International Journal for Modern Trends in Science and Technology, 7(01): 44-47, 2021

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST070110
Available online at: http://www.ijmtst.com/vol7issue01.html

Over the Air Smart Card Update via Secure Channel Protocol & Universal E-Card

Sankalp Singh Chauhan

B. Tech Scholar, Information Technology Department, Maharaja Agrasen Institute of Technology, New Delhi, India

To Cite this Article
Sankalp Singh Chauhan, "Over the Air Smart Card Update via Secure Channel Protocol & Universal E-Card", *International Journal for Modern Trends in Science and Technology*, Vol. 07, Issue 01, January 2021, pp.- 44-47.

Article Info
Received on 22-November-2020, Revised on 18-December-2020, Accepted on 22-December-2020, Published on 29-December-2020.

ABSTRACT

Smart cards have been used in the industry from a very long time but the recent technological advancements are yet to reach this industry. As we know Modern technologies can easily be updated via internet and any new feature can be added on the go. For smart cards (like bank cards, sim, ID cards etc.) still the traditional approach is used of replacing an existing card and provide a new one or to provide a end of lifetime for the card for issuance of new one. This paper proposes a solution to update the cards on the go, like a software update thereby reducing the hassle for user, saving logistics cost for the issuing authority, increasing longevity of cards and reducing the overall resources used in card manufacture. The paper also discusses how the proposed solution integrates with the existing hardware and modified for any custom needs. The paper further expands the scope to a proposed universal E-Card system wherein a concept of single card for all purposes is introduced.

KEYWORDS: *Smart Card, Secure Channel Protocol, Data Encryption Algorithm*

I. INTRODUCTION

Smart Cards are used everywhere, like bank cards, sim cards today even ID cards are based on Smart Cards with contact pins. The last major change for Smart Card Industry occurred in 1999, after that the industry pretty much remained the same. One problem due to this stagnation of industry is that it is untouched by modern technological developments.

Nowadays, as we all have noticed, pretty much everything is upgradable/replaceable in terms of software. For example if your phone is running an old version of operating system, one can upgrade it to the latest version just by downloading it to device, we do not purchase a new phone every time an upgrade becomes available.

But same is not the case with the cards, they expire and the customer gets issued a new one. Also a card is tied to the issuing bank. In this era of e-sim tech, where an electronic sim is not particularly tied with any operator but can be registered on any available network. This kind of inter-operability gives the user a flexible choice which is not there with the Global Platform Smart Card at the moment, each bank issues their card separately and that too in various flavours.

This raises the following problems:-

- User has to carry cards of multiple banks in their wallet
- In case any malfunction occurs the user has to replace the card with the bank, which is a hassle for user
- Each card has an expiration period of around 3 years after which it is replaced,

which again is a hassle for user and wastage of money and resources for the bank.

The solution proposed eliminates all above problems and introduces a new perspective to Smart Card Industry, A **Single Upgradable Universal E-Card,** which works anywhere, everywhere and can be fixed for any problems via user's mobile through Near Field Communication (NFC) or nearby ATM. Much like a factory reset for a phone. It gives more choices and control to the user to choose his bank without being tied to a single card and it saves the manpower, resources and money for the bank/institution. Since security is a major part in this scenario for the secure communication between the card and the bank server,Secure Channel Protocol is being used, which uses military grade encryption to properly authenticate the card from the bank/institution's side and establishes a secure channel for any updates, which cannot be traced by anyone.

Structure Of Paper

The paper is organized as follows:

Section 1:The introductionalongwith the structure, objectives and overalldescription.

Section 2: Discussion about the existing work that has been done in this field.

Section 3:Discussionabout the methodology, security & processes along with the sequence diagram of the proposed solution.

Section 4:Listing of the notable points of the proposed solution.

Section 5:Lists the resources and limitations of the proposed system.

Section 6:Describes the future scope and concludes the paper with acknowledgement and references.

Objectives

- To eliminate bottlenecks in the current system, by providing a fast and efficient way for adding and upgrading new features in java card applets
- To make the process as seamless as possible for the user by eliminating any physical visits to the card issuing authority
- To increase the longevity of the card thereby reducing the wastage of cards and saving materials and cost for the manufacture of new ones
- To reduce the logistics cost for the card issuing authority

II. Related Works

There are works that has been done in this direction:

Montgomery, Michael, and Ksheerabdhi Krishna in their proceedings "Secure object sharing in Java Card"[1] describes a way to share the objects between the server and the applet in which an approach to object sharing based on delegation is described using challenge/response phrases to avoid revealing the shared secret

The proposed approach takes this one step further to provide sharing via SCP on the internet to provide over the air update to card users.

III. Methodology

The process requires a standard smart card tool like JavaCard Open Platform (JCOP) to compile, build and release card side updates and packages from the issuing institution's end.

That update file is hosted on a server which is then served APDU by APDU (Application Protocol Data Unit) to the client. The client in this case can be implemented on any existing technology that can contact with the card, like NFC, Card Reader or any other tech. **The solution is completely client or server independent.** One can use any server or client as long as communication between the server and card is established.

Process Description

- The client establishes a connection with server.
- The server hosts the update file which is provided by trusted and verified authority.
- A secure channel is established between the server and the card, if security cannot be ensured or the file is not verified the process halts and refuses to continue till a valid channel is established
- The APDU is sent over the channel and waits for acknowledgement.
- The card key is then set and the system is authenticated
- The contents of the cap file is parsed and APDU's are continuously sent over the secure channel.
- If the update fails it restarts from the point of failure till it reaches completion.
- Once completed the client disconnects and the

card becomes ready to use with the upgraded version.

The process description stated is applicable for all valid channels be it NFC, TCP\IP or any other channel

SECURITY OF THE SYSTEM

This is an important part of the solution, as the security in financial matter is of utmost importance and must not fail in any case. For this the channel used here is secured by Secure Channel Protocol.

The solution as such is completely modular and can use any security system, this paper uses SCP for the following reasons.

Secure Channel Protocol provides the following three levels of security[2]:

Mutual authentication

Mutual authentication is achieved through the process of initiating a **Secure Channel** and provides assurance to both; card and host, that they are communicating with an authenticated entity. This process include the creation of new challenges and secure channel session keys. If any step in the mutual authentication process fails, the process shall be restarted, i.e. new challenges and Secure Channel Session keys shall be generated again.

Data Integrity

Data or message integrity is checked by comparing C-MAC received from off-card entity (Host) with the card internally generated C-MAC. Note that this comparison is done using same Secure Channel session key, generated in Mutual authentication step.

Data Confidentiality

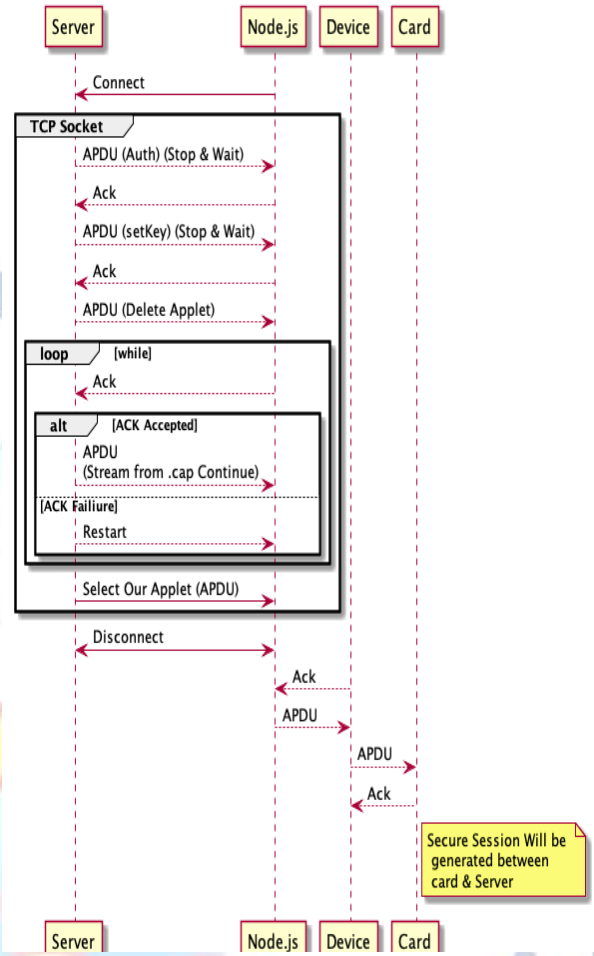
The date received from host to card or card to host is not viewable by an unauthorized entity rather it is encrypted with Secure Channel session key generated during the mutual authentication process.

The next level of security is applied to sensitive data (e.g. secret keys) that shall always be transmitted as confidential data.

The keys are secured via Triple DES which encrypts and decrypts the data in 64 bit chunks the encryption though slower is much more secure than the traditional DES encryption[3]

The encryption is paired with the card serial number and passphrase to produce encrypted text. This key is used for authentication and establishing secure channel between the card and the server.

SEQUENCE DIAGRAM



IV. NOTABLE POINTS FOR THE SOLUTION

- Completely modular solution with simple integration in any existing system.
- Completely backward compatible, can integrate with any existing system
- Provides an on-par security as that of established system
- Independent of Architecture i.e. any Client or Server may be used as long as card and server can communicate
- Uses existing infrastructurewhich is common in Smart Card Industry

V. RESOURCES AND LIMITATION

The solution does not require much resources and uses the existing architecture i.e. any new implementation would not be required to integrate the solution into existing system.

The basic requirements are:

- An IDE that can run JCOP plugin (eg. Eclipse)
- A smart card reader
- A smart card
- Any client that can communicate with card

(can be a NFC mobile or the reader itself)

The first limitation is the security which can be compromised if advanced system comes into existence which can decrypt the full SCP channel, which is highly unlikely in near future.
Next limitation is of latency[4], areas with slow internet or no internet will not be able to get the full benefit. High availability of the server must be ensured to provide this solution globally.

VI. Future Scope

Scope of this solution may be expand nationally & internationally, where a central agency can issue a single Smart card to the user, which they can use to register with different banks and agencies. A single card can be used for multiple applets and each can be updated individually without compromising the security of the other.

Conclusion

This is an unexplored approach in Smart Card Industry and gives a whole new dimension and upgrade systeminexisting technologies by introducing a universal smart card without any restriction with uncompromised security, while maintaining fully backward compatible and modular approach.

Acknowledgement

I expressmy sincere thanks to Mr. Nitesh Wardha of Maharaja Agrasen Institute of Technology to encourage me to the highest peak and to provide me the opportunity to prepare the paper. Last but not least my family is also a source of inspiration for me. So, with due regards I express my gratitude to them.

References

[1] Montgomery, Michael, and Ksheerabdhi Krishna. "Secure object sharing in Java Card." *Proceedings of the USENIX Workshop on Smartcard Technology*, 1999.

[2] Global Platform Card Secure Channel Protocol '11' Card Specification v2.2- Amendment F v1.0: Global Platform Inc, 2015, pp. 16–17.

[3] Alani, Mohammed M. "Neuro-cryptanalysis of des and triple-des." International Conference on Neural Information Processing. Springer, Berlin, Heidelberg, 2012.

[4] B. Rees, Jim, and Peter Honeyman. "Webcard: a Java Card web server." *Smart card research and advanced applications*. Springer, Boston, MA, 2000. 197-207.