International Journal of Pure and Applied Mathematics
Volume 120 No. 5 2018, 803-813
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

LEVERAGE OF CLOUD COMPUTING TECHNIQUE IN THE STANDARD OF IRAQI CARD

Hayder Hussein Azeez, Southren Technical Institue, Thi Qar,Iraq
hayder.hussein@stu.edu.iq

Abstract

Electronic transaction have for quite some time been a typical event, and since they manage such a touchy subject as fund, their security is absolutely critical. The security of electronic exchanges have extraordinarily enhanced with the presentation of the EMV standard and its chip and PIN cards, however these new cards have carried with them new security defects, and now and again continuing the blemishes of their ancestor attractive stripe cards, accordingly making it conceivable to make attractive stripe clones of chip and PIN cards. Moreover, it is likewise conceivable to dupe people with the utilization of assaults, for example, the hand-off and pre-play assaults which make utilization of the vulnerabilities presented by chip and PIN. This paper will propose a more secure other option to current installment cards as the Iraq National ID Card (NID). Notwithstanding depicting the advances behind the NID and EMV, a proposed model will be advanced that will have the capacity to assess the qualification of the NID for use in electronic exchanges.

Keywords: Authentication, Biometrics, Digital Signature, EMV, Identification, NID, Iraq National ID.

1.Introduction

The solid association of innovation with regular day to day existence caused the expanding requirement for eGovernment and its significance comes into see in this day and age. The eGovernment conspire is at a beginning period of improvement. The eNID venture one of the activities began venture under eGovernment of Afghanistan was begun in 2010, and concurring the Iraq Ministry of Communication and Information Technology; eNID task will fill in as one of the real mainstays of eGovernment and scale up the effectiveness of the legislature in giving administrations to subjects, clearing the ground for change in the national, social and regulatory condition by laying the foundation to separate brief, auspicious and applicable data [1]. Quantities

of national and universal in the field specialists are procured through favoring the most qualified candidate and this task is mutually executed by Ministry of Communication and Information Technology and Ministry of Interior. As indicated by UN eGovernment Survey in 2010, Afghanistan positioned 168 out of 192 nations and the most minimal in South Asia [2]. For eGovernment advancement in Afghanistan, diverse assets are under way or proposed to accomplish, for example, building up a system among key services, increment in data transfer capacity ranges from 128kbps to 4Mbps, and web transmission capacity utilized by outside partners extend from 64kbps to 30Mbps in the specialized arrangement, and also and in Human assets and monetary divisions are considered. EGovernment can assume an imperative part to destroy the defilement issue, while it needs specialists and learning to drive the framework.

The key reason for this examination is to have bits of knowledge review of electronic National Identification Documents (eNID) venture including [3] eGovernment and eID card plan, and ePassport from different viewpoints, for example, usage, obstructions, achievements, significance, inspiration, social effects and part of private division as an impassioned supporter. This paper brings up some extensive accomplishments, endeavors, dangers, and obstructions related with eNID (counting eID, ePassport, and different gadgets administrations) application in Afghanistan that draws the essential picture of Afghanistan present day electronic administrations. The eGovernment[4] talk is generally committed on eNID including eID and ePassport issuance in Afghanistan from various angle from activity stage to execution. In addition, the paper will center to show the national and worldwide significance of eNID for administration of Afghanistan at current circumstance. In the continuation of the subject, clarifies the inspiration driving eNID and its social effect [5].

Electronic exchanges have for quite some time been a typical event, and since they manage such a delicate subject as fund, their security is absolutely critical. While EMV and their chip and PIN cards have done much to build the security of these exchanges, their usage isn't immaculate as examined. While not as evident as the security imperfections of its ancestors, the vulnerabilities show in the EMV chip and PIN execution are similarly unsafe, and should be tended to. This paper will propose a conceivable, more secure contrasting option to current installment card usage, the South African National ID Card (NID).[6] With a specific end goal to guarantee that the NID is qualified as a trade for current installment cards, it is important to make a working model that will assess the NID's qualification[7]. The segments that will be incorporated into this paper are: The goals that we have set for our task, the procedure that will be taken after, and an innovation depiction, that will portray every one of the advances that have an imperative influence in our framework, and in addition giving a portrayal on our proposed model [8].

2. Literature Survey

Mir Sayed Shah Danish et al [9] acquainted the paper will center with exhibit the national and worldwide significance of eNID for legislature of Afghanistan at current circumstance. In the

continuation of the subject, clarifies the inspiration driving eNID and its social effect. A piece of this investigation is distributed to investigate the unmistakable quality of private segment to help administration of Afghanistan for productive eNID venture satisfaction, what they do as such far? What part the private division will play later on (in perspective of the current openings and dangers). eGovernment discourse is for the most part devoted on eNID including eID and ePassport issuance in Afghanistan from different viewpoint from activity stage to usage, boundaries, achievements and expectation.

Ramaswamy Chandramouli et al [10] Smart ID cards control physical access to secure offices and sensible access to IT frameworks (Web servers, database servers, and workstations) and applications. Validation of the card and holder happens utilizing an arrangement of qualifications. An association conveying such cards must have a foundation for creating, gathering, putting away, provisioning, and looking after certifications. The parts associated with these qualification life-cycle administration exercises constitute what we'll call the shrewd ID card framework foundation, which underpins brilliant ID card arrangement. Not all segments associated with this foundation have institutionalized interfaces. Additionally, no hearty informing models exist for data trade among the parts. However, a few endeavors are under approach to somewhat address the gauges hole around there.

Plain Pimenta et al [11] presented Federated Identity Management answer for the Web to diminish the security issues and evade the lost of secrecy that may happen when clients trade their specific data inside web settings. We will utilize an accumulation of openly accessible solid ID systems, for example, the clients (Portuguese) National Electronic Citizen Identity Card, and a Federated Identity activity to make the GlobaliD, a Federated Identity Provider to address the already said reflections. Our point with the improvement of GlobaliD is to make a stride facilitate in the computerized personality administration and in this way in the protection and secrecy wellbeing of the clients character Online by making it more adaptable, dependable, reliable, uprightness and security safe, anonym and in this manner secure.

Dongsheng Liu et al [12] presented the outline of a minimal effort low-control ring oscillator-based really arbitrary number generator (TRNG) macrocell, which is appropriate to be incorporated in brilliant cards, is exhibited. The oscillator examining method is misused, and a tetrahedral oscillator with substantial jitter has been utilized to understand the TRNG. Procedures to enhance the factual nature of the ring oscillator based TRNGs' bit successions have been introduced and confirmed by reproduction and estimation. A post digital processor is added to additionally upgrade the haphazardness of the yield bits. Created in the HHNEC 0.13-μm standard CMOS process, the proposed TRNG has a region as low as 0.005 mm2. Fueled by a solitary 1.8-V supply voltage, the TRNG has a power utilization of 40 μW. The bit rate of the TRNG subsequent to post processing is 100 kb/s. The proposed TRNG has been made into an IP and effectively connected in a SD card for encryption application. The proposed TRNG has passed the National Institute of Standards and Technology tests and Diehard tests.

3.Technology Description

We might want to propose the NID as a conceivable option for cards utilized as a part of current electronic exchanges. What takes after will be an exchange of the NID and its capacities. The NID, appeared in Figure 1, is a polycarbonate card that fills in as the substitution for the Iraqbased ID archive and was acquainted to a limited extent with battle the security dangers postured by the paper based ID record. Practically speaking the card will take into account the recognizable proof and confirmation of a cardholder using the cardholder data put away physically and sensibly on the card, and the biometric coordinating of the cardholder's fingerprints to the unique finger impression formats put away on the card separately. As already said, the NID is a polycarbonate card, which manages more noteworthy physical security for the NID and particularly gives the accompanying: The NID is nondelaminable, which implies that it isn't conceivable to disengage any of the layers from the card itself [13], along these lines keeping a person from performing deceitful acts, for example, supplanting the first cardholder's photograph with one of their own picking; promote physical security highlights including yet not constrained to guilloches, windows, small scale content, and inert surface images, which make it hard to deliver a persuading false physical duplicate of the NID.

The NID additionally gives coherent security far beyond its physical insurance, made conceivable with the utilization of its implanted 80kB microchip [14]. This chip stores the cardholder's distinguishing data, for example, their name, their ID photo and their caught fingerprints. The way that the chip holds this data makes it simple to distinguish deceitful physical duplicates of the NID as the right points of interest can be checked by speaking with the chip. As indicated by [15], the NID's chip bolster 2048b RSA cryptography, which is the thing that takes into account the NID's capacity to make computerized marks, and is utilized to secure the private data contained on the card.

Fig 1. Iraq NID

The biometric coordinating of a cardholder's fingerprints is refined through matchon-card (MOC) [16], which is when card itself plays out the assignment of unique mark coordinating. MOC guarantees that the NID's put away unique mark formats never need to leave the card and shields said layouts from being endangered. If a cardholder is physically unfit to give fingerprints e.g. because of inability, the NID takes into account the utilization of a PIN to validate the cardholder. Ultimately, the NID chip contains its own particular PKI declaration, which can be utilized to verify the card as having been issued by the South African Department of Home Affairs (DHA) [17]. By and by, secure recognizable proof and validation are the main abilities of the NID, anyway it is inside the card's capacities to go about as an e-wallet, yet the DHA has picked not to make utilization of this capacity [18]. The following segment will examine electronic exchanges and the procedures that they include keeping in mind the end goal to feature the vital territories in exchanges that can be enhanced with respect to their security[19].

4.Proposed System

So as to assess the appropriateness of the NID for use in electronic exchanges, it is important to make a model framework, alluded to from this point forward as the "framework", that will exhibit its execution in an electronic exchange condition. Moreover, while this model serves just to assess the previously mentioned reasonableness of the NID, it isn't expected for business utilize.

This framework will approach the issue from three essential focuses, to be specific the execution of: card confirmation, cardholder check, and exchange authorisation. The framework when all is said in done will be examined, trailed by and clarification of every one of the essential focuses specified previously.

4.1 General Description

The framework will comprise of numerous parts, each satisfying a particular part in the exchange procedure, these parts are: An occurrence of the NID itself, this will be utilized to give a segment of the card confirmation and cardholder check functionalities of the framework; A POS terminal, which will have a connected unique mark filtering gadget and will go about as the fundamental purpose of association with a client; Lastly, a back end framework, which will house data administrations, for example, a deride up of managing an account data, hazard appraisal criteria, and an exchange authorisation server.

4.2 Card Authentication

As already talked about in this paper, card confirmation is the way toward guaranteeing that a displayed card is the first which was introduced to its approved cardholder. The framework will make us of a mix of the one of a kind PKI testament which is available on the NID, and the cryptographic marking capacities of the NID. At the point when an exchange happens and it is important to validate the NID, the framework will ask for a marked duplicate of its declaration for assessment. Once the NID has gone along, the framework will utilize the NID's open key to unscramble the marked endorsement, and thusly utilize the fitting DHA open key to check the validness of the declaration itself. When this procedure finishes effectively, the NID will have been verified.

4.3 Cardholder Verification

The framework will execute cardholder confirmation, the way toward checking the personality of the cardholder, with the utilization of the biometric MOC usefulness that is offered by the NID. At the point when the cardholder check advance of the framework's exchange procedure is achieved, the framework will ask for that the cardholder filter their unique finger impression with the utilization of a connected unique mark peruser. This caught unique finger impression will then be sent to the NID with a demand to check that the caught finger impression coordinates the NID's put away layout. The NID will then react to the framework with the consequence of the coordinating task, with either an effective or falling flat match result.

4.4 Transaction Authorisation

Exchange approval, as specified already, is a mix of ventures from the EMV standard which likewise considers the aftereffects of card validation and cardholder check.

In this way the framework will also take into consideration the utilization of configurable exchange chance appraisal criteria, which will assess every one of the significant parts of the exchange which is occurring. Also, the framework will utilize the aftereffects of the NID based cardholder check and card validation keeping in mind the end goal to decide if an exchange should finish effectively.

4.5 Intellectual Property Rights Issues Regarding the NID and the Resultant Simulation

The past segment examined our proposed framework which will evaluate the NID's reasonableness for use in electronic exchanges. This segment will depict the issues we have experienced in accessing the functionalities offered by the NID and its card peruser and the resultant requirement for the production of a NID reproduction in their nonattendance.

We have endured a few misfortunes in its endeavors at increasing full access to the abilities of the NID and its related card peruser. We have reached the DHA through anintermediary, LawTrust, and Gemalto, the organization in charge of the card innovation behind the NID, with an end goal to get the fundamental innovation required to interface with the NID through a card peruser, however have been met with clashing records on regardless of whether the South African Government claims the Intellectual Property (IP) rights to their own particular NID. Therefore, it isn't at present conceivable to make a model that uses the NID. In lieu of full access to the NID's capacities, we have regarded it important to make a reproduction of the NID which will offer an indistinguishable usefulness from the NID. This reenactment will incorporate the usefulness gave by two gadgets, the Marx Crypto-Box SC, and the Precise Biometrics Sense X-S.

Every one of these gadgets will be utilized to make a legitimate NID reenactment segment in the framework that will play out every one of the capacities required from the NID. What takes after is a short depiction of every one of the above gadgets and how they will be utilized as a part of the reenactment. While it is as of now important to utilize a reproduction, if the usefulness of the NID ends up accessible over the span of this task, it might be utilized as a part of the model.

4.5.1 Marx Crypto-Box SC

The Marx Crypto-Box SC is a USB gadget which offers on board 128b AES and 2048b RSA cryptography. The Crypto-Box will be utilized to store a private key, speaking to the private key of the NID, and will utilize it to cryptographically sign information for use in card verification.

4.5.2 Precise Sense X-S

The Precise Sense X-S is a mix shrewd card peruser and unique finger impression scanner .This gadget will be utilized to reenact the finger impression coordinating capacities of the NID for use in cardholder check.

5. Conclusions

This paper has presented the EMV standard, the upgrades that its chip and PIN cards have made to the security of electronic exchanges, and the security defects that have been presented through roads, for example, fallback and the blemished executions of the installment cards and their terminals. Furthermore, an exchange has been given on the functionalities of the NID that make it a possibility for an other option to current installment cards in electronic exchanges. In conclusion, the proposed model was talked about, which points of interest how the NID's appropriateness will be evaluated.It is clear that there is a requirement for a more secure contrasting option to current installment frameworks because of the way that they contain noteworthy vulnerabilities as sketched out in this paper, and it is conceivable that the NID will work well for as that option. The NID won't influence the electronic exchanges to process totally secure, however once our model has been executed and tried it will assess regardless of whether the NID stands the opportunity to enhance the security offered in card validation, with the utilization of its declaration and cryptographic capacities, and cardholder check, through its capacity to perform MOC confirmation. The consummation of this task will give a sign of the reasonableness of the NID for use in electronic exchanges, and on the off chance that it ends up being appropriate, this paper prescribes that the subsequent stage to be taken after is to access the full usefulness of the NID, and straightforwardly assessing its appropriateness for use in electronic exchanges.

References

[1] MCIT (Ministry of Communication and Information Technology). (2014, April). Islamic Republic of Afghanistan, eNID Project. [Online]. Available: http://www.mcit.gov.af.

[2] Zamira Dzhusupova, Mohamed Shareef, and Tomasz Janowski, "Developing Electronic Governance in Afghanistan Assessment, Strategy, Implementation, EGovernment Strategy Draft for Afghanistan," United Nations University, International Institute for Software Technology., UNU-IIST Center for Electronic Governance, Policy Report. Rep. 1.0 , 24 Jan. 2011.

[3] Mi Jung Kim, Open Innovation & Collaboration beyond Trade, eNID Project case study:, 25 Sep 2013.

[4] GTR. (2014, April). Grand Technology Resources, eNID Project. [Online]. Available: http://www.gtr.com.my.

[5] Barbara Meserve and Joe deSpautz, "Use of electronic identification (eID) and signatures for integrated operations," International Journal. ISA Trans, vol., no. 32, pp. 215–224, Jan. 1993.

[6] M. T. Naseem et al., "Preprocessing and signal processing techniques on genomic data sequences," Biomed. Res., 2017.

[7] CA. (2007, 10/2009). The bussiness value of Identity Federation. Available: http://www.comnews.com/WhitePaper_Library/Security/pdfs/C Afedbiz_drivers.pdf

[8] M. H. Ali, M. F. Zolkipli, M. A. Mohammed, and M. M. Jaber, "Enhance of extreme learning machine-genetic algorithm hybrid based on intrusion detection system," J. Eng. Appl. Sci., vol. 12, no. 16, 2017.

[9] Mir Sayed Shah Danish, "Insights Overview of Afghanistan Electronic National Identification Documents", 2014 IEEE International Conference on Internet of Things (iThings 2014), Green Computing and Communications,pp251-255,2014.

[10] Ramaswamy Chandramouli, "Infrastructure Standards for Smart ID Card Deployment", Emerging standards, IEEE COMPUTER SOCIETY,pp 92-96,2007.

[11] K. D. Saifuldun Mostafa, Hayder Saad, Mustafa Musa Jaber, Mohammed Hasan Ali, "The Design Trends of Keystream Generator for Stream Cipher for High Immunity Attacks," in Advanced Computer and Communication Engineering Technology, Springer International Publishing, 2016, pp. 877–889.

[12] M. Hassan, A. Fuad, M. A. Mohammed, and M. M. Jaber, "Follow up System for Directorate of Scholarship and Cultural Relations in Iraq," in International Conference on Computer, Communication, and Control Technology, 2014, no. I4ct, pp. 182–187.

[13] Smart Card Alliance. 2013. Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure? Available at: http://www.smartcardalliance.org/resources/pdf/Payments_Roadmap_in_the_US_012413.pdf (Accessed 11 April 2015)

[14] M. K. A. Ghani, and M. M. Jaber, "The Effect of Patient Privacy on Telemedicine Implementation in Developing Countries: Iraq Case Study," Res. J. Appl. Sci. Eng. Technol., vol. 11, no. 11, 2015.

[15] Anderson, R. Murdoch, S.J. 2014. EMV: Why Payment Systems Fail, Communications of the ACM.Available at: http://www.cl.cam.ac.uk/~sjm217/papers/cacm14emv.pdf. (Accessed 15 April 2015)

[16] Mercator Advisory Group, Inc. 2014. EMV Adoption and Its Impact on Fraud Management Worldwide. Available at: http://www.fico.com/en/wp-content/secure_upload/Mercator-for-FICO-EMVwhitepaper.pdf (Accessed 15 April 2015)

[17] Bond, M. Choudary, O. Murdoch, S.J., Skorobogatov, S. Anderson, R. 2012. Chip and Skim: cloningEMV cards with the pre-play attack. Available at: http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf(Accessed 11 April 2015)

[18] M. K. A. Ghani and M. M. Jaber, "Willingness to Adopt Telemedicine in Major Iraqi Hospitals : A Pilot Study," Int. J. Telemed. Appl., vol. 2015, no. 3, pp. 1–7, 2015.

[19]Precise Biometrics. 2014. Precise Sense X-S. Available at: http://precisebiometrics.com/wpcontent/uploads/2014/11/Product-Sheet-Precise-Sense-X-S.pdf (Accessed 03 December 2015)