Scientific Journal of Informatics
Vol. 4, No. 1, May 2017

p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

Implementation of QR Code and Digital Signature to Determine the Validity of KRS and KHS Documents

Fatich Fazlur Rochman[1], Indra Kharisma Raharjana[2], Taufik[3]

[1,2,3]Information System Department, Science and Technology College, Universitas Airlangga Campus Mulyorejo, Surabaya
Email: [1]faz-12@fst.unair.ac.id, [2]indra.kharisma@fst.unair.ac.id, [3]taufik@fst.unair.ac.id

Abstract

Universitas Airlangga students often find it difficult to verify the mark that came out in the Kartu Hasil Studi (KHS) is called Study Result Card or courses taken in the Kartu Rencana Studi (KRS) is called Study Plan Card, if there are changes to the data on the system used Universitas Airlangga. This complicated KRS and KHS verification process happened because the KRS and KHS documents that owned by student is easier to counterfeit than the data in the system. Implementation digital signature and QR Code technology as a solution that can prove the validity of KRS or KHS. The KRS and KHS validation system developed by Digital Signature and QR Code. QR Code is a type of matrix code that was developed as a code that allows its contents to be decoded at high speed while the Digital Signature has a function as a marker on the data to ensure that the data is the original data. The verification process was divided into two types are reading the Digital Signature and printing document that works by scanning the data from QR Code. The application of the system is carried out were the addition of the QR Code on KRS and KHS, required a readiness of human resources.

Keywords: Study Plan Card, Study Result Card, Digital Signature, QR Code

1. INTRODUCTION

In the information technology era like today, people more incentive to change the processes that occur from manual to computerized for ease of use. This change also applies to processes that involving the student’s Study Plan Card (KRS) and student’s Study Results Card (KHS). The changed KRS and KHS process from manual to computerized has many positive effects such as the ease of data inputting, the ease of printing, as well as ease of data storing. Apart from many of its positive impact, there are still some risks that can occur in this concept changes, such as data loss and data destruction that can lead to doubts about the validity of the data KRS and the KHS.

The data validity issues become a very important point, given the problems of data loss or destruction of data KRS and KHS either intentionally or unintentionally may occur. Data forgery is still managed to occur given the absence of procedures that can demonstrate the validity of the KRS and KHS data copies that owned by University.

Something that can prove the validity of KRS and KHS data copies that owned by University is the KRS and KHS data that held by students in the form of printed documents. If the data owned by the University and the data owned by the students is same, it can be ascertained that the KRS and KHS data is genuine, but when that data is different, it would be hard to determine which data is genuine.

During this time the KRS and KHS data owned by University serve as a reference for determining the validity of the printed KRS and KHS documents owned by Students. This procedure is used because the printed document is an easy subject for some crimes such as unauthorized reproduction and counterfeiting [1]. However this procedure is considered to be unfair if the printed KRS and KHS documents that owned by Student is the genuine one.

Based from the data validity problem, came an idea to create a system that can prove the validity of the KRS and KHS which has been printed by applying Quick Response (QR) Code together with Digital Signature technology. QR Code is a type of matrix code that was developed as a code that allows its contents to be decoded at high speed [2] while the Digital Signature has a function as a marker on the data to ensure that the data is the original data [3].

The application of QR Code and Digital Signature technology is certainly made an impacts that occur in the processes involving KRS and KHS at the University. It is necessary to test the use of this technology. In this case, the Fakultas Sains dan Teknologi (FST) Universitas Airlangga is used as research object, where has implemented the computerized process of making the KRS and KHS, which need a validity system.

2. METHODS

The method used in this research consists of five stages, including the data collection, design system, development system, test and evaluation system. The execution of each step in this study run sequentially and not precede each other. The description of each stage is as follows.

2.1. Data Collection

The beginning stage of this research is the collection of data from FST Universitas Airlangga everyday in May 2016 about KRS and KHS.

2.2. Design System

The system that built in this research is a software that can performs validation process in KRS and KHS documentation by implementing QR Code and Digital Signature technology. The system has two process that must be done, namely the process of providing QR Code and Digital Signature to KRS and KHS and the validation process that can prove the validity of the document.

1) Process of Providing QR Code and Digital Signature
In the process of providing the QR Code and Digital Signature, there are three steps that must be done as shown in Figure 1 that denoted by stages A, B, and C. A is a stage to create a QR Code for documents KRS and KHS students. B is a stage to create a digital signature for documents and KHS Student KRS. C is a stage to give a QR Code and Digital Signature has been made on a digital KRS and KHS document.

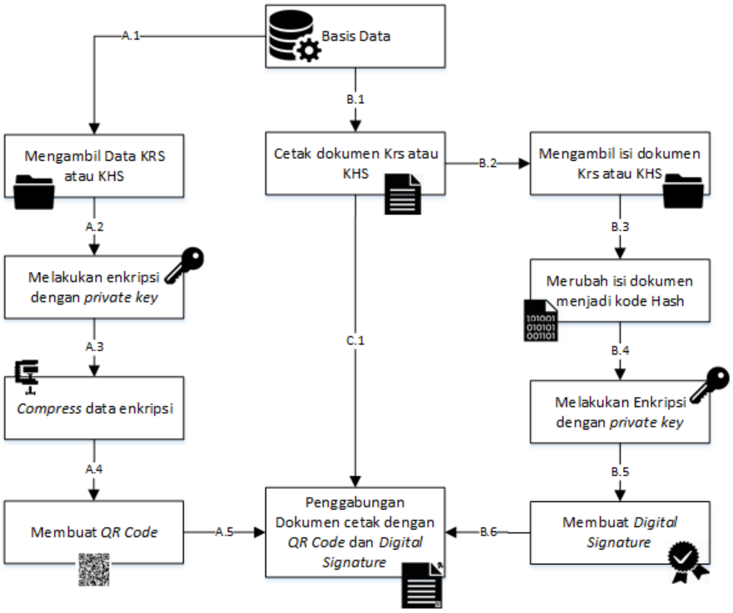

Basis Data
A.1
B.1
Mengambil Data KRS atau KHS
Cetak dokumen Krs atau KHS
B.2
Mengambil isi dokumen Krs atau KHS
A.2
B.3
Melakukan enkripsi dengan *private key*
Merubah isi dokumen menjadi kode Hash
A.3
C.1
B.4
Compress data enkripsi
Melakukan Enkripsi dengan *private key*
A.4
B.5
Membuat *QR Code*
A.5
Penggabungan Dokumen cetak dengan *QR Code* dan *Digital Signature*
B.6
Membuat *Digital Signature*

Figure 1. Process of Providing QR Code and Digital Signature

2) Validation Process of Digital KRS and KHS Documents

In the validation process of digital KRS and KHS documents, there are two steps that must be carried out as shown in Figure 2 that denoted with the stages A and B. A is a stage to make a hash code from the contents of digital KRS and KHS documents. B is a stage to get the Hash code stored in digital KRS and KHS document's Digital Signature. After that, it will do a comparison of both the Hash code. If the comparison results is same, the documents stated genuine, otherwise if the result is different, then the document was forged.

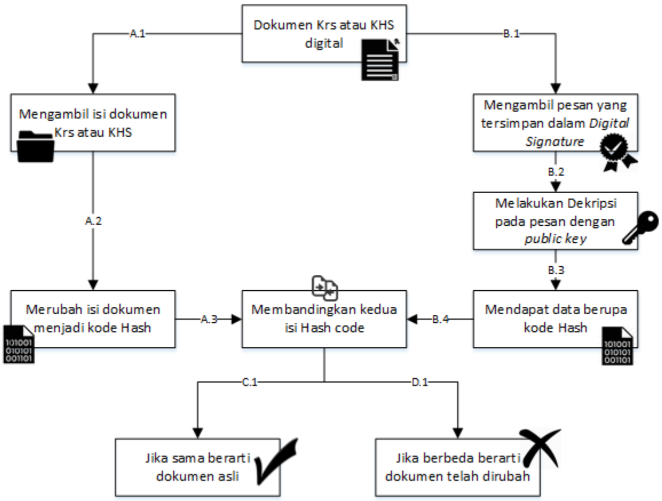

Dokumen Krs atau KHS digital
A.1
B.1
Mengambil isi dokumen Krs atau KHS
Mengambil pesan yang tersimpan dalam *Digital Signature*
B.2
Melakukan Dekripsi pada pesan dengan *public key*
A.2
B.3
Merubah isi dokumen menjadi kode Hash
A.3
Membandingkan kedua isi Hash code
B.4
Mendapat data berupa kode Hash
C.1
D.1
Jika sama berarti dokumen asli
Jika berbeda berarti dokumen telah dirubah

Figure 2. Validation Process of Digital KRS and KHS Documents

3) Validation Process of Printed KRS and KHS Documents

In the validation process of printed KRS and KHS documents, there is one step that must be carried out as shown in Figure 3 that denoted by stage A. A is a stage to retrieve data from printed KRS and KHS documents by scanning the QR Code in that documents. After the phase A is completed, then proceed with manual comparisons of the data scanned from the QR Code and data from printed KRS and KHS documents. If the results of that comparisons is same, the documents stated genuine, otherwise if the result is different, then the document was forged.

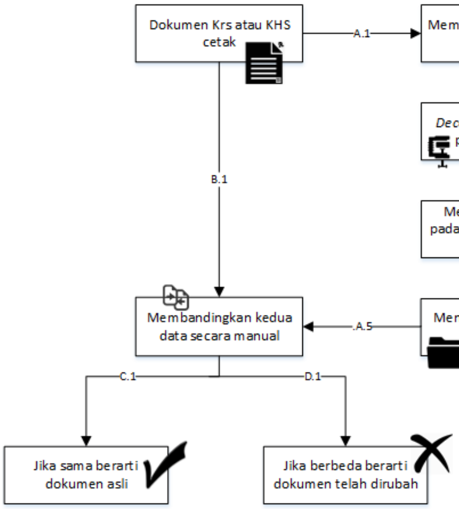

Dokumen Krs atau KHS cetak
A.1
Memindai *QR Code pada dokumen*
A.2
Decompress data hasil pindai dokumen
A.3
Melakukan Dekripsi pada data dengan *public key*
A.4
Mendapat data berupa isi dokumen
A.5
B.1
Membandingkan kedua data secara manual
C.1
D.1
Jika sama berarti dokumen asli
Jika berbeda berarti dokumen telah dirubah

Figure 3. Validation Process of Printed KRS and KHS Documents

2.3. Development System

This research applies a system with several stages of development. The main concept of the development of this system is the division of the entire workflow into several stages that are interrelated [4]. Stages to be run in this study were divided into six, as shown in Figure 4. Stage 1, stage 2, stage 3 and stage 4 are independent so it can be done together. For stage 5 must wait for stage 1, stage 2, and stage 3 are completed, as well as stage 6 that must wait stage 3 and stage 4 are completed. In each stage there are several steps that must be completed. The stages and their full descriptions are shown in Table 1.

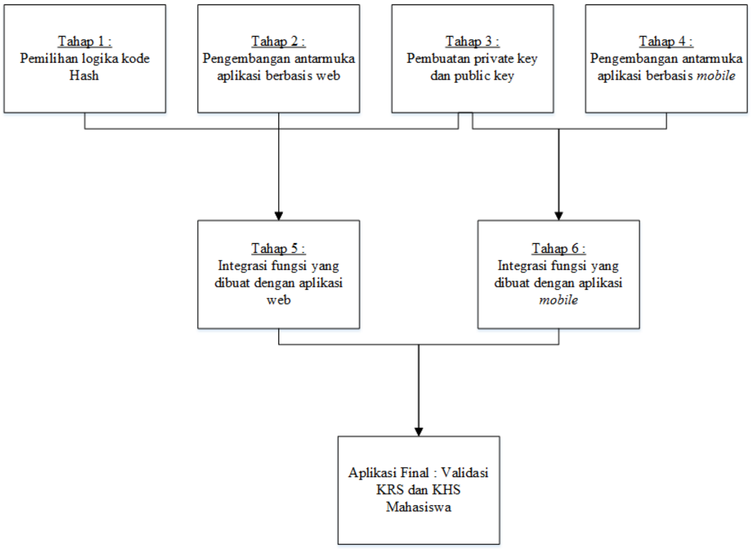

Tahap 1 :
Pemilihan logika kode Hash
Tahap 2 :
Pengembangan antarmuka aplikasi berbasis web
Tahap 3 :
Pembuatan private key dan public key
Tahap 4 :
Pengembangan antarmuka aplikasi berbasis *mobile*
Tahap 5 :
Integrasi fungsi yang dibuat dengan aplikasi web
Tahap 6 :
Integrasi fungsi yang dibuat dengan aplikasi *mobile*
Aplikasi Final : Validasi KRS dan KHS Mahasiswa

Figure 4. System Development Stages

2.4. Test System

System test is a critical element of the quality assurances of system itself and represent the basic study of the specification, design and coding. Testing was done to meet the requirements of the quality system by making the test scenarios and execute programs based on the scenario to look for the error code, and verify the suitability of the system to view the existing functionality in the system.

2.5. System Evaluation

In the application of the system, there are some impacts that accompany it. To determine the impact that may occur as a result of the implementation of this system, it would require a simulation for the System. A questionnaires were distributed following the simulation to the FST Airlangga University's students and conduct interviews with the main actors of this process namely the Academic Unit of FST Airlangga University.

Tabel 1. System Development Stages

No	Activity	Explanation
		Stage 1 : The Selection of Hash Code Logic
1	Hash code literature study	Studying and comparing the hash code types that already exist and pick the most suitable Hash code logic for this research
		Stage 2 : Development-Based Web Application
1	Application design	Creating a workflow design web-based application based on the viewpoint of the actor that used the application

2	Database design	Creating a clone database design used by Universitas Airlanggawith MYSQL DBMS (Database Management System)
3	Interface design	Creating an interface design for KRS and KHS documents creation with the addition of QR Code and Digital Signature function, and digital KRS and KHS documents validation function
Stage 3 : Making Private Key and Public Key		
1	Digital Signature algorithm literature study	Studying and comparing Digital Signature algorithms that already exist and choose the most suitable Digital Signature algorithms for this research
2	Making private key	Make private key from Digital Signature algorithms that have been choosen previously
3	Making public key	Mske a private key from the public key that has been previously msde
Stage 4 : Development-Based Mobile Application		
1	Application design	Creating a workflow design mobile-based application based on the viewpoint of the actor that used the application
2	Interface design	Creating an interface design for printed KRS and KHS documents validation function
Stage 5 : The Integration of Functions with Web Application		
1	Develop a web application's interface	Creating interfaces that have been designed with the php programming language
2	Adding the functions to Web application	Adding functions that previously defined on a web program thar the interface has been completed
Stage 6 : The Integration of Functions with Mobile Application		
1	Develop a mobile application's interface	Creating interfaces that have been designed with the java (android) programming language
2	Adding the functions to Mobile application	Adding functions that previously defined on a mobile program thar the interface has been completed

3. RESULTS AND DISCUSSION

3.1. Results of Data Collection

The data collection was done by interviewing Dr. Eridani, M.Sc. as Head of Academic Unit of FST on May 4, 2016. The results showed that the issue of the validity of documents and KHS Student KRS indeed rare, but the faculty also do not circumvent about the difficulties process of determining the validity of the KRS and KHS documents, so the faculty gave permission and willing to help associated with this research.

3.2. System Implementation

The System Implementation stage was done by referring to the System Design and System Development stages which has been described in section 2.2 of System Design and section 2.3 of the System Development. System Design stage is the flow of the functional of the system, while System Development stage is the creation flow or implementation of the system. As for the achievements of Implementation System stage will be described following the activity order based on table 1.

In phase 1 activity number 1, a comparison of Hash codes logic was done based on the literature study [5] to select the suited logic for this research. Comparisons were Ade by referring to three kriteria, the size of the message digest which is the size of Hash code that generated, the size of the message block which is the amount of data size that can be converted into Hash code, and collisions which is a marker of whether the logic produces the same output with different input, Based on these criteria RIPEMD – 128 logic chosen because it has a small size of the message digest (128 bits), a large message block size (512 bits), and did not experience any collisions.

In phase 2 activity number 1, created an Unified Modeling Language (UML), which is the standard in the development of object-based applications [6] for web based applications. Of the several existing UML, in this research only uses three models, namely Use Case Diagram, Activity Diagram and Sequence Diagram. The results of these activities in the form of design functions on systems described by Use Case Diagram as shown in Figure 5. Then each of the functions described in the Activity Diagram and Sequence Diagram.

In phase 2 activity number 2, created a database design in the form of Conceptual Data Model (CDM) and Physical Data Model (PDM), which is based on the data that required in the manufacture of KRS and KHS. The required data is determined by analyzing the printed document KRS and KHS from Universitas Airlangga.

In stage 2 activity number 3, created an interface design for web-based system. The interface design of this system refers to the interface system that has been used by the Universitas Airlanggatoday. This was done in order to make the research resemble the events that occurred at Airlangga University.

In stage 3 activity number 1, a comparison of private key and a public key algorithm was done based on the literature study [7] to select the suited algorithm for this research. Rivest Shamir Adleman (RSA) Algorithm was selected because it can identify the user by verification process which is the concept of Digital Signature.

In stage 3 activity number 2 and 3, the generation of the private key and public key was done using OpenSSL PHP function. The generation of the private key and the public key using the RSA algorithm with a size of 6144-bit.

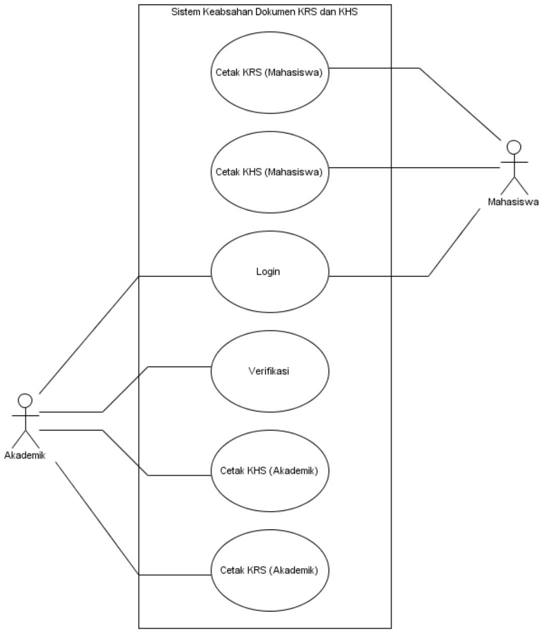


Figure 5. Use Case Diagram Web-Based System

In stage 4 activity number 1, created Unified Modeling Language (UML), which is the standard in the development of object-based applications [6] for mobile based applications. Of the several existing UML, in this study only uses three models, namely Use Case Diagram, Activity Diagram and Sequence Diagram. The results of these activities in the form of design functions on systems described by Use Case Diagram as shown in Figure 6. Then each of the functions described in the Activity Diagram and Sequence Diagram.

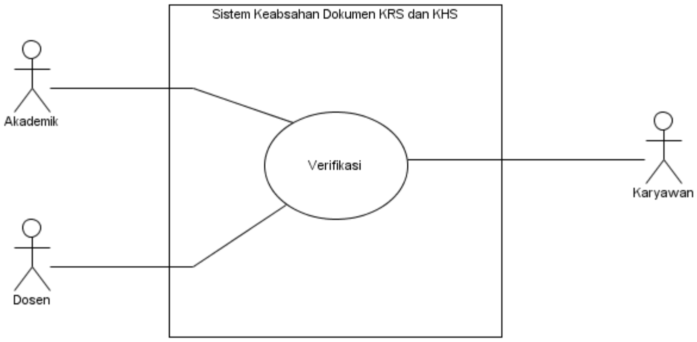


Figure 6. Use Case Diagram Mobile-Based System

In stage 4 activity number 2, created an interface design for mobile-based systems. The interface of this system is designed according to the system requirements for verification of printed KRS and KHS documents in Universitas Airlangga.

In stage 5 the activity number 1, entire web-based interfaces was created based on the designs that have been created on stage 2 activity number 3. The web-based interface system created with PHP programming language and CodeIgniter framework.

In stage 5 activity number 2, all the functions on web-based system with a description of functions that have been made on stage 2 activity number 1 was created. All of the functions created with PHP programming language and integrated to the system interface that was created in step 5 is the number 1 activity.

In stage 6 activity number 1, entire mobile-based interfaces was created based on the design that have been created in stage 4 activity number 2. The mobile-based interface system created with Java programming language that works on android operating system.

In stage 6 activity number 2, all the functions on web-based system with a description of functions that have been made on stage 4 activity number 1 was created. All of the functions created with php programming language and integrated to the system interface that was created in step 6 is the number 1 activity.

After going through the System Implementation stage, the system has been completed. Figure 7 is the verification of digital KRS and KHS documents using a digital signature in the documents. Figure 8 is the verification of printed KRS and KHS documents by scanning the QR Code in the documents.

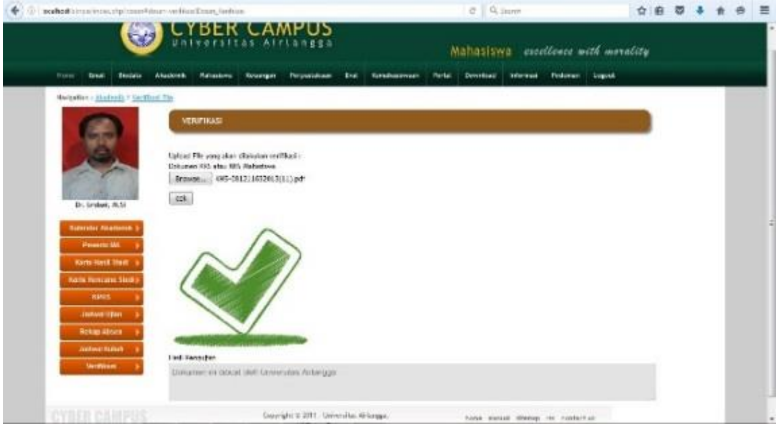
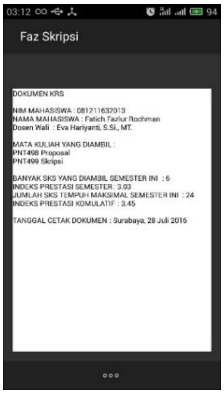


Figure 7. Verification of digital KRS and KHS documents



DOKUMEN KRS

NIM MAHASISWA : 081211632013
NAMA MAHASISWA : Fatich Fazlur Rochman
Dosen Wali : Eva Hariyanti, S.Si., MT.

MATA KULIAH YANG DIAMBIL :
PNT498 Proposal
PNT499 Skripsi

BANYAK SKS YANG DIAMBIL SEMESTER INI : 6
INDEKS PRESTASI SEMESTER : 3.03
JUMLAH SKS TEMPUH MAKSIMAL SEMESTER INI : 24
INDEKS PRESTASI KOMULATIF : 3.45

TANGGAL CETAK DOKUMEN : Surabaya, 28 Juli 2016

Figure 8. Verification of printed KRS and KHS documents

3.3. Result of System Test

Test was done on the system using the Black Box testing. Black Box testing method does not need to know how the mechanisms within the system works, but only its inputs and outputs were tested for compliance [8]. Testing of this system was applied only to the functionality of the system itself.

The first step was make the test plan for the system. The test plan was divided into two terms, which are a web-based application test plan and a mobile-based applications test plan. After creating the test plan, the test system can be done.

The result test by Black Box method shows that the system that was made either web-based or mobile-based already has the appropriate output with the expected output. So it can be stated that based on functionality, the system has been run in accordance with the wishes. This is because the system generates an output in accordance with the expected output for each scenario tested.

3.4. Result of System Evaluation

The System evaluation was done by performing a demonstration on how the system works, then describes the functions and explains the procedures involved in each process. Evaluation system is divided into two, first were the parties FST Universitas Airlangga, represented by the Academic Unit and lecturers as the main actor in the business functions that involve KRS and KHS, second were the Students of FST Universitas Airlangga represented by 20 students with notes of at least 1 Students of each study program in FST Airlangga University.

The evaluation that was done to the Academic Unit and Lecturers conducted by interview to obtain feedback on the system. As for the process evaluation of students was done by distributing a questionnaire to determine the responses of students to the system. The result of the evaluation can be explained as follows.

The first evaluation question was about the creation of the system as a solution to the the validity problem of KRS and KHS documents at FST Airlangga University. The majority of students support the system as a solution to the validity problem of KRS and KHS documents. The Academic and Lecturers give an appreciation for developing the system and stated that the system was great Ana innovative.

The second evaluation question was about the addition of the QR Code on the KRS and KHS documents. The majority of students support the addition of QR Code because it can help determine the validity of KRS and KHS documents, but some students advise that the size of the QR Code is reduced because it is quite disturbing. The majority of lecturers understand the importance of adding the QR Code, but there is another response from one of the lecturers claimed that the size of the QR Code perceived as annoying.

The third evaluation question was about the benefit of the system as a solution of KRS and KHS documents validation problem. The majority of students stated that the system was very useful because it can strengthen the system owned by the Universitas Airlangga today. The response of the Academic and Lecturers slightly different one from another, some claim that this system was very useful, but there was a thought that using this system alone was not enough to be used as a reference in determining the validity but was sufficient as additional security for the contents of the document.

The fourth evaluation question is about the prosedur changed on the KRS and KHS documents download that limited to only once. Some students agree to this because it was necessary to limit the number of documents downloaded so there are no different dates for a single document with the same details, but some of them think that these procedure make it difficult for students itself because the students were no longer able to perform the download at any time. Lecturer and Academic provide a supportive feedback of the concept of download process that proposed.

The fifth evaluation question was about the level of need in FST to implementing this system. The majority of students stated that this system has already appropriately to be implemented in FST Airlangga University, so it can expedite the administration involving the validity of KRS and KHS documents. Lecturer and Academic gave a mixed response, some support for the implementation of the system, but some have suggested that the application of the system was not entirely necessary.

The results of the evaluation show Thar the Students, Lecturers and Academic really appreciates about the system as a solution to the validity problem of KRS and KHS documents. This was stated by the opinions and feedback that beneficial to the sustainability of the system. The majority informant stated that this system deserves to be an alternative solution to the validity problem of KRS and KHS documents at Airlangga University.

4. CONCLUSION

The development a KRS and KHS documents validation system by applying digital signature and QR Code technology could be an alternative solution for determine the validity of KRS and KHS documents in Universitas Airlangga. It was based on the evaluation of the system given by the Students, Lecturers, and Academic.

The impacts that occur for using this system were the addition of the QR Code on the KRS and KHS documents, required readiness of the Human Resources (HR) that directly involved in the KRS and KHS process at Universitas Airlangga, and the integration between this system with the system that already used by Universitas Airlangga today.

The large size of the QR Code generated in KRS and KHS documents feels quite disturbing, so it needs the addition of methods that can reduce the size of the QR Code. In addition, it also needs for additional mechanisms in the system that can adapt to the curriculum changes that can occur at Universitas Airlangga.

5. REFERENCES

[1] Husain, A., Bakhtiari, M., and Zainal, A. 2014. Printed Document Integrity Verification Using Barcode. *Jurnal Teknologi (Sciences & Engineering)*, pp. 99-106.

[2] Rouillard, J. 2008. Contextual QR codes. In *Computing in the Global Information Technology. ICCGI'08. The Third International Multi-Conference on* (pp. 50-55).

[3] Singhal, A. and Pavithr, R.S. 2015. Degree Certificate Authentication using QR Code and Smartphone. *International Journal of Computer Applications*, 120(16).

[4] Hidayat, E. Y. and Firdausillah, F. 2014. *Sistem Legalisir Scan Ijasah Online*. Universitas Dian Nuswantoro, Semarang.

[5] Dwiperdana, A. 2008. *Cryptographic Hash Function dan Penggunaannya Dalam Digital Signature*. Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, pp. 1-10.

[6] Lee, S. 2012. Unified Modeling Language (UML) for Database Systems and Computer Applications. *International Journal of Database Theory and Application*, vol. 5, no. 1, pp. 157-164.

[7] Arya, P.K., Aswal, M.S. and Kumar, V. 2012. Comparative Study of Asymmetric Key Cryptographic Algorithms. *International Journal of Computer Science & Communication Networks*, 5(1), pp.17-21.

[8] Wibisono, W. and Baskoro, F. 2002. Pengujian Perangkat Lunak dengan Menggunakan Model Behaviour UML. *JUTI: Jurnal Ilmiah Teknologi Informasi*, 1(1), pp.43-50.