Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 4, October 2024
https://doi.org/10.47709/cnahpc.v6i4.4765

Submitted : Oct 02, 2024
Accepted : Oct 25, 2024
Published : Oct 28, 2024

Use of QRCode and Digital Signature Using The DSA Method to Authenticate Student Academic Documents

Suhardi[1)*]
[1)]Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
[1)] suhardi@uinsu.ac.id

ABSTRACT

Verification of digital documents is no longer done conventionally but is also done digitally, such as signatures on documents. A signature is a means of authentic evidence as well as proving a person's identity, is a means of proving the authenticity or validity of an agreement or approval for something in a document issued by two or more parties so that it can be used as a solution to verify the integrity of valid data in a document. Application of signatures Digital is also commonly used at the North Sumatra Islamic University (UINSU) Medan, especially in student study documents. Even though UINSU Medan has implemented digital signatures, this application is still a signature image obtained through scanning or photos and manually inserted into a document so that other people can easily reuse the signature image and it can even be misused. To facilitate the digital signature process, the code generated from the signature formation process is entered into a QR code so that it is easy to use to carry out the electronic document authentication process. Researchers will use QR codes and digital signatures to authenticate student documents using the DSA method. This research will be implemented into an application model with PHP and MySQL programming. The student document authentication application model using the DSA method works well as evidenced by the QRCode which contains document token information which is different for each document so that it cannot be duplicated by non-owners of the document.

Keywords: digital documents, digital signatures, qrcode, dsa

INTRODUCTION

In the current industrial era 4.0, data in the form of photos, sounds, documents and others is no longer in physical form but is in digital form so that data that previously could be seen in databases or archives can now be accessed online. Physical data storage is starting to be abandoned and digital data storage is starting to be considered to handle various important data. Data will self-destruct if stored in a conventional way even if it is maintained and repaired optimally. The composition of data or archive material has its own time limit, resulting in the data being damaged or lost.

Data storage digitally can be in the form of graphics, text, sound and also video, which will then be entered into the computer. According to NASA (National Archives and Records Administration) in the United States, digital data storage is data that is stored and processed in a certain format. Only using a computer can process it, therefore digital data storage is often called a “Machine Readable Record.".

Along with this development, verification of digital documents is no longer carried out using conventional methods but is also carried out digitally, such as signatures on documents. A signature is proof of authentication and also verification of a person's identity which is proof of the originality or validity of an agreement or approval of something in a document made by two or more parties (KOMINFO, 2021). Meanwhile, digital signature is a technology that can be used to prove mathematically that the data has not been modified illegally, so it can be used as a solution to check the data integrity of valid documents (Finandhita & Afrianto, 2018). Electronic or digital signatures are one solution that can be inserted into digital documents or archives to maintain their authenticity (Rifauddin, 2016).

The application of digital signatures is also often used at the State Islamic University of North Sumatra (UINSU) Medan, especially on student academic documents. This implementation has become more frequent during the Covid-19 period due to conditions that require all activities to be carried out online. Even after the Covid-19 period has passed, the application of digital signatures is still ongoing. This is because it can shorten the time for signing documents. Signing paper documents with a conventional signature usually takes relatively longer. Even though UINSU Medan has implemented digital signatures, this application is still in the form of a signature image obtained through a scanning process or photo and then inserted into the document manually so that the signature image can easily be reused by other people and can even be misused.

A digital signature mechanism is needed that utilizes cryptographic technology that can guarantee the authentication of the document owner. The National Institute of Standards and Technology (NIST) has published

[*] Suhardi

Submitted : Oct 02, 2024
Accepted : Oct 25, 2024
Published : Oct 28, 2024

several standards-compliant signing algorithms, one of which is the Digital Signature Algorithm (DSA). This algorithm has two functions, namely forming a signature and also verifying a valid signature (Munir, 2019)

The process of forming a signature usually produces quite a long code, therefore a technique for inserting a digital signature in the document is needed (Nuraeni et al., 2020). To facilitate the digital signature process, the code generated from the signature formation process is inserted into the QR-code so that it is easy to use to carry out the process of validating electronic documents (Kartika & Yudi, 2020).

Based on the background of the problem above, researchers will use QRcode and Digital Signature to authenticate student documents using the DSA method

LITERATURE REVIEW

In 1994, Denso Wave developed a two-dimensional symbol known as QR-Code. Each QR-Code attribute is presented in segment form. QRcode consists of a coding region and a function pattern. Each attribute is surrounded by a quiet zone boundary on its sides. There are four types of patterns which have separator functions, time patterns, alignment patterns, and finder patterns. The coding area contains data that includes info about version, form of information, data, also contains error correction (Priyambodo et al., 2020).

Digital Signature or what is called a digital signature is a technology that can be used to prove it mathematically. This data has not been modified illegally, so it can be used as a solution to check the data integrity of legitimate documents (Finandhita & Afrianto, 2018). Digital signatures really depend on the contents of the document being signed, so each document will create a digital signature that is different from other documents (Afrianto et al., 2020). Digital signatures are created with the help of cryptographic methods, with the purpose like regular signatures of placing the authentication of the author on the document (ismael & Okumus, 2017).

The digital signature algorithm is called the Digital Signature Algorithm (DSA). DSA is a public-key cryptographic algorithm. DSA is a cryptographic algorithm such as AES and others (Jasman et al., 2017). DSA is a type of public key cryptography that is used for authentication, data security, and anti-repudiation devices. DSA cannot be used for encryption. DSA is specifically specified for digital signatures. The DSA algorithm requires a special program to be used to generate the key so that the user trusts the program. Every time you carry out the process of creating a digital signature you need two keys, namely a public key and a private key. This key is dynamic so the value is different every time the digital signature is formed (Yassein et al., 2018).

Secure Hash Algorithm (SHA) was developed by NIST (National Institute of Standards and Technology) which is used with DSS (Digital Signature Standard). SHA-1 is a revision of SHA published in SHA is called secure because it is made computationally so that it is impossible to find a message that corresponds to the message digest given. SHA1 has a length of 20 bytes or 40 characters, for example : 356a192b7913b04c54574d18c28d46e6395428ab (Eritza et al., 2022)

Hypertext Preprocessor (PHP) is a scripting language that can be embedded or inserted into HTML. PHP is widely used to program dynamic websites. PHP can be used to build a CMS. Even though PHP is the same basic structure language as HTML, PHP has its own differences. The difference between PHP and HTML is that PHP is a programming language that is on the server side and requires connectivity to the database, which cannot be done using HTML (Oetomo et al., 2020).

JavaScript is a program in script form, which will be executed by an interpreter that has been embedded in a web browser, so that the web browser can execute JavaScript programs. JavaScript programs are inserted into HTML documents marked with tags starting with <script> and ending with </script>. If the web browser has a JavaScript interpreter, then this JavaScript program will be executed. The results of this execution are generally HTML document elements as well, so that the results of the program are displayed as one unit with other HTML documents, so that as a whole an HTML document will be produced that can be displayed. by a web browser (Aziz et al., 2018).

MySQL is a multiuser and multi-threaded database server. So this allows MySQL to receive several commands at once from several different users. MySQL database server is an RDMS (Relational Database Management System) that can handle large volumes of data. Even so, it doesn't require large resources (Surya & Sara, 2018).

METHOD

The research method used in this research is the Research and Development (R&D) method because this research aims to develop products. while the definition of Research and Development (R&D) methods lies in the methods used to produce certain products and test the effectiveness of these products. So that this research can be carried out on target, a research framework is needed. This research framework uses a waterfall or System Development Life Cycle (SDLC).

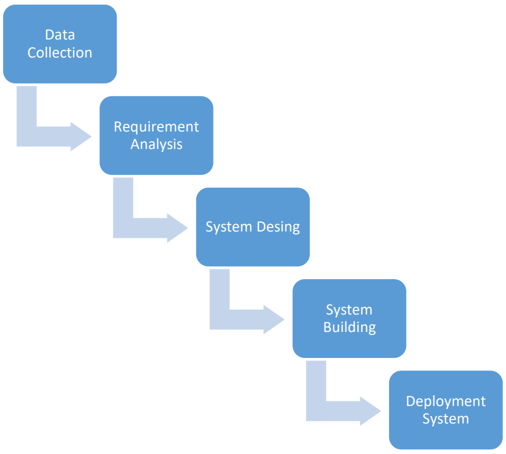


Fig. 1 Steps for Conducting Research

Meanwhile, the method used to authenticate signatures and QR codes on student academic documents is the DSA method. DSA uses the SHA (Secure Hash Algorithm) hash function to convert a message into a 160-bit message digest. The SHA function used is SHA-1 which functions to protect messages during the distribution process by calculating the hash value of the document. DSA and other digital signature algorithms have three main processes, namely:

1. Key Pair Generation
2. Digital Signature Generation
3. Digital Signature Verification

Key Pair Generation

1. Choose the prime numbers p and q, where $(p-1) \bmod q = 0$
2. Calculate $g = h^{(p-1)/q}$ mod p, where $1 < h < p\text{-}1$ *and* $g > 1$. The parameter p is public
3. Determine the private key $x < q$
4. Calculate the public key $y = g^x \bmod p$

So we get the public key (p,q,g,y) and the private key (p,q,g,x)

Digital Signature Generation

1. Convert message m into message digest with Hash SHA function produces SHA(M)
2. Determine random number $k < q$
3. The signature of message m is the number r and s obtained from:

$$r = (g^k \bmod p) \bmod q \qquad (1)$$

$$s = (k^{-1}\,(SHA(M) + x.r)) \bmod q \qquad (2)$$

k^{-1} is the inverse of k modulo q.

4. In calculating the value of s, the 160-bit string SHA(M) is first converted into an integer. If the resulting signature is correct then the value of r and/or s cannot be 0.
5. The digital signature on message m is (s, r).

Digital Signature Verification

1. Retrieve the public key (p, q, g, y)
2. If $1 \leq r \leq q$ *and* $1 \leq s \leq q$ accept the signature. Otherwise, reject the signature
3. Compute $w = s\text{-}1 \bmod q$ and SHA(M)
4. Compute $u1 = (SHA(M)*w) \bmod q$
5. Compute $u2 = (r*w) \bmod q$
6. $v = ((g^{u1} * y^{u2}\ ) \bmod p) \bmod q)$
7. If v = r, then the signature is valid, meaning that the message is authentic and was sent by the correct sender.

RESULT

System Development Life Cycle (SDLC)

1. Data Collection

Data collection is carried out in the following way:

a. Observation, in this research, researchers made direct observations at the Computer Science Study Program, Faculty of Science and Technology, UINSU, Medan.

b. Interviews, at this stage the researcher conducted a direct interview with the Head of the Computer Science Study Program, Faculty of Science and Technology, UINSU, Medan regarding the system that is currently running. This aims to ensure that researchers understand what development is needed for existing systems in the FST UINSU Medan, Computer Science Study Program.

c. Literature Study, at this stage the researcher looks for literature studies related to the research which will be used as a theoretical basis and related previous research. This is intended to help researchers deepen their understanding and expand the knowledge of researchers and readers about the research conducted.

2. Requirement Analysis

At this stage the researcher carries out planning by analyzing functional requirements, explaining the number of access rights that can be accessed by each user when using the application. Meanwhile, the requirements used in the system start from design to implementation.

3. System Design

This stage consists of 3 parts, namely designing algorithms, designing databases and designing interfaces. In designing the algorithm, the researcher used a flowchart diagram to describe the algorithm stages of the student academic document authentication application. Meanwhile, the system modeling used in this research is UML. The UML model used is the Use Case diagram. To design a database, researchers will use ERD to determine what entities, attributes and relationships exist in the database that will be created. The ERD will later become an illustration in creating a database using the MySQL DBMS. Meanwhile, to design the interface, researchers use various tools and programming languages HTML, CSS, Javascript and PHP which will produce a responsive website appearance.

4. System Building

At this stage, an academic document authentication application is created for students following system design steps using various programming languages such as HTML, CSS, Javascript, PHP and MySQLi..

5. Deployment System

At this stage, the application will be deployed to the research program with the research program manager to see the completeness of the system and methods used. At this stage, black box model testing is also carried out to ensure the suitability of the system obtained with the intended purpose of creating the system.

Application of DSA method

Documents that have been approved will be accompanied by a digital signature in the form of a QRCode containing token information. The QRcode generated by each document is different so it cannot be duplicated by someone who is not the owner of the document. One example of token information is “d5a”. The token information will be used as a message that will be encrypted using the SHA-1 hash function to produce a message digest.

1. Key Pair Generation
   a. p and q are prime numbers, where p is L bits long or $512 \le L \le 1024$ with a multiple of 64, $(p-1)$ $Mod\ q = 0$
   $p = 59419$ dan $q = 3301$ $(59419 - 1)$ $Mod\ 3301 = 0$
   b. Calculating the public parameter $g = h^{(p-1)/q}\ Mod\ p$, where $1 < h < p - 1$ and $h^{(p-1)/q}\ Mod\ p > 1$
   $h = 100$
   $g = h^{(59419\text{-}1)/3301}\ Mod\ 59419 = 18870$
   c. Determine an arbitrary value for the parameter x or private key which is an integer, where $x < q$.
   $x = 3223$ (as a private key)
   d. Calculating the value of the public key $y = g^{x}\ Mod\ p$.
   $y = 18870^{\ 3223}\ Mod\ 59419$
   $y = 29245$ (as a public key)

2. Digital Signature Generation
   Input : Message (M) and private key (x)

Submitted : Oct 02, 2024
Accepted : Oct 25, 2024
Published : Oct 28, 2024

Output : Message (M) and signature (r, s)

a. Change the SHA-1 hash value from "d5a" (hexadecimal) into integer (decimal), as follows:
H(m) = 595654fae357026b461aca187a27b0162d547e23
H(m) = 510025445495191883276053425757507154808084397603

b. Determine the random number $k < q$
$k = 997$
$k * k^{-1} = 1 \bmod q$
$997 * k^{-1} = 1 \bmod 3301$
$k^{-1} = 2907$

c. Calculating the r and s signs of the message, namely as follows:
r = (g^k mod p) mod q
= (18870^{997} mod 59419) mod 3301
= 848
s = (k^{-1} (H(m)+x*r)) mod q
= $(2907(510025445495191883276053425757507154808084397603 + 3223 * 848)$ mod 3301
= 2446

d. Message (M) can be sent along with signatures r and s.
Student academic document data along with digital signatures 848 and 2446

3. Digital Signature Verification
Theorem 1: (Proof of v = r')
If M' = M, r' = r, and s' = s in signature verification, then v = r'.

a. $\boldsymbol{s}$ = 2446
$2446 * s^{-1}$ = 1 mod 3301
$\boldsymbol{s^{-1}}$ = 2552

b. $\boldsymbol{w}$ = s^{-1} mod q
= 2552 mod 3301 = 2552

c. u1 = (H(m) * w) mod q
= (510025445495191883276053425757507154808084397603 * 2552) mod 3301
= 549

d. u2 = (r * w) mod q
= (848 * 2552) mod 3301
= 1941

e. v = ((g^{u1} * y^{u2}) mod p) mod q)
= ((18870^{549} * 29245^{1941}) mod 59419) mod 3301
= 848
v = r', then the signature is genuine.

Application Model

The UINSU Medan student academic document authentication application model is a web application that can be accessed via a browser. The following is the initial display of the application in the form of a login page which is useful for setting Admin and User access rights. Only registered Admins or Users can log in.

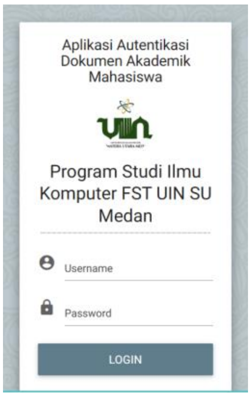
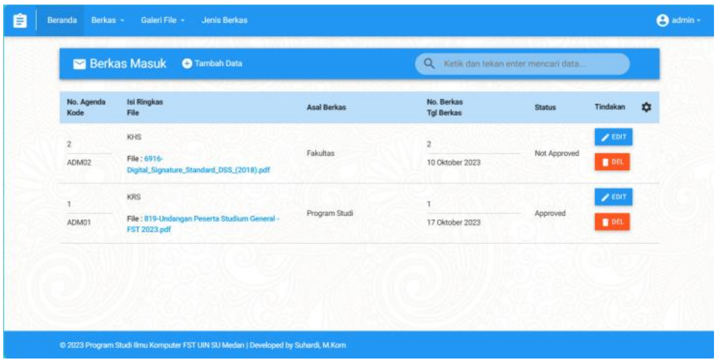

Aplikasi Autentikasi Dokumen Akademik Mahasiswa
Program Studi Ilmu Komputer FST UIN SU Medan
Username
Password
LOGIN

Fig. 2 UINSU Student Academic Document Authentication Application Login Page

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 4, October 2024
https://doi.org/10.47709/cnahpc.v6i4.4765

Submitted : Oct 02, 2024
Accepted : Oct 25, 2024
Published : Oct 28, 2024

On the Incoming Files page, there is a display of data on all files that have been uploaded by the User (student). Admin can add files by uploading files via the Add Data button



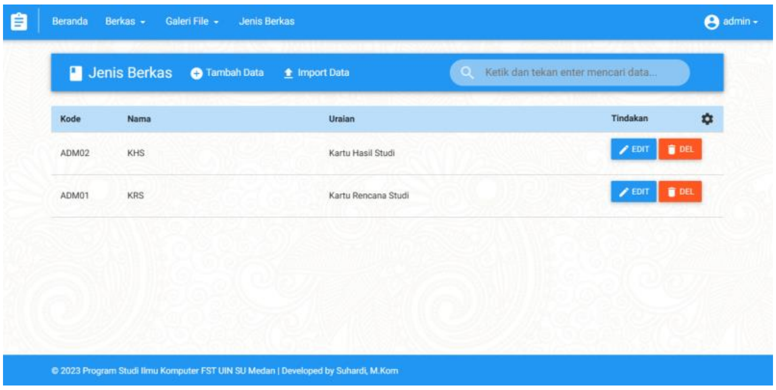
Berkas Masuk

No. Agenda Kode	Isi Ringkas File	Asal Berkas	No. Berkas Tgl Berkas	Status	Tindakan
2 ADM02	KHS File : 6916-Digital_Signature_Standard_DSS_(2018).pdf	Fakultas	2 10 Oktober 2023	Not Approved	EDIT DEL
1 ADM01	KRS File : 819-Undangan Peserta Studium General - FST 2023.pdf	Program Studi	1 17 Oktober 2023	Approved	EDIT DEL

© 2023 Program Studi Ilmu Komputer FST UIN SU Medan | Developed by Suhardi, M.Kom

Fig. 3 Incoming Files Page

The file type menu is useful for displaying the types of files or academic documents of students that will go through the approval process by the study program such as KRS, KHS and others. Admin can add, edit, delete and search for file type data.



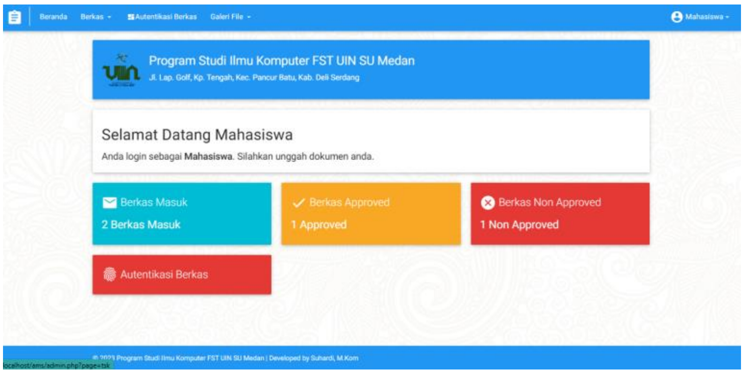
Jenis Berkas

Kode	Nama	Uraian	Tindakan
ADM02	KHS	Kartu Hasil Studi	EDIT DEL
ADM01	KRS	Kartu Rencana Studi	EDIT DEL

© 2023 Program Studi Ilmu Komputer FST UIN SU Medan | Developed by Suhardi, M.Kom

Fig 4 . File Types page

Students can only access incoming files, approved files, non-approved files, file gallery, file authentication, accounts and logout.



Program Studi Ilmu Komputer FST UIN SU Medan
Jl. Lap. Golf, Kp. Tengah, Kec. Pancur Batu, Kab. Deli Serdang

Selamat Datang Mahasiswa
Anda login sebagai **Mahasiswa**. Silahkan unggah dokumen anda.

Berkas Masuk
2 Berkas Masuk

Berkas Approved
1 Approved

Berkas Non Approved
1 Non Approved

Autentikasi Berkas

© 2023 Program Studi Ilmu Komputer FST UIN SU Medan | Developed by Suhardi, M.Kom
localhost/ams/admin.php?page=tsk

Fig 5. User Main Page

The file authentication page functions to check student academic documents that have been approved by the study program (Admin). In the document there is a QRCode that has been added to the student's document when approved by the Admin. QRCode containing a token from the DSA method. If the QRCode contains token information and the digital signature input matches the registered token information, then the Document still maintains its integrity by displaying the information "Original Document". If the QRCode does not contain token information and the digital signature input does not match the registered token information, then the Document does not maintain its integrity by displaying the information "Document is not original".

Submitted : Oct 02, 2024
Accepted : Oct 25, 2024
Published : Oct 28, 2024

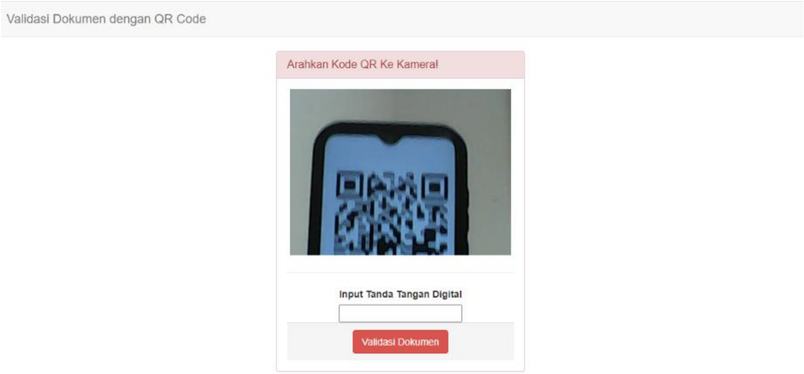
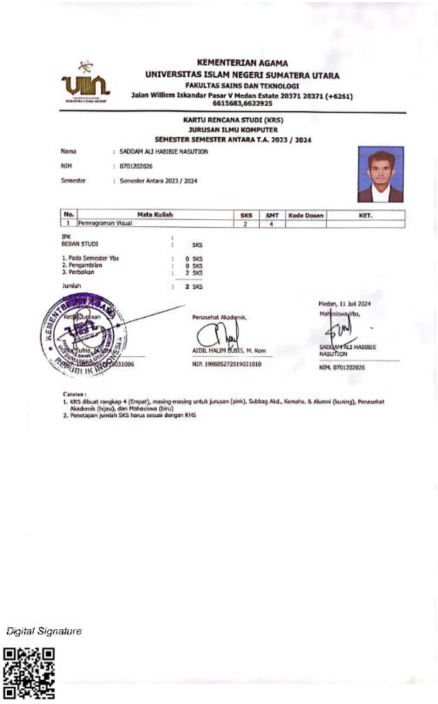

Validasi Dokumen dengan QR Code
Arahkan Kode QR Ke Kamera!
Input Tanda Tangan Digital
Validasi Dokumen

Fig 6. File Authentication Page with QRCode and Digital Signature

Documents that have been approved will be accompanied by a digital signature in the form of a QRCode containing token information. The QRcode generated by each document is different so it cannot be duplicated by someone who is not the owner of the document



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA
FAKULTAS SAINS DAN TEKNOLOGI
Jalan Williem Iskandar Pasar V Medan Estate 20371 20371 (+6261) 6615683,6622925

KARTU RENCANA STUDI (KRS)
JURUSAN ILMU KOMPUTER
SEMESTER SEMESTER ANTARA T.A. 2023 / 2024

Nama : SADDAM ALI HABIBIE NASUTION
NIM : 0701202026
Semester : Semester Antara 2023 / 2024

No.	Mata Kuliah	SKS	SMT	Kode Dosen	KET.
1	Pemrograman Visual	2	4		

IPK	:	
BEBAN STUDI	:	SKS
1. Pada Semester Ybs	:	0 SKS
2. Pengambilan	:	0 SKS
3. Perbaikan	:	2 SKS
Jumlah	:	2 SKS

Medan, 11 Juli 2024

Ketua Jurusan
[illegible] Zufria, M.Kom
NIP. [illegible]031006

Penasehat Akademik,
AIDIL HALIM LUBIS, M. Kom
NIP. 198805272019031010

Mahasiswa Ybs,
SADDAM ALI HABIBIE NASUTION
NIM. 0701202026

KEMENTERIAN AGAMA REPUBLIK INDONESIA

Catatan :
1. KRS dibuat rangkap 4 (Empat), masing-masing untuk jurusan (pink), Subbag Akd., Kemahs. & Alumni (kuning), Penasehat Akademik (hijau), dan Mahasiswa (biru)
2. Penetapan jumlah SKS harus sesuai dengan KHS

Digital Signature

Fig 7. Approved Student KRS Document with Digital Signature

System Testing

Testing of the system is carried out using the black box method by testing the functions and features in the system such as the function of saving data, changing data, deleting data, displaying data and searching for data in Incoming Data Files, Approved Files, Non Approved Files, File Type, Profile Account and Process of adding a QRCode containing a token from the DSA method to the Document. The data tested used 10 different student academic documents

Table 1. Black-box Test Results

Pages	Features	Results
Login Page	- Verify data that is eligible to log in	Success
File Input Page	- View, Add, Change, Delete Data	Success
Add File Input Page	- Fill in file data information - Save file data	Success

Edit File Input Page	-	Changing File Data Content	Success
Delete File Input Page	-	Displays Admin's notification of permission to delete files	
	-	Deleting file data Successfully	
File Input Gallery Page	-	Displays the Incoming File Gallery	Success
Incoming File Details Page	-	View all information about the incoming file data for a document.	Success
File Types Page	-	View, Add, Change, Delete File Type Data	Success
Admin Data Page	-	View, Add, Change, Delete Data	Success
User Profile Page	-	View profile data	Success
Edit Profile Page	-	Changing Profile Data	Success
QRCode Verification Page	-	Verifying the QRcode in the file	Success

CONCLUSION

Based on the results of the research that has been carried out, it can be concluded that this application model can run well in a browser and makes it easier for users to carry out the signature process from using traditional methods to become a digital signature. Documents that have been approved will be accompanied by a digital signature in the form of a QRCode containing token information. The QRcode generated by each document is different so it cannot be duplicated by someone who is not the owner of the document. This model is also an alternative solution for students who want to verify their signature with the study program. It is hoped that this research can become a reference for future researchers and can be continued by adding more innovative and relevant features. Hopefully this research will be useful for readers and especially UINSU Medan.

REFERENCES

Afrianto, I., Heryandi, A., Finandhita, A., & Atin, S. (2020). Prototype of E-Document Application Based on Digital Signatures to Support Digital Document Authentication. *IOP Conference Series: Materials Science and Engineering*, *879*(1). https://doi.org/10.1088/1757-899X/879/1/012042

Aziz, A., Setiawan, I., & Krisbiantoro, D. (2018). *Panduan Pemilu Desa Berbasis Website (Teknologi Sistem Cerdas dan Implementasi di Masyarakat)*. Gava Media.

Eritza, A., Ramadhan, M., & Hafizah, H. (2022). Penerapan Digital Signature Metode SHA dan DSA Pada Slip Gaji Pegawai. *Jurnal Sistem Informasi Triguna Dharma (JURSI TGD)*, *1*(6), 906. https://doi.org/10.53513/jursi.v1i6.6002

Finandhita, A., & Afrianto, I. (2018). Development of E-Diploma System Model with Digital Signature Authentication. *IOP Conference Series: Materials Science and Engineering*, *407*(1). https://doi.org/10.1088/1757-899X/407/1/012109

ismael, arkan, & Okumus, I. (2017). Design and Implementation of an Electronic Document Management System. In *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi* (Vol. 1, Issue 1, pp. 9–17). https://doi.org/10.31200/makuubd.321093

Jasman, J., Arisandi, D., & Sukri, S. (2017). Rancang Bangun Aplikasi Enkripsi Coding Berbasis Php Program Menggunakan Algoritma Aes. *2th Celscitech-UMRI 2017 Vol*, *2*, 49–61.

Kartika, L., & Yudi, Y. (2020). Rancang Bangun Aplikasi Penyembunyian Pesan QRCode Dengan Menggunakan Metode Caesar Cipher Berbasis Android. In *Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer* (Vol. 1, Issue 1, pp. 511–518).

KOMINFO. (2021). *Keuntungan Pakai TTE Tersertifikasi*. https://tte.kominfo.go.id/blog/60f0f35a7eec0973a8711c38

Munir, R. (2019). *Kriptografi* (Edisi Kedu). Penerbit Informatika.

Nuraeni, F., Agustin, Y. H., Kurniadi, D., & Ariyanti, I. D. (2020). Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik. *Seminar Nasional Teknologi Informasi, Komunikasi Dan Industri (SNTIKI) 12*, 43–52.

Oetomo, W., Hening, & Mahargiano, P. B. (2020). *E-Commerce Aplikasi PHP dan MySQL pada Bidang Manajemen*. Andi.

Priyambodo, A., Usman, K., & Novamizanti, L. (2020). Implementation of Android-Based Qr Code in the Presence System. In *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)* (Vol. 7, Issue 5, pp. 1011–1020).

Rifauddin, M. (2016). Pengelolaan Arsip Elektronik Berbasis Teknologi. *Khizanah Al- Hikmah Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, *4*(2), 168–178. https://doi.org/https://doi.org/10.24252/kah.v4i27

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 4, October 2024
https://doi.org/10.47709/cnahpc.v6i4.4765

Submitted : Oct 02, 2024
Accepted : Oct 25, 2024
Published : Oct 28, 2024

Surya, C., & Sara, S. (2018). Perancangan Sistem Informasi Kontrak Karyawan Pada Rs. Thursina Mengunakan Bahasa Pemrograman Vb.Net Dan Database Mysql. In *Jaringan Sistem Informasi Robotik* (Vol. 2, Issue 02, pp. 115–129).

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2018). Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017* (Vols. 2018-Janua, pp. 1–7). https://doi.org/10.1109/ICEngTechnol.2017.8308215