

e-Certificate system based on Portable Document Format and QR Code for Academic Activities

Bernard Renaldy Suteja¹, Radiant Victor Imbar², Meliana Christianti Johan³

^{1,2,3} Faculty of Information Technology, Maranatha Christian University
Bandung, Indonesia

Abstract

Many academic activities are held in an educational institution. This activity is to increase knowledge beyond what is obtained during classroom learning. Participation is always proven by the existence of a certificate. Issuance of certificates costs money for paper, printing and distribution. The emergence of the paperless era should be able to change the existence of certificates. Paperless can be done with the presence of digital documents that can be accessed independently (portable), easily and across platforms. Another issue is how this portable certificate document is also protected from the problem of unauthorized transmission or reproduction. For this, it is necessary to develop a good application to facilitate the existence of a secure e-certificate, and a solution related to the authenticity of the certificate produced.

Keywords: *e-certificate, secure portable document, paper less*

1. Introduction

Every participation in the activity is always proven by the presence of a certificate. Issue of certificates requires fees for paper, printing and distribution. Distribution is done by distributing participants - of course, with shipping costs, and can also be done with participants taking themselves to the secretariat. Many observations, the participant did not take the certificate. So Institutions often keep certificates that have been printed for a long period of time. The emergence of the era of paperless should be able to transform the presence of the certificate. Paper less is more precisely interpreted as minimizing the use of the paper itself. Paper less is stopped by the presence of digital documents that can be accessed independently (portable), easily and across platforms.

Portable Document Format or abbreviated as PDF one of the popular documents that can be distributed via the internet. PDF files become popular because of their

relatively small size and light weight in their distribution via the internet when compared to other document formats. Until now there have been many PDF document reader applications, in fact almost every browser has included them. So that PDF can be used as a document base to realize e-Certificate

Creating an e-Certificate should be able to overcome the problems that exist in conventional paper-based certificates. Some of the problems that are lacking from conventional certificates are that they are easily damaged, are lost, and are easily faked (reproduction). E-certificates that are present in the form of softcopy or document files will be able to reduce the problem of damaged certificates, good file archiving will be able to reduce the problem of lost certificates. However, the problem of counterfeiting is difficult to overcome. The most common way in conventional certificates is to detect the authenticity of signatures and other features. In this era of rapid technology, conventional certificates can be made very similar. Therefore, e-Certificate must also involve digital signatures to present solutions related to authenticity.

The Government of Indonesia is actively making changes in governance, from conventional governance to digital-based governance or we often hear it as e-government. With the support of advances in the field of technology and information that is growing rapidly at this time, opening opportunities in terms of utilization, management and access to information quickly and accurately [1]. In Indonesia, there are legal products that support the legality of e-certificates. Like PPs signing Government Regulation (PP) Number 24 regarding Electronically Integrated Business Licensing Services, electronic signatures are likened to manual signatures as guaranteed in the elucidation of Article 11 of the ITE Law. Then Article 1869 jo Article 1874 of the Civil Code and Article 1 of 1867 Ordinance No. 29 also applies to electronic signatures so that with an electronic signature the electronic documents have the force of law [2]. One electronic signature that can be utilized is the QR Code. Bank Indonesia also has regulations regarding guidelines

for implementing the Indonesian Standard Quick Response (QR) Code (QRIS). The guideline was stated in the Regulation of the Members of the Board of Governors (PADG) No.21 / 18 / PADG / 2019 concerning the Implementation of the National Quick Response Code Standard for Payment on August 16, 2019 [3].

This research will develop an e-Certificate system for organizing activities at Maranatha Christian University, by implementing a QR Code-based digital signature as a guarantee of the authenticity of the e-Certificate generated. The authenticity of the e-Certificate is done by verifying the QR Code contained in the e-Certificate.

2. Research Method

e-Certificate itself is short for electronic certificate or electronic certificate or better known as digital certificate. There is an explanation regarding e-Certificate:

1. The certificate is present in a file with a certain document format (can be PDF, or image file) or scan results. The purpose of this certificate is to replace the existence of conventional certificates which must be printed in certain paper media.

2. The certificate is also present in the form of an encrypted text file. This certificate file becomes an identity that can be used for an activity or secure data exchange transaction. Said to be safe because in the encryption there is a digital signature that is included.

In the context of this study, what is meant by e-Certificate is a digital document in PDF format that has a digital signature as a validation and for testing the authenticity of the certificate. The signature used is based on the QR Code.

QR Code is a two-dimensional matrix image that has the ability to store data in it. QR Code is the evolution of barcode (barcode). Barcode is a symbol of marking a real object made from a pattern of black and white bars to be easily recognized by computers [4]. An example of a QR Code can be seen in Figure 1.



Figure 1. Example QR Code

QR Code is an abbreviation for Quick Response Code, or can be translated into a fast response code. QR Code was developed by Denso Corporation, a Japanese company that engages in many automotive fields. This QR Code was published in 1994 with the aim of tracking vehicles in manufacturing quickly and getting responses quickly. The procedure for generating a QR Code [6] from a text can be explained by the diagram in Figure 2.

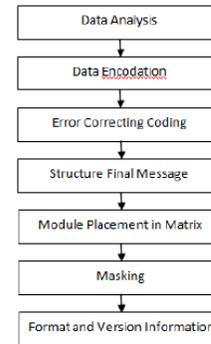


Figure 2. Diagram of the QR Code generation process

The steps for reading the QR Code [6] into the original text are reverse or reverse steps for the generation of the QR Code. In general, the procedure for reading the QR Code can be explained by the diagram in Figure 3.

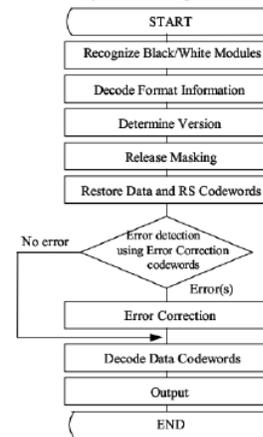


Figure 3. Flow chart of reading the QR Code

The e-Certificate system is realized in the form of a web-based application that has two main tasks: the first task is to produce an e-certificate complete with QR Code and the second task is to verify the QR Code so that it can be used to test the authenticity of certificates generated by the application.

The use case diagram of this system (figure 4) involves three actors namely administrator, personal in charge (PIC) and users namely lecturers and students. The administrator actor manages the event and inputs the event participants. Administrators within the university can be units, institutions, bodies, faculties to study programs. The PIC Actor is responsible for organizing the event as well as certifying the certificate. The user actor selects the events that have been attended, downloads the certificate, and can verify the authenticity of the certificate based on the QRCode in the certificate.

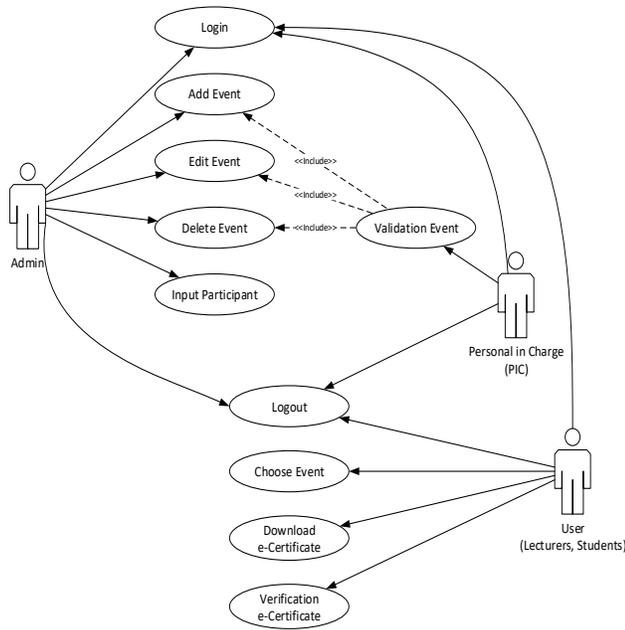


Figure 4. Use Case e-Certificate System

The e-Certificate system created involves integration with the integrated academic system (SAT) of Maranatha Christian University. SAT is a database of lecturers and students. The identities of lecturers and students will be identified from a registration number, for lecturers the Employee Identification Number (NIK) and students are the Principal Registration Number (NRP). NIK and NRP are used to log in on a SAT.

Web service (WS) can be used to exchange data that has different platforms [5]. SAT has a WS that can be used in a software development environment at Maranatha Christian University. WS as an application programming interface (API), which is used by the e-Certificate System to communicate. The e-Certificate system logs in with the help of the WS (figure 5).

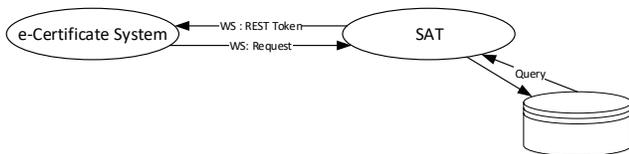


Figure 5. Architecture e-Certificate System

The system was developed using the design pattern approach (design pattern) architecture of MVC application development (Model, View, Controller). MVC divides the application into three functional parts: model, view, and controller (figure 5).

1. Models are codes for business models and data. usually dealing directly with the database to manipulate data (insert, update, delete, search), handle validation from the controller part, but cannot be directly related to the view

part. The model created is to get certificate data such as events and PIC and certificate verification.

2. View is the part that handles presentation logic. contains codes for display. The view created is the login, certificate view, and verification view

3. The controller is the part that regulates the relationship between the model and the view, the controller functions to receive requests and data from the user and then determine what the application will process. The controller is made to communicate to WS, generate QRCode and certificate key, communicate with model and view.

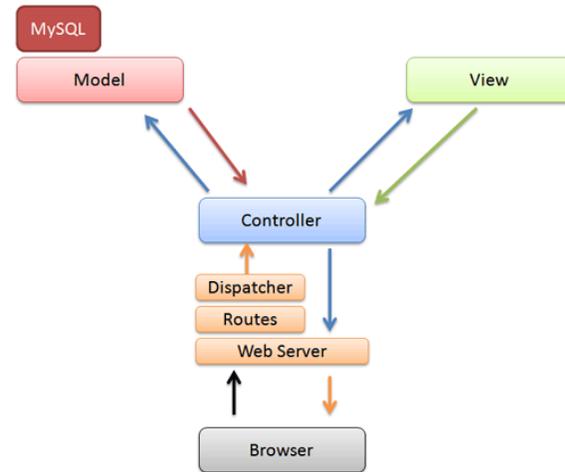


Figure 6. MVC e-Certificate System

3. RESEARCH AND TEST RESULTS

In the application that is made, the e-Certificate system is implemented in two processes, namely: obtaining a certificate and testing the authenticity of the certificates produced (figure 7). The process of obtaining goes through five stages, starting with the selected event data to finally produce an e-certificate. An important part of this process is the stage of producing key protection consisting of 5 random characters, a combination of numbers and letters and the stage of producing a QR Code containing information for verification



Figure 7. Steps to produce an e-Certificate

Key protection is a combination of event and user data which then hashing (part of the digest technique) is then followed by an encryption process and then randomly taken 5 characters 2 times. The first 5 characters will be used to generate a QR Code and then the next 5 characters will be placed at the bottom of the QR Code. Key protection is used in the process of verifying the authenticity of e-certificates. Illustration related to key protection as shown in Figure 8.



Figure 8. Key Protection on e-Certificate

The process of certifying the authenticity of the certificate (figure 9) starts from the QR Code scan followed by verification of the captcha and then decrypting the two keys in the QR Code and the 5 characters placed under the QR Code. The results of the verification process will bring up important information related to seminar information and participants who took part. If there is no authenticity, invalid certificate information will appear.

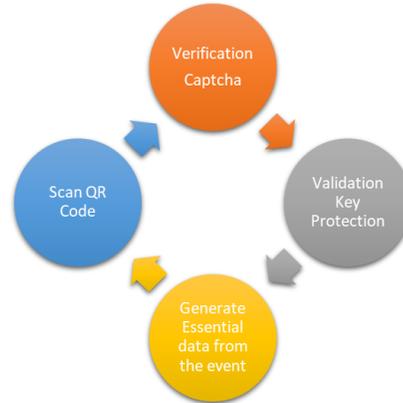


Figure 9. The stages of testing the authenticity of e-Certificate

Following is the implementation of the application to generate e-certificates, which starts from the login process to the certificate download process. Figure 10 shows the sequence of steps in this process.

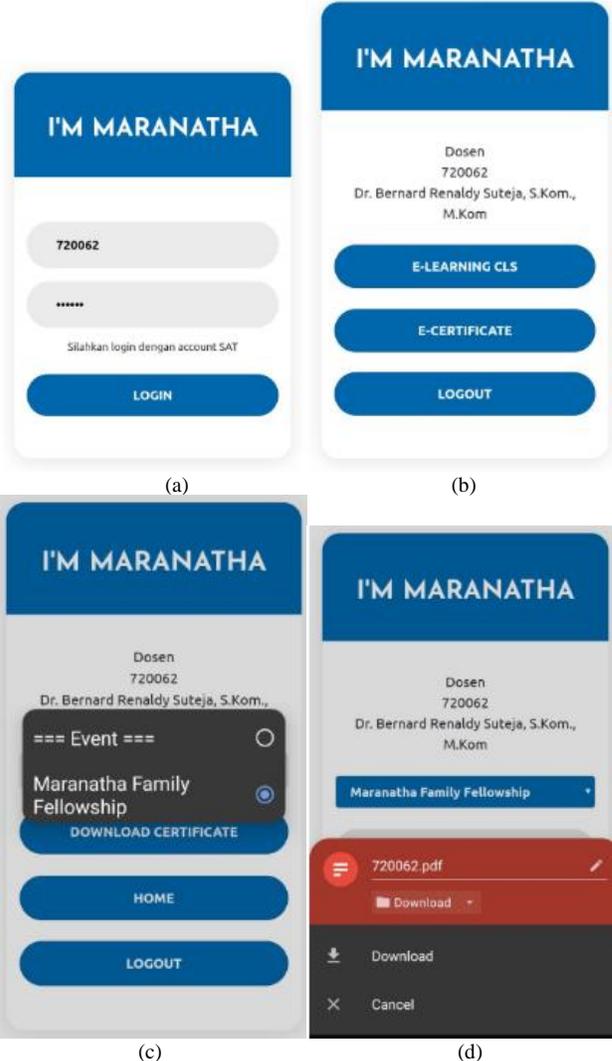


Figure 10. Order of user interface obtaining e-Certificate



Figure 11. Example e-Certificate

e-Certificate generated by this application (figure 11) has been through a good compression process so that it does not reduce the quality of both the image and the characters listed. E-Certificate generated through the application has a file size of less than 50Kb. The results of the e-certificate that has been downloaded as shown in Figure 10 can be tested for authenticity. Testing by scanning the QR Code with any QR Code reader application.

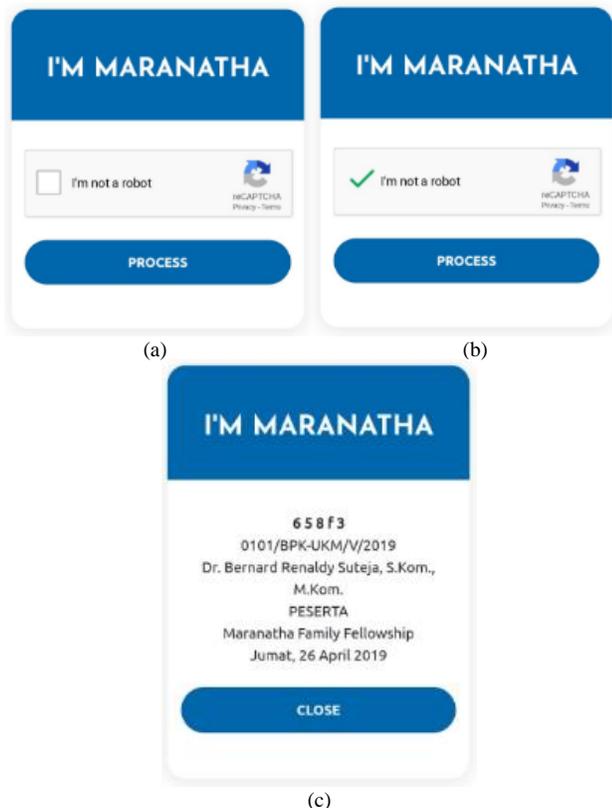


Figure 12. The sequence of the e-Certificate verification user interface

Testing e-Certificate is done by scanning the QR Code in the e-Certificate. By going through the verification stage, if the certificate does not match the key protection that has been included, the certificate is declared false.



Figure 13. The e-Certificate declared to be false

4. Conclusions

The e-Certificate system can be implemented into an application. The application can produce a secure e-Certificate with double protection in accordance with an event that is attended by a participant either a lecturer or a student of Maranatha Christian University. E-Certificates can be downloaded and printed for the requirements needed by participants. Testing the authenticity of e-Certificates can also be done well.

References

- [1] Nugraha, A. dan Mahardika A., Penerapan Tanda Tangan Elektronik pada Sistem Elektronik Pemerintahan Guna Mendukung *E-Government*. Seminar Nasional Sistem Informasi, 2016.
- [2] Angel Firstia Kresna, LEGALITAS TANDA TANGAN ELEKTRONIK PEJABAT DALAM RANGKA MENDUKUNG E-GOVERNMENT, <https://www.mahkamahagung.go.id/artikel/3737/legalitas-tanda-tangan-elektronik-pejabat-dalam-rangka-mendukung-e-government>, diakses Senin, 4 November 2019 13:03 WIB
- [3] Bank Indonesia, QRIS, Satu QR Code untuk Semua Pembayaran, https://www.bi.go.id/ruang-media/siaran-pers/Pages/SP_216219.aspx, diakses Selasa, 5 November 2019 10:50 WIB
- [4] Ching-yin law, Simon so. QR Codes in Education, *Journal of Educationan Technology Development and Exchange*, 3(1), 85-100
- [5] Bernard Renaldy Suteja, PENCARIAN CONTENT PORTAL WEB BERITA DENGAN TEKNIK SINDIKASI BERBASIS AJAX-SOAP WEB SERVICE, *Journal Compiler STTA vol 7 no 1*. Issn 2252-3839, <http://dx.doi.org/10.28989/compiler.v7i1.261>
- [6] Ariadi. Penerapan Aplikasi QR Code Reader dan QR Code Generator Secara Mobile Untuk mengelola Benda Cagar Budaya Kota Salatiga, *Jurnal sistem Informasi* 2010 p-ISSN: 1979-0767.