On the security & design of MyKad

This item was submitted to Loughborough University's Institutional Repository by the/an author.


Additional Information:

• This is a conference paper [© IEEE]. It is also available at: http://ieeexplore.ieee.org/ Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

Metadata Record: https://dspace.lboro.ac.uk/2134/5695

Version: Published

Publisher: © IEEE

Please cite the published version.
This item was submitted to Loughborough’s Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
http://creativecommons.org/licenses/by-nc-nd/2.5/
ON THE SECURITY & DESIGN OF MYKAD

Raphael C.-W. Phan, Lawan A. Mohammed
Swinburne Sarawak Institute of Technology,
1st Floor, State Complex,
93576 Kuching, Malaysia.

{rphan, lmohammed}@swinburne.edu.my

ABSTRACT
Within 5 years, all Malaysians are expected to have their ICs, driving licenses, passport and e-cash (ATM) all rolled into one card: MyKad. As one of the Multimedia Super Corridor's (MSC) Multipurpose Smart Card flagships, MyKad will become the most important card that Malaysians carry in their pockets. Therefore, the security of information stored in MyKad should be the emphasis of all parties involved in the design, manufacturing, implementation and applications development of MyKad. In this paper, we discuss the security mechanisms used in MyKad and highlight areas where security analysis should be given the top priority. We also present the rationale for open scrutiny and analysis of MyKad and conclude with some additional recommendations on the security and design of MyKad in the presence of a limited memory capacity.

Keywords
Information security, smart card, MyKad, security analysis, attacks.

1. INTRODUCTION
MyKad, also known as the Government Multi-Purpose Card (GMPC) is one of the flagships of the MSC and will be used as the one card embedded with IC, driving license, passport and e-cash (ATM) information. It is expected that within 5 years' time, all Malaysians would have their own MyKad so MyKad will be the most important card in a Malaysian's pocket in the very near future.

It is therefore vital that the security of all the information stored in MyKad be given the top priority. If any of the information is compromised, this will lead to problems and crime such as frauds, impersonations, and thefts.

In Section 2, we will discuss the basic security requirements that should be available in the smart card. We then proceed to describe in Section 3, how the various security mechanisms in MyKad could meet the security requirements outlined in Section 2. We also highlight in Section 4 areas where security analysis is vital. In Section 5, we present the rationale behind the need for open scrutiny and analysis of MyKad, versus the "security via obscurity" belief. We conclude in Section 6 with some recommendations on MyKad to fully optimize its limited memory capacity.

2. SECURITY REQUIREMENTS
Be it in a physical safe, a PC, an online server or even in smart cards, the information stored in those places should be kept secure and safe from possible threats and attacks from attackers. For the owner and user of the information, the basic security requirements that should exist include:

☐ Confidentiality
Confidentiality means that the information can only be accessed and understood by authorized parties.

☐ Integrity
Integrity means that the information is kept intact. Even if unauthorized modifications are made to the information, such changes should be detectable.

☐ Authentication
Authentication means that you could prove the identity of another party.

☐ Non-repudiation
Non-repudiation means that a party cannot deny in future of having made a certain transaction or sent or produced some specific information.
3. SECURITY MECHANISMS IN MYKAD

In this section, we discuss the various security mechanisms built into MyKad. MyKad has an embedded Public-Key Infrastructure (PKI) that supports security mechanisms such as encryption, message authentication, and digital signatures.

The PKI in MyKad performs encryption and digital signatures by making use of public-key techniques. Such techniques make use of a pair of keys, namely a private key which is kept secret and a public key which is widely broadcast to the public. The two keys are generated such that when one key is used to transform some information into an unintelligible form (encryption), the only way to reverse the process (via decryption) is by using the other key.

For example, if some information is encrypted with the public key, then only the private key can be used to reverse the process. Now, since everyone knows Ali's public key, anyone could use Ali's public key to encrypt some information intended only for Ali's eyes and then send that to him. Since only Ali would know what his private key is, only he would be able to decrypt that. Therefore, encryption with the recipient's public key ensures confidentiality.

Alternatively, if Ali uses his private key to encrypt some information and sends it to Baba. Upon receiving that, if Baba can successfully decrypt it with Ali's public key, then Baba knows for sure that it was really encrypted (or in this case, we would say it was signed) by Ali since only Ali knew his private key would be able to encrypt it in the first place. This concept is called a digital signature and ensures that the information is authentic, meaning that it really came from who it was supposed to come from.

The PKI in MyKad is mostly controlled by the iVEST software which stands for Virtual Environment for Secure Transactions, where the prefix “i” stands for “information”, “internet” or “I” as in the first person reference.

iVEST, developed by the Cryptography Group of MIMOS, enables the MyKad user to experience a wide range of security mechanisms such as those outlined above. When a user is issued a MyKad, he will first go through the following steps:

1. Plug in the MyKad reader to the PC
2. Install the iVEST software on the PC
3. Insert MyKad into the reader
4. Launch a web browser to access either DigiCert’s or MSC
5. Trustgate’s websites

6. Fill up a web registration form
7. Wait for his key pair and corresponding digital certificate to be generated and stored in MyKad
8. Key in an activation password to activate the PKI functions

After this, his MyKad would be ready for action, and his private key as well as his digital certificate containing his personal information and public key would be stored in MyKad.

To perform encryption, iVEST uses the standard techniques such as RSA or the latest Advanced Encryption Standard (AES), both of which have gone through many years of public scrutiny and security analysis and have shown to withstand attacks. Meanwhile, the digital signature technique is based on the popular Public-Key Cryptography Standard number 7 (PKCS#7) whereas online transactions would be protected by the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols, the former being a de facto standard used by many online shops such as Amazon.com, and the latter being a predecessor to the SSL.

It apparent that MyKad has all the makings of an important and secure smart card, with iVEST as its backing.

4. AREAS OF POSSIBLE ATTACKS

Due to the fact that a MyKad is to be issued to all Malaysians, it will be very common place and hence should be able to withstand all sorts of attacks and probes at its interface. In this section, we highlight some areas of possible attacks and stress that extreme caution be put into designing and implementing MyKad components prone to such threats.

4.1 Physical Attacks

MyKad would be owned by every single Malaysian within the next 5 years and thus would be exposed to physical attacks. The situation is similar to leaving your safe deposit box lying right in the middle of the road. It is therefore vital that MyKad be able to withstand conventional as well as the latest physical attacks such as the power analysis [4, 9], fault analysis [2, 4], timing analysis [4, 5] and newer variants like the differential power analysis [4], differential fault analysis [4] and the optical fault induction attack [13].

4.2 Implementation Flaws

Consider the design of a very high-security padlock, with the state-of-the-art technology that not even the strongest nor sharpest of tools could cut through. When it comes to being manufactured, if the specifications are not followed correctly, no matter how good the design was, the final product would have defects and thus be weaker than desired.

The same applies to security mechanisms. Techniques such as the RSA or the AES are strong designs, but if any
mistakes are made in the process of implementing them in either hardware or software, then the final product would not be as strong as conceived by the designer. Hence, implementations of security mechanisms in MyKad should be thoroughly checked for bugs or flaws.

4.3 Protocol Weaknesses
A protocol is a set of rules that define how you do something when communicating between parties. Since MyKad would be required to communicate with smart card readers, PCs, servers, websites, government officers and the like, each instance of the communication need to follow a certain protocol. For example, what protocol should be used to authenticate MyKad against a website? These authentication protocols and other security-related protocols are at times the target of attacks. The most common of such attacks are replay attacks [1, 3, 6, 7, 14], impersonation attacks [14], interleaving attacks [14], reflection attacks [14], deflection attacks [14] and multiplicity attacks [8]. Again, the protocols used in MyKad should go through comprehensive analysis to show resistance against these attacks.

5. THE NEED FOR PUBLIC SCRUTINY
The current norm in information security is to base the security of a protection mechanism purely on some secret information known as the key, and not on the fact that the security mechanism is kept secret and obscure. Security via obscurity would not work at all [11] since for a mechanism to be useful, it would have to be implemented, but once implemented, it would be prone to various reverse engineering techniques that would easily uncover the details of how the security mechanism works.

Sadly enough, some security providers still hold strong to the belief of security via obscurity partly because they feel safer knowing that their security mechanisms are unknown, and partly because most of their mechanisms are home-made and have not gone through much security analysis by the public and research community. It is often that such mechanisms are proven to be insecure [11].

6. RECOMMENDATIONS
Besides the need for a more open approach to the security analysis of MyKad, we also give the following recommendations related to the security and design of MyKad with respect to its limited memory capacity:

- **Multiple Memory Chips**
  As the demand for MyKad is to perform multi-applications, the standard memory of 32 or 64 KBytes can prove a serious limitation. A solution to this is to look at incorporating multiple memory chips (twin or even triple chips) in a single MyKad.

- **Alternative Memory Technologies**
  Some researchers believe that the EEPROM used in current smart cards (or in our case MyKad) is reaching its scalability limits, particularly for smart card devices built using 0.13-micron technology and beyond. An alternative such as the use of magnetic RAM instead of EEPROM could be a better option. Currently some companies like Philips [15] are leaning towards this technology.

- **Memory Optimization**
  Since most of MyKad's memory will be used to store keys, cryptographic certificates etc. this indicates that only applications that require a minimal amount of memory can be fully implemented. It is therefore vital to do a more thorough investigation of suitable means (such as data compression techniques) to manage and optimize the remaining available memory.

- **Alternative Security Technologies**
  Another important security issue that will help in managing the limited memory is the use of Elliptic Curve Cryptosystems (ECC) instead of RSA. For instance, to achieve reasonable security, RSA should employ a 1024-bit modulus, while a 160-bit modulus is sufficient for ECC. The smaller key size means that signatures and certificates would be smaller and since less data would then need to be transmitted between the card and the terminal, the communication time would be reduced as well.

- **Embedding Photographs & Establishing a Standard for Smart Card Image Formats**
  Since MyKad will be used as a Malaysian passport, this implies that the cardholder's photograph must be physically attached to the card (as is currently being done) or stored in a server database for checking at the immigration. In any case, the system should not rely on storing the photos in the database alone. We recommend instead that the photos be also stored in MyKad itself. However, this may not be easy considering its limited memory capacity, hence it would be worthwhile to work on obtaining a set of smart card image standards to include details such as image formats, forms of storage and modes of compression.
7. CONCLUSIONS
We have discussed the security mechanisms used in MyKad. We have also outlined various MyKad-related areas that could be vulnerable to attacks and suggested that extra care be put to designing and implementing the MyKad components prone to these attacks. We also put forth the rationale for public scrutiny and analysis of the security mechanisms used in MyKad since the strength of a fort yet to be attacked by enemy troops remains just a question mark. It is only when the fort has been attacked numerous times and yet remains standing, would it be known far and wide as a really be an unquestionably strong fort. With adequate security analysis, we believe MyKad would be such a fort. We also included some recommendations for consideration in the future design and analysis of MyKad to fully optimize its limited memory capacity.

8. REFERENCES
[10] Ng, K. S. Details of MyKad and iVEST. iVEST Product Development Manager, MIMOS. Personal communication. (2003).