Object Oriented Approach of Digital Certificate based E-Governance Mechanism

Abhishek Roy[1], Sunil Karforma [2]

[1]. Research Scholar, Dept. of Computer Science, The University of Burdwan, W.B, India
Website https://sites.google.com/site/diaryofaroy
Email: abhishek.roy@aol.in

[2]. Associate Professor, Dept. of Computer Science, The University of Burdwan, W.B, India
Email: dr.sunilkarforma@gmail.com

Abstract: The successful implementation of E-Governance depends on the secured transmission of information between the Citizen and the Government. Intruders are generating smart ways to listen the information un-authentically whereas the information scientists have to find even smarter ways for neutralizing these attempts. Citizens being the digital identities should be able to access various electronic facilities by communicating with the E-Governance mechanism. Digital certificates are the online passport generated by the trusted certificate authorities for authentication of the Citizens. By the incorporation of the object oriented approach, the entire mechanism can be implemented more efficiently. In this paper the authors have described the application of digital certificates through the UML based approach to explain the secured smart card based data transmission in the C2G model of E-Governance.

Keywords: Information Security, Digital Certificate, Authentication, UML.

1 Introduction

The successful implementation of E-Governance depends mainly on the secured transmission of information between the Citizen and the Government using ICT [3]. Intruders are generating smart ways to listen the information un-authentically whereas the information scientists have to find even smarter ways for neutralizing these attempts. Citizens being the digital identities should be able to access various electronic facilities by communicating with the E-Governance [1, 2, 4, 6, 7, 8, 9] mechanism. The industry standard data encryption and decryption techniques, digital signature algorithms [10], digital certificates [11, 12], etc may be deployed for secured mobilization of information in the entire mechanism. Digital certificates are the online passport generated by the trusted certificate authorities for authentication [5] of the Citizens. Moreover, the benefits of object oriented approach [13] will act an value addition to the proposed smart card based C2G type of E-Governance model. Section – 2 contains the relevant literature review in precise form. The UML based proposed model is mentioned in the section – 3. The conclusion drawn is stated in section – 4. The references are cited in the last section.
2 Literature Review

Digital certificate is mainly used to digitally authenticate the identity of its user [14]. In the entire process, the Certificate Authority (CA) has a vital role to play in deployment of secured network for E-Governance system [15]. Also the necessity of proper verification of these digital certificates by the Validation Authority (VA) for its successful implementation in E-Governance mechanism can not be denied under any circumstances [19]. The researchers have also worked on the protocol of issuance of sub-certificates by the Certificate Authority (CA) to the end users connected to Internet [20]. The application of hybrid encryption technology i.e encryption technology, digital digest, digital authentication, digital signature for secure transmission of electronic documents have also evolved as the point of interest for the researchers [21]. Furthermore, the concept of secured self-generated-certificate digital signature have also evolved recently [22]. Specifically the Elliptic Curve Cryptosystem (ECC) based digital certificate have been applied to deal with the limitations of memory size and processing power of multivariant smart card based E-Governance system [16]. The ECC based digital certificate have also been implemented to solve the security related issues between the client operation and the service operation using modified security tech-lab management model and key management protocol [18]. Even advanced research work have also been conducted to provide ratings to these digital certificates [17].

3 Proposed OOM of Smart Card Based E-Governance Mechanism

The schematic diagram of the proposed model is as follows –

![Fig 1](image)

Fig 1. – Schematic diagram of proposed model.

The description of the above mentioned system is as follows – Citizen initiates the E-Governance transaction using Multipurpose Electronic Card (MEC). The Trusted Third Party (TTP) i.e the Certificate Authority (CA) generates the Identity Certificate and the Authorization Certificate using the unique ID of the MEC. MEC connects to the E-Governance mechanism using the ICT. E-Governance mechanism initiates validation procedure for the digital certificates used by the Citizen. In case of
successful validation, the Citizen access the E-Service server and proceeds to successful completion of the E-Governance transaction. Else the Citizen fails to access the services and receives a negative acknowledgement via same route. Class diagram, Use Case diagram and Sequence diagram of the proposed model are –

3.1 Class Diagram

The Class diagram shows the static structure of the proposed model alongwith its important operations –

![Class Diagram](image)

**Fig 2.** – Class diagram of the proposed C2G type of E-Governance model

Class MEC communicates the unique ID of the Citizen to the Class CA. Class CA (i.e Certificate Authority) issue the certificates for the Citizen based on the unique ID received from the Class MEC. Class GOVT validates the certificates of the Citizen with its counterparts. On successful authentication of the certificates, the Citizen is allowed to access the E-Governance services, else the Citizen is barred from its access.

3.2 Use Case Diagram

The role of individual Citizen and the objective of the Government is as follows –

![Use Case Diagram](image)

**Fig 3.** – Use Case diagram of the proposed model.

The text description of the above mentioned use case diagram is as follows –
U1: **INITIATE TRANSACTION** – The Citizen initiates the E-Governance transaction using MEC.

Scenario 1: Mainline sequence.
1 – Citizen initiates the E-Governance transaction using ICT.
2 – ICT communicates with the E-Governance mechanism.
3 – E-Governance mechanism gets ready to accept further inputs from the Citizen.

U2: **PROVIDE IDENTITY CERTIFICATE** – Here the Citizen provides its Identity certificate to the E-Governance mechanism.

Scenario 1: Mainline sequence.
1 – Citizen uses the MEC to produce its identity certificate electronically.
2 – ICT sends the identity certificate to the E-Governance mechanism.

U3: **PROVIDE AUTHORIZATION CERTIFICATE** – Here the Citizen provides its Authorization certificate to the E-Governance mechanism.

Scenario 1: Mainline sequence.
1 – Citizen uses the MEC to produce its authorization certificate electronically.
2 – ICT sends the authorization certificate to the E-Governance mechanism.

U4: **RECEIVE IDENTITY CERTIFICATE** – Here the E-Governance mechanism receives the identity certificate of the Citizen electronically.

U5: **RECEIVE AUTHORIZATION CERTIFICATE** – Here the E-Governance mechanism receives the authorization certificate of the Citizen electronically.

U6: **VALIDATE IDENTITY CERTIFICATE** – Here the E-Governance system validates the identity certificate of the Citizen.

Scenario 1: Mainline sequence.
1 – The system matches the received identity certificate with its counterpart stored in the E-Governance server.

Scenario 2: At step-1 of mainline sequence.
1 – If match is found the transaction proceeds further.

Scenario 3: At step-1 of mainline sequence.
1 – If match is not found the transaction terminates unsuccessfully.
2 – Citizen is notified about the unsuccessful termination of the E-Governance transaction.

U7: **VALIDATE AUTHORIZATION CERTIFICATE** – Here the E-Governance system validates the authorization certificate of the Citizen.

Scenario 1: Mainline sequence.
1 – The system matches the received authorization certificate with its counterpart stored in the E-Governance server.

Scenario 2: At step-1 of mainline sequence.
1 – If match is found the transaction proceeds further.

Scenario 3: At step-1 of mainline sequence.
1 – If match is not found the transaction terminates unsuccessfully.
2 – Citizen is notified about the unsuccessful termination of the E-Governance transaction.

U8: **GRANT FACILITIES** – Here the E-Governance mechanism uses ICT to grant access permission of the electronic facilities to the Citizen.
3.3 Sequence Diagram

Sequence diagram shows the message communication among different actors of proposed E-Governance mechanism with respect to time –

![Sequence Diagram](image)

**Fig 4.** – Sequence diagram of the proposed model.

The detailed description of the above shown sequence diagram is as follows –

1 – Citizen initiates the E-Governance transaction.
   1.1 – Citizen provides its Identity Certificate.
   1.2 – Citizen provides its Authorization Certificate.
2 – Government receives the Identity Certificate used by the Citizen
   2.1 – Government receives the Authorization Certificate used by the Citizen
3 – Government initiates the validation procedure for the received certificates.
   3.1 – In case of successful validation, the Citizen is allowed to access the facilities.
   3.1.1 – Citizen accesses the facilities electronically.
   3.2 – In case of validation failure, the Citizen is not allowed to access the facilities.

4 Conclusion

The Citizen can access various E-Governance services using MEC. Moreover its features can be further enhanced to access other related governmental services. And in the entire process of further up-gradation, the prime focus on the information security in the platform of object oriented software engineering using other tools of Unified Modelling Language (UML) will explore new areas of research work in this sector.
Acknowledgement. The authors express their sincere thanks to the Cryptology Research Society of India (CRSI), especially to Honorable Prof. Bimal Roy, The General Secretary, CRSI and The Director, Indian Statistical Institute (ISI) for providing generous fund support.

References