Journal of Computer Science 6 (7): 723-727, 2010
ISSN 1549-3636


# E-Visas Verification Schemes Based on Public-Key Infrastructure and Identity Based Encryption

Najlaa A. Abuadhmah, Muawya Naser and Azman Samsudin
School of Computer Sciences, University Sains Malaysia,
11800 Penang, Malaysia

**Abstract: Problem statement:** Visa is a very important travelling document, which is an essential need at the point of entry of any country we are visiting. However an important document such as visa is still handled manually which affects the accuracy and efficiency of processing the visa. Work on e-visa is almost unexplored. **Approach:** This study provided a detailed description of a newly proposed e-visa verification system prototyped based on RFID technology. The core technology of the proposed e-visa verification system is based on Identity Based Encryption (IBE) and Public Key Infrastructure (PKI). This research provided comparison between both methods in terms of processing time and application usability. **Results:** The result showed the e-visa verification system is highly flexible when implemented with IBE and on the other hand produces better processing speed when implemented with PKI. **Conclusion:** Therefore, it is believed that the proposed e-visa verification schemes are valuable security protocol for future study on e-visa.

**Key words:** E-visa, Identity Based Encryption (IBE), Public Key Infrastructure (PKI), Radio Frequency Identification (RFID)

## INTRODUCTION

In recent years, new electronic e-passport has started to replace conventional study-based passport around the world. In line with this development, a new protocol for e-visa is proposed in this study that can work hand in hand with current e-passport technology. E-visa is a very promising technology because of its wide range of applications and high security measures that can be implemented with it. The paper-based visa is very easy to clone, especially when it takes the form of an ink stamp. On the other hand, e-visa can hold more information, such as health and criminal records. In terms of legal and privacy issue, e-visa has minimal constraint, since the e-visa is created and used by the same issuing country.

If e-passport is being implemented, e-visa can highly increase the security of the e-passport. In addition, the implementation of e-visa could retain the use of a paper passport if countries choose to do so. As mentioned earlier, the e-visa can be processed easily since the e-visa is being verified by the same country that issued the e-visa. Consequently, countries that wish to delay the implementation of e-passports or e-visas can now easily wait until a time of their choosing without affecting the countries that opt for the e-visa implementation.

In this study the proposed e-visa verification system uses Identity Based Encryption (IBE) or Public Key Infrastructure (PKI), which contains a highly secured mechanism; as such, this technology would pose no inconvenience to any of the parties involved. Lastly, e-visas can also be deployed for other uses, such as criminal detection systems and other related applications involving border-crossings.

**E-visa system:** So far, there has not been much research in the area of e-visa. The few existing researches on e-visa focus mainly on creating e-visa method that can strengthen the development of e-visa system. In the e-visa system, the traditional document of the visa is replaced by an electronic version of the visa, which is a chip embedded in the e-visa that contains personal information and digital biometric data of the e-visa holder. When a traveler comes to the immigration area, he/she has to insert his/her passport into a reader and place himself/herself in a biometric reading device for identification.

After being confirmed as the correct individual, personal information is sent to a central computer server for further verification regarding, e.g., whether

**Corresponding Author:** Azman Samsudin, School of Computer Sciences, University Sains Malaysia, 11800 Penang, Malaysia
Tel: (+604) 6533635 Fax: (+604) 6573335

the person is on a criminal wanted list or whether the person has any liabilities to the government. After the information is validated, the central computer will send a signal to open the gate and let the passenger pass through; otherwise, a signal will be sent to an alarm to alert the security officer. In addition, the RFID based e-visa is considered as contactless technology which allows high speed data transfer of up to 424 Kb per second. The e-visa can be implemented either as a smart label of size 50×50 mm to be attached to the passport or issued in an ISO ID1 card (El-Smart, 2010).

**Data store technology:** The existing infrastructure of each country help in determining the techniques used to transport data. RFID tag and barcode techniques are used to transport information. RFID is a generic term for technology that uses radio waves for automatic identification of entities and individual coffers. RFID technology is the next generation after barcodes in the area of identification technology. The first use of RFID technology was implemented in the 1940s. The British Air Force used RFID technology in World War II to identify whether airplanes were belonged to them. RFID theory was initially introduced by Stockman (1948). Nonetheless, according to Juels (2006), one of the main obstacles in RFID deployment is security attacks, which may threaten to manipulate the RFID technology.

There are important differences between RFID and barcode technologies. Finkenzeller and Waddingtonn, (2003) compared the two technologies in terms of security, machine readability, cost, reading speed, maximum distance between data carrier, read rate and others. For e-visa, contactless chip card technology is seemed to be the optimal solution for providing information of travelers in a reliable manner.

**Security module (IBE and PKI):** In this study, there are two different cryptographic secure modules which are proposed to access e-visa: Identity-Based Encryption (IBE) and Public Key Infrastructure (PKI). IBE is a form of public-key cryptography in which a third-party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting electronic messages. Compared to the typical public-key cryptography, this greatly reduces the complexity of the encryption process for both users and administrators. IBE technology enables us to send encrypted and signed messages without first obtaining key of the receiver.

The first patent for IBE and signature schemes was filed by Shamir (1985). In 2001, an IBE scheme was developed by Boneh and Franklin (2001). An IBE scheme is specified by four algorithms: Setup, Extract, Encrypt and Decrypt. An example of IBE implementation is the work of Liang and Rong (2008). They described how the system can generate keys to the readers and tags and how the readers and tags can use these keys to protect their privacy and authenticate each other.

On the other hand, PKI technology requires us to obtain a public key of the receiver from the key server before sending encrypted and signed message to the receiver. In a real life scenario, public and private keys are generated by the third party, which mean this third party cannot be completely trusted where the third party probably would have a high loyalty for certain country. At the same time, not all countries are in good relation which leads to a big obstacle to the trust mechanism needed by PKI.

## MATERIALS AND METHODS

**System architecture and settings:** This research proposes a verification method to examine the authenticity of the e-visa based on PKI and IBE and identify which technology can satisfy security requirements with better performance at lower cost.

Figure 1 shows the proposed mechanisms in situations in which the RFID chip is used in the inspection system at the issuance stage. Here, the hashed data *R* can be signed by the server private key using the PKI method or signed using a traveler's public identity under IBE. Also R, which is the traveler's visa information, is hashed and stored in the RFID tag.

The same scenario occurs with barcodes if barcodes were to be used in the inspection system. Instead of storing the signed hashed data and the visa identification number in the chip, such information can be stored in two barcodes that are printed on the first page of the visa. The first barcode carries signed hashed data on all visa information and the other barcode bears the visa number identification.

Once the passenger produces his/her passport at the checkpoint, the inspection system scans the RFID tag or the barcodes. Because the inspection system can retrieve the corresponding private key, the inspection system can then decrypt the signed data and compare it with the retrieved data from the RFID tag or the other barcode after hashing. This verification step is illustrated in Fig. 2.

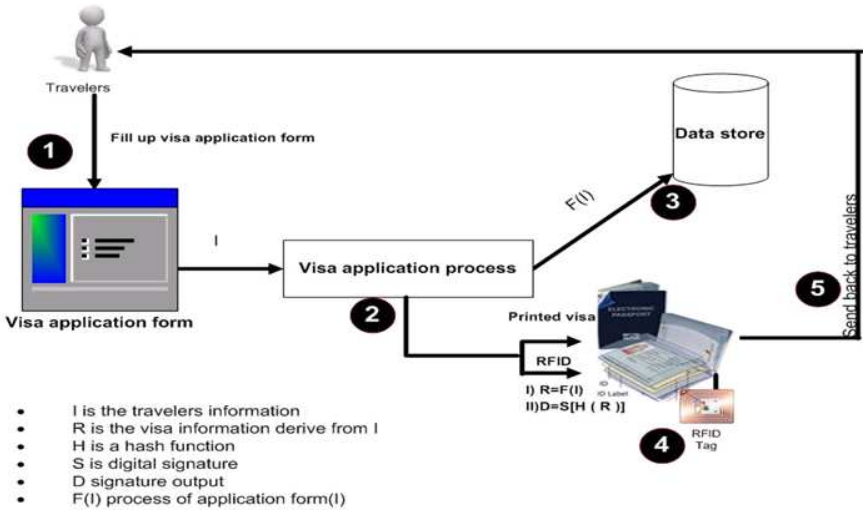


Fig. 1: E-visa registration framework

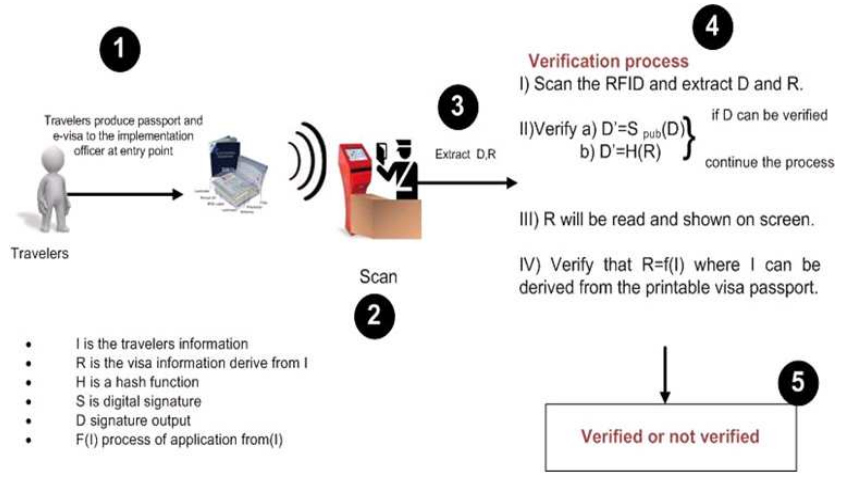


Fig. 2: E-visa verification framework

Note that, ICAO MRTD (Vaudenay and Vuagnoux, 2007), where PKI is used, is excessively complex. The need for cross-certification and maintaining the Certificate Revocation Lists (CRL) exacerbates the situation. The certificate-based PKI scheme of the International Civil Aviation Organization (ICAO) is subject to certain problems, especially regarding the distribution of the public key. The need to manage the private key signing, which corresponds to public key certificates and CRL, also contributes to the complexity of this problem.

This research seeks to avoid these issues by proposing IBE and PKI as mechanisms to overcome the mentioned limitations. The mathematical equation that implements IBE is a special type of function called a "bi-linear map" (Galindo, 2005). It is a pairing that has the following property: Pair (a • X, b • Y) = Pair (b • X, a • Y). The PKI scheme is based on the RSA algorithm (Ron *et al*., 1978; Stallings, 2006).

## RESULTS

**Implementation and result:** We implement a protocol to verify e-visa based on the proposal described in the previous section. The following discussion provides a "proof of concept" by prototyping. In addition, processing time analysis for the new protocol validates the work. Furthermore, comparisons are provided between PKI and IBE in the context of e-visa verification to highlight the strength of each method.

Table 1: Processing time comparison between IBE and PKI implementation of the e-vise registration

| | IBE (μs) | | | PKI (μs) | | |
|---|---|---|---|---|---|---|
| Visa number | Hash generation | Decryption | Total time | Hash generation | Decryption | Total time |
| Visa1 | 102 | 4238134 | 4238236 | 36.0 | 2388 | 2424.0 |
| Visa2 | 99 | 4308582 | 4308681 | 45.0 | 2374 | 2419.0 |
| Visa3 | 85 | 4301828 | 4301913 | 43.0 | 1797 | 1840.0 |
| Visa4 | 87 | 4267821 | 4267908 | 46.0 | 1542 | 1588.0 |
| Visa5 | 80 | 4287367 | 4287447 | 46.0 | 1786 | 1832.0 |
| Visa6 | 76 | 4221295 | 4221371 | 26.0 | 1811 | 1837.0 |
| Visa7 | 77 | 4285046 | 4285123 | 25.0 | 1577 | 1602.0 |
| Visa8 | 82 | 4301535 | 4301617 | 27.0 | 1810 | 1837.0 |
| Visa9 | 67 | 4123165 | 4123232 | 18.0 | 1570 | 1588.0 |
| Visa10 | 51 | 4234709 | 4234760 | 220.0 | 1833 | 1855.0 |
| Average | | | 4257029 | | | 1882.2 |

Table 2: Processing time comparison between IBE and PKI implementation of the e-visa verification

| | IBE (μs) | | | | PKI (μs) | | | |
|---|---|---|---|---|---|---|---|---|
| Visa number | Key generation | Hash generation | Encryption | Total time | Key generation | Hash generation | Encryption | Total time |
| Visa1 | 2680192 | 70 | 5610752 | 8291014 | 29521 | 57 | 231 | 29809.0 |
| Visa2 | 2568807 | 77 | 5546412 | 8115296 | 35526 | 61 | 288 | 35875.0 |
| Visa3 | 2867600 | 69 | 5677198 | 8544867 | 25677 | 49 | 230 | 25956.0 |
| Visa4 | 2326220 | 74 | 5764624 | 8090918 | 41961 | 45 | 243 | 42249.0 |
| Visa5 | 2348492 | 71 | 5558308 | 7906871 | 31854 | 45 | 235 | 32134.0 |
| Visa6 | 372997 | 68 | 5638545 | 8011610 | 35459 | 42 | 216 | 35717.0 |
| Visa7 | 2853996 | 66 | 5730692 | 8584754 | 31326 | 40 | 242 | 31608.0 |
| Visa8 | 2832080 | 54 | 5834411 | 8666545 | 39284 | 46 | 243 | 39573.0 |
| Visa9 | 2529091 | 49 | 5471316 | 8000456 | 33118 | 47 | 264 | 33429.0 |
| Visa10 | 2127278 | 52 | 5451985 | 7579315 | 28249 | 48 | 219 | 28516.0 |
| Average | | | | 8179765 | | | | 33486.6 |

**Processing time:** To demonstrate the validity of our proposed system, the processing times of e-visa registration and verification using IBE are examined. The IBE processing time is compared with the processing times of e-visa registration and verification using PKI. As a sample, we chose 10 e-visas profiles that were randomly created. There is no variance across the visa data because visa data are processed as binary data. Table 1 illustrates the time difference between PKI and IBE in the e-visa verification system. Table 2 illustrates the time difference between the PKI-based and IBE-based visa verification systems.

In the case of all 10 visas we examined, we found that the time spent using PKI was much shorter than that spent using IBE-based implementation. The average time for registration processing under PKI was 1882.2 μs; while the average time under IBE was 4257029 μs (Table 2). The average time for verification processing under PKI was 33486.6 μs, while the average time for IBE implementation was 8179765 μs (Table 1). In addition, the results showed that this value may vary slightly between visas. We believe that the variations shown in the Table 1 and 2 were caused by background processes running on the workstation during the prototype test. However, the fluctuation is not substantial and the proof of concept shown by the prototype still holds.

## DISCUSSION

IBE is a natural choice for managing keys. The IBE encryption keys form the only architecture that meets all six requirements of an effective key management system. First, the IBE encryption key is derived mathematically from the receiver's identity and IBE keys are always available for all recipients. On the other hand, PKI often cannot encrypt data when the recipient's certificate is not available. Second, IBE interfaces with existing authentication infrastructures and so any authentication resources that are already deployed can be reused. Third, IBE enables the sender to select a local key server, a partner's key server, or a service to protect the data, depending on the particular requirements, while PKI must publish a directory externally. Fourth, because IBE mathematically generates all keys at the server, the server can securely regenerate keys for infrastructure components as needed and thus deliver keys to trusted infrastructure components. All keys in an IBE-based system are generated from a base secret stored at the key server

and therefore any key can be securely regenerated, whereas the PKI maintains a key database.

Furthermore, scalability without a need for databases grows over time and/or is required for per-transaction connections to the key server. IBE enables additional applications and transactions to be added with very little, if any, additional key management infrastructure. Key servers can operate independently, allowing for geographic dispersion and load balancing. However, PKI has limited scalability due to operational complexity. In summary, IBE uniquely meets all six requirements of an affective key management system, while PKI fails to fulfill some of these requirements.

**Security discussion:** Many security threats and attacks could flood the e-visa system. In the following, some potential threats to the e-visa system are identified and we discuss how they might be resolved by this proposal.

The interception of the data contained in a passport could lead to fraud, either in its original form or through modifications. The problem of protecting data integrity could be solved by using a hash function for the data. With the secure hash algorithm, once the e-visa is issued, any change to the visa data would be easily detected. Data in the e-visa chip could be subjected to changes by adversaries to ruin e-visas as well as disturb the verification system; by using a hash function, we can ensure that there is no modification in the data because any modification leads to changes in the hash value. Furthermore, signing the data by the private key owned by the issuing authority guarantees data authentication. Note that the e-visa carries two values that are stored in RFID chips, namely, the original data and the signing hash data. This method enables the proposed system to work offline securely. On top of the hashing, e-visa data is encrypted by the private key to prevent modification on the data.

## CONCLUSION

We have proposed e-visa verification schemes that greatly increase the efficiency and security of visa processing. In the propose schemes, the e-visa is issued by the same country, who will later verify the e-visa and therefore, gives minimum legal or privacy issues implication. In addition, the propose e-visa schemes can enhance the security of paper-based passport before a fully workable e-passport program is launched. The research has also sought to avoid the e-passport problem by proposing a high-level security mechanism for e-visa verification that enables the use of IBE and PKI to form a strong security and politically safe system. Based on the performance applicability and security discussion, we found that PKI performs at a higher processing speed than IBE. However IBE provides a better solution in terms of security. Security discussion shows that our protocol is safe against security threats. Moreover, IBE and PKI scheme may exist together, which provides more implementation choices to participating countries.

## REFERENCES

Boneh, D. and M. Franklin, 2001. Identity-based encryption from the Weil pairing. SIAM J. Comput., 32: 213-229. DOI: 10-1007/3-540-44647-8-13.

El-Smart, 2010. E-visa. Electronia. http://www.electronia.com/products/evisa.pdf

Finkenzeller, K. and R. Waddingtonn, 2003. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. 2nd Edn., John Wiley and Sons Inc., ISBN: 0-470-84402-7, pp: 470.

Galindo, D., 2005. Boneh-Franklin Identity Based Encryption Revisited. Springer, ISBN: 978-3-540-27580-0, pp: 791-802.

Juels, A., 2006. RFID Security and privacy: A research survey. IEEE J. Select. Areas Commun., 24: 381-394. DOI: 10.1109/JSAC.2005.861395

Liang, Y. and C. Rong, 2008. RFID System Security Using Identity-Based Cryptography. Springer, ISBN: 978-3-540-69292-8, pp: 482-489.

Ron, R., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 26: 96-99. DOI: 10.1145/357980.358017

Shamir, A., 1985. Identity-Based Cryptosystems and Signature Schemes. Springer, ISBN: 978-3-540-15658-1, pp: 47-53.

Stallings, W., 2006. Cryptography and Network Security: Principles and Practice. 4th Edn., Prentice Hall, ISBN: 0-13-202322-9, pp: 428-430.

Stockman, H., 1948. Communication by means of reflected power. Proceedings of the IRE, Oct. 1948, Citeulike, pp: 1196-1204. http://www.citeulike.org/group/1396/article/169507

Vaudenay, S. and M. Vuagnoux, 2007. About machine-readable travel documents. J. Phys.: Conf. Ser., 77: 1-9. DOI: 10.1088/1742-6596/77/1/012006