HOW THE SMRTCARD MAKES THE CERTIFICATION VERIFICATION EASY

[1]L.JAGAJEEVAN RAO, [2]M.VENKATA RAO, [3]T.VIJAYA SARADHI
[1]Assistant Professor, Department of Computer Science and Engineering, KL University, Vaddeswaram, Guntur Dt.
[2] Assistant Professot, Department of Computer Science and Engineering, Vignan's Nirula Institute of Technology, Guntur.
[3]Assistant Professor, Department of Computer Science and Engineering, KL University, Vaddeswaram, Guntur Dt.
E-mail: [1] jeevan@kluniversity.in. [2] venkatmaddumala@gmail.com. [3]saradhi1440@kluniversity.in

ABSTRACT

The main idea of this paper is to create a paperless atmosphere without fraud using the well-used Smart card technology which can not only reduce the effort of maintaining the certificates but also used to create the technological innovation in the Educational field with the help of ongoing trend. In this paper, we first know about the basics of the Smart card and then we deploy those basics to implement our proposed system. To incorporate the existing system in to the proposed system we must follow some phases like Knowing requirements, design, analysis, and implementation. Introducing these Smart cards in to the Educational Field may avoid fraud and miscellaneous certificates. These pocket sized cards will be unique and authenticated for each individual, easy to carry and maintenance free.

Keywords: *Authentication, Smart card Technology, Application protocol data unit (APDU), Public Key Infrastructure (PKI), Certificate Management Protocol (CMP), unique Certificate Identification Number(UCIN)*

1. INTRODUCTION

We daily deal with many documents in professional and personal phases. In routine, dealing with these enormous documents Have you ever thought of how would it be if everything is carried out with a single swipe or click of a card without any papers or documents or certificates?

Most of the things in present day are managed just by one click or one swipe. We are habituated to the ease of living in most secured way by the introduction of different technologies that can help us to improve the quality of life with minimum effort. The idea of bringing the Smart card Technology in to existence is also one of the kinds to reduce the human effort of dealing the day to day issues. Handling the certificates, protecting them from the environmental conditions and also the fraud detection is one of the major issues in the existing Educational system. Introducing the concept of Smart Cards in to Educational certificates management may be one of the keys to the issues concerned.

To achieve the proposed system we need to instrument some strategies like requirements gathering, planning, designing, and implementation. Considering the credit card system as the base for this paper, the main idea is to create a paper free environment. The front end (i.e., the user's view) of the proposed system involves two phases.

1) The Edu-card (i.e., smart card) is inserted into the card reader the information of the user is displayed on the screen of the machine reader, and

2) To view or to access the data the user has to enter the PIN which is unique to every user and is allotted by the concerned authority (i.e., Educational institute). The back end involves some steps similar to the existing technology like processing the card using protocols and specifications.

2. REQUIREMENTS:

2.1 Providing confidentiality of data: It is necessary to assure cardholders that this information is safe and accessible only to the intended recipient. Confidentiality also reduces the risk of fraud by either party to the transaction or by malicious third parties.

2.2 Ensuring the integrity of all transmitted data: That is, ensure that no changes in content occur during transmission of messages.

Providing authentication that a cardholder is a legitimate user: A mechanism that links a cardholder to a specific account number reduces the incidence of fraud and the overall processing

2.3 Safeguarding the use of the best security practices and system design techniques: Via well-tested scheme based on highly secure cryptographic algorithms and protocols.

3. EXISTING SYSTEM

The credit card financial transaction process technology is the base for our certificate verification process. So credit card technology is the existing system.

3.1 The participants involved in the existing system are:

First, we will have an idea on how the credit transaction processing system and conceptual framework for the policies and procedures. The people involved in the credit transaction processing are as follows:

- **A cardholder** is an authorized user of Visa payment cards or other Visa payment products.
- **A merchant** is any business entity that is authorized to accept Visa cards for the payment of goods and services.
- **An acquirer[2]** is a financial institution that contracts with merchants to accept Visa cards for payment of goods and services. An acquirer may also contract with third party processors to provide processing services.
- **A card issuer** is a financial institution that maintains the Visa cardholder relationship. It issues Visa cards and contracts with its cardholders for billing and payment of transactions.
- **A Payment Service Provider (PSP)[7]** can enter into a contract with an acquirer to provide payment services to a sponsored merchant.
- **Visa Inc**. is a publicly-traded corporation that works with financial institutions that issue Visa cards (card issuers) and/or sign merchants to accept Visa cards for payment of goods and services (acquirers). Visa provides card products, promotes the Visa brand, and establishes the rules and regulations governing participation in Visa programs. Visa also operates the world's largest retail electronic payments network to facilitate the flow of transactions between acquirers and card issuers.
- **VisaNet®** is part of Visa's retail electronic payment system[8]. It is a collection of systems that includes:

3.2 Transaction Life Cycle: Processing events and activities may vary for any particular merchant, acquirer, or card issuer, depending on card and transaction type, and the processing system used.

An authorization service through which card issuers can approve or decline individual Visa card transactions.A clearing and settlement service that processes transactions electronically between acquirers and card issuers to ensure that:

- ✓ Visa transaction information moves from acquirers to card issuers for posting to cardholders' accounts.
- ✓ Payment for Visa transactions moves from card issuers to acquirers to be credited to the merchant accounts.
- ✓

The following illustrations show the life cycle of Visa card transactions for both card-present and card-absent purchases.

3.3 Authorization Process for Credit or Debit Transactions:

During the authorization process, Visa card transactions[4] are approved or declined by the issuer or by Visa on the issuer's behalf.

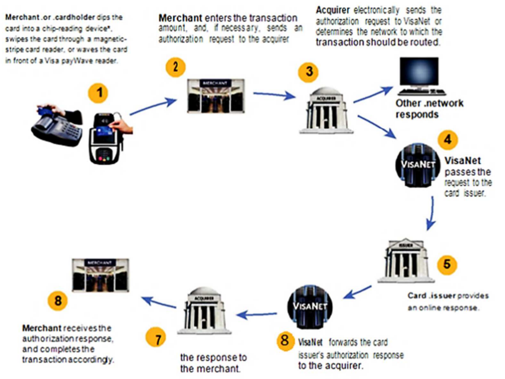
Merchant .or .cardholder dips the card into a chip-reading device*, swipes the card through a magnetic-stripe card reader, or waves the card in front of a Visa payWave reader.
Merchant enters the transaction amount, and, if necessary, sends an authorization request to the acquirer
Acquirer electronically sends the authorization request to VisaNet or determines the network to which the transaction should be routed.
1
2
MERCHANT
3
ACQUIRER
Other .network responds
4
VISANET
VisaNet passes the request to the card issuer.
ISSUER
5
Card .issuer provides an online response.
MERCHANT
8
Merchant receives the authorization response, and completes the transaction accordingly.
7
the response to the merchant.
8
VisaNet forwards the card issuer's authorization response to the acquirer.

Fig-1 Authorization Process For Credit Transactions

3.4 Process of Clearing and Settlement of a Transaction

During the clearing and settlement of a transaction, the transaction information moves from acquirers to card issuers for posting to cardholders' accounts. VisaNet facilitates the payment to the acquirer for a Visa transaction and the debit to the card issuer.

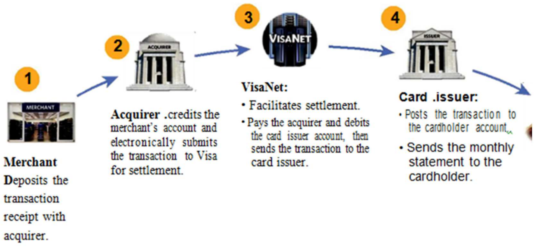
1
MERCHANT
Merchant Deposits the transaction receipt with acquirer.
2
ACQUIRER
Acquirer .credits the merchant's account and electronically submits the transaction to Visa for settlement.
3
VISANET
VisaNet:
• Facilitates settlement.
• Pays the acquirer and debits the card issuer account, then sends the transaction to the card issuer.
4
ISSUER
Card .issuer:
• Posts the transaction to the cardholder account.
• Sends the monthly statement to the cardholder.

Fig-2 Clearing and Settlement of a Transaction

In some cases, POS[3] and ATM transactions are authorized and cleared (posted) at the same time within a single message. This is sometimes referred to as an "online" or "Single-Message System (SMS)"[3] debit transaction. Settlement occurs from single message processing at certain cut-off times during the day. The following diagrams illustrate the basic processing steps for a single message POS (Visa/Interlink) and ATM (Visa/Plus) transaction

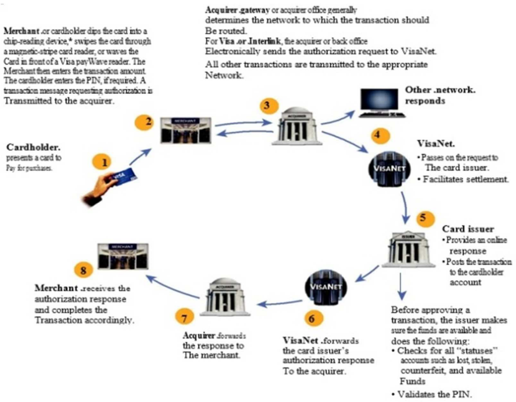
Merchant .or cardholder dips the card into a chip-reading device,* swipes the card through a magnetic-stripe card reader, or waves the Card in front of a Visa payWave reader. The Merchant then enters the transaction amount. The cardholder enters the PIN, if required. A transaction message requesting authorization is Transmitted to the acquirer.
Acquirer .gateway or acquirer office generally determines the network to which the transaction should Be routed.
For Visa .or .Interlink, the acquirer or back office Electronically sends the authorization request to VisaNet.
All other transactions are transmitted to the appropriate Network.
Cardholder. presents a card to Pay for purchases.
1
VISA
2
MERCHANT
3
ACQUIRER
Other .network. responds
4
VISANET
VisaNet.
• Passes on the request to The card issuer.
• Facilitates settlement.
5
ISSUER
Card issuer
• Provides an online response
• Posts the transaction to the cardholder account
Before approving a transaction, the issuer makes sure the funds are available and does the following:
• Checks for all "statuses" accounts such as lost, stolen, counterfeit, and available Funds
• Validates the PIN.
6
VisaNet .forwards the card issuer's authorization response To the acquirer.
7
Acquirer .forwards the response to The merchant.
MERCHANT
8
Merchant .receives the authorization response and completes the Transaction accordingly.

Fig-3 Visa/Interlink Authorization, Clearing And Settlement

Note: Payment Service Provider (PSP) – In some circumstances, a Payment Service Provider (PSP) may transmit the authorization request and response between the merchant and the acquirer. The potential presence of a PSP during the transaction process is dependent on acquirer and merchant payment service contractual agreement with the PSP

1. Merchant or cardholder dips thecard into a chip-reading device, swipes the card through a magnetic-stripe card reader, or waves the card in front of a Visa pay Wave reader.

2. Merchant enters the transaction amount and if necessary sends an authorization request to the acquirer.

3. Acquirer electronically sends the authorization request to VisaNet or determines the network to which the transaction should be routed.

4. Visa Net passes the request to the card issuer

5. Card issuer provides an online response.

6. VisaNet forwards the card issuer authorization response to the acquirer

7. Response to the merchant.

8. Merchant receives the authorization response, and completes the transaction accordingly.

4. PROPOSED SYSTEM

Based on the credit card transaction processing we will implementing the new methodology that will help all the users who are handling the certificates, the employers and the universities who verifies the certificates for different purposes in various fields could use this technique and get the results within fraction of seconds. Usually all employers, universities, and Foreign embassies do face problems with the fake certificates. To overcome these problems Govt., Universities and Organisations are depending upon various methods and approaching detective agencies for certificates authorization and verification. Only for the verification they are investing lakhs of rupees. But still thousands of fake degrees and certificates are being populated in the society. People are depending upon getting these fake certificates for getting job purposes. In our daily life, we experience such kind of news through newspapers, and media. Many talented people losing their opportunities by the fake certificates.

Our proposed technique faces this problem and gives the effective results. Through this technique every student from his Secondary schooling level gets a **unique certification identification number** issued itself by the Secondary board of education, as a Smart card. After completing their secondary education SSC board maintains each student's marks memos with the unique identification in their server database. After the secondary education same students approaching for Intermediate education are also registered with the same unique certificate identification number by the Board of Intermediate education with which they are registered for SSC. The Intermediate board also maintains the student marks memo with that unique certificate identification number in their server database. Likewise, for every higher study students are registered with the same unique certificate identification number and the smart card is credited with all their certificates. Where ever they go they can simply carry the smart card without any of the physical certificates.

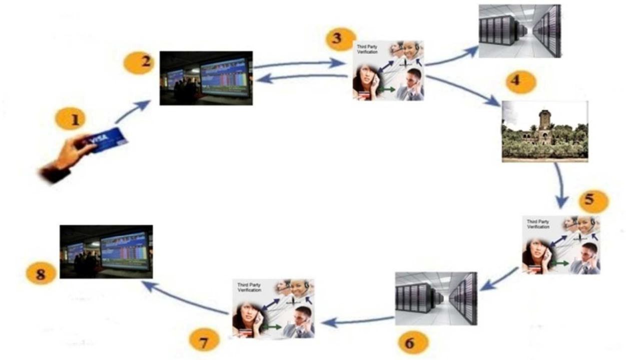

Fig-4 Certification Verification Process By The Smart Card

1. Student or cardholder dips the card into a chip-reading device, swipes the card through a magnetic-stripe card reader, or waves the card in front of a Wave reader.

2. Counselling authority enters the certificates transaction details and if necessary sends an authorization request to the third party verification.

3. Third party verification electronically sends the authorization request to Higher Education server for card Authorization or determines the network to which the transaction should be routed.

4. Higher Education server passes the request to the card issuer(University server)

5. Card issuer(University) provides an online response.

6. Higher Education server forwards the card issuer authorization response to the Third party verification.

7. Response to the Counselling Authority.

8.Counselling Authority receives the authorization response, and completes the transaction accordingly.

For retrieving the data every University, Organisation (Employer) maintains the Smart card readers. When the person approaches them for higher study or job, they swipe their smart card and the data is viewed with Smart card reader. Smart card reader sends a request to the concerned universities and boards which he claimed and through the third party that request is sent to the concerned boards and Universities Servers. These boards and universities check their Server database with the unique certificate identification number and sends response to the third party. The third party sends that Authorization along with the soft copy of the certificate and unique certificate identification number. The employer gets the genuine certification information, authorization without any expenses and delay.

4.1 The Design phase:

The designing phase of the card involves both the hardware and the software design. The Hardware design comprises the manufacturing of the card.

The Manufacturing:

The manufacture of a smart card involves a large number of processes of which the embedding of the chip into the plastic card is the key in achieving an overall quality product. This latter process is usually referred to as card fabrication. The whole operation starts with the application requirements specification. From the requirements individual specifications can be prepared for the chip, card, mask ROM software and the application software. The ROM software is provided to the semiconductor supplier who manufactures the chips. The card fabricator embeds the chip in the plastic card. It is also quite normal for the fabricator to load the application software and personalization data. Security is a fundamental aspect in the manufacture of a smart card and is intrinsic to the total process.

Sample Layout of the card:

State Board Of Education
Name: XXXXX
768 763 399

Fig-5 Sample Layout Of The Smartcard For Certificate Verification

4.2 How it works in different sectors:

Example of using the smart card at Admission process and overall process of the certification verification.

Suppose a student completes his intermediate education and got qualified in the Engineering entrance examination and he is entering in to the counselling centre with educational smart card. The counselling authority first verifies the student certificates with smart card, for which they are already registered with the state or central education ministry, Ministry issues a registered number and smart card swiping machine. Through registration they have the authority to swipe the smart cards and get the information through the third party. The third party is also authorised by the education ministry.The student swipes his smartcard and next the counselling authority gets the student initial information like student name, unique education identification number and how many degrees he is having in his unique education registered account, in a menu listed as follows

1. SSC Marks memo

2. Intermediate Marks memo

The counselling authority selects the certificates displayed on the swiping machine monitors numbers one by one finally press enter button.

The selected certificates request is send to the third party. Third party receives the request, first it verifies the student initial information like UEIN(Unique education identification number), Name, date of Birth, it forwards authorisation request to the Board of secondary education, Board of Intermediate education main servers. These servers response back to the third party initial information authorisation request. Third party forwards that response to the counselling authority. The selected certificates authorisation request forwarded by the third party to the board of secondary education and board of intermediate education servers and send back the student certificates soft copy in digital format to the third party. Along with the authorisation,the information send to the counselling authority.

4.3 Advantages:

1.Security: Smart card technology for certificate verification is secure for the student and university also. Universities can maintain the student certificates data for a long time with security. University server grants the accessing authority to only registered users. Only the persons with the smart card can get the data. There is no alternative to access the certificate information without the smart cards. Smart card is embedded with a memory chip, which gives the minimum information like student unique identification number, student name, and date of birth. Certificates are accessed as digital format so there is no chance to threat or hack the certificate information

2. Easy to access: Only authorised users can access the information by the smart card. Through the third party they will access the information easily. Certificates are viewed in digital format so are easily transferred and clear information is available.

3. Time saving: Users can get the data within a fraction of seconds through the network and decision making is done easily. There is no excess process in enquiry of the certificates, because all the information is verified by the third party and university data administration. The authenticated information is available without time delay.And decision making is easy.

4. Easy to detect the Fraud: Using the smart card system there is no chance for frauds. This technology is mainly concentrated on fraud detection. Certificates are in digital format and authorisation is done multiple times. Only authorised user with smart cars can access the data. Authoritiesalso issued with the registration number through that number only they will get the swiping machine

5. Save money and paper.

4.4 Protocols used in this proposed system are:

- **TCP/IP:** The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite (IP)[1], and is so common that the entire suite is often called TCP/IP. TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet.
- **CMP:** The Certificate Management Protocol (CMP)[1] is an Internet protocol used for obtaining X.509 digital certificates in a public key infrastructure (PKI). It is described in RFC 4210.
- **OCSP:** The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate[1]. It is described in RFC 6960 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI).
- **Transport Layer Security (TLS)** and its predecessor, **Secure Sockets Layer (SSL),** are cryptographic protocols which are designed to provide communication security over the Internet.
- **ISO/IEC 7816** is an international standard related to electronic identification cards with contacts, especially smart cards, managed jointly by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).

- **ISO/IEC 24727** is the first international standard to address the need for creation of a layered framework to support interoperability of smart cards providing identification, authentication, and (digital) signature services

5. CONCLUSIONS AND FUTURE WORK

The intent of this paper is to implant the existing Smart card technology in to the Educational Certificates Management System. With this concept we can eliminate the fraud in Educational certificates by simplifying the work and we can also achieve the maintenance free environment. Another important use of these Edu-cards is that at the time of recruitment process the decision making is made simple and swift. Starting from the Secondary school Certificate (SSC) to the highest possible degree a person's all genuine certificates from the authenticated boards are included in this Edu-cards. All the educational institutes are connected to the concerned university server and the data is updated to the issuer server (i.e., the main server). We can extend the ideology further to the development of Indian educational system.

As the extension of this paper we can start huge project in support for the Indian education system by involving all the educational institutes and their concerned universities by connecting all the servers with the issuer server. Initially, considering the SSC board server as the main server (Issuer of the primary authenticated certificates to the people in educational field) and connecting all the recognized universities and their affiliated organizations with the issuer we can implement the project and all the data is communicated and updated by the concerned servers using the unique numbers allotted to the individuals. These unique numbers are given at the time of registration for the primary examination held by the SSC board. All the protocols used in this execution are same as the existing system.

Finally, deploying the existing technology and making some vital modifications in proposed system can bring a better solution to the present educational system and can be helpful to the people who are struggling to uphold and organize the certificates. The paper free environment is also an additional benefit which supports the GO GREEN concept.

REFERENCES:

[1]. William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, Published on: November 26, 2005.

[2]. Ashutosh Saxena and Aditya Gaiha, "A Framework for Smart Card Payment Systems".

[3].Hamed Taherdoost, Shamsul Sahibuddin & Neda Jalaliyoon "Smart Card Security; Technology and Adoption"

[4]. Saad Ahmed Siddiqi "Smart Card Packaging Process Control System"

[5]. "Smart Card Growth," Cartes 2002. http://www.cartesexpo.com

[6]. Smart Card Tutorial - First Published in September 1992

[7]. http://www.smartcardbasics.com/

[8].http://en.wikipedia.org/wiki/Smart_card

[9].http://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

[10].http://en.wikipedia.org/wiki/Registration_authority

[11].http://people.cs.uchicago.edu/~dinoj/smartcard/security.html