OPEN ACCESS at journalijcir.com

Research Article

E- AUTHENTICATION FRAMEWORK FOR SECURE E-GOVERNANCE SERVICES

*Rahul Bhatt and Sanjay Kumar

Abstract

This paper is about the "How to deliver the secure services by the government to citizen without losing the privacy". E-Governance is the service which is provide by the government to deliver and transform the government services in easy, efficient, effective, transparent and accountable manner .e-Governance services may exchanges with in government, between government & government agencies of National, State, Municipal & Local levels, citizen & businesses, to empower citizens through access & use of information. The services should trusted, secure and highly private. To meet these requirements, mechanisms, which provide secure management of information and facilities without compromising privacy and human rights, we need such mechanisms that relies on effective identity authentication. While traditional security measure such as passwords and PIN may be forgotten, stolen , or cracked ,by any unauthorized user to misuse .at that time biometrics system provides a very secure authentication mechanisms which is based on unique human physiological and behavioural characteristics that can be used to identify an individual or authenticate the claimed identity of an individual, but cannot be easily duplicated or forget or cracked . This paper discusses the role of biometric authentication in e-Governance environment to provide services efficiently and securely over the internet.

Key Words: e-authentication , Biometrics, UIDAI , e- Governance, security framework for e-Authentication for e- Governance Service Deliver.

INTRODUCTION

The term 'Governance' means activity of governing and controlling a country by its Government, controlling of an organization or a company by its CEO or Board of Directors or controlling of a house hold by the head of the house, Accordingly E-Governance may also involve governing of a country, organization, company or a household, however with the help of Information and Communication Technology (ICT).

But when we talk of E-Governance popularity then we only refer to the governing of a Country/State using ICT. E-Governance therefore means the application of ICT to transform the efficiency, effectiveness, transparency and accountability of exchange of information and transaction.

E- Goverence Services Divide In Four Catagories

Government-to-Citizen (G2C)

e-Governance in G2C relationship will involve facilitation of the services flowing from Government towards Citizens with the use of Information and Communications Technology (ICT).

- PAN Card services
- AADHAAR Services.
- Election services.
- PASSPORT

Government-to-Business (G2B)

e-Governance in G2B relationship will involve facilitation of the services flowing from Government towards business with the use of Information and Communications Technology (ICT).

- Mobile Recharges
- Mobile Bill Payment
- DTH Recharge
- Money Transfer
- Data Card Recharge
- CSC Bazaar

Department. of CSE Uttarakhand Technical university Dehradun, India

Correspondence and Reprint Requests: Rahul Bhatt

Received: April 04 , 2015 | **Accepted:** April19, 2015 | **Published Online:** April 28, 2015

Conflict of interest: None declared | **Source of funding:** Nil

- LIC Premium
- Red Bus
- SBI Life
- Bill Cloud

Government-to-Government (G2G)

G2G relationship would include the relationships between Central and State Government and also the relationship between two or more Government departments.

- e-Administration
- e-Police
- oe-Courts

Citizen to Government (C2G)

e-Governance in C2G relationship will involve facilitation of the services flowing from citizen towards goverments with the use of Information and Communications Technology (ICT).

- e-Democracy
- e-Feedback

e-Governance also aims to empower people through giving them access to information. authentication verifies user's claimed identity by comparing an encoded value with a stored value of the concerned biometric characteristic.

Biometric system is An automated system which do following things.

- Step -1 It capturing a biometric sample from an end user;
- Step-2 Extracting biometric data from that sample
- Step-3 Comparing the biometric data with that contained in one or more reference templates;
- Step-4 Deciding how well they match; and
- Step-5 Indicating whether or not an identification or verification of identify has been achieved.

Hat Is Authentication And E-Authentication

Authentication is a process that ensures and confirms a user's identity. Authentication is one of the five pillars of information assurance (IA). The other four are integrity, availability, confidentiality and nonrepudiation

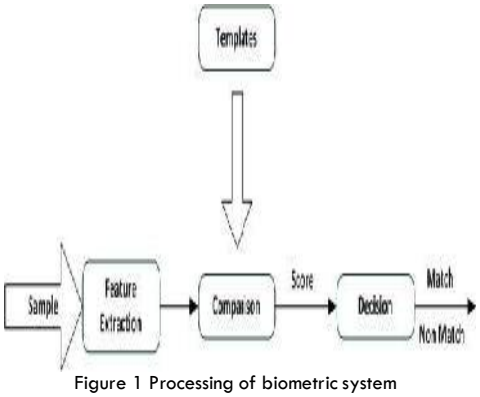

Figure 1 Processing of biometric system

Types of authentication

- Passwords and PINs based Authentication
- Public-Key Authentication
- Symmetric-key Authentication
- SMS based Authentication
- Biometric Authentication

Electronic authentication (e-Authentication) is the process of establishing confidence in user identities presented electronically to an information system. This may involve verifying with what the user knows (e.g. password), what the user has (e.g. an ID card), and/or what the user is or does (e.g. fingerprint or written signature recognition). The greater the number of factors being verified, the higher the confidence can be established.

Biometrics e-Authentication Methods

Biometrics is a method by which a person's authentication information is generated by digitizing measurements of a physiological or behavioral characteristic. Biometric

Types of biometrics

Fingerprint / **Palmprint** recognizes the physical structure of a person's finger print/palmprint, e.g. the minutiae points that include bifurcations and ridge endings

- **Hand geometry** recognizes the shape of a person's hand
- **Retina Scan** recognizes the patterns of the blood vessels on the backside of the eyeball
- **Iris Scan** recognizes the unique patterns, rings,

and corona in the iris, which is the colored portion of the eye

- **Signature dynamics** recognizes the electrical signals, pressure used, slant of the pen, the amount of time and patterns captured in creating a signature
- **Keyboard dynamics** recognizes the electrical signals when a person types a certain phrase on a keyboard, such as speed and movement
- **Voice print** recognizes the subtle difference in people's speech sounds and patterns
- **Facial scan** recognizes the attributes of a person's face, bone structure, nose ridges, and eye widths

The assurance level that can be met by a biometric authentication depends on the physical control and security of the biometric device. This method will be most useful for physical access control types of applications (e.g. entrance to a computer centre) where the biometric scanner can be secured and controlled by the business owner.

Figure 2 Biometric e-authentication methods

Biometric standard in e-Governance

Biometric data is the data representing a biometric characteristic. For Example, Image data, behavioral data, sensor data, etc. The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

Biometric Standards are developed to ensure interoperability of biometric devices and algorithms so as to avoid vendor lock-in and also ensure long term storage of data with technology independence. The defined biometric standards are applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

The accuracy of a biometric system is determined through a series of tests in the following order:

i. **Technology Evaluation:** Assessment of matching algorithm accuracy
ii. **Scenario Evaluation:** Assessment of performance in a mock environment
iii. **Operational evaluation:** Live testing on site If all the tests done properly, users will come to know, to a high degree of accuracy, how the system will perform.

Biometric Recognition – It refers to automated recognition of individuals based on their behavioral and biological characteristics. Automated recognition implies that a machine based system is used for the recognition either for the full process or assisted by a human being. Biometric recognition encompasses biometric verification and identification.

e-Governance applications in India using Biometrics

UIDAI (Aadhar) , NPR (National Population Register) , E- Passport , PDS (Public Distribution System) ,SBY (Rashtriya Swasthya Bima Yojna) ,Transport department for issuing or renewing Driving License, etc.

e-authentication framework for e-Governance

e-Pramaan framework for e-Governance

e-Pramaan provides a guiding framework that enables various government departments and agencies to address the access management, authorization requirements, and authentication mechanism associated with the deployment of e-Governance applications and services..

Objective

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

Components of e-Pramaan Framework

i. Identity Management;
ii. e- Authentication;
iii. Authorization;
iv. Credential Registration; Permission Assignment; Deregistration; and
v. Single Sign-on

e- Authentication Assurance Levels for Internet based applications

There are five levels of web based application ranging from Level 0 to Level 4. Level 0 will not require any form of authentication and will be used for providing public information over the web.

Level 0

This level has 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 level using user name and password. User could provide the capability to self-registration by which can generate a user name and password. After successful enrolment in e-Pramaan the user will receive the password through SMS or by mail.

Level 2

This level user will be able to prove his/her identity using OTP token along with his/her credentials that user name and password or Aadhaar number and demographic information. The user will be required to download and install an OTP Generator from trusted website that is provided by the government or by an authorized agency.

Level 3

This level user would require ro his/her identity through a hardware or software token along with PIN and user name and password through two factor authentication. For this service token would be a digila certificate/digital signature of smart card.

Level 4

This level user will prove his/her identity using two factor authentication which necessarily include biometrics as one of the factors while other factor could be hardware/software token or a username/password. Biometric based verification would be done in accordance with the Aadhaar authentication process.

National e-Authenticaton Framework (NeAF) for e- Governance

The National e-Authentication Framework (NeAF) is a guiding framework for providing a mechanism to the government for electronic authentication and authorizations of the identity of the citizens to a desired level of assurance and confidence. National e-Authentication Framework has been prepared by the National e-Governance Division (NeGD) with Department of Information Technology (DIT). This framework deliver Government services in a seamless and paperless manner to the country through internet. Government of India has conceptualized the National e-Authentication Framework (NeAF) to provide a uniform approach to managing identity authentications of all citizens for the delivery of various public services over internet and mobile platforms. This framework defines the principles of e-Authentication along with its various components such as Identity Management, Authentication, Authorization, Credential Registration, Permission Assignment, Deregistration and Single Sign on. Document proposed architecture of National e-Authentication Gateway leveraging the National Service Delivery Gateway (NSDG), State Service Delivery Gateway (SSDG) and Mobile Service Delivery Gateway (MSDG).

There are five levels of web based applications ranging from Level 0 to Level 4. Level 0 is not require any form of authentication and will be used for providing public information over the web. All applications will authenticate users using Level 1 authentication over the web.

Level 0

This level implies no authentication. User can access all information that is made available for public use from government website.

Level 1

This level user would receive username and password after successful registration which may be done either directly by government or by an authorized agency, the agency may send password using SMS of print mailer. User could provide the capability of self-registration and generate a username and password

by himself/herself.

Level 2

This level user will prove his/her identity using X.509 digital certificate along with his Level 1 credentials that is username and password. User will prove his/her identity using user name password and Question and Answer. This would enable building a trust between the user and the government website.

Level 3

This level user would need to prove his/her identity through a One-Time Token plus username and password that is two factor authentication using digital certificate. The user will be required to download and install an OTP Generator from trusted website

Level 4

This level user would prove his/her identity using biometrics that is two factor authentication, biometric is as the one of the factors while the other factor could either be a soft token (OTP) or a user name/password. This authentication security would be provided to citizen, internal privilege user like department user. Biometric authentication should be done in accordance with biometric authentication mechanism as defined by the Unique Identification Authority of India (UIDAI) that will help to avoid the duplication of citizen information.

e-Government Authentication Framework

The authentication Framework is one of a series developed as part of the Government's commitment, in the Modernizing Government White Paper, to developing a corporate IT strategy for government. this document builds on the Information Age (IAG) security policy as defined in the IAG Security Policy Framework document that sets out the IAG security requirements expressed in the corporate government IT strategy. Government release personal or commercially sensitive information only against reliably verified identity and protect people against misuse of their identities. This framework is concerned with the authentication of citizens and businesses

seeking to access government services electronically. This framework applies to all electronic transactions carried behalf of government where there is a need for authentication. This framework in order to allocate the transaction to an authentication level and require any authentication service provider.

This Framework describes the four authentication levels and government transaction:

Level 0: Informal Transaction

Level 0 authentication is appropriate for IAG transactions where the communications between the parties are of an informal nature. A citizen downloads publicly available information from a government web site. Level 0 is use when no trust is put in the identities claimed by the transacting parties. A client seeking public information from a government web site may access that information anonymously. A citizen e-mails a government department with a request for general information and expects the material to be returned via e-mails a government department with a request for general information and expects the material to be returned via e-mail.

Level 1: Personal Transactions

Level I transactions would generally cover supply of information of a personal but non-sensitive in nature. A citizen orders to government publication over the internet, the impact is inconvenience and possible minor financial loss to the relying party but there is no lasting impact on either party.

Level 2: Transactions with financial or statutory consequential

This level authentication is appropriate for IAG transaction between parties which are of official nature and failure to undertake a transaction may incur a penalty or may involve the communication of information of a commercially or personally sensitive nature. A citizen files an income tax return electronically. The return should not be open to forgery and details of the income tax assessment should not be released to an unauthorized third party.

Level 3: Transaction with substantial financial, statutory or safety consequential

This level is appropriate for IAG transactions between parties which are of official nature and where mistaken identity may have significant financial impact. A citizen is issued a recall notice arising from participation in a health screening programme. Wrongly identifying the recipient could result in unnecessary treatment for one citizen and

an absence of treatment for another.

No specific implementation guidance is applicable to Level 0. Authentication at Level 1 is designed to prevent possible inconvenience to client. Authentication at Level 2 and 3 is designed to prevent consequences of a more serious nature. Face to Face registration is preferred at Level 3.

National e-Authentication Framework

The National e-Authentication Framework (NeAF) is primarily concerned with the electronic authentication of identity. The Australian Government Information Management Office (AGIMO) of the Department of Finance and Deregulation has developed the National Authentication Framework (NeAF) to provide a consistent, whole of government approach to managing identity related risks. The NeAF is advertisement by the Australian Online and Communications Council (OCC) which operates as the peak ministerial forum across Australia on strategic approaches to information and communications technology issues. The scope of NeAF covers two aspects of authentication one is electronic authentication of the identity of individuals and businesses and second is authentication of government websites. The NeAF focuses on electronic authentication of the identity of individuals and businesses including their agents or representatives and electronic authentication of government websites. The NeAF consists of this document and associated guidelines as well as the supporting standards and procedures that provide guidance in their implementation.

The NeAF is the seven step process, the process is iterative should undertaken in the context of the agency's wider information security risk management processes. The NeAF recognizes range of solutions are possible to mitigate and identity related risk. NeAF seven steps are given below:

Determine the business requirements

This step is undertaken the requirement definition of a business and systems project that is seeking to develop online services and identify the services to be provided, information to be accessed and the user community.

Determine the assurance level requirements

This step involves identity related threats and risks to determine an assurance level for a transaction and assessment ot the required e-Authentication assurance level by identifying the severity of the impacts of getting wrong e-Authentication. Assurance level are used to describe the level of importance of getting e-Authentication right and the resultant level of robustness of the required solution.

3 - Select the registration approach

The registration approach will be determined the nature of the assertion to be authenticated and assurance level required. Registration involves verifying the subscriber's identity or attribute to an understood assurance level prior to creating an e-Authentication credential. Three approaches are most commonly used:

Evidence of identity (EoI)

Evidence of identity requires individuals to present a range of documentation ot valedate their claim to identity.

Evidence of relationship (EoR)

Evidence of relationship (EoR) requires individuals to establish an existing relationship with the agency. This approach to registration usually involves the presentation of documentary or knowledge based evidence that relates to the relationship between the subscriber and the relying party.

Select the e-Authentication mechanism

An authentication credential is something tangible controlled by the subscriber that could incorporate one or a combination of attributes:

Something the subscriber knows

Something the subscriber has in their possession

Something the subscriber is

The method of management and usage of the credential over its life time

Select an implementation model

e-Authentication implementation approaches are possible, ranging from agency or application centric approaches to centralized whole government or whole sector schemes. The require agencies to determine the model will fit with the :

Assurance levels determine

Registration approach determined e-Authentication credential and credential management solutions identified this step should also include consideration of the use of intermediating trust-broker services (e.g.VANguard). single identifier linked to the authentication credential to be used for access to all application and agencies. Trust broker verify the service between the credential issuer and the relying party.

Assess the business case and feasibility of the e-Authentication model

This step is involves using ICT business case guide and tools to model costs and benefits to financially justify the implementation of the e-Authentication approach. A three step approach are given below:

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

Review the e-Authentication solution

Once an e-Authentication solution has been selected, it is necessary to validate it . validation should include consideration of whether the selected registration approach and authentication mechanism provide the required e-Authentication assurance level.

CONCLUSION

One of the biggest problems in e-Governance is the security which should necessary the greatest protection to be government information that is protected by the third party attacker or opponents. Due to these problems of accessing the information from the government website or portal is extremely hard to protect the attacker and reduce the problem work is still in the research stage. This proposed work is expected to be significant contribution to e-Governance area which will effectively access the information from the government website or portal.

Reference

1. Vaisla K. S., Pant Durgesh, "Framework of G2C Stragegies for Uttarakhand" ARPN Journal of Science and Technology; Vol.2 No.7,ISSN 2225-7217,August 2012.
2. Ratneshwer and A K Tripathi, "Some Component Generation Approach for E-Governance System", International Journal of Public Information System, Volume 2010,2,pages. 113-147 ,2010.
3. Shefali Nandan, "E-Governance: overcoming obstacles through Effective Human Resources Management Stragegies".
4. Vaisla Kunwar Singh, Pant Dr. Durgesh, "Impact Analysis of Government To Citizen Initiatives of Uttarakhand, India" in International Journal of Research and Reviews in Applied Sciences (IJRRAS), ISSN 2076-734X, PP 486-502, Vol 9 Issue 3,2011.
5. Bhatnagar, Subhash E Government: From Vision to implementation : A practical guide with use studies New Delhi: sage Publication 2004.202p.
6. The E-Government Handbook for Developing Counries-A Project of infoDev and the center for Democreacy and Technology.
7. Nandita Chaudhri and Shefali S Dash "Community Information Centre"
8. Kunwar Singh Vaisla, Manoj Kumar Bisht "SWOT Analysis of e-Initiative in Uttarakhand,"International Journal of Computer Application(0975-8887), Volume 12-No.5,December 2010.
9. Smeer Sachdeva,"White paper on E-Governance Strategy in India", December 2012.
10. Electronic Authentication and OECD Guidance for Electronic Authentication, june 2007,www.oece,org/sti/security- privacy
11. E-authentication: A Fedrated Approach to Identity Management, November 2004.

****