National e-Authentication Framework

Cini Radhakrishnan, Shilpa Oswal, Ankita Dubey, Padmaja Joshi
Centre for Development of Advanced Computing (C-DAC)
email: {cini}{soswal}{ankitad}{padmaja}@cdac.in

ABSTRACT
This paper provides a glimpse of the proposed National e-Authentication Framework for India. It introduces the concept and need for an e-Authentication framework. It further discusses the process for authentication from users' perspective where the user can be a Citizen or an e-Governance Service. It also elicits the benefits for the user and possible future extensions of the system.

Categories and Subject Descriptors
Usable Security, Information Security

General Terms
e-Governance, Framework

Keywords
e-Authentication, Security, Privacy, Identity Management

1. INTRODUCTION
Due to widespread usage of technology, a large number of Indian central and state government services are readily accessible though internet as well as mobile devices. Although this leads to easy access and quick responses from the government departments; it poses many security and privacy issues. Departments may have some authentication mechanism in place that attempts to address these issues. But all these applications are implemented in isolation, and authentication mechanisms offered may not be adequate and up to date to address the latest security threats. Disparate authentication mechanism results in data and effort duplication, increase in cost and multiple user credentials for various authentications.

The National e-Authentication Framework (NeAF) for e-authentication is a comprehensive framework to deliver government services to the intended recipient in a secure manner through both internet and mobile platform. It is a secure framework for central/state government departments with configurable authentication levels.

To bring uniformity across various e-authentication mechanisms currently in use by Government departments, NeAF will provide a solution that conforms to the well accepted industry standards and protocols.

NeAF further allows the user to be compliant with various levels of authentication like One Time Password (OTP), Digital Certificates (DSC) and biometrics. For the e-Gov service providers who require standard compliant authentication solution, NeAF will provide e-authentication modules as per their desired security levels.

NeAF supports different types of single or multifactor authentications. Levels of authentication defined in NeAF are:

Level 1 is the basic authentication mechanism with username and password, and is mandatory for all levels.

Level 2 uses One Time Password (OTP) token either received on Mobile device and/or email or generated on the mobile device.

Level 3 uses tokens such as digital certificate/digital signature or a smart card.

Level 4 uses biometric information for authentication through Aadhaar.

NeAF levels of authentication are in accordance with NIST guidelines [1].Levels can be combined to achieve multi-factor authentication. In NeAF Level-1 is mandatory and sequence for multi-factor authentication is configurable.

2. CITIZEN'S PERSPECTIVE
As an authenticating server, NeAF provides a single window access to all those e-Gov services that uses authentication mechanism provided by NeAF. In effect NeAF needs to verify the eligibility of the citizen accessing any of these services for a level of authentication desired by the service
This provides a great degree of convenience as the citizen now needs to remember only a single userID and password to access any of the e-Gov services. The citizen also has the flexibility to modify his profile and get authenticated for any level of authentication that is supported by NeAF.

2.1 Process
Citizen should first register himself/herself with NeAF by providing basic demographic information such as Name, Address, Date of Birth (DOB) etc. The registration gives sufficient input to NeAF for authenticating the citizen for Level-1. If the citizen wants to register for higher levels then additional information is captured at NeAF.

After registering, the citizen should enrol himself/herself to the service he/she wants to use in future. The process of enrolment in NeAF is similar to creating aliases. However, NeAF does not persist any unsolicited private user information in the system. During enrolment for a particular service NeAF ensures that the user is registered for the level required by the requested service.

After registration and enrolment user is ready to use the service. The process is depicted in Figure 1.

2.1 Benefits of NeAF for the Citizen
A citizen who registers with NeAF will have ready access to all integrated e-Gov Services. NeAF ensures privacy and protects the citizen from cyber thefts along with following benefits:

- **Single Window Access:** NeAF implements Single Sign On across all registered e-Gov services. Now citizen is

required to remember only a single username and password for accessing all e-Gov services registered with NeAF.

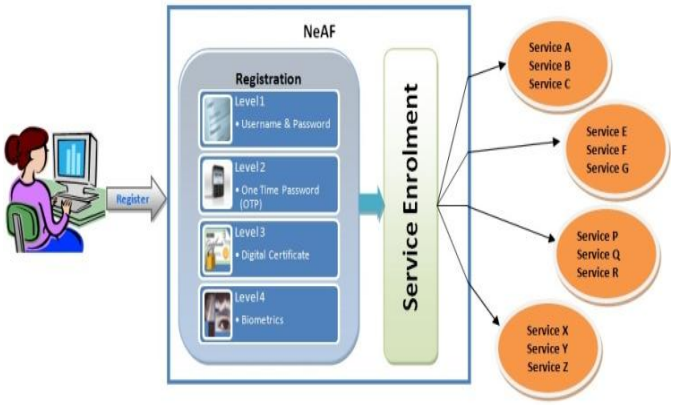

Figure 1: Process flow for Citizen at NeAF

- **Secure Communication**: Regardless of SSL channel for communication, NeAF provides an encrypted and secure communication channel between the service and citizen that protects user privacy and data.
- **Two-Way Authentication:** A citizen and an e-Gov portal both are authenticated to each other when NeAF is used. The citizen is assured that the e-Gov site can be trusted since the service is registered with NeAF via pre-defined registration protocol, to prevent acts like phishing or man-in-the-middle attacks. On the other hand, the service is certain on the authenticity of the citizen because the citizen is compliant with the desired level of authentication.

3. e-GOV SERVICES PERSPECTIVE

NeAF provides a standard based mechanism to e-Gov services for e-Authentication that provides single or multi-factor authentication. Services get configurable authentication modules to their preferences in terms of the levels of authentication required or a combination of these levels.

3.1 Process

This section covers the communication process between service and NeAF. An e-Gov service that wishes to use NeAF as their authentication platform needs to be registered with NeAF. On request for registration, NeAF will establish a secure communication channel between the service and NeAF through handshake. The service will have to configure its authentication module by selecting authentication level (Level 1, 2, 3 or 4) or selecting a combination of authentication levels and creating authentication chain.

The process is depicted in Figure 2.

3.2 Benefits of NeAF for the Department

A standard based authentication solution of NeAF which is easily integrable to service's existing infrastructure. Additionally, the service can take advantage of the following:

- **Authentication as a Service:** A strong authentication system based on well accepted industry standards and protocols.
- **Flexible authentication chaining:** Services can easily set their minimum authentication level and also go for customised authentication chaining.
- **Compliance with Aadhaar:** NeAF proposes to use Aadhaar based authentication for Level 4.Thus, the services will get compliant with Aadhaar by default. Aadhaar is a service provided by Indian Government that captures demographic as well as biometric details of every Indian citizen[2]. The service provides APIs to get yes/no kind of an response for a query.

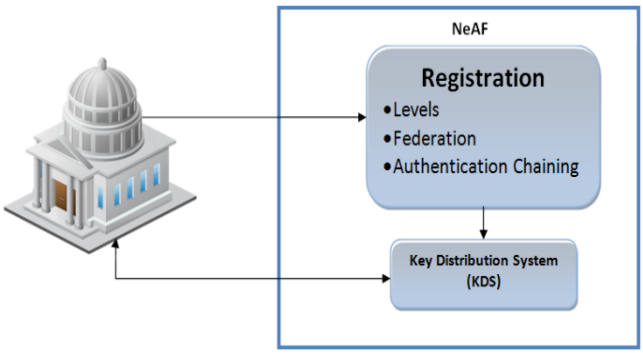

Figure 2: Process flow for e-Governance Services at NeAF

4. CONCLUSION & FUTURE ENHANCEMENTS

The widespread use and misuse of the internet medium indisputably demands for a strong e-authentication system. Solutions like the proposed NeAF are the path ahead for addressing the pressing issues of privacy and security.

In future, the following possible extensions could be added to strengthen the authentication at NeAF:

- **Voice Biometrics:** Voice authentication or Voice recognition protocols use the person unique voiceprint to control access to information.
- **Behavioural Biometrics:** Daily routine activities like driving, using computer, talking on phone are governed by a person's ability, approach, knowledge, preference or strategy which varies and is thus could be used for authentication.
- **Graphical User Authentication (GUA):** User password is selected from a set of images, in a specific order, presented in a graphical user interface.

NeAF also provides the flexibility of introducing upcoming new authentication techniques and hence, providing advanced authentication in lower cost.

5. ACKNOWLEDGMENTS

We would like to thank Department of Electronics & Information Technology (DeitY) for sponsoring this project for India. We would also like to thank Dr. Zia Saquib, executive director of C-DAC, Mumbai for providing us the opportunity to work on this project.

6. REFERENCES

[1]. Electronic Authentication Guidelines on Information Security by NIST, Special publication 800-63-1

[2]. Aadhaar, http://uidai.gov.in/