Research Article

Efficiency Comparison of Cryptographic Applications, Match-off-Card vs. Match-on-Card, Using National Biometric eID Card

Gazmend Krasniqi

University of Vlora "Ismail Qemali",
Faculty of Technical Sciences, Vlora, Albania
Corresponding Author

Kristaq Filipi

Polytechnic University of Tirana,
Tirana, Albania

Doi: 10.2478/ajis-2019-0008

Abstract

Recently, not only the Internet and mobile devices are changing our daily life but also the usage of national biometric card for every government electronic services. Beside citizen authentication these electronic services require users to encrypt and digitally sign their data or documents. Therefore, biometric cards are used as processing devices for cryptographic applications, whereby there are a lot of security aspects required for secure communication, authentication and encryption among them. Those aspects will be tested in different environments, platforms, devices, PCs, mobile devices and smartcards. This paper compares those two processing systems, Match off Card vs. Match on Card, and their efficiency of encryption and signatures on the data used. How different parameters, time and size of test vectors impacts the process and the role they play on the overall system. The derived results will serve us as a guide for using one processing system in certain environment, minding the efficiency of the data.

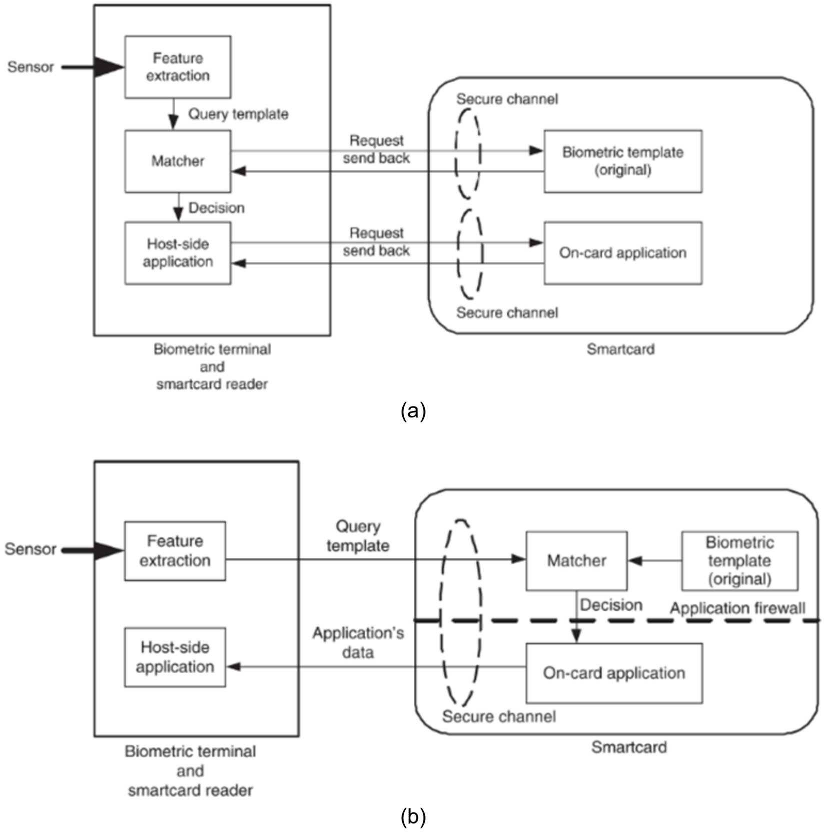
Keywords: *eID biometric card, encryption, Match off Card, Match on Card*

1. Introduction

The basic security protocols can be performed using biometrics today. Encryption, digital signature and authentication are essential security protocols used on the Internet. Biometrics takes those protocols in different levels, because they are based on biometric traits. Those traits are universal and unique, implemented in biometric cards or electronic identification card (eID).

Biometric eID cards have public and private parameters, which are used to perform authentication, encryption and data signature. Those parameters are stored on the card during the enrolment stage, as biometric template.

Two processing systems, used to perform the security protocols motioned before, are Match off Card and Match on Card. Match off Card processing is not done on the card, but on a device or system, whereas Match on Card compares the template of the card with the fresh template. The processing of biometric data in match on card is done on the card and never leaves the card, for security purposes. In Figure 1 are presented Match off Card and Match on Card processing systems.



(a)

(b)

Figure 1. (a) Match off Card, (b) Match on Card (Pang, Yun, & Xudong, 2009)

Each processing system has its own advantages and disadvantages. Match off Card has processing power from the system, meaning it is faster, but presents a security risk for the sensitive information inside the card, because the biometric template leaves the card. On the other hand, Match on Card has higher security because the biometric template doesn't leave the card, lower computation power and lack of interoperability is a problem in this processing system (Smart Payment Association, 2013). A general introduction on the Match on Card can be found on (Pang, Yun, & Xudong, 2009), where the main advantages of this processing system are discussed, like decentralized database, data mobility, enhanced privacy and security (Smart Card Alliance, 2011).

The encryption processed with biometric card was proposed in (Bringer, Chabanne, Pointcheval, & Zimmer, 2008). The encryption is done using the biometric key, a unique key generated from the biometric template inside the card. Except for the encryption process, this key can be used for matching and authentication process also (Bringer, Chabanne, Pointcheval, & Zimmer, 2008).

National Institute of Standards and Technology (NIST) has done an evaluation of the accuracy and speed of fingerprint Match on Card process. Minimum error rate, the speed of execution and the accuracy were only few of the parameters tested in this experiment and discussed in an extended report (Grother, Salamon, Watson, Indovina, & Flanagan, 2009). NIST has done other similar interesting experiments, among them an experiment to determine if biometric Match on Card authentication could be performed faster than 2.5 seconds. In the report, the main parameters measured are average time to establish secure session, average time for transmission of encrypted biometric data and average total time to perform this complete process (Cooper, Dang, Lee, MacGregor, & Mehta, 2007).

An interesting experiment is presented in (Vibert, Ninassi, & Rosenberger, 2013). In this paper, performance of enrollment and false acceptance rate of the verification process are analyzed, focusing on the time of successful and failed authentication. The experiments are done using fingerprint authentication in Match on Card processing system. The positive verification time is slower than the negative verification time, which is a security issue, giving a hint to a potential attacker.

This paper takes a different approach than the papers mentioned above. This paper doesn't involve the enrolment stage, verification of biometric card or authentication of the user. This paper uses the biometric template, already burned on the smartcard, for the encryption and data signature protocols. The parameter tested in this paper is the efficiency of two processing system, Match on Card against Match off Card. The file size, processing algorithms for encryption or signature are parameters, each plays a significant role in the whole process, regarding the efficiency of the protocol, presented in this paper.

2. Biometric Identity Cards

A biometric identity card (ID) contains personal and biometric information about its holder in printed form as well as in electronic format. The main purpose is used to authenticate its user in real worlds, as well in Internet.

Those ID card uses proven smart card technology to communicate to outside world. The guidelines for this technology are issued by the International Civil Aviation Organization (ICAO), a body run by the United Nations with a mandate for setting international travel document standards (ICAO, 2018).

Such electronic eID card contains a digital X.509 certificate and its corresponding private key, stored as a user profile, is in compliance with ICAO Public Key Infrastructure (PKI), signed by certification authority of the country issuing the card.

The first national biometric ID has issued cards in December 2013, from the Ministry of Internal Affairs of Government of Kosovo, becoming the first country supporting the new Supplemental Access Control (SAC) protocol for mutual authentication (Rexha, Imeraj, & Shabani, Using efficient TRNGs for PSEUDO profile in national eID card, 2018).

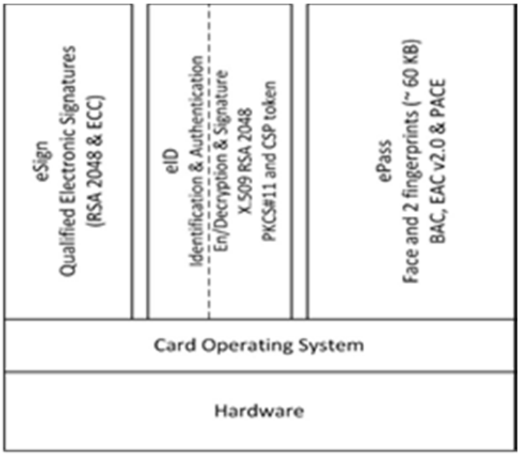

eSign
Qualified Electronic Signatures
(RSA 2048 & ECC)
eID
Identification & Authentication
En/Decryption & Signature
X.509 RSA 2048
PKCS#11 and CSP token
ePass
Face and 2 fingerprints (~ 60 KB)
BAC, EAC v2.0 & PACE
Card Operating System
Hardware

Figure 2. The architecture of national biometric ID card and hosted apps

Figure 2 presents the architecture and the hosted applications. The specifications of the national card are as following: 128 Kbyte EEPROM and uses SLE 78CLX1280P 16-bit crypto processor from Infineon. It supports RSA 4096 key bit length, ECC up to 521 bits and 3DES and AES up to 256-bit length. The communication with outside world is done using the Near Field Communication (NFC) protocol (Infineon, 2013).

The card middleware uses the Public Key Cryptographic Standard (PKCS) #11 and Crypto Service Provider (CSP) to communicate with cryptographic apps. The X.509 certificates is used to authenticate the holder on a web application, which can be done in two forms, either using identity certificate or anonym certificate, whereby the corresponding 2048-bit private key never leaves the card (Giesecke & Devrient GmbH, 2014). The private key is protected with a PIN, which is issued to citizen in protected paper format. In (Rexha, Qerimi, Neziri, & Dervishi, 2015) is presented an Internet authentication scenario using user's real and anonym profile.

3. Preparing Testing Environment

3.1 Middleware of the smart card

Microsoft has integrated the usage of smart cards in Windows applications staring from Windows 2000, presented in Figure 3 (Microsoft, 2015).

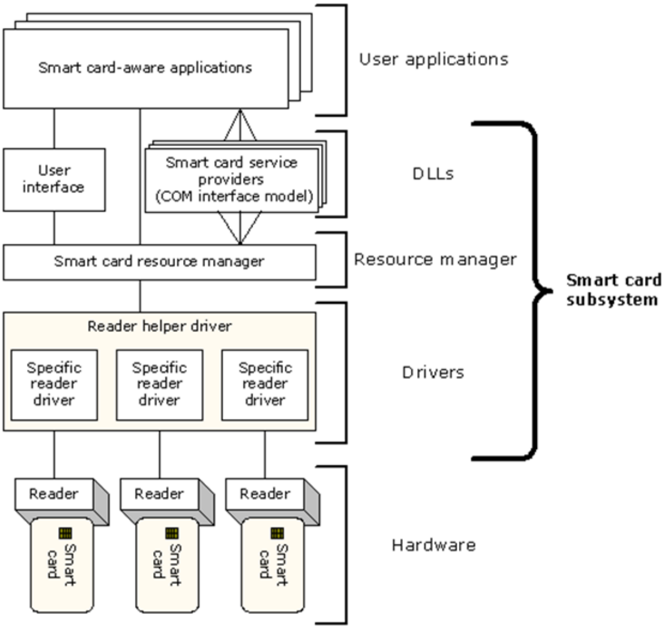


Figure 3. Smartcard architecture in Windows Platform (Microsoft, 2015)

To access full functionality of national biometric eID card cryptographic protocols, such as: encryption, decryption, data signature and verification stage, *BiometricEfficiency_FIEK* uses vendor specific Crypto Service Provider (CSP) functionalities, wrapped as middleware software.

3.2 The application BiometricEfficiency_FIEK

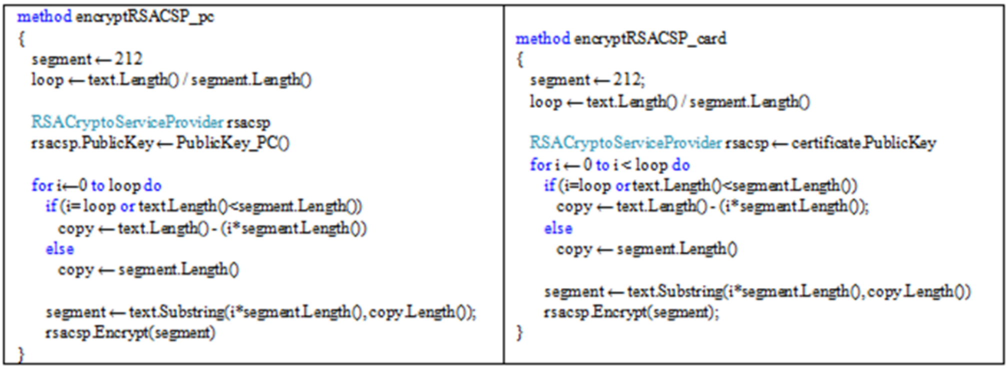
BiometricEfficiency_FIEK is an application developed in C# using Microsoft Visual Studio 2015 for Windows 10 platform. It is open source application.

3.3 Pseudocode from the application

The main functions of the application are encryption and digital signature, function which are organized in helper classes.

The encryption helper class contains the following methods for implementing Match off Card and Match on Card encryption using RSA CryptoServiceProvider and RSA:

- **encryptRSACSP_pc(text)** encrypts the string *text*, using the public key stored locally on the PC.
- **encryptRSACSP_card(text, certificate)** encrypts the string *text*, using the RSA CSP class, with the public key from the *certificate* on the national eID biometric card.
- **encryptRSA_card(text, certificate)** encrypts the *text*, using the *certificate* on the national eID biometric card, using RSA class.

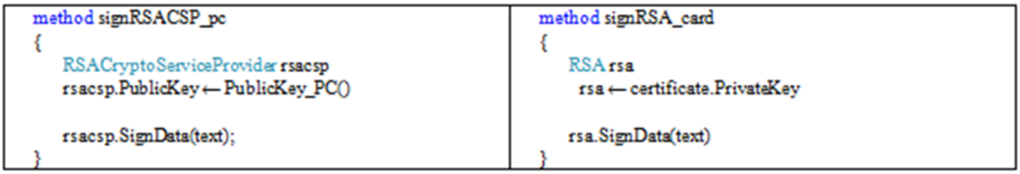


```
method encryptRSACSP_pc
{
  segment ← 212
  loop ← text.Length() / segment.Length()

  RSACryptoServiceProvider rsacsp
  rsacsp.PublicKey ← PublicKey_PC()

  for i←0 to loop do
    if (i=loop or text.Length()<segment.Length())
      copy ← text.Length() - (i*segment.Length())
    else
      copy ← segment.Length()

    segment ← text.Substring(i*segment.Length(), copy.Length());
    rsacsp.Encrypt(segment)
}
```

```
method encryptRSACSP_card
{
  segment ← 212;
  loop ← text.Length() / segment.Length()

  RSACryptoServiceProvider rsacsp ← certificate.PublicKey
  for i ← 0 to i < loop do
    if (i=loop or text.Length()<segment.Length())
      copy ← text.Length() - (i*segment.Length());
    else
      copy ← segment.Length()

    segment ← text.Substring(i*segment.Length(), copy.Length())
    rsacsp.Encrypt(segment);
}
```

The signature helper class performs data signature using RSA and RSA CSP classes, using the following methods for implementing Match off Card and Match on Card:

- **signRSACSP_pc(text)** is used to sign the string *text*, with the private key stored on the PC using the RSA CSP class.
- **signRSACSP_card(text, certificate)** is used to sign the string *text*, using the *certificates* private key.
- **signRSA_card(text, certificate)** is used to sign the string *text*, with the *certificates* private key to , using RSA class.



```
method signRSACSP_pc
{
  RSACryptoServiceProvider rsacsp
  rsacsp.PublicKey ← PublicKey_PC()

  rsacsp.SignData(text);
}
```

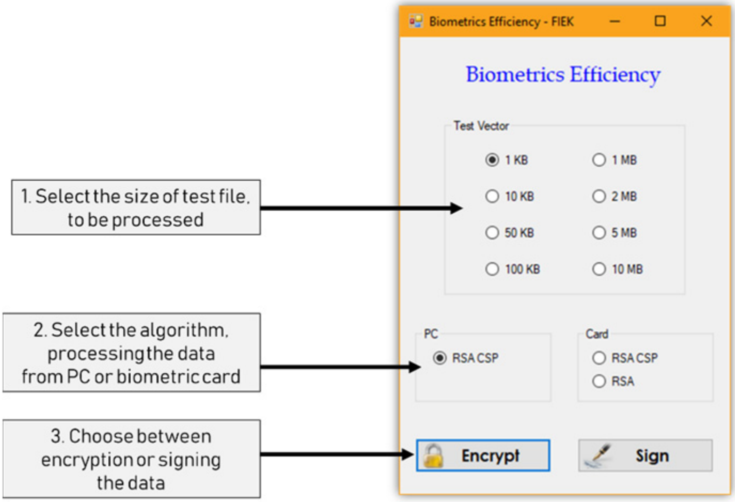
```
method signRSA_card
{
  RSA rsa
   rsa ← certificate.PrivateKey

  rsa.SignData(text)
}
```

Each method initially divides the test vector in blocks, to encrypt each block in one step, since the experiment works with block encryption algorithms.

3.4 BiometricEfficiency_FIEK Functionalities

Figure 4 shows the simple interface of the application. The main aim of this paper is to evaluate the efficiency or the time needed to process the security protocols, using both those processing systems, Match off Card and Match on Card.

BiometricEfficiency_FIEK is used to encrypt or sign data, using the processing power of eID biometric card or processing power of the PC, primarily used for experimental purposes, not for encryption or digital signature.



Biometrics Efficiency - FIEK

Biometrics Efficiency

Test Vector

● 1 KB ○ 1 MB
○ 10 KB ○ 2 MB
○ 50 KB ○ 5 MB
○ 100 KB ○ 10 MB

PC
● RSA CSP

Card
○ RSA CSP
○ RSA

1. Select the size of test file, to be processed

2. Select the algorithm, processing the data from PC or biometric card

3. Choose between encryption or signing the data

Figure 4. The interface of Biometric Efficiency app

The application can encrypt or sign the text data, with one of the processing methods, following the simple steps below:

1. The first step is to encrypt or sign the text file. The test vector contains eight text files with random text of different size, from minimum 1KB to maximum 10MB.
2. The next step is to choose the algorithm and the processing method. Match off Card uses the PC as outside processing system, implementing only the RSA CSP (Crypto Service Provider) (Microsoft, 2017). Match on Card with national eID biometric card as processing system, implementing RSA CSP and RSA (Microsoft, 2014).
3. The last step is to choose the processing system, the algorithm and encryption or signature. Each experiment shows the the best time, worst time and the average time, from the loop of ten execution.

4. Results from the Experiments

The experiments are set in different environment and in different parameters, all using *biometricefficiency_FIEK* as the application. Different parameters will have impact on the efficiency. The experiments are grouped in three test sections.

4.1 RSA vs RSA CSP – Encryption – eID biometric card

The experiments will be executed ten times for each of eight test vectors and will compare the RSA and RSA CSP. This experiment encrypts the test data using the match-on-card processing method on eID biometric card.

Two things characterize this experiment. Firstly, processing time is greater in the first cycle, because the time needed to load the data on the memory, as elementary property of smart card, from the operating system and memory organization of them (Rankl & Effing, 2003). After that, the time needed for processing is shorter.

The second phenomenon, when we process larger amount of data the processing time increases, meaning the efficiency of decreases by increasing the length of data.

Table 1. Average time RSA vs. RSA CSP

Average Time [ms]			
	RSA	**RSA CSP**	Diff
1 KB	1.10	1.56	*41.72%*
10 KB	9.12	12.99	*42.45%*
50 KB	42.00	60.80	*44.76%*
100 KB	86.24	120.27	*39.46%*
1 MB	820.46	1,311.71	*59.88%*
2 MB	1,619.16	2,452.83	*51.49%*
5 MB	4,144.82	6,305.64	*52.13%*
10 MB	8,176.34	12,375.17	*51.35%*

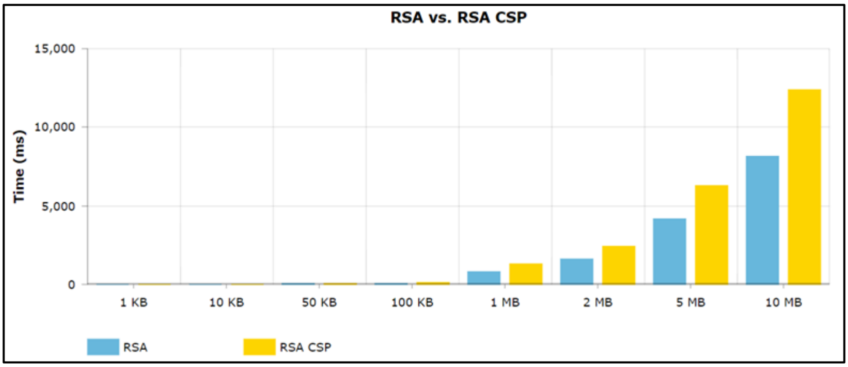


Figure 5. Graphical results RSA vs. RSA CSP

One can determine that RSA is more efficient than RSA CSP, particularly when there is a lot of data to process. The difference in processing time increases with each larger data, as shown in Table 1 and Figure 5

4.2 PC vs Card – Encryption – RSA CSP

The PC will be used as match-off-card processing method. The specification of the PC used in this experiment is Intel Core i5 5200U CPU 2.20GHz, Windows 10 64-bit operating and 8 GB of RAM. Whereas, match-on-card uses the national eID biometric card smart card, specification as described in section 2. A smart card reader will be used to transfer the information between the biometric smart card and the PC.

The environment will be the same as in the first experiment, with the same application and test vector. Similar from the previous experiment, more time will be needed at the beginning of each cycle. More time is needed for the test vector to load and store the data in the internal memory of the PC (Stallings, 2012).

Table 2. Average time PC vs. Card

Average Time [ms]			
	PC	**Card**	Diff
1 KB	1.5	1.6	6.20%
10 KB	13.1	13.0	-0.59%
50 KB	60.7	60.8	0.16%
100 KB	119.1	120.3	0.95%
1 MB	1,218.1	1,311.7	7.69%
2 MB	2,447.2	2,452.8	0.23%
5 MB	6,219.7	6,305.6	1.38%
10 MB	12,370.7	12,375.2	0.04%

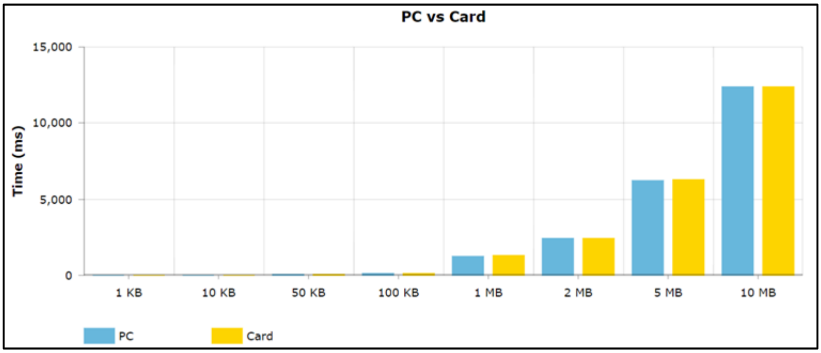


Figure 6. Average time PC vs. Card

As shown in Table 2 and Figure 6, the conclusion that we can draw form this experiment, is that the processing time increases dramatically with the size of text vector. But, since both processing methods perform nearly the same, one can't conclude which processing time is more efficient and both can be used for encryption of information of different sizes.

4.3 PC vs Card – Digital Signature – RSA CSP

This experiment will use the same environment and the same devices before, national biometric card for match-on-card processing method and PC for the match-off-card processing method.

One can notice that match-off-card processing time increases very little, when we increase the size of the test vector, whereas this is not the case in the match-on-card processing method. The processing time increases exponentially when we increase the size of test vector.

Table 3. Average time PC vs. Card

	Average Time [ms]		
	PC	**Card**	Diff
1 KB	7.5	2.0	-72.77%
10 KB	7.2	13.00	80.45%
50 KB	7.5	61.3	713.49%
100 KB	7.8	121.2	1451.75%
1 MB	14.0	1,243.5	8772.78%
2 MB	20.6	2,522.9	12165.59%
5 MB	42.6	6,214.7	14500.78%
10 MB	80.7	12,373.4	15237.16%

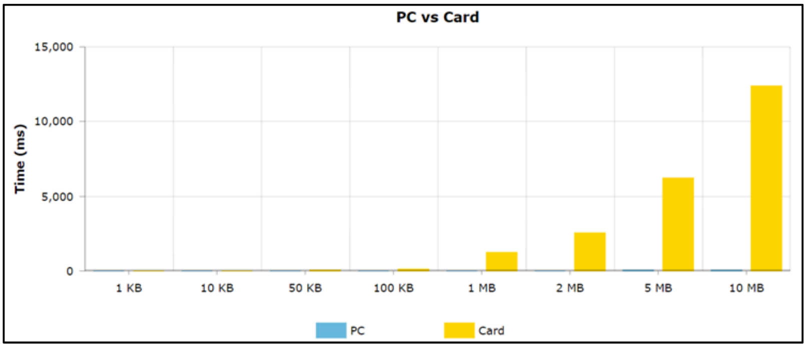


Figure 7. Average time PC vs. Card

As shown in Table 3 and Figure 7, one can conclude that, digital signature process on Match on Card is more efficient than on Match off Card, especially for larger files. Match on Card can still be used, in case when we have small files to process.

5. Conclusion

Different security protocols can be processed today on different machines. Match on Card and Match off Card are two processing methods, which can be used to perform some basic security protocols.

In this paper, national eID biometric card is used as match-on-card processing method, with very advanced hardware specification and architecture processing different kind of data. On the other hand, PC is used as a device in the Match off Card processing method. Each method has many advantages and disadvantages, each playing a significate role for choosing them as the processing device.

From section 4, which show the experimental results, overall, national eID smart card has better performance. This, independent from the size of the text vector, especially when handling small amount of data. When one increases the length of text vector, the performance of the biometric card decreases. This because of the limited hardware resources of national eID biometric card.

As future work remains adding more functionality to *biometricefficiency_FIEK* application, such as more encryption algorithms such as Advanced Encryption Algorithm (AES), elliptic curve algorithms encryption and signature support and digital signature verification process.

References

Bringer, J., Chabanne, H., Pointcheval, D., & Zimmer, S. (2008). An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication. *Proceedings of the 3rd International Workshop on Security (IWSEC '08).* Kagawa, Japan: Springer-Verlag.

Cooper, D., Dang, H., Lee, P., MacGregor, W., & Mehta, K. (2007). *Secure Biometric Match-on-Card Feasibility Report.* National Institute of Standards and Technology. National Institute of Standards and Technology: NIST Interagency Report 7452.

Giesecke & Devrient GmbH. (2014). *Help files and technical notes for HIGHSEC eID App.*

Grother, P., Salamon, W., Watson, C., Indovina, M., & Flanagan, P. (2009). *MINEX II Performance of Fingerprint Match-on-Card Algorithms Phase II / III Report - NIST Interagency Report 7477.* Information Access Division - National Institute of Standards and Technology.

ICAO. (2018). *Machine Readable Travel Documents 9303, Seventh Edition.* ICAO - UN.

Infineon. (2013). *Technical details for SLE 78CLX1280P.* Retrieved August 2018, from http://www.infineon.com/

Microsoft. (2014). *RSA Class.* (.NET Framework) Retrieved July 20, 2018, from https://msdn.microsoft.com/en-us/library/system.security.cryptography.rsa(v=vs.110).aspx

Microsoft. (2015). *Smart Card Authentication.* (Microsoft) Retrieved August 22, 2018, from https://docs.microsoft.com/en-us/windows/desktop/secauthn/smart-card-authentication

Microsoft. (2017). *RSACryptoServiceProvider Class.* (.NET Framework) Retrieved July 20, 2018, from https://msdn.microsoft.com/en-us/library/system.security.cryptography.rsacryptoserviceprovider(v=vs.110).aspx

Pang, C. T., Yun, Y. W., & Xudong, J. (2009). On-Card Matching. In *Encyclopedia of Biometrics.* Institute for Infocomm Research.

Rankl, W., & Effing, W. (2003). *Smart Card Handbook.* England: John Wiley & Sons Ltd.

Rexha, B., Imeraj, D., & Shabani, I. (2018). Using efficient TRNGs for PSEUDO profile in national eID card. *International Journal of Recent Contributions from Engineering, Science & IT (iJES), 6*(1), 57-73.

Rexha, B., Qerimi, E., Neziri, V., & Dervishi, R. (2015). Using eID pseudonymity and anonmity for strengthing user freedom in Internet. *CEEE|Gov Days 2015 Central and Eastern European e|Dem and e|Gov Days 2015 Independence Day: Time for a European Internet.* Budapest,.

Smart Card Alliance. (2011). *A Smart Card Alliance Physical Access Council White Paper.* Princeton Junction, NJ 08550: Smart Card Alliance.

Smart Payment Association. (2013). *Biometrics for Payment Applications - The SPA Vision on Financial Match-on-Card.* Smart Payment Association (SPA).

Stallings, W. (2012). *Operating Systems: Internals and Design Principles.* New Jersey: Prentice Hall, Pearson.

Vibert, B., Ninassi, A., & Rosenberger, C. (2013). Security and Performance Evaluation Platform of Biometric Match On Card. *International Conference on Mobile Applications and Security Management (ICMASM)*, (pp. 6-14). Tunisia.