Unique Identity Enabled Service Delivery through NSDG

Swapnil Shrivastava, Zia Saquib, Gopinath P., and Peeyush Chomal

Centre for Development of Advanced Computing, Mumbai, India
{swapnil,saquib,gopinath,peeyush}@cdac.in

Abstract. Unique Identity (Aadhaar) is issued by Unique Identification Authority of India (UIDAI) to the residents of India. With Aadhaar enrolment happening in full swing across the country, there is a strong need to formulate and furnish Aadhaar-enabled Service Delivery for the citizens. The National e-Governance Service Delivery Gateway (NSDG) as a messaging middleware provides Integrated Service Delivery based on Service Oriented Architecture for various government services. By positioning NSDG as Authentication User Agency (AUA) in Aadhaar Authentication Ecosystem, it can cater Aadhaar Authentication Service to all the government departments who wish to offer Aadhaar-enabled services and benefit schemes to the citizens. NSDG as AUA will provide Aadhaar authentication in conjunction with service access portal authentication process. With this NSDG can deliver Aadhaar-enabled Services to citizens based on online identity verification, thus improving efficiency, reliability and transparency in service delivery to the citizens. In this paper we will present integration of Aadhaar Authentication service with Messaging service of NSDG and its benefits.

Keywords: NSDG, Aadhaar Authentication, Unique Identity, Service Delivery, Aadhaar-enabled Service Delivery.

1 Introduction

"Make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realise the basic needs of the common man." [1]

This is the vision statement of the National e-Governance Plan (NeGP) which was formulated by the Department of Information Technology (DIT), Government of India (GoI), for implementation of e-Governance across the country. India, the world's largest democracy is a federal republic comprising of states and union territories [3]. NeGP comprises of 27 Mission Mode Projects (MMPs) to be implemented at the Central, State and Local Government levels and 8 Common Core and Support Infrastructure [1-2]. In this paper we will discuss integration of key features of two MMPs viz. Authentication service of Aadhaar with Messaging service of National eGovernance Service Delivery Gateway (NSDG) in order to provide Aadhaar-enabled Services via NSDG.

A. Kő et al. (Eds.): EGOVIS/EDEM 2012, LNCS 7452, pp. 103–111, 2012.

In general, to avail certain service offered by government department, a citizen is required to prove his/her identity. In such situation, an authentication process precedes service delivery. Authentication in a traditional sense could be carried out by verifying credentials owned by the citizen. These credentials could be physical documents such as an identity card, passport and so on. Sometimes signature or thumb impression that is unique to a citizen may also be used. Lately authentication can also be done by verifying citizen's biometrics such as fingerprint or iris. On successful verification of the citizen's credentials, requested service is delivered to him/her.

In e-Governance, similar service delivery process is automated and can be accessed online by the citizen. Under NeGP, various e-Governance applications are being implemented in order to provide speedy delivery of government services to the citizens at affordable costs [4-5]. NSDG is an integrated MMP executed by DIT, GoI and implemented by CDAC Mumbai, India [1]. NSDG is a messaging middleware which enables interoperability and integration of various central government department services. It comprises a set of e-Governance Gateway specific protocols (IIP, IIS, IGIS) that are based on open standards (XML and SOAP) [8]. To integrate e-Governance application as a service with NSDG, front-end and back-end functionalities of this application is identified as service access portal and department server/back office respectively. These entities then become connected with NSDG by implementing SAP (Service Access Provider) and SP (Service Provider) connectors. Detailed discussion of these components and integration of a service with NSDG will be discussed in section 2. Go Live of NSDG happened in August 2008 and integration of services such as Trademark Service and Uttar Pradesh State's e-District is complete. There are several integrations underway such as Police Verification and Permanent Account Number (PAN) Verification.

Aadhaar (UID) project is a central MMP which aim to provide unique identity (Aadhaar Number) to all the residents of India. Unique Identity Authority of India (UIDAI) [11] established by Government of India is the overseer and regulatory body of this project. UIDAI provides two services for the citizen viz. Aadhaar Enrolment Service and Aadhaar Authentication Service [1]. Aadhaar Enrolment Service initiates generation of Aadhaar Number for the citizens. Currently this service is available at many locations in the country. By the time this paper is written almost 17 crore Aadhaar Numbers are already issued [10]. With Aadhaar enrolment already taking place there is a strong need to formulate and make operational Aadhaar-enabled Service Delivery for the citizens. Aadhaar-enabled Service Delivery is to provide requested service to citizen after successful Aadhaar authentication. Aadhaar Authentication Service enables agencies (government/private) to verify identity of citizens using an online and electronic means [6]. The Aadhaar Authentication Ecosystem and types of authentication will be discussed in section 3.

By positioning NSDG as Authentication User Agency (AUA) in Aadhaar Authentication Ecosystem, it will provide Aadhaar authentication to all the government departments who wish to offer Aadhaar-enabled services and benefit schemes to the citizens. NSDG as AUA will use Aadhaar authentication in conjunction with service access portal authentication process. Aadhaar authentication will facilitate NSDG to deliver Aadhaar-enabled Services to citizens based on establishing their identity, thus improving efficiency, reliability and transparency in service delivery to the citizen. Positioning of NSDG in Aadhaar Authentication Ecosystem is described in section 4.

2 Messaging Service of National e-Governance Service Delivery Gateway (NSDG)

Messaging service of NSDG provides secure and standard based communication channel for service request/ response between service access portal on Service Access Provider (SAP) side and department server/back office on Service Provider (SP) side. NSDG consists of four major components as shown in figure 1 and as described below:

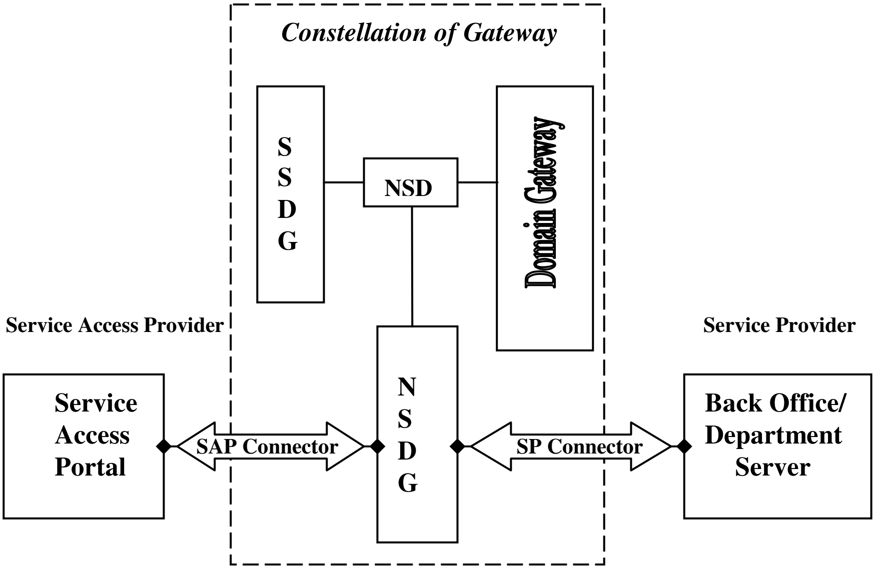

Fig. 1. NSDG Components

Service Provider (SP) is government department or any other third-party agency offering services to citizens and businesses, and to other government departments. Service Access Provider (SAP) is an entity, which facilitates government service access for citizens, by providing a front-end infrastructure. Access to service access portal (India Portal, State Portal and so on) is provided to citizen through Citizen Service Centre (CSC) available across the country. NSDG provides gateway for services offered by central government departments. The SSDGs' are the productized version of NSDG and will act as gateway for services offered by various state government departments. In addition, there are departmental applications gateways like MCA21, Passport which are identified as Domain Gateways. All these put together forms Constellation of Gateways. National Services Directory (NSD) provides a registry, which acts as a service resolution point for all the services in the Gateway constellation [8]. This constellation is a novel constellation initiative in the world. It goes well with federated form of governance in India.

For integration of e-Governance application as a service with Gateway the SAP and SP connectors have to be implemented for the front-end and back-end functionalities of this application respectively. The SAP/SP connector wraps/unwraps the message into/from the e-Governance Gateway specific protocol. We will take an example of "Service Request" use case to explain message flow when a citizen applies for a service which is integrated with NSDG. The citizen visit CSC to put-up a request for service such as Age Certificate. The operator opens eform [9] of Age Certificate from service access portal and fills the required details of the citizen. Set of identity proof documents of the citizen are verified, scanned and uploaded along with the eform. When the operator submits eform application, SAP connector wraps the service request into IIP packet. This IIP packet will be routed to the SP connector of the corresponding department server/ back office through NSDG. The SP connector extracts service request from the received IIP packet and sends it for updation to Department Server. Department Server will send system generated application id after successful update or error message for failed update. The SP connector wraps the response received from department server in IIP packet. The response is routed to SAP connector of request originating SAP through NSDG. The SAP connector unwrap the service response and sends it to service access portal for display. The end-to-end message flow of this use case is also shown in figure 2:

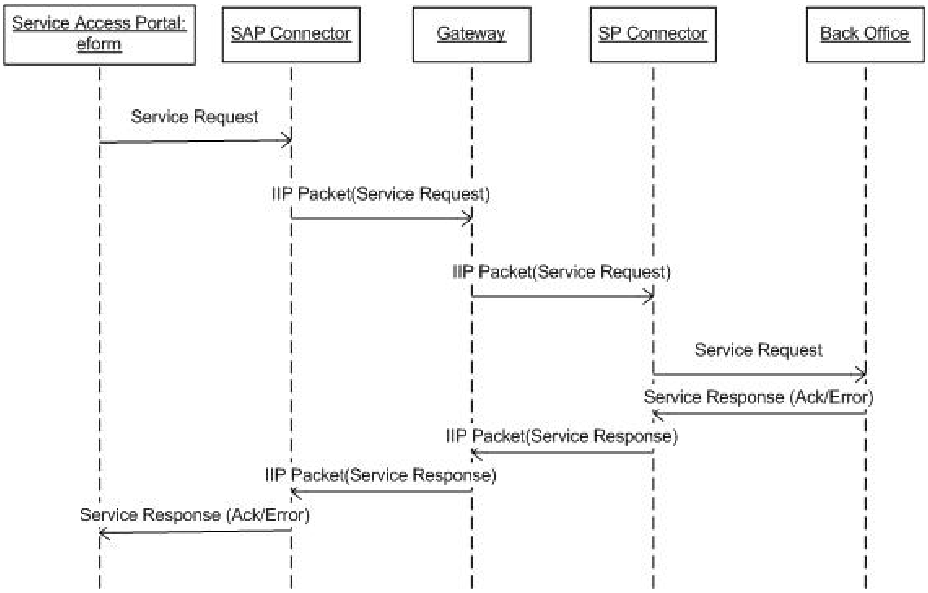
Service Access Portal: eform
SAP Connector
Gateway
SP Connector
Back Office
Service Request
IIP Packet(Service Request)
IIP Packet(Service Request)
Service Request
Service Response (Ack/Error)
IIP Packet(Service Response)
IIP Packet(Service Response)
Service Response (Ack/Error)

Fig. 2. End to end message flow for "Service Request" use case

NSDG offers number of benefits to the citizens as well as government departments. Some of them are listed below:

- NSDG is built on open standards and implemented using open source technologies and tools.
- It enables service delivery to citizen from a single point by facilitating an assortment of service models which supports one or more departments on SP side.
- It is a secure messaging middleware. It doesn't read or store the message body and thus ensure privacy and confidentiality of the data.
- It uses bidirectional SSL for end to end communication. This guarantees security during transmission of message.
- Gateway constellation will help the citizen to request for services offered by various central/state government departments from any part of the country.

3 Aadhaar Authentication Service

Aadhaar Authentication Service is an online process in which citizen's Aadhaar Number along with his/her personal identity information are submitted to CIDR for verification. Personal identity information can be a combination of biometric (fingerprints, iris) and/or demographic (such as Name, Date of birth, Address) and/or a secret PIN/OTP number known only to the citizen. During verification, the submitted details are matched with the data against the citizen's Aadhaar number in CIDR. If they match then CIDR sends "Yes" as response else "No" [6-7].

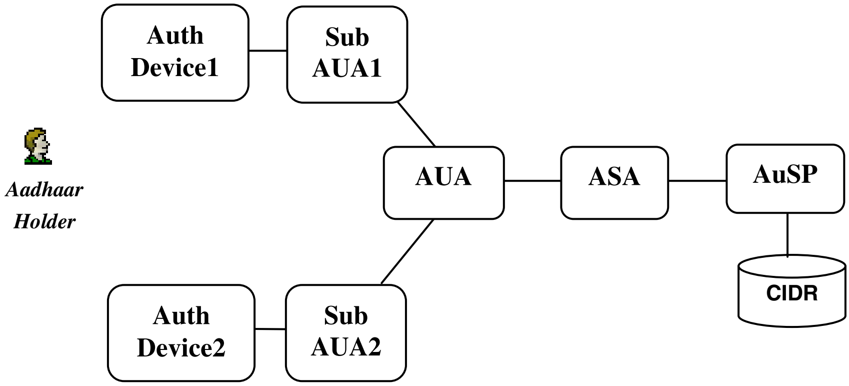

Fig. 3. Aadhaar Authentication Service Ecosystem

The key components of Aadhaar Authentication Service ecosystem are as shown in figure 3. *Aadhaar Holders* are those with a valid Aadhaar Number. CIDR contains the identity information of all Aadhaar holders. *Authentication Service Provider (AuSP)* offers Aadhaar based authentication service on behalf of UIDAI. *Authentication Service Agency (ASA)* establishes secure network connectivity (through leased line) with the CIDR. *Authentication User Agency (AUA)* uses Aadhaar authentication to enable its services or transmit authentication requests from *Sub AUAs* to *ASA*. *Sub AUAs* access authentication service through an existing *AUA*. *Authentication device* collects the personal identity information, prepare the information for transmission, transmit the authentication packets through AUA and receive the authentication results from them.

UIDAI provides 5 types of Aadhaar-based authentication as listed below:

- Type 1:Demographic attributes (name and/or DoB and/or address and so on)
- Type 2:One Time Password (OTP/Mobile)
- Type 3: Biometric attributes (FingerPrint/Iris scan)
- Type 4 :OTP/Mobile and Biometric attributes (FingerPrint/Iris scan)
- Type 5 :OTP/Mobile and FingerPrint and Iris scan

The SubAUA/ AUAs can choose any of these authentication types based on their security requirements. The personal identity information captured by Aadhaar enabled Authentication Application running on Authentication Device are packaged into an XML termed as Personal Identity Data (PID) block.

Aadhaar has defined security policies and standards to protect personal identity information of Aadhaar Holder at the time Aadhaar authentication. They are as follows:

- The PID block should be encrypted and encoded before it is transmitted over network.
- Encrypted and encoded PID block, encrypted Session key and HMAC value of PID block are sent from device to prevent data loss or tampering due to any malicious attack at the network level.
- The key components (AUA, ASA) should log metadata of authentication request and response for audit purpose.
- PID block should not be stored in the Authentication Devices as well as audit logs.
- Secure transmission of data between the key components is recommended.

4 Positioning of NSDG in Aadhaar Authentication Ecosystem

In Aadhaar Authentication Ecosystem, NSDG is positioned as AUA and various government departments who wish to provide Aadhaar enabled services and benefit schemes to citizens through NSDG will become Sub AUAs.

Aadhaar-NSDG integration model is shown as block diagram in figure 4. Citizen can avail Aadhaar-enabled service by accessing service access portal from home via public devices and from CSC through terminal devices. Aadhaar Number, personal identity information and department service request specific attributes provided by the citizen will be entered in the eform by front office operator at the CSC. The personal identity information will be packaged in form of PID block. The device will send encrypted and encoded PID block along with security credentials (HMAC value, Session Key) and department service request data to Sub AUA. In case of public devices, citizen will enter necessary demographic information, OTP in addition to department service request specific attributes.

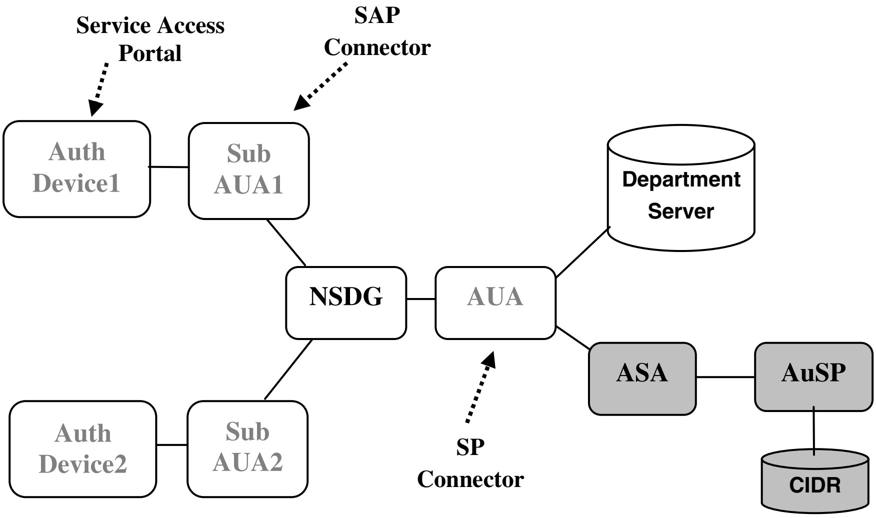

Fig. 4. Block diagram representation of Aadhaar-NSDG Integration Model

Sub AUA role is played by various government departments who wish to offer Aadhaar-enabled services and benefit schemes to citizens through NSDG. The set of job performed by Sub AUA is implemented in the SAP connector. The SAP connector package encrypted and encoded PID block along with security credential and department service request data as XML into the body of IIP packet as shown in figure 5.

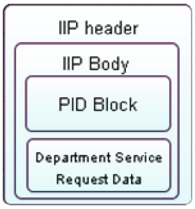

Fig. 5. IIP Packet structure of Aadhaar enabled Service Request

NSDG as AUA will provide Aadhaar Authentication service to Sub AUAs. The AUA's functionalities are implemented in NSDG SP connector. The IIP packet created at Sub AUA is routed to AUA via NSDG. AUA would validate, adds the necessary header to Authentication request and send it to CIDR via ASA. If CIDR's response is “Yes” then SP connector will perform certain additional tasks, such as it would extract department service request XML file from IIP packet, route and update it in the corresponding Department Server, and acknowledge to request originating SAP. The end-to-end service request flow for successful Aadhaar-enabled Service Delivery is as shown in figure 6. If CIDR's response is “No”, then the SP connector will send the corresponding error message to the request originating SAP as indication of authentication failure.

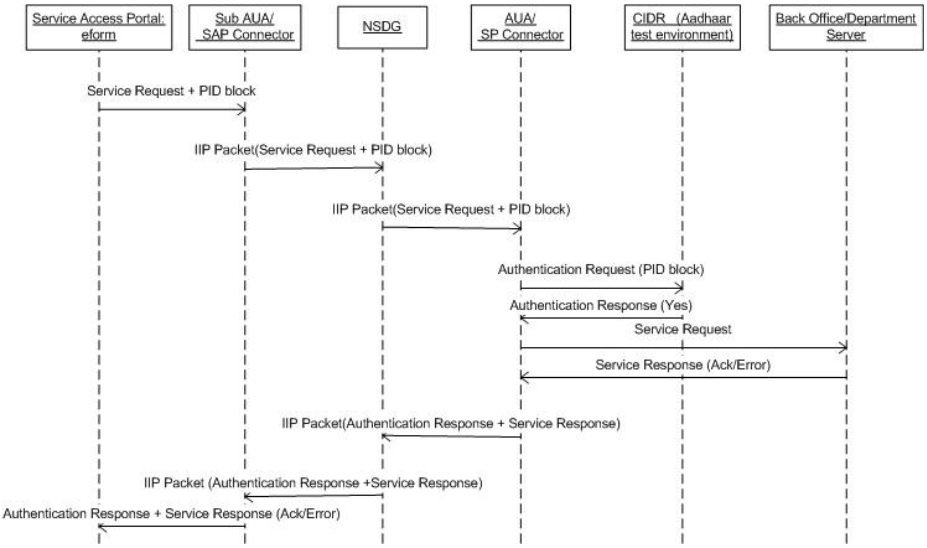
Service Access Portal: eform
Sub AUA/ SAP Connector
NSDG
AUA/ SP Connector
CIDR (Aadhaar test environment)
Back Office/Department Server
Service Request + PID block
IIP Packet(Service Request + PID block)
IIP Packet(Service Request + PID block)
Authentication Request (PID block)
Authentication Response (Yes)
Service Request
Service Response (Ack/Error)
IIP Packet(Authentication Response + Service Response)
IIP Packet (Authentication Response +Service Response)
Authentication Response + Service Response (Ack/Error)

Fig. 6. End-to-end flow for Aadhaar-enabled Service in case of service request from CSC

A Proof of Concept (PoC) is implemented based on the proposed Aadhaar-NSDG integration model. In this PoC, Jammu & Kashmir state portal's Indira Gandhi Old Age Pension Scheme (IGNOAPS) service is made Aadhaar-enabled. Aadhaar type1, type 2 and type 3 authentications are implemented for this service. This PoC is successfully tested against test records as well as live Aadhaar Number record present in Aadhaar test environment.

5 Benefits

- The Constellation of Gateways enables service request/delivery from/to any location across the length and breadth of the country. As a result, Aadhaar-enabled Service Delivery via constellation may come in handy for services and benefit schemes such as Public Distribution System (PDS) especially for migrant workers.
- Aadhaar-enabled Service request processing via NSDG brings transparency in service delivery to the citizen. Since there is no dependency on any middle-man, the risk related to service delivery such as poor service or denial of service is reduced.
- Any government department wanting to offer Aadhaar-enabled Services become AUA and sign agreement with UIDAI as well as ASA. Rather, if integration model discussed in this paper is followed, the department as Sub AUA will merely need to register with AUA (NSDG).
- NSDG will not store PID block, since as a policy decision it doesn't log or store message body. NSDG would thus provide personal data protection which in turn is a critical security requirement in Aadhaar authentication environment.

6 Future Work

The Aadhaar-NSDG integration model can be extended further by integrating Mobile Service Delivery Gateway (MSDG) to provide Aadhaar Authentication through mobile devices. Recently Aadhaar Authentication Service was launched for Aadhaar live data. As a result proposed work can move into production phase. Though this model serves integration of Aadhaar Authentication with NSDG, still it cannot be moved in its present form into production. It is observed that implementation of AUA functionalities in SP connector will cause difficulty in compliance to security standards. Hence in production, AUA functionalities should be implemented in a service, which can be registered on SP side of the gateway. This slight deviation in approach will result in NSDG to provide Aadhaar Authentication as a Verification Service for all the government departments who are registered with it. It will also facilitate compliance of security standards at a single location.

Acknowledgements. As per the directions of DIT, CDAC conducted a study on positioning of NSDG in Aadhaar Authentication Ecosystem. We are grateful to eGovernance Group of DIT and NeGD for entrusting us with this opportunity. We would like to thank Dr Pramod K Varma, Chief Architect, UIDAI for his perpetual support and guidance. First and third author appreciate our team member Mr Ahmad Hassan for his valuable contribution and also extend our sincere thanks to Mr Ravi K Sinha, Mr B Ravi Kumar, Ms Anna Thomas and Ms Kriti Kulshrestha for their valuable contribution in resolving integration issues related to J&K state portal.

References

1. Saaransh- A compendium of Mission Mode Projects under NeGP, Department of Information Technology, Government of India (2011)
2. Mathur, D., Gupta, P., Sridevi, A.: Transforming Government e-Governance Initiatives in India. In: Bagga, R.K., Gupta, P. (eds.), pp. 3–50. The ICFAI University Press, Hyderabad (2009)
3. Chauhan, R.: National E-Governance Plan in India, Report No. 414, UNU-IIST, Macao (2009)
4. Monga, A.: E-government in India: Opportunities and Challenges. JOAAG 3(2) (2008)
5. Thapliyal, M.P.: Challenges in Developing Citizen-Centric E-Governance in India. In: International Congress on eGovernment, pp. 1–5 (2008)
6. Aadhaar Authentication Framework 2.0, `http://www.uidai.gov.in/`
7. Aadhaar Authentication API Specification - Version 1.5 (Revision 1) (September 2011), `http://www.uidai.gov.in/`
8. Official website of National e-Governance Service Delivery Gateway (NSDG), `http://www.nsdg.gov.in`
9. eFiling through Fulcrum and NSDG, `http://eforms.gov.in`
10. Aadhaar Portal, `http://portal.uidai.gov.in/uidwebportal/dashboard.do`
11. Official website of Unique Identification Authority of India (UIDAI), `http://www.uidai.gov.in/`