

A Secured e-Governance Enterprise Framework using Aadhaar Based eSign System



Siddhartha Sen, Sunil Karforma, Sripati Mukhopadhyay

Abstract: Over the wide expansion of internet and e-Governance, many services of government are nowadays provided online. In any online services, confidentiality, authentication and non-repudiation are of foremost priority in setting up any e-Governance framework. Strong cryptographic security protocols and framework must be deployed for large scale e-Governance transactions. We have proposed an open source based secured e-Governance enterprise framework, using Aadhaar based eSign system to integrate all available existing e-Governance services from different sources to seamlessly perform secured transactions in very large-scale and cost-effective manner.

Key Words: eSign, e-Governance, Framework, Secured Transaction, Aadhaar, XML

I. INTRODUCTION:

In the decade of e-Governance, most Governments use Information and Communication Technology (ICT), to provide public services to achieve good governance. In providing those services, most of the communications use public communication channel i.e. Internet which is highly susceptible to interceptions by the adversaries [1][2][3]. Different levels of the government already have discrete e-Governance service providing systems which are built on different heterogeneous technology platforms. Conventional legacy transaction systems do not provide any uniform standard mode of communication which can support different technology platform. To provide and integrate all existing e-Governance services for a huge population an enterprise framework should be in place. The enterprise framework should be capable of holding all existing e-Governance systems without making major changes in the existing running systems and also making it scalable to support very large transactions arising from the citizens and government. It should also support to integrate heterogeneous technology platforms [4]. In any G2C services, a transaction is required to fulfill all four levels of security, confidentiality, integrity, authentication and non-repudiation [5]. Data security is the foremost objective of government when any transaction on e-Governance services takes place.

All communication of data should be in encrypted format and digitally signed. Traditional Current scheme of physical verification, document-based identity validation, and issuance of physical dongles does not scale to a billion people. The major cost of the DSC is found to be the verification cost [6].

Thus, the main challenge is to setup a uniform common framework which can support all kinds of different technology platforms of various e-Governance service providers to communicate, integrate and also provide a robust data security in an economically feasible & scalable to a very large number of citizens.

Our proposed framework divides the whole G2C e-Governance transaction system into three levels. First, the citizen who are participating in the system to avail available e-Governance services [7]. Second, the e-Governance Service Providers (eGSP) who are providing the e-Governance services through electronic transaction system. They include all existing transactional system built on different technology platform in a heterogeneous system. Third, a central framework called Secured e-Governance Enterprise Framework (SeGEF) which includes government's online digital signature service and Aadhaar based eKYC system. This proposed framework is holding and integrating the heterogeneous environment of all available existing e-Governance transaction system with an open technology platform and also ensuring secured encrypted data communication. The authentication of citizen and non-repudiation of transactions are made using Aadhaar based eKYC and eSign system. The proposed model is using existing eSign service which is exposing it as stateless service over HTTPS. Usage of XML open data format and HTTPS protocol allows easy adoption and deployment of this service [8]. To support strong end to end security and avoid request tampering and man-in-the-middle attacks, transactions are digitally signed [9]. The usage of HTTPS shall ensure transport layer encryption, while digital signing of XML data shall ensure integrity & authenticity of data.

Contributions. The main contribution of this paper is to conceptualize a comprehensive framework to create general-purpose secured e-Governance transaction platform in large-scale cost-effective manner. The design of our framework is aimed to address the challenges faced in existing available e-Governance platforms [10].

In this paper we intend to achieve information security using cryptography during e-Governance transactions. Section 2 is providing a brief insight of online electronic signature scheme, eSign System. The detail architecture, processes, message-structure of the proposed framework are described in Section 3.

Manuscript published on 30 September 2019

* Correspondence Author

Siddhartha Sen*, Scientist in National Informatics Centre, Ministry of Electronics and Information Technology, Government of India.

Sunil Karforma, head of the Department of Computer Science, University of Burdwan, West Bengal.

Sripati Mukhopadhyay, Professor and head of the Department of Computer Science, University of Burdwan, West Bengal.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

A Secured e-Governance Enterprise Framework using Aadhaar Based eSign System

Conclusions drawn from the entire discussion are mentioned in Section 4. References are listed at the last part of this paper.

II. EFFECTIVE USAGE OF AADHAAR BASED ESIGN SYSTEM:

Individual digital signature requires the individual's identity verification and issuance of USB dongle having private key, secured by a pin. The major cost of the DSC is found to be the verification cost. Registration Authorities are engaged by Certifying Authorities (CA) to carry out the verification of credentials before issuance of DSC. To maintain the compliance of mandated standard of Physical USB Dongle also adds to the cost. Current conventional scheme of issuance of physical dongles after physical verification and document-based identity validation, is not scalable to billion people. UIDAI is already having citizen's KYC information on public database and this provides an alternate to manual verification. The Unique Identification Authority of India (UIDAI) has been established with the objective of providing a Unique Identification Number (Aadhaar Number) to all residents of India [11][12]. The UIDAI also offers an authentication service to authenticate citizen's identity using biometric credentials or OTP sent over mobile or email. As part of the e-KYC process of Aadhaar, the citizens agree to authorize UIDAI to provide their demographic data along with their photograph (electronically signed and encrypted) to service providers. eSign facilitates for any citizen having Aadhaar ID to electronically signing a document using an Online Electronic Signature Service of the Government of India [13][14]. Aadhaar ID is mandatory for availing this service. Electronic Signature is created using authentication of citizen through Aadhaar eKYC service.

In the existing conventional system, any document or transaction is required to be digitally signed to make it compliant to IT Act 2000 [15]. In order to digitally sign, DSC is required.

Digital or Electronic Signature creation:

1. Signer is required to have DSC from a CA licensed by CCA under IT Act 2000.

2. To issue a DSC, the CA is required to have physical verification of identity and address of the signer.

3. In conventional system, the private key used for creating the electronic signature is stored in hardware cryptographic token. This conventional scheme of in-person physical verification of paper document-based identity and then issuance of hardware based cryptographic tokens is not scalable to billion people of the India. For offering fully paperless citizen services, large-scale mass adoption of digital signature is necessary. A simple online service is required to be put in place for everyone to have the ability to digitally sign electronic documents and that has been provided in the eSign System of the Government.

III. PROPOSED SECURED E-GOVERNANCE ENTERPRISE FRAMEWORK (SEGEF) OVERVIEW

The proposed enterprise framework would support huge requirements of billions of people of country like India. This framework is supposed to accommodate all existing e-Governance systems of the country. This framework would work a level above the existing e-Governance systems. All e-Governance Service Providers (eGSP) providing e-Governance services would board themselves on the proposed SeGEF to provide their services in more secured and authenticated way. To ensure strong level of data security during transaction between the government and the citizen, RSA-1024 encryption technique is proposed to be used by eGSP and DSA may be used as signing algorithm for the purpose of authentication and non-repudiation [16].

3.1 Components and Architecture

We first introduce the three main layers of the framework as depicted in Fig.1:

- (1) Citizen (i.e., requester requesting for eGov services),
- (2) eGSP (e-Governance Service Provider who are providing the eGov services), and
- (3) SeGEF (Secured e-Governance Enterprise Framework which is integrating all eGov services securely with existing eSign architecture of government)

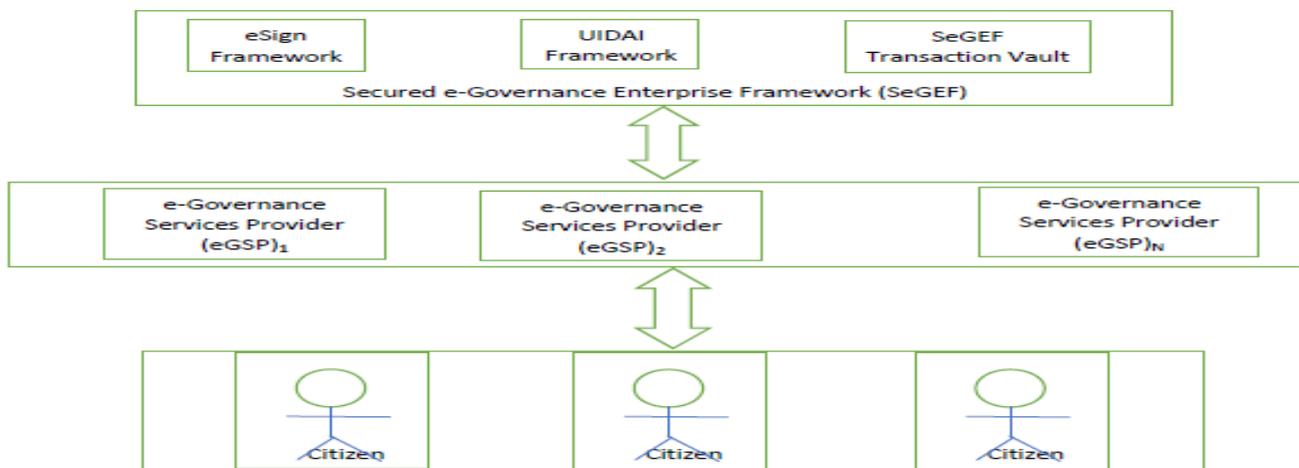


Fig.1 SeGEF : Framework Architecture

Citizen: Citizens are applying for and getting many eGov services of government over the existing eGov service platform. They use various devices like smart phones, tablets, ipads, laptops, desktops etc. After Digital India initiatives of government, many citizens are having mobile phones and even the remote places are at least covered with Community Service Centre (CSC) having internet connectivity.

eGSP: eGSP are e-Governance Service Provider who are providing the e-Governance services provided by the various state governments and local bodies. Generally, eGSP are having service portal on different technology platform with 2-tier, 3-tier or multi-tier architecture. eGSP

are running on different heterogenous platform using different technologies.

SeGEF: Secured e-Governance Enterprise Framework is aimed to integrate all available existing e-Governance services offered by various eGSP to seamlessly perform secured transactions and provide eGov services to the citizens in a very efficient manner to a very large scale and cost-effective way. This uses inter operable open technology over various heterogenous platform. It allows to create a very large repository of verifiable eGov transactions. It uses existing eSign and Aadhaar based system of the central government.

3.2 System Flow Chart

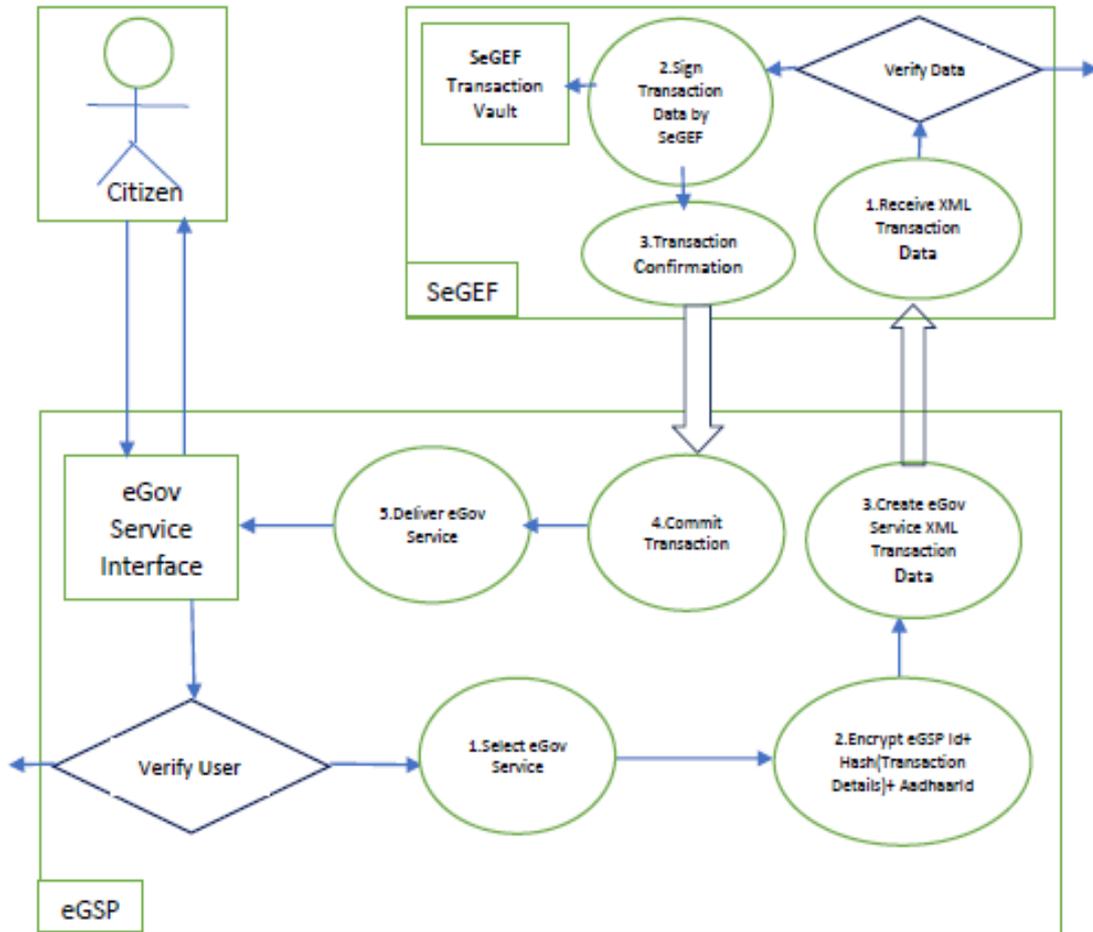


Fig.2 SeGEF: System Flow chart

Algorithm for Registration Process of eGSP :

Step 1. eGSP would register their agency into SeGEF using their Class2 DSC.

Step 2. A session key generated by SeGEF. eGSP would fill up information eGSP_info like Name of eGSP, Address, Postal Zip code, State Name.

Step 3. eGSP would sign (Hash(eGSP_info+session_key)) with their Private Key and submit eGSP_info & signed(Hash(eGSP_info+session_key))

Step 4. SeGEF would verify signature & Hash value and if found ok, sends encrypted Registration Number (eGSP_Id) encrypted by Public Key of the eGSP

Step 5. SeGEF would register the eGSP along with the eGSP_public_key, validity period, eGSP_Id in eGSP_Registration Vault. SeGEF keeps eKYC repository of all registered eGSP.

eGSP_Id	eGSP_public_key	validity	eGSP_name	address	Postal code	State name
---------	-----------------	----------	-----------	---------	-------------	------------

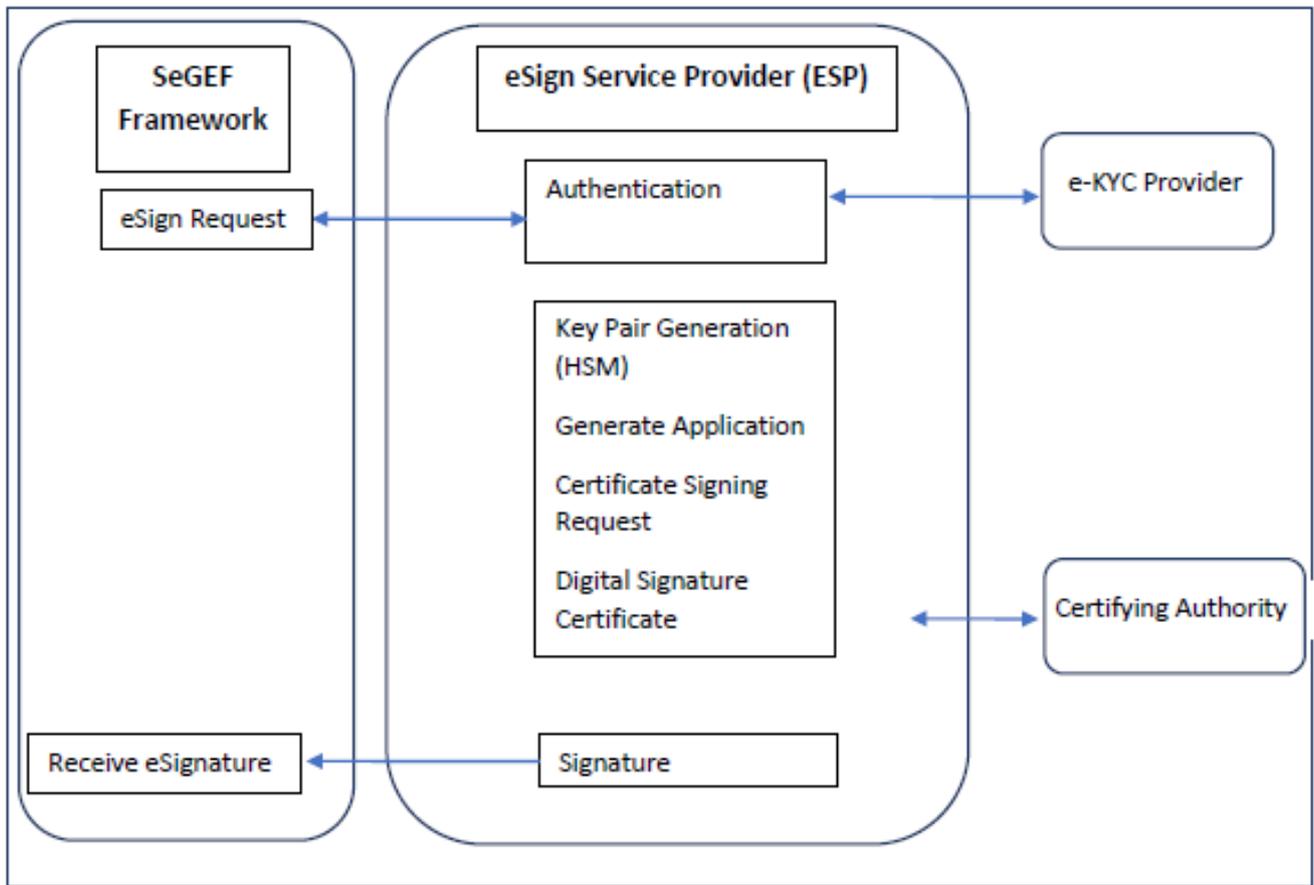


Fig.3 System Interaction for eSign

The Algorithm of Transaction Processing System:

Step 1. Citizen Part: Citizen initiates transaction as shown in Fig.2. Citizen selects the service he/she wants to avail from the service-portal of eGSP service portal.

Step 2. Citizen Part: Inputs required data (transaction_data, Aadhaar Id, timestamp) with reference to the service applying for (ServiceID) and submit request.

Step 3. eGSP Part: eGSP application calculates Hash(eGSP_Id + Service_Id + transaction_data + Aadhaar Id + Unique_Transaction_Reference +Time-stamp). And generates eGSP signature i.e. eGSP signed Hash.

```
Hash_Generator(int eGSP_Id , int Service_Id, String
transaction_data[], int aadhaar_id, int
Unique_Transaction_Reference, datetime Time-stamp) {
transaction_hash=SHA2(eGSP_Id
transaction_data[]+aadhaar_id+
Unique_Transaction_Reference +Timestamp);
return eGSP_transaction_hash[];
}
```

```
eGSP_signing(String eGSP_transaction_hash[], int
eGSP_private_key) {
eGSP_signature=encrypt(transaction_hash[]);
return eGSP_signature[];
}
```

Step 4. eGSP Part: eGSP encrypts with RSA-1024 using the public key of SeGEF prepares XML data and sends to SeGEF.

```
data_encryption (int eGSP_Id , int aadhaar_id, int
Unique_Transaction_Reference, datetime Time-stamp,
eGSP_transaction_hash[], int SeGEF_publicKey) {
```

```
return encrypted_eGSP_message[];
}
```

```
xml_generator(String encrypted_eGSP_message[], String
eGSP_signature[], String return_response_return_url) {
return xml_transaction_data[];
}
```

Step 5. SeGEF Part: SeGEF receives encrypted XML transaction data. It decrypts and verifies signature. If verified true, then only processes otherwise reject.

```
data_decryption (String xml_transaction_data[], String
eGSP_signature[], int SeGEF_privateKey) {
return decrypted_eGSP_message[];
}
```

```
trans_verification (String decrypted_eGSP_message[],
String eGSP_signature[]) {
get_eGSP_Id;
get_String transaction_data[];
get_aadhaar_id;
get_Unique_Transaction_Reference;
get_Time-stamp;
get_eGSP_transaction_hash[];
calculate_transaction_hash=SHA2(eGSP_Id
transaction_data[]+aadhaar_id+
Unique_Transaction_Reference +Timestamp);
get_public_key_eGSP(int eGSP_Id);
dycrypted_eGSP_signature(int eGSP_publicKey, String
eGSP_signature[]);
```

```
if ( (eGSP_Id==registered_eGSP_Id) &&
(eGSP_publicKey==registered_eGSP_publicKey) )
verified_eGSP=true;
```

```

if(calculated_hash==decrypted_eGSP_signature)
return verified_eGSP_transaction=true;
proceed_for_eSign();
else
return verified_eGSP_transaction=false;
reject_transaction();
else
return verified_eGSP_transaction=false;
reject_transaction();
}

```

Step 6. SeGEF Part: eSign Framework sends OTP to Citizen and on verification signs the transaction_data as shown in Fig.3.

```

send_for_esigning(String eGSP_transaction_hash[], int
aadhaar_id) {
get_aadhaar_id();
docID=serialized_doc_id();
docInfo= eGSP_transaction_hash[];
hashAlgorithm=SHA256;
return(aadhaar_id, docID, docInfo, hashAlgorithm)
}

```

Step 7. SeGEF Part: Committed transaction is stored in SeGEF vault and SUCCESS message in XML format is sent to eGSP.

```

segef_trans_commit(boolean esign_status, int
esign_signature_id, String esign_signature_data[]) {
if (esign_status==1) {
generate_SeGEF_Transaction_Reference();
store_to_segef_vault(int aadhaar_id , int eGSP_Id , int
Unique_Transaction_Reference, int
SeGEF_Transaction_Reference, String
eGSP_transaction_hash[], int esign_signature_id, String
esign_signature_data[]);
commit_transaction;
return segef_success_msg=1;
}
else
return segef_success_msg=0;
}
xml_generator(int aadhaar_id , int eGSP_Id , int
Unique_Transaction_Reference, int
SeGEF_Transaction_Reference, String
eGSP_transaction_hash[], int esign_signature_id, String
esign_signature_data[]) {
return xml_transaction_commit_data[];
}

```

Step 8. eGSP Part: eGSP commits transaction and stores transaction details at their level and makes necessary service delivery.

```

eGSP_trans_commit(int aadhaar_id,String
transaction_hash[],boolean segef_success_msg) {
if (segef_success_msg==1) {
store_to_eGSP_database(int aadhaar_id,transaction_data,
transaction_hash[]);
commit_transaction;
}
else
abort_transaction;
}

```

Step 9. Citizen Part: Receives service from eGSP and transaction completes.

3.3 Proposed Structure of message

The data communication in all three levels are made in XML format following standard open source technology platform [12]. This allows all existing e-Governance Service Providers running with different technology platform to communicate seamlessly. XML is platform independent, truly portable data format which can be used by any programming languages. It enables existing heterogenous systems to integrate. The structure of the XML messages at all three levels of SeGEF are mentioned below:

A. Citizen Level

Following are the XML data format for communication between Citizen to eGSP:

```

<Citizen AadhaarId="" service-id="" service-name=""
timestamp="">
<eGSP-Transaction-data id="">
<Attribute-1 attrib-name="" attrib-value="" />
<Attribute-2 attrib-name="" attrib-value="" />
...
<Attribute-n attrib-name="" attrib-value="" />
</eGSP-Transaction-data>
</Citizen>

```

B. eGSP Level

Following are the XML data format for communication between eGSP to SeGEF:

```

<eGSP eGSP_Id="" Aadhaar_Id="" UTR="" timestamp=""
AuthMode="" responseSigType="" responseUrl=""
redirectUrl="">
<eGSP-Message EncryptionAlgorithm=""
HashAlgorithm=""> Encrypted Message from eGSP to
SeGEF
< eGSP-signature>
DSA Digital Signature by eGSP
</eGSP-signature>
</eGSP-Message>
</eGSP>

```

C. SeGEF Level

Following are the XML data format for communication between SeGEF to eGSP:

```

<SeGEF ver="" eGSP_Id="" Aadhaar_Id="" UTR=""
STR="" timestamp="" AuthMode="" responseSigType=""
responseUrl="" redirectUrl="">
<SeGEF-Message EncryptionAlgorithm=""
HashAlgorithm=""> Encrypted Message from SeGEF to
eGSP containing Transaction Hash
< SeGEF-signature>
DSA Digital Signature by SeGEF
</ SeGEF-signature>
</SeGEF-Message>
</SeGEF>

```

Following is the XML data format for Digital Signature of eGSP, SeGEF:

```

<Signature ID>
<SigningAlgorithm="" />
<SignedInfo>
<CanonicalizationMethod />
<SignatureMethod />
(<Reference URI>
(<Transforms>)
<DigestMethod>

```

<DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>
(<KeyInfo>
(<Object ID>
</Signature>

IV. CONCLUSION

The proposed framework is built on XML and Java platform. XML is platform independent, truly portable data format which can be used by any programming languages. It enables existing heterogenous systems to integrate. Java is also platform-independent at both source and binary levels. It has the ability to run same program on many different systems which is crucial for any web platform. eSign system with Aadhaar based eKYC enables all citizens to participate the e-Governance system. eSign is already a proven secured system conforming the latest cryptographic techniques. Citizens are not required to go through the expensive and cumbersome procurement of DSC. They are not required to carry any DSC. These all makes it scalable to billions of citizens of the country. It is easily implementable as it does not require to make major changes in the existing e-Governance ecosystem.

REFERENCES

1. Tri Kuntoro Priyambodo, Uzayisenga Venant, Tatang Irawan and Devi Valentino Waas, "A Comprehensive Review of e-Governance Security".Asian Journal of Information Technology 16(2-5): 282-286,2017
2. "Security of eGovernment Systems", The conference report for the STOA project "Security of e-Government Systems", European Parliament, 2013
3. Zhitian Zhou, Congyang Hu, "Study on the E-government Security Risk Management", International Journal of Computer Science and Network 208 Security, VOL.8 No.5, May 2008, pp.208-213
4. Sun, Ruonan & Gregor, Shirley & Keating, Byron., "Information Technology Platforms: Definition and Research Directions", Australasian Conference on Information Systems, Adelaide, 2015
5. Sattarova Feruza Y. and Prof.Tao-hoon Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security",International Journal of Multimedia and Ubiquitous Engineering, Vol. 2, No. 2, April, 2007, pp. 17-31
6. eSign API Specification version 3.1,2019, CCA, Ministry of Electronics and Information Technology, Government of India
7. A.M. Riad 1, Hazem M. El-Bakry 2 and Gamal H. El-Adl, "E-government Frameworks Survey", International Journal of Computer Science Issues, Vol. 10, Issue 1, No 2, January 2013
8. Malik, K.R., Ahmad, T., Farhan, M. et al., "Big-data: transformation from heterogeneous data to semantically-enriched simplified data", Multimedia Tools and Application (2016) 75: 12727, Springer US.
9. Mauro Conti,Nicola Dragoni and Viktor Lesyk, "A Survey of Man In The Middle Attacks",IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 3, THIRD QUARTER 2016, pp. 2027-2051
10. A.M. Riad, Hazem M. El-Bakry and Gamal H. El-Adl, "E-government Frameworks Survey",IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011, pp. 319-323
11. A cost-benefit analysis of Aadhaar, National Institute of Public Finance and Policy, November 9, 2012
12. Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016
13. The Gazette of India (Extraordinary). No. 59 (PART II—Section 3—Sub-section (i)). 28 January 2015.
14. Government of India, GSR 446(E)-Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2016
15. Information Technology Act, Government of India, 2000 and IT (Amendment) Act 2008
16. Farah Jihan Aufa, Endroyono, Achmad Affandi, "Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm", IEEE Xplore: 15 November 2018, 4th International Conference on Science and Technology (ICST), Yogyakarta, Indonesia

AUTHORS PROFILE



Siddhartha Sen, PGDCA and MBA (Systems & Operations) is working as Scientist in National Informatics Centre, Ministry of Electronics and Information Technology, Government of India. He is working in the field of Information Security, e-Governance and Cryptography for Ph D degree under the supervision of Prof. Sripati Mukhopadhyay.



Sunil Karforma, M.E., Ph D, is holding the post of the head of the Department of Computer Science, University of Burdwan, West Bengal. Network Security, e-Commerce, e-Learning, e-Governance and cryptography are the fields of interest in research area.



Sripati Mukhopadhyay, M Tech., Ph D, is a former Professor and head of the Department of Computer Science, University of Burdwan, West Bengal. He has served in Indian School of Mines, Visva-Bharati University, North Bengal University, Rabindra Bharati University, etc. He has 33 years of teaching and research experience. His research interests include Information Security, Artificial Intelligence & Data Mining.