

CERTIFICACIÓN DIGITAL CON QR </>

<center>

<div id="imagen">

Certificados ENTREGADOS

En Investigación

<?php echo \$nombres?> <?php e

CODICIÓN 1 QR 1 ACCIÓN

ACTIVO

</center>

</body>

</html>

<?php

ACTIVO

require_once 'dompdf/autoload.inc.p

use Dompdf\Dompdf

\$dompdf = new DOMPDF();

\$dompdf->set_paper ('a4','landscape

\$dompdf->load_html(ob_get_clean());

\$dompdf->render();

\$pdf = \$dompdf->output();

\$dompdf->stream('certificado.pdf'

?>

CERTIFICATION DIGITAL WITH QR

Gianmarco Garcia Curo

Lima - 2022



DIGITAL CERTIFICATION WITH QR

© Gianmarco Garcia Curo
Address: Jr. La Mar N° 127, Huancayo – Junín, Peru
gianmarco.garcia.c@gmail.com
Tel. contact: +51 925 622 439

Edited by:

© Professionals On Line SAC. (FEPOL) - Editorial Fund.
Address: Av. La Marina No: 2900, San Miguel – Lima, Peru
professionalsonline.net@gmail.com
Tel. mobile: +51 999 140 920
Website: <https://professionalsonline.net/>

Co-editor
National Library of Peru
Address: Av. De La Poesía 160, 15034 San Borja - Lima, Peru

First digital edition: August 2022
Digital book available at: <https://editorialfondo.com/>

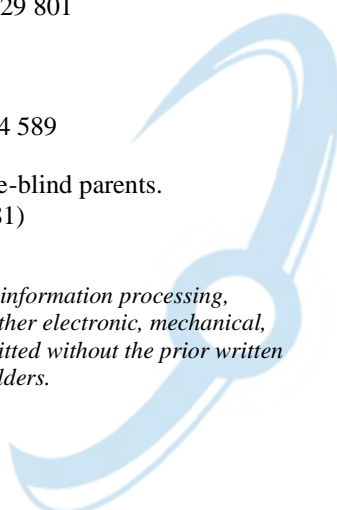
I made the Legal Deposit in the National Library of Peru N° 2022-08157
ISBN: 978-612-48981-4-3
DOI: <https://doi.org/10.47422/fepol.6>

Style correction: Luis Pablo Diaz Tito
luisp.diaz@upsjb.edu.pe / Tel. contact: +51 955 129 801

Design and Diagramming: "image" graphics
Manuel Enrique Sampen Antonio
sampen25@gmail.com / Tel. contact: +51 990 064 589

Book result of research and with review by double-blind parents.
Publishing stamp: Fondo Editorial (978-612-48981)

*The total or partial reproduction of this book, its information processing,
transmission in any other form or by any means, whether electronic, mechanical,
photocopying, recording or other methods, is not permitted without the prior written
permission of the copyright holders.*



CONTENT

SUMMARY

INTRODUCTION

CHAPTER I

General aspects of digital certificates.

CHAPTER II

QR codes.

CHAPTER III

Resources and development of the digital certificate generation software.

CHAPTER IV

Accessibility and validation of digital certificates.

CHAPTER V

Legal support in Peru.

CONCLUSIONS

RECOMMENDATIONS

BIBLIOGRAPHICAL REFERENCES



Gianmarco Garcia Curo

National University of Huancavelica



THANK YOU

*I thank God and my mother, for allowing
me to continue publishing continuously and
to contribute to passionate readers in
general.*

Gianmarco Garcia Curo



SUMMARY

The certification attributes to a user having fulfilled a designation, course or having satisfactorily completed a certain activity; however, over the years its physical version is being displaced by digital certificates, positioning itself as an excellent alternative.

The digital certification itself must have identifiers that allow you to verify its originality; however, embedding the QR verification gives it an added value, access with this type of identifier simplifies the originality verification process, since it can be accessed from any device with a QR reader. The system for issuing digital certificates is a web system, given its accessibility characteristics, for its development, a set of tools and the application of a methodology are necessary to guarantee the fulfillment of requirements that an entity establishes for its own system of issuing certificates. Regulating the issuance of certificates is important, the large number of providers allows a higher rate of falsifications, therefore in Peru the Law and Regulation of Digital Signatures and Certificates was

promulgated which has the objective of guaranteeing the authentication and in turn the integrity of digital certificates.

Keywords:Digital certificates, QR code, Accessibility, Certification system.



INTRODUCTION

This manuscript provides general information on digital certificates with QR code embedding. The relevance and massification of this type of certificate began with the appearance of COVID 19. The versatility that they have in their various presentations has allowed state and private institutions to facilitate their certification process in Peru and the world, validating users who are participants in their different events or activities.

The physical certificates, were susceptible to falsifications continuously, and the process to verify the originality in turn complex to realize; however, digital certificates contain identifiers on the web, allowing the originality verification process to be simplified and fast.

The embedding of the QR code has allowed access to digital certificates from various devices, facilitating the availability of verification of originality.

The manuscript unfolds in 5 chapters, which are detailed below:
Chapter I: Generalities of digital certificates, concepts, classification and detailed information on the subject are presented.

Chapter II: Generalities of QR codes are presented, related to the investigation detailing relevant aspects.

Chapter III: The resources for the development of the digital certification system are presented.

Chapter IV: Information is presented on the accessibility of digital certificates and how they are validated.

Chapter V: Legal aspects are presented that allow the validity of digital certificates in Peru.





CHAPTER I

Context of visual impairment around learning





Definition of digital certificates

According to law N° 27269, digital signatures and certificates law, it defines the digital certificate as "the electronic document generated and digitally signed by a certification entity, which links a pair of keys with a person confirming their identity" (p. 187). It uses information and communication technologies with the levels of information that officials have for the implementation of the digital certificate and allows the reduction of bureaucratic barriers.

Types of certificates

- a. Certificates of authority: Root certificate issuing entities have the ability to assign certificates to certificates of authority. They correspond to entities that certify. The root certificates are the only self-signed ones.
- b. Server certificates: Certifies that a server is from the company it claims to be and that the server identifier is correct. Server certificates identify servers that participate in secure communications with other computers through the use of communications protocols. These certificates allow the server to prove its identity to clients.
- c. Personal certificates: Personal certificates ensure that an email address and public key correspond to a person. These

certificates identify people and can be used to authenticate users with a server.

- d. Certificates of software producers: They are used to "sign" the software and ensure that it has not been modified. This does not imply that it can be executed safely, but it informs the user that the software manufacturer participates in the infrastructure of companies and entities issuing trust certificates. These certificates are used to sign the software that is distributed over the Internet.

Components of a certificate

- a. Version: Contains the version number of the coded certificate.
- b. Serial number: It is an integer assigned by the certifying authority. Each certificate issued by a CA must have a unique serial number.
- c. Signing algorithm identifier: Identifies the algorithm used to sign the certificate.
- d. Issuer number: Identifies the CA that signed and issued the certificate.
- e. Validity period: Indicates the period of time during which the certificate is valid. Number of the subject. Identifies the user number for which the certificate is issued.

- f. Number of the subject: Indicates the number of the user for whom the certificate is issued.
- g. Public key information of the subject
- h. Issuer's unique identifier: Information on the user's public key for which the certificate is issued (number, algorithm, etc.).
- i. Unique identifier of the subject: It is an optional field that allows reuse of subject numbers.
- j. Extensions: Other fields specific to each protocol that are subject to their own regulations.

Certificate properties

a. Authentication

For the recipient of a document, authentication involves ensuring that the data received has been sent by whoever declares to be the owner of the identity contained in the digital signature. Asymmetric key authentication allows a message encrypted with a private key to only be sent by its owner.

b. Confidentiality

Confidentiality means ensuring that the information sent cannot be intercepted by third parties. To achieve confidentiality, the sender (emitter) of a message must encrypt it with the recipient's (receiver) public key, which can

be obtained from their Digital Certificate. In this way, the sender ensures that the message can only be decrypted with the receiver's private key, that is, it can only be read by the recipient.

c. Integrity

The integrity of the documents involves both the sender and the recipient ensuring that the information sent will not be modified by third parties. To guarantee integrity, the sender applies a hash algorithm before sending a message. In this way, when sending a message, the sender sends the encrypted hashing result together with the original message. When the recipient receives the message, it recalculates the hashing of the message and compares it if it is equal to the hashing received, to check if the message has not been modified.

d. Privacy

The privacy of the messages implies that the data can only be read by the recipient because they contain encrypted elements.

e. I do not repudiate

The non-repudiation implies for the receiver of a message to ensure that the sender will not deny having sent the information received. Also as a direct consequence of the digital signature concept, the mere existence of the message "signed" by its private key, once its integrity has been verified, prevents the sender from repudiating the message, since it could not have been generated in another way. The recipient keeps the signed document as proof of the operation.



CHAPTER II

QR codes



QR code

It is the acronym for Quick Response. A QR code is a two-dimensional bar code that must be read by QR code readers (such as cell phone cameras). They are similar to the barcodes used in inventories and in products sold at retail, with the exception that they can contain more information. In fact, QR codes can contain thousands of alphanumeric characters (up to 4000 characters in a single code), making them very useful for any organization. Generally, they consist of black squares arranged on a white background. However, the boxes can be different colors than black, and the background does not necessarily have to be white.

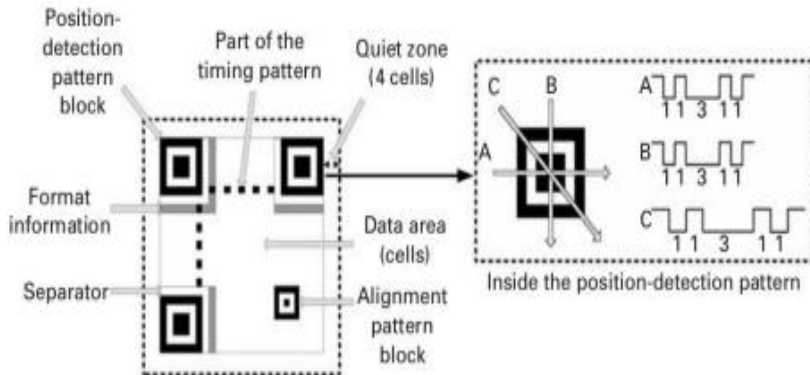
structure

The QR code consists of seven elements known as: search pattern, time pattern, alignment pattern, reserved area, format information, information area and separator.



Figure 1

Structure of the QR code



a. Search pattern

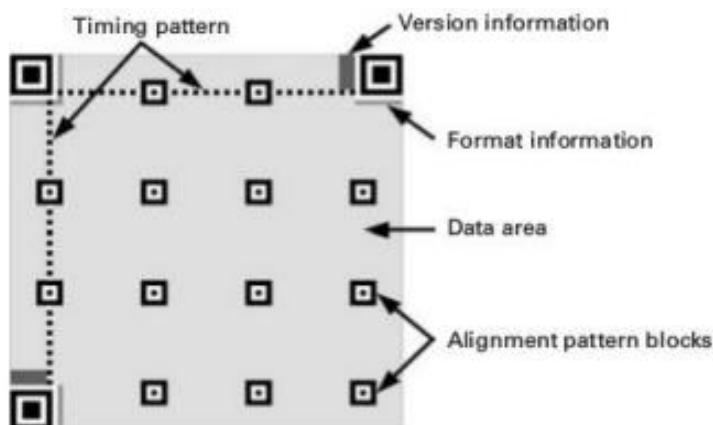
It is located in three corners (Illustration 2). When the code is scanned, these patterns are the first to be located by the reader (mobile device camera), which locates the position of the code very quickly. The radii of the white and black spaces in a line that crosses the center of the pattern are 1 : 1 : 3 : 1 : 1, at any angle. This set of radios allows the rapid detection of the three search patterns. Once the position of the code is found, the size L, the angle and the orientation are calculated from the position of the three search patterns. This allows the QR code to be read in any direction.

b. Time pattern

It consists of a pair of borders (horizontal and vertical) located between the search patterns (Illustration 3). These borders are used to calculate the centroid of each cell and modify it when distortions are found in the QR code or changes in the field of the cell.

Figure 2

time pattern



c. Alignment pattern

It allows the correction of any distortion. This is possible by determining the central coordinates of each alignment pattern and adjusting the centroids of the cells. The isolated black cell within each alignment pattern allows you to quickly calculate the center coordinate of the pattern.

d. Format information

It indicates the QR code version, the error correction level and the mask used for the QR code. In addition, this area is the first to be read in the decoding process.

e. Information area

This is where the original information and the Reed-Solomon code are encoded. The Reed-Solomon code is a mathematical error correction method initially developed for planetary probes and artificial satellites as a measure to mitigate noise in communications. It has the ability to make corrections at the byte level.

f. Reserved area

The QR code requires a reserved area or margin. This area allows the code to be distinguished from its background color, which produces an accurate reading quickly.

Error correction

The QR code has the ability to correct the error, restoring the original information if the code is dirty or damaged. Up to 30% of the code can be restored even if the QR code is damaged.

Figure 3

Correction of the QR error



Error correction is performed by applying the Reed Solomon code to the original data. There are four levels of error correction:

- L, about 7%
- M, about 15%
- Q, about 25%
- H, about 30%

The user can select this option according to their needs. The higher the error correction, the more the amount of information to be coded increases, which implies a larger QR code. Option M is the most used. The level of error correction must be chosen according to the amount of information that needs it. For example, for every 50 of 100 words (in code) that need correction, 100 words of Reed Solomon code are required. Therefore, the total number of words is 200. It means that 50

words (in code) of 200 can be corrected. This is a rate of 25% error correction in relation to the total number of words, which corresponds to the level of error correction Q.

Decoding

The decoding process consists of four steps:

- a. The search patterns are located, and the center of each one is calculated.

Figure 4

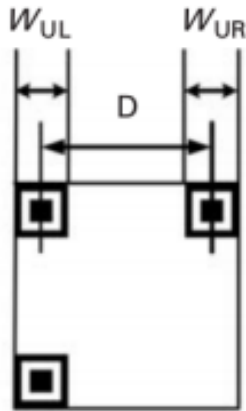
Localization of search patterns



- b. The size of the symbol module is determined by measuring W_{ul} and W_{ur} ; and the size of the symbol is determined by calculating the size of D .
- c.

Figure 5

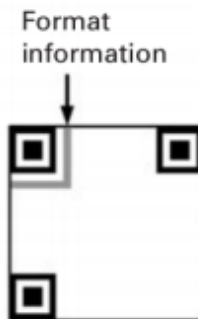
Module size calculation



- d. The format information is decoded and the level of error correction and the masking pattern to be used are defined.

Figure 6

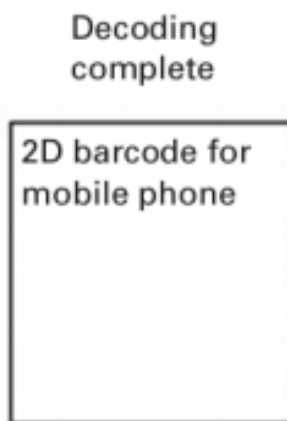
Format information



- e. The information block is detected and the words used for error correction are removed. The unprocessed information is decoded according to the defined error correction level and masking pattern. As a result, the flat text is obtained.

Figure 7

QR decoding



Encryption

It is the process by which a message in normal text or plaintext can be transformed into encrypted or coded text, which ensures that said text cannot be read without using an opposite process called decryption that results in the conversion of the encrypted text into text normal To carry out these processes, an encryption algorithm (mathematical function), encryption keys (encryption password) and the length of the key are required. This should be

used to achieve things like: protection of data transmitted through communication networks, so that they cannot be intercepted, read or manipulated; detect alterations that may occur in the data; verify the authenticity of a transaction, document or message; among others



CHAPTER III

Resources for the development of digital certificate generation software



The digital certification system is a web system given its accessibility characteristics, some basic tools are required for its development, for this it is necessary to consider the programming language, the database to be used to store the records, together they will allow the development of the system. Another important aspect to carry out development properly is to make use of a software development methodology, which will facilitate the process by organizing tasks and speeding up development, since fewer errors will be made when following a guide.

Methodology

They are a set of techniques and methods that applied together are applied to the design of software solutions, currently there are two large groups of methodologies, those of traditional development and agile ones.

Traditional methodology: Its main characteristic is its rigid process, which is specific to the inflexible development line, which does not allow changes to be included during the development process. Some of these methodologies are:

- Waterfall
- Spiral

Agile methodology: They are highly flexible and agile methodologies, it is incremental allowing in each cycle to add extra functionalities that the user needs to incorporate. Some methodologies are:

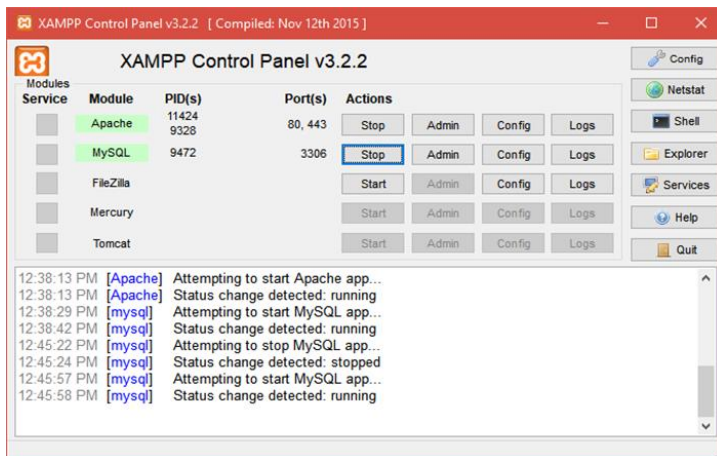
- Kanban
- Scrum
- Lean

CHAMPP

XAMPP is a platform-independent server, free software, which mainly consists of the MYSQL database management system, the Apache web server and interpreters for script languages: PHP and Perl.

Figure 8

CHAMPP

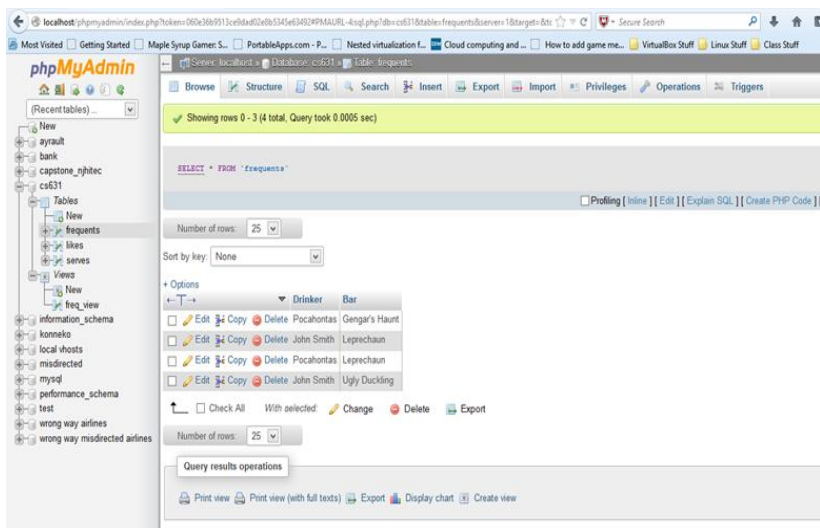


MySQL

MYSQL is a database management system (Database Management System, DBMS) for relational databases, so MYSQL is nothing more than an application that allows you to manage files called databases, as a relational database, it uses multiple tables to store and organize information. MYSQL was written in C and C++ and stands out for its great adaptation to different development environments, allowing its interaction with the most used programming languages such as PHP, Perl and Java and its integration in different operating systems.

Figure 9

PhpMyAdmin



ISO 25010

It is interpreted as the degree to which said product satisfies the requirements of its users, thereby providing value (ISO25010, 2019).

To determine quality, 8 characteristics will be determined:

1. Functional adaptation
2. Performance efficiency
3. Compatibility
4. Usability
5. Reliability
6. Security
7. Maintainability
8. Portability

For research purposes, only some of the 8 characteristics will be used, which are functionality, usability and compatibility.

Compatibility

The ability of the system to exchange information with other systems or between its own components when it shares the same hardware and software environment. This feature is divided into two:

- Coexistence Ability to coexist with other different software in the same environment, sharing resources.
- Interoperability Ability to exchange information between systems and make use of the information exchanged.

Usability

Ability of the software to be understood, used and be attractive to the user when used in certain conditions. It is subdivided into other characteristics:

- Ability to recognize its adequacy. Ability to recognize if the product is suitable for the type of user and their needs.
- Learning capacity. Ability that allows the user to learn how to use it.
- Ability to be used. Capacity of the product that allows the user to handle and use it with ease.
- Protection against user errors. Capability that protects the user from making mistakes.
- Aesthetics of the user interface. Ability to please and satisfy an adequate interaction with the user.
- Accessibility Capacity that allows the product to be used by users with specific characteristics.

Reliability

Capacity of the product to perform its function when put into use. This feature is subdivided into 4 features:

- **Maturity** Ability to satisfy reliably under normal conditions.
- **Availability** Capacity of the system to be operative and available for use when required.
- **Fault tolerance.** Ability of the system to continue running in the presence of hardware or software failures.
- **Recovery capacity.** Ability to recover and restore the state of the system in case of interruption or failure.

Web programming languages

Definition

These are languages that are assimilated directly by the browser and do not need pre-treatment. Web programming languages have been emerging according to the needs of the platforms, trying to facilitate the work of application developers. They are classified into client-side languages and server-side languages.

PHP

PHP is a recursive acronym for "PHP: Hypertext Preprocessor", originally Personal Home Page, is a free interpreted language, originally used only for the development of present applications that will act on the server side, capable of generating dynamic

content in the World Wide Web. It is among the first possible languages for insertion into HTML documents, dispensing in many cases the use of external files for eventual data processing. The code is interpreted on the server side by the PHP module, which also generates the web page to be displayed on the client side. The language evolved, went on to offer functionalities in the command line, and also gained additional characteristics, which made possible additional uses of PHP.

HTML

Since the rise of the Internet, websites have been published thanks to the HTML language. It is a static language for the development of websites (acronym in English for HyperText Markup Language, in Spanish Lenguaje de Marcas Hipertextuales). Developed by the World Wide Web Consortium (W3C). Files can have extensions (htm, html).

JavaScript

This is an interpreted language, it does not require compilation. It was created by Brendan Eich in the company Netscape Communications. Mainly used in web pages. It is similar to Java, although it is not an object-oriented language, it does not have inheritance. Most browsers in their latest versions interpret Javascript code.

The Javascript code can be integrated within our web pages. To avoid incompatibilities the World Wide Web Consortium (W3C) designed a standard called DOM (in English Document Object Model, in its Spanish translation Modelo de Objetos del Documento).

Ajax

Acronyms in English "Asynchronous JavaScript and XML". It is a set of new techniques, which involve various old technologies such as JavaScript, XML, Document Object Model (DOM), which allows the client to communicate with the server through this request, which is made in the background, without reloading the page, effectively and efficiently combining client-side technology with server-side technology and enhancing communication.

CSS

Its acronym in English comes from Cascading Style Sheets (CSS), they are blocks of code in the XML or XHTML language that are responsible for separating within the HTML document the logical style from the physical style, the logical style being the structure of the document and the physical style its final aspect. Style sheets allow you to redefine the rules for presenting a web page.

Terms on digital certificates with QR

The definition of terms will clarify the key terms presented.

Digital certificate:The Digital Certificate is a digital document that guarantees and allows people to be identified on the Internet.

QR code:Combination of bars and boxes that accompanies a product or unit of consumption so that it can be read and deciphered by means of an optical reader that transmits the data to a machine or a computer.

Verification of originality:It is the act of confirming that a document or creation is original.

Methodology:Set of rational procedures used to reach the objective or the range of objectives that governs a scientific investigation.



CHAPTER IV

Resources for the development of digital certificate generation software



Accessibility

The accessibility of digital certificates is one of the characteristics that give it added value, allowing both users and providers of the certificates to access them in real time, as well as being able to acquire them again and again, since the original document is stored in Internet. To access these in real time it is necessary:

Cell phone, computer or access point: You must have the one that has the technology to access the internet.

Electronic Intermediation System. - It is the WEB system that allows the transmission and storage of information, guaranteeing the non-repudiation, confidentiality and integrity of transactions through the use of electronic signature components, authentication and secure channels.

WEB System ("World Wide Web"): System of electronic documents linked and accessible via the Internet. Using a Web browser, a user views Web pages that may contain text, images, videos or other multimedia content, and navigates through them using hyperlinks.

Verification

Although the certificate itself, whether in its digital or physical format, allows you to verify certain data and credentials, at first sight they can be falsified for malicious purposes, corrupting its integrity. In order to verify originality, the following are considered:

Serial Number: It is the whole assigned by the certifying authority. Each certificate has a unique and unrepeatable number for the type of certificate provided by the provider.

QR code: It has a unique identifier that on the web directs to the location of the digital certificate, in which the same characteristics of the certificate that is verified must be seen, if the information does not match, it would be a falsification of the same.



CHAPTER V

Legal support in Peru



Digital certification has gone from being a trend to becoming a widely accepted document in both state and private entities. The certificates issued are unique for each user; however, the mass issue of these allows criminals to carry out counterfeiting for business or personal purposes, this is a serious problem that must be faced.

The regularization is necessary to avoid fraud and in turn to give validity to this type of certificate, the Peruvian State has promulgated Law No. 27269 of Firms of Digital Certificates and the Regulation of the Law of Firms and Digital Certificates (2008) which establish clear parameters that must be considered for a certificate to be recognized as original.

The actors in this process are not only the organizations that provide the certification, the receiving user must adhere to aspects of the law.

Some relevant aspects according to Law No. 27269 on Digital Certificate Signatures and the Regulation of the Digital Signature and Certificate Law (2008) are:

Purpose of the digital signatures and certificates law

The purpose of the law is to regulate the use of the digital signature which has the same validity and effectiveness as a handwritten signature, if this is attached to any electronic

document there is already a link with the signatory, therefore, entity authentication must be guaranteed of these documents.

Digital signature

Article 3.-Digital signature The digital signature is that electronic signature that uses an asymmetric cryptography technique, based on the use of a unique pair of keys; associated with a private key and a public key mathematically related to each other, in such a way that people who know the public key cannot derive the private key from it.

From the owner of the firm

Article 4.-Holder of the digital signature The holder of the digital signature is the person to whom a digital certificate containing a digital signature is exclusively attributed, identifying him objectively in relation to the data message.

Article 5.-Obligations of the holder of the digital signature The holder of the digital signature has the obligation to provide the certification bodies and the third parties with whom it relates through the use of the digital signature, accurate and complete declarations or material manifestations.

Of digital certificates

Article 6.-Digital certificate The digital certificate is the electronic document generated and digitally signed by a

certification entity, which links a pair of keys to a specific person confirming their identity. Article 7.- Content of the digital certificate The digital certificates issued by the certification entities must contain at least:

1. Data that undoubtedly identify the subscriber.
2. Data that identify the Certification Body.
3. The public key.
4. The methodology to verify the subscriber's digital signature imposed on a data message.
5. Serial number of the certificate.
6. Validity of the certificate.
7. Digital signature of the Certification Body.

Article 8.-Confidentiality of information The registration entity will collect the personal data of the applicant for the digital signature directly from him and for the purposes indicated in this law. Likewise, information relating to private keys and data that are not subject to certification is kept under the corresponding reserve. It can only be lifted by court order or express request of the subscriber of the digital signature.

Article 9.-Cancellation of the digital certificate The cancellation of the digital certificate can be:

1. At the request of the holder of the digital signature.

2. Fear of revocation by the certifying entity.
3. By expiration of the validity period.
4. For cessation of operations of the Certification Body.

Article 10.-Revocation of the digital certificate The Certification Body will revoke the digital certificate in the following cases:

1. It is determined that the information contained in the digital certificate is inaccurate or has been modified.
2. By death of the holder of the digital signature.
3. For non-compliance arising from the contractual relationship with the Certification Body.

Article 11.-Digital Signature Certificates issued by Foreign Entities will have the same validity and legal effectiveness recognized in this Law, provided that such certificates are recognized by the competent administrative authority.

Certifying entity

Article 12.-Certification Body The Certification Body fulfills the function of issuing or canceling digital certificates, as well as providing other services inherent to the certificate itself or those that provide security to the certificate system in particular or electronic commerce in general. Certification Entities may

also assume the functions of Registration or Verification Entities.

Article 13.-Registration or Verification Entity The Registration or Verification Entity fulfills the function of collecting data and verifying the information of a digital certificate applicant; identification and authentication of the digital signature subscriber; acceptance and authorization of requests to issue digital certificates; acceptance and authorization of requests to cancel digital certificates.

Article 14.-Deposit of Digital Certificates Each Certification Entity must have a permanently available Registry, which will be used to verify the public key of a given certificate and cannot be used for purposes other than those stipulated in this law. The Registry will have a section referring to the digital certificates that have been issued and will list the circumstances that affect the cancellation or validity of them, and must include the date and time of start and date and time of completion. This Register can be accessed by electronic means and its content will be available to those who request it.

Article 15.- Registration of Certification and Registration or Verification Entities The Executive Power, by Supreme Decree, will determine the competent administrative authority and will

indicate its functions and powers. The competent authority will be in charge of the Registry of Certification Entities and Registration or Verification Entities, which must comply with international technical standards. The data contained in the aforementioned Registry must mainly fulfill the function of identifying the Certification Entities and Registration or Verification Entities. “Article 15-A.- Regime of Infractions and Sanctions The competent administrative authority has the power to classify infractions for non-compliance with the provisions of Law 27269, Law of Digital Signatures and Certificates, its Regulations and the Accreditation Guides of the Authority Competent Administrative. The competent authority may impose the following sanctions:

1. Fine, up to a maximum amount of fifty (50) UIT.
2. Temporary suspension of accreditation.
3. Accreditation cancellation.

The infractions will be established as minor, serious and very serious; and the determination of the sanction will be established taking into account criteria of proportionality. In the case of very serious infractions, the competent authority may additionally order disqualification for up to ten (10) years to request accreditation again as a certification entity, data registration or

verification entity, provider of value-added services or as an entity of digital signature software. The competent authority will approve the corresponding regulation of infractions and sanctions that includes the typification of administrative infractions, the sanctioning administrative procedure and the corresponding scale of sanctions.”

Regulation of the law of digital signatures and certificates

Article 12.- Requirements To obtain a digital certificate, the applicant must prove the following:

- a) In the case of natural persons, have full capacity to exercise their civil rights.
- b) In the case of legal persons, prove the existence of the legal person and its validity through public instruments or the respective legal norm, and must have a duly accredited representative for such purposes.

Article 13.- Of the additional specifications to be the owner To be the owner of a digital certificate, additionally, the information requested by the Registration or Verification Entity must be delivered, in accordance with the provisions of the corresponding Certification Entity, the owner assuming responsibility for the veracity and accuracy of the information provided, without prejudice to the respective verification. In the

case of natural persons, the request for the digital certificate and the registration or verification of their identity are strictly personal. The requesting natural person will become the holder and subscriber of the digital certificate.

Article 15.- Of the obligations of the holder The obligations of the holder are:

- a) Deliver truthful information during the request for the issuance of certificates and other certification processes (cancellation, suspension, re-issuance and modification).
- b) Update the information provided both to the Certification Entity and to the Registration or Verification Entity, assuming responsibility for its veracity and accuracy.
- c) Request the cancellation of your digital certificate in case the reserve on the private key has been compromised, under the responsibility.
- d) Permanently comply with the conditions established by the Certifying Entity for the use of the certificate.

Article 16.- Content and validity The certificates issued within the Official Electronic Signature Infrastructure must contain at least, in addition to what is established in article 7 of the Law, the following:

- a) For natural persons:

- * Complete names
- * Official identity document number
- * Document type

b) For legal entities:

- * Business name
- * Unique Taxpayer Registry Number (RUC)
- * Full names of the subscriber
- * Subscriber's official identity document number
- * Document type of the subscriber

The Certification Entity may include, without distinction, at the request of the applicant for the certificate, the official email address of the subscriber, the official email address of the legal person or the email address of the applicant. Likewise, it may include additional information as long as the Registration or Verification Entity reliably verifies its veracity. The period of validity of the digital certificates begins and ends on the dates indicated therein, except in the event of cancellation in accordance with the provisions of article 17 of this Regulation.”

Conclusions

Digital certificates are a viable alternative for any entity that requires providing them to its users; traditionally these require an extensive process for their dispatch and have a tendency to be falsified, given their characteristics and tedious way of verifying originality. The digital alternative is an option that replaces the traditional physical certification, providing continuous accessibility and facilitating the way to verify originality



Recommendations

It is recommended to progressively replace traditional certification and migrate to digital certification, digitalization provides benefits to both users and suppliers, allowing processes to be simplified and automated.

It is necessary to have knowledge of some rules that allow to regulate the certification process, as well as define the structure that will be handled at the organizational level, achieving the differentiation and recognition of the organization.

It is recommended to have a backup of the digital certificates, given their storage on the web, having a backup will allow you not to lose the files and avoid future accessibility problems.



References

- Official Diario del Bicentenario El Peruano. (2008). The Peruvian
Obtained from <https://diariooficial.elperuano.pe/pdf/0030/ley-27269.pdf>
- Bravo Carranza, LA, & Aguilar Arboleda, GH (2019). Certificate
issuance module with QR code and debugging of the web
system for tracking the activities of the interns of the Law
Office of the Faculty of Jurisprudence of the University of
Guayaquil. Institutional Repository of the University of
Guayaquil. Retrieved from
<http://repositorio.ug.edu.ec/handle/redug/39743>
- Date C, C. (sf). Introduction to data systems. Ed. Pearson.
- Espino Canelo, JA (2018). Web application to improve the
management of the supply warehouse in San Fernando SAC
Thesis, Universidad Inca Garcilzo de la Vega. Obtained from
<http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/3320/TESIS-JESUS%20ALBERTO%20ESPINO%20CANELO.pdf?sequence=2&isAllowed=y>
- Gabaldón, LG, & Pereira, W. (2008). Identity theft and digital
certification: proposals for the control of electronic fraud.

Sociologías, 20. doi:<https://doi.org/10.1590/S1517-45222008000200008>

Gamboa Cruzado, J., Comun Manrique, U., & Bruno Luciani, I. (2016). Development of an information system, based on the RUP methodology, to improve the registration process at the Von Humboldt del Sur school. Autonomous University of Peru. Autonomous University of Peru. Obtained from <http://repositorio.autonoma.edu.pe/handle/AUTONOMA/149>

Jayo Cusipoma, H. (2019). Web information system to optimize the management of hermeticity inspection certificates of the Hertig company, Lima - 2019. Universidad Científica del Sur. Obtained from [https://repositorio.cientifica.edu.pe/bitstream/handle/20.500.12805/852/TB-](https://repositorio.cientifica.edu.pe/bitstream/handle/20.500.12805/852/TB-Herica%20J%28Restringido%29.pdf?sequence=1&isAllowed=y)

[Herica%20J%28Restringido%29.pdf?sequence=1&isAllowed=y](https://repositorio.cientifica.edu.pe/bitstream/handle/20.500.12805/852/TB-Herica%20J%28Restringido%29.pdf?sequence=1&isAllowed=y)

Munevar Bejarano, FA, & Chavarro Muñoz, JK (2018). Web document validation system by scanning QR codes using mobile devices. Francisco José de Caldas District University. Retrieved from <https://repository.udistrital.edu.co/bitstream/handle/11349/14196/ChavarroMu%c3%bl%20JohnKenedy2018.pdf?sequence=1&isAllowed=y>

Rivas Lara, AE (sf). Influence of the use of the digital certificate in the business formalization process in the District Municipality of Pítipo - Ferreñafe in 2020. University of Lambayeque. Obtained from https://repositorio.udl.edu.pe/bitstream/UDL/408/1/RivasLara_Tesis%20IC.pdf

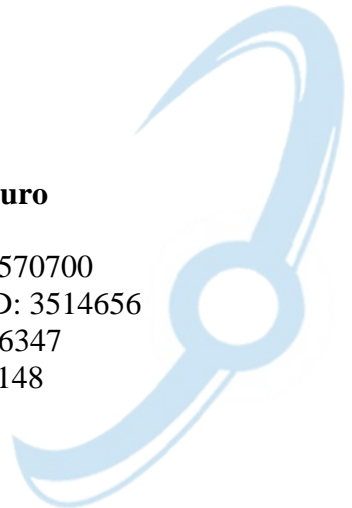
Sandoval Medrano, HA, & Sandoval Medrano, GB (2015). Analysis and design of a JavaScript Framework based on W3C standards for the front-end implementation of Juliaca.com. Andean University Néstor Cáceres Velásquez. Andean University Néstor Cáceres Velásquez. Obtained from <http://repositorio.uancv.edu.pe/bitstream/handle/UANCV/747/TESIS%2041440198%20%26%2002549288.pdf?sequence=3&isAllowed=y>



DIGITAL CERTIFICATION WITH QR

Gianmarco Garcia Curo

Scopus Author ID: 57290570700
Web of Science Researcher ID: 3514656
Dialnet Author ID: 5436347
Code Renacyt: P0224148



Estudiantes

Eventos

Certificado

Soporte

Activa Certificados 0✓

Reportes

Cerrar sesión

```
<center>
```

```
<div id="imagen">
```

Certificados ENTREGADOS

En Investigación

```
<?php echo $nombres?> <?php echo
```

```

```

CODIFICIÓN ↑

QR

ACCIÓN

ACTIVO

```
</center>
```

```
</body>
```

```
</html>
```

```
<?php
```

ACTIVO

Professionals Online S.A.C.

```
require_once('vendor/autoload.inc.php');
```

```
use Dompdf\Dompdf;
```

```
$dompdf = new Dompdf();
```

```
$dompdf->set_paper('a4', 'landscape');
```

```
$dompdf->load_html(ob_get_clean());
```

```
$dompdf->render();
```

```
$pdf = $dompdf->output();
```

ACTIVO

```
$dompdf->stream('certificado.pdf');
```

CERTIFICACIÓN DIGITAL CON QR