THE HONG KONG GOVERNMENT AUTOMATED PASSENGER CLEARANCE SYSTEM (E-CHANNEL)

A Study of Channel Management Strategies

Tak Ming Lam
Hong Kong Polytechnic University, Kowloon, Hong Kong

Keywords: e-Government, e-channel, channel management.

Abstract: This paper studies the operation and IT applications in Hong Kong e-channel, including the network, authentication, and database management, the overall benefits and costs, the evaluation of the IT investment justification, followed by potential problems of e-channel and possible solutions, finally, a comparison will be made between Hong Kong e-channel and US e-channel, with further recommendations, followed by a brief conclusion. E-channel is an Automated Passenger Clearance System which was launched on 16 December 2004, in order to enhance the efficiency of the clearance system.

1 INTRODUCTION

Each terminal is connected to the central management and database server to transfer the in/out record and report any abnormal situation. For data flow, as those in/out records are confidential, a good protection to prevent from leaking information is necessary. Wired connection is the best way as the information can hardly be unauthorized accessed. The Hong Kong Immigration Department also has the authority to use dedicated line to build WAN connecting among different locations. That is, using CAT5 or optical fiber to connect from different passenger control points such as Lo Wu, Lok Ma Chau to the central database server, located in Wai Chai. Apart from that, there is a wireless network (WiFi) connecting to palms of inspectors who monitor the operation of e-channel. As the information transferred through the wireless network is not that confidential, it is justifiable to use it. In fact, WiFi has certain kinds of protections for data transmission.

In terms of the authentication, the most important part of the e-channel, a double identification is implemented, which contains verification of smart ID card and biometric verifying using fingerprint. A Public Key Infrastructure (PKI) is applied in the e-channel system. Both the private key and public key are saved in the smart ID card and the private key is encrypted by user's fingerprint. When obtaining the fingerprint after the user inserting the smart ID card, data of the fingerprint will decode the private key and check whether the pair of private key and the public key is valid, so that it will be able to identify the authentication. The database of Hong Kong Immigration Department is one of the most confidential and important databases in the government. A large amount of in/out records has to be processed every day.

2 BENEFITS

First, the implementation of e-channel can save labor cost. The traditional counter needs one inspector for each counter to monitor people who go through the customs and check their identities. However, in order to help those people who have difficulty in passing through the e-channel, in practice, one inspector is needed to monitor 4 to 5 e-channels. Therefore, the number of inspectors to be employed can be reduced, which helps to save much labor cost.

The second benefit is that immigration inspection with e-channel is more reliable than using the traditional counter. In the traditional counter, the inspector will just check whether the ID card is valid or not, and then check whether the photo on the ID card is similar to the user's face. They seldom check

Ming Lam T. (2008).
THE HONG KONG GOVERNMENT AUTOMATED PASSENGER CLEARANCE SYSTEM (E-CHANNEL) - A Study of Channel Management Strategies.
In *Proceedings of the International Conference on e-Business*, pages 470-472
DOI: 10.5220/0001911104700472

in detail whether the user is the owner of the ID card. The reason is that the validity of your ID card will be checked before you can enter the e-channel, and it will then check your fingerprint to ensure that you are the owner of the ID card. Besides, in the e-channel system, there is an infrared ray scan.

The third main benefit of implementing e-channel is that it can save the space and time for the customs service. Some space is needed for placing the computer, some is for the inspectors to sit and some is left for the corridor. However, the e-channel does not need any computer or inspectors sitting there, but only a corridor for people to go through.

Last but not least, the implementation of e-channel can improve the image of Hong Kong. Since not many countries have adopted similar systems, having the automatic e-channel implemented may give Hong Kong a superior representation as a more internationalized city, so that the image of Hong Kong can be improved.

3 PROBLEMS

The first problem is about the data security. In the traditional ID card, only basic information is provided. However, in order to match the new e-channel system and other new functions of Hong Kong smart ID card, extra information which is more important and confidential has been added it. Thus, private information of citizens may leak out if the key is exposed.

The second problem is concerning about the fingerprint identification used in e-channel. Sometimes, a person may be blocked in the e-channel. The most possible reason is that some people may have problems in their fingerprints

The final problem is the chance of chip damage. Theoretically, the card reader retrieves information by detecting the yellow chip in the ID card. If there are any damages in the chip, the card reader may not read the information properly.

To cope with this problem, Hong Kong government has already provided a cover for the card. Furthermore, a landing contact of the card reader instead of the friction contact is adopted. For card readers of friction contact, the contact part is fixed.

4 COMPARISON

US e-channel is designed for the application of the US e-passport, which was newly introduced. The United States requires that travelers entering the United States under the Visa Waiver Program must have an e-passport if their passports were issued on or after October 26, 2006. According to the relevant information provided on the website of United States Department of State, the US e-passport contains a contact-less integrated circuit, which is a 64 Kbit RFID chip.

Compared to the technology used in Hong Kong smart ID card and the chip reader in e-channel, the application of RFID technology in the US e-channel helps to speed up immigration inspections. However, there are several security concerns about the application of RFID in e-channel, such as skimming the data in e-passport, eavesdropping communications between the chip and reader, tracking user of the e-passport, and cloning the passport chip in order to facilitate identity theft crimes.

Basic Access Control (BAC) is implemented to minimize the risk of skimming and eavesdropping. A pair of secret cryptographic keys is stored in the chip embedded in the e-passport. When the reader attempts to read the information in the chip, it engages in a challenge-response protocol that proves knowledge of the pair of keys and derives a session key. Only if authentication is successful can the RFID reader access the data stored in the chip, so that Basic Access Control reduces the possibility of unauthorized access to the data.

However, the Unique Identifier (UID) can still be communicated with the reader in this process, which could theoretically allow the passport user to be tracked. The United States Department of State uses a Random Unique Identifier (RUID) to prevent the use of UID for tracking. Each time the chip is accessed, the e-passport presents a different UID which is not associated with the UID used in sessions that precede or follow the current session.

Cloning is another security concern that someone may copy the information in one chip and store it in another fake chip. The simplest way to mitigate this action is to verify that the data in the chip match the data presented in the e-passport, by checking the photos and biographical data, etc. Additionally, Public Key Infrastructure (PKI) has been introduced to automatically confirm that the identity of the person presenting the e-passport matches the data stored in the chip and shown on the passport.

Even though there have been many security protections in the application of the US e-passport and e-channel, the technology is still not mature enough. In August 2006, a security researcher Lukas Grunwald demonstrated the cloning of a European Union e-passport at the Black Hat and DEFCON security conferences in Las Vegas. (Martin, 2006) The EU e-passport uses similar RFID technology to the US e-passport. However, Randy Vanderhoof, executive director of the Smart Card Alliance, claimed that the data encoded in the chip is digitally signed and locked by the issuing nation, and could not be altered even if the chip was cloned. (O'Connor, 2006) Besides, these data are only basic information presented on the passport data page, and a digital photo. Even if the chip is cloned, there will not be serious problems except that the photo may be used for other purposes. (Reid, 2006) Nevertheless, people still worry about the security of e-passport and the RFID technology used in e-channel.

As mentioned above, US e-channel adopts the RFID technology so that data in the chip can be accessed about 10 centimeters away from the RFID reader. Using Hong Kong e-channel, people need to insert smart ID card, and the reader will contact the chip to read data. This makes the immigration inspection in Hong Kong slower than that in US. However, since RFID technology has more security problems, protections for the US e-passport and e-channel are more than those in Hong Kong.

In terms of the biometric identification, US e-channel uses face recognition while Hong Kong e-channel uses fingerprint. Comparatively, fingerprint is more accurate according to security experts (Kanellos, 2004).

Last but not least, electronic visa may also be introduced for further convenience. When the visa is stored in the chip in electronic form, it will save time for the Customs officers to check. Costs especially labor cost can be saved. However, it seems not appropriate to introduce electronic visa until security protection technologies become mature enough.

5 CONCLUSIONS

From the above, it is clear that various IT applications in Hong Kong e-channel have brought lots of benefits to citizens and the Hong Kong government. However, problems and concerns still exist. Therefore, Hong Kong government may constantly revise the system and learn from other countries for further improvement. E-channel is only one of the IT applications of Hong Kong smart ID card. More functions, such as public library service, can be performed with the smart ID card. The development of e-government has offered citizens and businesses quicker and more convenient access to government information and public services. There is a future trend to achieve a more accessible, accountable and efficient government for Hong Kong as a leading digital city.

REFERENCES

Corcoran, D. et, al. (1999). *Smart Cards and Biometrics: Your Key to PKI.* Retrieved April 2, 2008 from http://www.linuxjournal.com/article/3013

E-channel (2003). Retrieved March 25, 2008 from Hong Kong Immigration Department http://www.immd.gov.hk/ehtml/20041216.htm

E-government in Hong Kong (2008). Retrieved April 10, 2008 from http://www.info.gov.hk/digital21/e-gov/eng/index.htm

Kanellos.M. (2004). *E-passports to put new face on old documents*. Retrieved March 25, 2008 from http://www.zdnetasia.com/news/hardware/0,39042972,39190596,00.htm

Martin. K. (2006). *U.S. deploys first e-Passport readers.* Retrieved March 25,2008 from http://www.securityfocus.com/brief/315

National Database and Registration Authority. (2005).*Multi-Biometric E-Passport.* Retrieved March 25, 2008 from http://www.nadra.gov.pk/site/410/default.aspx

NXP. (2006).*U.S. State Department Advances NXP Technology for ePassport Program*. Retrieved March 25, 2008 from http://www.nxp.com/news/content/file_1257.html

O'Connor. C. M. (2006). *Industry Group Says E-Passport Clone Poses Little Risk*. Retrieved March 25, 2008 from http://www.rfidjournal.com/article/articleview/2559/1/1/

Reid. D. (2006). *ePassports 'at risk' from cloning.* Retrieved March 25, 2008 from http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/programmes/click_online/6182207.stm

Stone. M. (2003) *E-government Challenges and the Hong Kong Case Study of Smart Identity Card.* Retrieved April 2, 2008 from http://www.info.gov.hk/digital21/e-gov/eng/press/doc/20030716s.pdf

The US Department of State. *The U.S. Electronic Passport Frequently Asked Questions.* Retrieved March 25,2008 from http://travel.state.gov/passport/eppt/eppt_2788.html

http://www.immd.gov.hk/zhtml/docs/facts/SB-c2_2007.pdf