receiving a request for de-provisioning, end-user will need to answer security question and verify email or mobile upon which her e-Pramaan account will be deprovisioned from the e-Pramaan. Account for which a deprovisioning request is being initiated will remain in suspended state till the time verification of email/mobile gets completed by the end-user. Username associated with the deprovisioned account cannot be used again and user has to register again if he/she wants to avail the services of e-Pramaan.

ii. *Suspension initiated by e-Pramaan administrator / Third Party Govt. Authority*

   An e-Pramaan end-user account may be suspended if the user is found to be involved in fraudulent, anti-national, cyber crime, duplicate registration activities etc. e-Pramaan will revoke the user credentials and will also de-provision the account based on the validiations.

iii. *Inactive Account Suspension initiated by e-Pramaan*

   Inactive end-user accounts for a period exceeding 12 months will be suspended by e-Pramaan. Suspended accounts can be revived or reactivated by providing login credentials. Upon successful authentication of login credentials, user will be asked to answer the security question and verify herself using mobile OTP or email verification link. On success of the above, her account will be reinstated or reactivated.

iv. User Account Re-activation

On receiving a request for account re-activation, end- user will need to answer security question and verify email or mobile upon which her e-Pramaan account will be reinstated.

Note: Username associated with suspended and deprovisioned accounts will never be available for future registrations on e-Pramaan. However, suspended users can reactivate his/her account to use their earlier allotted username whereas deprovisioned user has to register again on e-Pramaan with a fresh username.

2.4 Service Provider (SP) Enlistment

Step 1: The service providers (SPs) who want to avail e-Pramaan authentication services MUST enlist with e-Pramaan through SP enlistment facility. SP will have an option to either choose Aadhaar Number for mapping the end-users or seeding SP User-ID at e-Pramaan. The enlistment form may have fields such as Organization type, Department name, Service name, Details of the administrator who will be operating the account, details of the contact person, Public Key Certificate of the service/department, official email ID and required authentication factors or chaining of authentication factors etc.

Step 2: Upon successful enlistment of SP, the MoU / Agreement is to be signed between e-Pramaan and SP.

Step 3: Integration of e-Pramaan with SP service shall be done. (Step 2 & 3 may go in parallel).

Step 4: Upon successful completion of process described in Steps 2 and 3, the SP can start availing the authentication service.

2.5 Service Provider (SP) Delisting

Service can be delisted from e-Pramaan upon delist request from a competent authority of the department and e-Pramaan repository will be updated accordingly. Users of such services will be notified through email/SMS about delist of the service from e-Pramaan.

2.6 Credential Handling in e-Pramaan

This section discusses guidelines for standard credential strength and process of credential issuance for different authentication levels of e-Pramaan.

2.6.1 Password

The e-Pramaan password based authentication MUST adhere to the following:

i. A password MUST be associated with a user, only when the user has met all the pre-defined criteria for setting a password at e-Pramaan.

ii. Password reset functionality SHOULD be provided by e-Pramaan.

iii. In cases where user chooses to reset the password, e-Pramaan SHOULD send a reset password link allowing the user to reset the password. e-Pramaan

SHOULD NOT display the User Password on screen.

2.6.1.1 Password Setting Requirement

This section describes the password setting policy for setting up strong passwords. The user MUST adhere to the following password strength requirements:

The User Password

i. MUST Contain a minimum of 8 characters;
ii. MUST Contain characters from the following categories
    a. English uppercase characters (A to Z)
    b. English lowercase characters (a to z)
    c. Numerals (0 to 9)
    d. Non-alphanumeric keyboard symbols (e.g. !@#&*)
iii. MUST NOT contain the user's name or surname of the user.

2.6.1.2 Password Policy

i. After initial registration or reset password, end-user should be advised to change / reset of password after a defined period.
ii. Password MUST be stored with a one way hash value to prevent various password guessing attacks.
iii. Password MUST be stored in the database ONLY in Message Digest format. SHA-2 algorithm is recommended for hashing the password.
iv. Password MUST always be transmitted in an encrypted form on all communication channels.
v. If password is forgotten by the e-Pramaan end- user it MUST be RESET and MUST NOT be RECOVERED.
vi. In cases of more than 3 unsuccessful authentication attempts by the end-user, the authentication system SHOULD display a Captcha to be entered by the end-user and notification will also be sent to the verified mobile number and/or email-id about the failed attempts.
vii. In cases of more than 3 unsuccessful attempts with Captcha, the end-user account SHOULD be locked for a defined period.

2.6.2 PIN Guidelines

The section covers guidelines to be followed to set Personal Identification Number (PIN) used to authenticate the end-user on mobile device or e-Pramaan application.

i. PIN MUST be set in numeric format only.
ii. PIN MUST be of 6 digits.
iii. PIN SHOULD be changed at regular intervals
iv. If 5 unsuccessful attempts are recorded, the account is to be locked.
v. The PIN SHOULD be RESET and not RECOVERD.

2.6.3 One Time Password (OTP)

One time password helps overcome replay attack where password based authentication may be susceptible, and thus provides a higher level of authentication. Authentication using assurance Level 2 of the e-Pramaan framework MUST use OTP as the second factor. e-Pramaan shall provide SMS and e-mail based OTP as well as mobile application based OTP i.e. client generated OTP.

2.6.3.1 OTP Schemes

This section discusses schemes and algorithms that can be used to generate and validate OTP [1]. The OTP schemes can be categorized into two types 1) HMAC based (HOTP) 2) Time based (TOTP). The RFC 4086 [7] can be used to generate SMS/email based OTP.

A brief description of both is given below.

i. HMAC based OTP (HOTP) - RFC 4868

The HOTP [2] algorithm is based on a counter value (C) and a static symmetric key (K) known only to the token and the server. Both the token and the server will have the counter set with the same predefined initial value. In order to generate the HOTP value, the HMAC-SHA-256+ algorithm is used which creates a minimum of 256 bits output. This value is truncated to a 6 digit OTP which can be easily entered by a user. The computation is done as

$$HOTP(K,C) = Truncate(HMAC\text{-}SHA\text{-}1(K,C))$$

ii. Time based OTP (TOTP) - RFC 6238

TOTP [3] is the time-based variant of HOTP algorithm, which specifies the calculation of OTP value, based on a representation of the counter as a time factor. Here the value T, derived from a time reference and a time step, replaces the counter C in the HOTP computation. TOTP implementations MAY use HMAC-SHA-256 or HMAC-SHA-512 functions, based on SHA-256 or SHA-512 [SHA2] hash functions, instead of the HMAC-SHA-1 function that has been specified for the HOTP computation [2].

$$TOTP = HOTP(K,C) = Truncate(HMAC\text{-}SHA\text{-}1(K,C))$$

iii. SMS/Email based OTP - RFC 2289

The server generates an OTP and may send through SMS to the user. It then compares it with the one received from the user.

2.6.3.2 OTP Guidelines

This section summarizes the requirements taken into account for using the OTP algorithms.

i. e-Pramaan MUST ensure two-factor authentication with OTP instead of using OTP as a single factor authentication.

ii. The Secret Seed values used for generating OTP MUST be stored securely.

iii. The Shared Secrets used for generation of HOTP and TOTP at token and server MUST be stored securely.

iv. The claimant (e.g., Token, Soft token) and verifier (authentication or validation server) MUST be in time sync for TOTP generation.

v. An OTP generated should be valid only for a fixed time and SHOULD NOT be valid for more than one transaction.

2.7 Digital Certificates

A Digital Certificate is an electronic document using digital signatures to bind together a public key with identity information such as the name of a person or an organization, their address, and so forth. The certificate is used to verify that a public key belongs to the individual. Digital certificates are the digital equivalent (i.e. electronic format) of physical or paper certificates.

e-Pramaan end-users accessing services, which require PKI based authentication, MUST possess a digital certificate for authentication. The user MAY use a Digital Certificate issued by any licensed Indian CA or digital certificates issued by e-PramaanCA. In both the cases, only X.509 v3 certificates will be recognized for authentication.

e-Pramaan shall not recognize digital certificates issued by any other CA except the Licensed Indian CAs and e-PramaanCA. For using digital signature based authentication, end- user MUST register DSC by uploading the Public Key Certificate at e-Pramaan.

e-Pramaan shall support certificates issued by licensed Indian CAs and e-PramaanCA. The CPS of e-PramaanCA is based on the CP and CPS of RCAI. The SPs SHOULD decide whether they will accept the user authentication using e-PramaanCA certificate or Licensed CA certificate. This is to be intimated to e-Pramaan at the time of SP enlistment with e-Pramaan.

2.7.1 e-PramaanCA

e-PramaanCA will be based on the Hierarchy based closed PKI model and will issue certificate using its Self-Signed RootCA. e-PramaanCA certificates will be issued based on the e-PramaanCA CPS. e-Pramaan shall issue Digital Certificate only to end-users. Digital Certificate issued by e-PramaanCA MUST be valid only for Digital Certificate based authentication at e-Pramaan. In addition, more documents may be asked for verification purposes as the case may be.

2.7.2 Licensed Indian CA

The CAs in India follow the Hierarchical Model for issuing a certificate as per IT Act 2000. The certificate issuance is based on their respective CPS which is prepared based on the CP of CCA. The CAs in India issue different types of certificates including Signing, Encryption, Code Signing, SSL certificate etc. However, e-Pramaan shall accept only Signing Certificates for user authentication. The details of certificate issuance process can be found in the respective CA's Certificate Practise Statement (CPS) available on CA's website [4].

2.7.3 Certificate Issuance through e-PramaanCA

e-PramaanCA shall issue Digital Certificates which shall be used only for authentication purposes at e-Pramaan.

The following procedure needs to be followed for acquiring a Digital Certificate from e-Pramaan.

Step 1: End-user requests for DSC after login.

Step 2: She fills in the Certificate Registration Form as required by the CPS.

Step 3: e-Pramaan verifies the Aadhaar number using e-KYC service of UIDAI.

Step 4: On successful verification, end-user generates the key pair. e-Pramaan creates CSR and submits it to e-PramaanCA for Digital Certificate creation. e-PramaanCA issues the Digital Certificate to end-user and uploads it to her e-Pramaan account. This generated digital certificate will be PIN protected.

2.7.4 Process for Revocation

e-Pramaan shall revoke a certificate issued by e-PramaanCA, if the user requests for certificate revocation.

2.7.4.1 Reasons for Revocation

A certificate shall be revoked by e-Pramaan, at its absolute discretion, on receipt of revocation request from the following:

i. The authorized user

ii. e-Pramaan

iii. A sensitive Govt. Agency dealing with National Security

The Digital Certificate will be revoked if

i. End-user's Private Key is compromised or misused.

ii. End-user's Private Key is suspected to be compromised or misused.

iii. End-user information in the certificate issued by e-PramaanCA has changed. Subsequently new certificate will be issued on user request reflecting the changed information. However, certificate will only be revoked if the information which is part of digital certificate is getting changed.

iv. End-user is known to have violated the rules and regulations laid by e-PramaanCA.

v. End-user wishes to deactivate her e-Pramaan account.

2.7.4.2 Process for Certificate Revocation

i. In cases where e-Pramaan by itself confirms that the certificate has been either compromised or misused, the Digital Certificate will be revoked.

ii. In all other cases e-Pramaan shall authenticate the revocation request before revoking the certificate by way of sending SMS or email. If the user is unreachable, then level 3 access using such a certificate for that user will be suspended until confirmation from the user is received.

iii. The reason for revocation MUST be provided by end-user.

iv. A user shall submit a certificate revocation request through e-Pramaan portal. On receipt of such a request, the certificate for which revocation is sought, shall be suspended. Only upon authentication of the certification revocation request, the certificate will be revoked.

v. Revoked certificates shall be included in the CRL.

vi. A certificate that is released from a "hold" status shall not be included in the succeeding CRL.

vii. In cases, where the revocation request cannot be authenticated, however e-Pramaan remains assured that the certificate is compromised based on the following circumstances, e-Pramaan shall initiate a revocation procedure for the issued digital certificates:

   a. A material fact represented in the Digital Certificate is false or has been concealed;

   b. User has been declared dead.

2.7.5 Certificate Practice Statement (CPS)

The CPS for e-PramaanCA shall be drafted based on the CP of India PKI, CPS of RCAI and CPS of NICCA. The CPS will be provided separately.

2.7.6 SSL Certificates for Secure Communication

i. e-PramaanCA MUST NOT issue SSL certificates for communication with the SPs.

ii. e-Pramaan MUST support SSL certificates issued only by licensed Indian CAs.

iii. e-Pramaan MUST get its own SSL certificate from the licensed CA.

2.7.7 Standards for Digital Certificates

The standards to be used for digital certificate based authentication and storage of digital certificates are in the purview of this section. Digital certificates generated and/or used in the authentication system should follow CCA India guidelines and X.509 /PKIX (RFC5280).

2.7.8 Requirements for e-Pramaan as CA

i. e-PramaanCA shall provide self-signed digital certificates to the system users.

ii. e-PramaanCA MUST accept digital certificates generated by licensed CAs.

iii. Digital certificates and private keys generated by e-PramaanCA MUST be stored in FIPS compliant validated key store.

iv. e-PramaanCA MUST maintain a list of revoked certificates generated by e-Pramaan.

v. e-PramaanCA MUST publish its Public Key Certificates for Trust validation.

vi. e-PramaanCA SHOULD support

   a. RSA algorithm with key length up to 2048 bits.

   b. DSA algorithm with key length 1024 bits.

c. ECDSA algorithm with named curves.

d. Support SHA-2 Hash Functions for signatures such as SHA-256, 512 etc.

e. Support SSL certificates that are used for communications with SP services.

f. Client certificates exported as PKCS12, JKS or PEM.

g. Mobile devices which store Digital Certificates for authentication.

h. Revocation and Certificate Revocation Lists (CRLs).

i. CRL creation and URL-based CRL Distribution Points as per RFC5280.

2.8 Biometrics

Authentication based on biometrics is considered as a strong authentication as it is based on what a person is and cannot be easily duplicated

2.8.1.1 Biometric Based Authentication

Biometrics based verification would be conducted in accordance with the standards and specifications laid out by UIDAI's Aadhaar authentication mechanism.

User credentials required to access Biometric based Authentication:

i. Aadhaar number;

ii. Fingerprint Biometric

On requirement of an e-Governance service to authenticate end-user for authentication, the end-user is requested to provide her biometric credentials. The biometrics information is then validated by Aadhaar through an Authentication Service Agency (ASA). On successful validation of the Aadhaar biometric credentials, e-Pramaan returns a successful authentication message to the service.

2.8.1.2 Standards for Biometrics

The section covers the biometric standards to be used by the authentication system.

i. e-Pramaan shall provide biometrics based authentication.

ii. Fingerprint biometric information captured by the system MUST be compliant with the standards specified by UIDAI for Aadhaar authentication.

iii. e-Pramaan shall not store any biometric data of the user.

iv. Biometric information of the user shall be forwarded to CIDR on a secured communication channel as specified by UIDAI.

3 Identity Attributes in e-Pramaan

Credentials provided during registration must include a user possession factor i.e. mobile number or e-mail ID, which will be verified by e-Pramaan during registration as well as during profile update. If the user has provided her Aadhaar number and/or PAN number, the same will be verified using respective identity providers.

Table 3: Credentials of the User to be taken during Registration

Credential	Min Length	Max Length	Required (Yes/No)	Format Validations
Given Name	2	99	Yes	Combination of English alphabet separated by "blank space" representing given name/middle name etc. in any order as per cultural practices.
Address (All specifications taken from the Demographics Standards [10] with the exception that Sub-District has not been taken separately, it is assumed that if required it will be given as part of the locality field).				
Address Line 1	1	60	No	Alphanumeric and special characters ();-.
Address Line 2	1	60	No	Alphanumeric and special characters ();-.
City / District	1	50	No	Letters of English Alphabet
State	1	50	No	Character Set – selected from a pre-populated list
Pincode	6	6	No	Numeric
Date Of Birth	10	10	Yes	dd/mm/yyyy format.
User Name	3	100	Yes	Alphanumeric with no special characters included
Password	8	30	Yes	As per Specifications in Section 2.5.1.1
Mobile Number	10	10	No	Numeric. Mobile number or e-mail

				ID: one of them is mandatory
e-Mail ID	5	254	No	Alphanumeric in valid email-ID format. Mobile number or e-mail ID: one of them is mandatory
PAN Card Number	10	10	No	Alphanumeric in standard PAN Card Number Format
Aadhaar Number	12	12	No	Numeric, display format NNNN NNNN NNNN.

4 Single Sign-on and Session Policy Management

When an authentication event is successful, the result of the authentication MUST be communicated to the SP department application or service which the end-user was trying to access. This communication is done in the form of an assertion, which states who the user claims to be, the attributes of the user etc. The assertion mechanism involves securely communicating this assertion and allowing it to expire after a period of time [14]. SSO sessions will be preconfigured for a defined period of time and will expire on lapse of such a period. Also, the session timeout will be uniform across all authentication factors/levels or combinations thereof.

e-Pramaan shall use the Security Assertion Mark-up Language (SAML v2.0), an XML based standard developed by the Organization for the Advancement of Structured Information Standards (OASIS), which defines messages for communicating a range of security-related statements about individual parties, including their authentication.

Security Assertion Mark-up Language 2.0 (SAML 2.0) is a version of the SAML standard for exchanging authentication and authorization data between security domains. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end- user) between a SAML authority, that is, an identity provider, and a SAML consumer, that is, a service provider. SAML 2.0 enables web-based authentication and authorization scenarios including cross-domain single sign-on (SSO), which helps reduce the administrative overhead of distributing multiple authentication tokens to the user. It aims to address use cases including single sign-on, federated identity, and secure web services [5].

4.1 Assertion Attributes

Standard Single Sign-on protocol requires assertion to be sent from e-Pramaan to the SP. The assertion will have attributes with which the user is identified at the SP site. The assertion attributes MAY contain parameters such as Primary communication IDs (SP-ID or Aadhaar number or Email ID etc), Session details (session ID, Session timeout) and other parameters (if any). These Assertion attributes MUST be sent in the form of Authentication Token.

4.2 Post-Authentication Action

When the user authentication is successful, e-Pramaan will create an Authentication Token for that user and communicate it to the SP. The SP checks the validity of the Authentication Token and availability of required assertion attributes, and then provides access to the user account. e-Pramaan shall ensure that the communication between e-Pramaan and SP is conducted through secure channels. It could be SSL / TLS or IPSec based communication

4.3 Session Logout Policy

e-Pramaan offers the Single Logout functionality wherein if the user is logged-out from either e-Pramaan or any other service accessed through e-Pramaan, the user MUST be logged-out from all the authenticated services.

5 Communication and Security

For any authentication system it is important to design communication protocols for securing channel to avoid attacks such as MITM, Replay and Phishing attacks.

5.1 Scope

The communication protocols to be used by e-Pramaan will be designed based on established cryptographic primitives as well as customized methods for key distribution.

5.2 Securing Communication

Communication between the authentication system and the service may use PKI or symmetric keys or hybrid methods. The encryption of the messages shall be done either with RSA-2048 or ECC if PKI solution is used or AES algorithm if symmetric key protocol is used.

5.2.1 Encrypted Channel

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are cryptographic protocols that are popularly used to provide secured communication over the Internet. These protocols use X.509 certificates to exchange symmetric keys. A session key generated in this protocol is then used to encrypt data flowing between the parties.

As the e-Gov applications in India support SSL, e-Pramaan shall support two way SSL communications with the backend services (SPs) to provide an encrypted channel with secure transmission of data. To provide a secured connection between the end-user or claimant and e-Pramaan, e-Pramaan shall have SSL connectivity between the end-user interface and e-Pramaan. The SSL certificate shall only be procured from a licensed CA. Version for SSL and TLS will be decided taking into consideration the security aspects, compatibility and interoperability of it on various browsers. Currently SSL 3.0 or TLS 1.0 will be considered due to its compatibility factor on various browser. However upgraded version will be supported in future based on the TLS version compatibility on various browsers.

5.2.2 Encrypted Data

The data encryption can be achieved using Asymmetric or Symmetric encryption methods. The most widely used asymmetric cipher is RSA whereas the AES is widely used for Symmetric encryption. e-Pramaan shall support encryption of data for transmission using RSA 2048 or ECC for asymmetric cryptography and will use AES for symmetric cryptography that will be used between e-Pramaan and e-Gov services.

5.2.3 Supported Communication Protocols / Standards

Communication between end- users and the authentication system will be based on standard communication protocol. The following are the open standards available: PKI (RSA or ECC algorithms).

i. The Security Assertion Markup Language (SAML) is driven by the Organization for the Advancement of Structured Information Standards (OASIS). SAML provides an XML dialect for embedding identity data in an XML message. SAML versions 1.2 and 2.0 are currently used in federation deployments. SAML 2.0 can be looked at as the convergence of SAML 1.2 and the Liberty Identity Federation Framework (ID-FF) 1.1 specification.

ii. As e-Pramaan shall act as an Identity provider with multiple e-Gov services as SP, the communication protocol with SSO shall be SAML 2.0 [6].

6 Service Agreements

This section provides the Service Agreement Requirements which are applied to the SP/e-Pramaan who shall be providing / implementing e-Pramaan authentication services. These include:

i. Legal Compliance Requirements
ii. Service Design Requirements
iii. e-Pramaan Service Requirements
iv. User Agreements and Notifications

6.1 Legal Compliance Requirements

The SPs MUST comply with relevant Indian law, including the Information Technology Act (IT Act) 2000 and IT Act 2008 Amendment.

6.2 Service Design Requirements

The departments SHOULD implement authentication technology, management processes and services that not only meet relevant Identity Assurance Levels but also incorporate good practice requirements in each of the following operational aspects:

6.2.1 Acceptability

The authentication technology, management processes and services SHOULD be generally acceptable to users. It SHOULD take into account the different needs of users and avoid the creation of unnecessary barriers. The process SHOULD be convenient, easy to use and as non-intrusive as possible.

6.2.2 Security and Privacy

i. Information MUST be suitably protected, whether it is owned by government departments or by users.

ii. Processes MUST be implemented for the retention of private (personal and business) information, its secure storage and protection against loss and/or destruction, and the protection of private information against unlawful or unauthorized access.

iii. Appropriate security policies should be in place and followed. Security policy will be detailed in a separate document as "e-Pramaan Data Security and Privacy Guidelines".

6.3 e-Pramaan Service Requirements

e-Pramaan should cater to the following requirements:

6.3.1 Affordability, Reliability and Timeliness

i. The authentication technology, management processes and services of e-Pramaan SHOULD be affordable and reliable and should not create unnecessary delays for either individuals or government departments.

ii. The Authentication services of e-Pramaan that are relied on by other departments or services (relying parties) MUST have a help desk will be available for inquiries and incident management.

6.3.2 Complaints handling

The authentication management processes and services of e-Pramaan MUST include a process for handling questions, concerns and complaints related to the collection, verification and use of identity information.

6.3.3 Fraud and Incident Management

i. The authentication management processes and services of e-Pramaan MUST include fraud and incident management processes.

ii. The processes for managing fraud MUST:

   a. Address all service delivery channels and partners.

   b. Include both proactive and reactive elements.

iii. Proactive activities would focus toward risk assessment, mitigation and fraud detection.

iv. Reactive activities would address investigation of, and response to, actual cases of fraud.

6.4 User Agreements and Notification Requirements

6.4.1 User Agreements

i. e-Pramaan MUST have a Terms of Use agreement with the enlisted SPs . It MUST include any conditions that apply to the use of the authentication services by e-Pramaan.

ii. e-Pramaan MUST inform and require the Citizen to accept the Terms of Use agreement before availing authentication service. e-Pramaan MUST also inform and require acceptance of any changes to the Terms of Use.

iii. Both e-Pramaan and the SPs MUST keep a record of the user's acceptance of the Terms of Use agreement.

6.4.2 Notification

e-Pramaan and SP MUST inform individuals of their Privacy Policy, including:

i. The legal authority and purpose for which their identity and contact information is being collected;

ii. How their information will be used;

iii. The circumstances under which their information will be disclosed, if any.

7 Audit Trail Management

An audit trail is a record of computer events, about an operating system, an application, or user activities. Audit trails provide a means to track transactions, events related to system failures, legal issues related to the information etc. Audit logs and reports that are useful for analysis can be generated using audit trails. A detailed Audit-trail implementation will be a separate document covering types of information which will be audited, security mechanism for audit logs, duration for retaining audit logs etc.

7.1 Types of Events Recorded

e-Pramaan shall maintain an event-oriented log which will have records describing system events, application events and/or user events. e-Pramaan shall maintain records of any activity that involves transaction data at e-Pramaan. Any time a data record is accessed, created, edited, or destroyed, e-Pramaan shall archive it for future reference.

The types of events that are recorded by e-Pramaan shall be (but not limited to) as follows:

i. e-Pramaan Servers Start-up and Shutdown.

ii. User Login and Logout, successful and failed attempts to e-Pramaan.

iii. Attempts to reset passwords.

iv. Unauthorized attempts at network to access e-Pramaan servers.

v. Unauthorized attempts to access protected data.

7.2 Protection of Audit Log

Only authorized personnel are allowed to view and process audit log files.

7.3 Audit Log Backup Procedures

A backup of the audit logs on physical removable media will be performed as per the backup policy of DC and DR sites. The backup media shall be maintained in safe storage.

7.4 Vulnerability Assessments

Events in the audit process shall be logged, in part, to monitor system vulnerabilities. A vulnerability assessment will be performed, reviewed and revised.

7.5 Audit Retention

ISO 27001 guidelines should be followed and compliance to IT ACT 2008 should be maintained.

8 References

[1]. A One-Time Password Systems – RFC 2289, http://tools.ietf.org/pdf/rfc2289.pdf

[2]. HOTP: An HMAC-Based One-Time Password Algorithm, http://tools.ietf.org/html/rfc4868

[3]. TOTP: Time-Based One-Time Password Algorithm, http://tools.ietf.org/pdf/rfc6238.pdf

[4]. CA List and CAs Certificate Practise Statement, www.cca.gov.in

[5]. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, Mar. 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[6]. Electronic Authentication Guidelines on Information Security by NIST, Special publication 800-63-1 http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

[7]. Randomness Requirements for Security, RFC 4086, https://tools.ietf.org/html/rfc4086

[8]. Key words for use in RFCs to Indicate Requirement Levels http://www.ietf.org/rfc/rfc2119.txt

[9]. Biometric Design Standards for UIDAI Applications http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf

[10]. Aadhaar Authentication API Specification Version 1.6 http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf

[11]. NIST Guide to Enterprise Password Management - http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

[12]. NIST Digital Signature Standard (DSS) - http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[13]. Guidelines for Usage of Digital Signatures in e-Governance v1.0 (Dec 2010), Published by DeitY, MCIT, GOI, http://www.icisa.cag.gov.in/images/Guidelines_for_Usage_of_Digital_Signatures_in_e-Governance_Ver.1.0.pdf

[14]. Electronic Credentials Authentication Guidelines v1.0 (April 2010), Published by Ministry of Citizen's Services, British Columbia, http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/electronic_credential_authentication_standard.pdf

[15]. Digital Signatures and the Indian Law, an extract from the book Ecommerce - Legal Issues authored by Rohas Nagpal, Asian School of Cyber Law, http://dict.mizoram.gov.in/uploads/attachments/cyber_crime/digital-signatures-law-india.pdf CPS of NICCA v4.4 – OID 2.16.356.100.1.4.2, August 24, 2009, https://nicca.nic.in/pdf/niccacps.pdf

[16]. X.509 Certificate Policy for India PKI v1.2, February 2014 by CCA, Govt. of India, http://cca.gov.in/cca/sites/default/files/files/X509CertificatePolicyforIndiaPKIv1.2.pdf

[17]. RCAI CPS v 2.0, September 2011, CCA, Govt. of India, http://cca.gov.in/cca/sites/default/files/files/RCAI-INDIA-CPS-VER-2.0.pdf

[18]. NIST - Audit Trails - http://csrc.nist.gov/publications/nistbul/itl97-03.txt

[19]. Reports and Audit Logs – IBM Security Privileged Identity Manager - http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.ispim.doc_10%2FPim_Guide%2Fconcepts%2Fc_audit_reports.html

9 List of Contributors

Reviewed by Committee for e-Authentication Standards

1	Dr. Rajendra Kumar	Joint Secretary(e-Gov), Department of Electronics and Information Technology(DeitY)
2	Ms. Debjani Nag	Deputy Controller, Controller of Certifying Authorities(CCA)
3	Dr. Ranjna Nagpal	DDG, National Informatics Centre
4	Sh. D C Misra	DDG, National Informatics Centre
5	Dr. MVNK Prasad	Associate Professor, Institute for Development and Research in Banking Technology(IDRBT)
6	Ms. Rama Vedashree	NASSCOM
7	Prof. Dhiren Patel	National Institute of Technology(SVNIT)
8	Prof. Anish Mathuria	Dean R&D, Dhirubhai Ambani Institute of IT
9	Dr. Pramod Varma	Chief Architect Technology, UIDAI
10	Sh. Lucius Lobo	Vice President, Tech Mahindra
11	Dr. Zia Saquib	Executive Director, C-DAC, Mumbai
12	Ms. Kavita Bhatia	Additional Director, Department of Electronics and Information Technology(DeitY)

Contributors

National e-Governance Division, DeitY	Sh. Sanjay Varyani
	Sh. Amit Kumar
Centre for Development of Advanced Computing: C-DAC	Dr. Padmaja Joshi
	Dr. Mohammed Misbahuddin
	Sh. Vijay Jain
	Ms. Cini Radhakrishnan
	Dr. Kumari Roshni
	Ms. Shivani Khanvilkar
	Sh. Anupam Saxena