DEVELOPMENT OF A TIMESTAMPING WEB APPLICATION FOR THE ELECTRONIC FACTORING PROCESS IN ECUADOR

[1]JESUS MENDOZA MACIAS, [1,2]SANG GUUN YOO

[1]Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE,

Av. General Rumiñahui s/n, Sangolquí, Ecuador

[2]Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional,

Ladrón de Guevara, E11-253, Quito, Ecuador

E-mail: [1]jimendoza@espe.edu.ec, [1]yysang@espe.edu.ec, [2]sang.yoo@epn.edu.ec

ABSTRACT

This document describes the experience in developing a Timestamping application for the Electronic Factoring process in Ecuador which executes the process of electronic signing of documents in XML format with timestamp. The need of this application has its origin in an Electronic Factoring platform developed by the company BIGDATA CA, where it was sought to have a mechanism that allows to guarantee the integrity and validity of the information over time of certain documents generated by the system. The UWE methodology was used for its approach to processes, obtaining requirements, and support with CASE tools that provide support for the treatment of the same, allowing to develop applications of better quality. The use of electronic signatures in conjunction with timestamps allowed greater legal validity and integrity to the information contained in the signed documents, so that they can be used in judicial proceedings or to avoid alteration of the same, the use of these Two mechanisms contributed to give greater security and agility to the process of Electronic Factoring, since the process of signing now is done in an entirely online environment and not in a manual way as it was being done.

Keywords: *Timestamping, UWE, Factoring, XML, Security.*

1. INTRODUCTION

The use of information technology has grown enormously in recent years in the world and it plays more important role in the society each day. One of the most important milestones related to information technologies in Ecuador is the use of electronic signature certificates, which guarantee the validity of the identity of a person, organization, or machine [1]. One of most important applications of electronic signature certificates in Ecuador is the electronic billing, which has been implemented extensively until it has almost completely replaced the traditional billing based on physical invoices [2]. The use of electronic signature certificates is not limited to the electronic invoicing process alone; it also can be applied to the signature of e-mails and digital documents (e.g. PDF, text files, spreadsheets) to guarantee their authenticity/integrity and to allow a non-repudiation mechanism [3][18].

An additional feature that can be added to the electronic signature to make more reliable and secure is timestamping. Timestamping allows to prove that a set of data existed before the time of the sealing and that they have not been modified since then [4] [5]. The timestamp becomes necessary since the electronic signature does not provide the way to check the integrity of the time when a document was signed. This is because the date of the computer or server of the signer could be altered. In this situation, it would be advisable that the timestamp process from a reliable source form part of the signature process. Such reliable source could be the Timestamping Authority (TSA) [6]. It is important to mention that the timestamps have been used in other applications such as secure communication protocols [7] [8] [9] to make sure the time of creation of a specific data.

In this document, we describe our experience in developing a Timestamping web application for the Electronic Factoring process in Ecuador. The proposed timestamping application allows to sign electronically XML documents and add a timestamp provided by a TSA. The proposed solution seeks to answer the following questions: What limitations exist when using only the electronic signature alone? What advantages does timestamps offer in the electronic signature process? Is it possible to use the documents with electronic signature and timestamp as evidence for judicial processes?

To respond the aforementioned questions, the present solution was applied in a real company in Ecuador called BIGDATA CA, which has an online Electronic Factoring platform that allows suppliers to prepay their invoices in exchange for a discount percentage applied to them and obtaining immediate liquidity without affecting the customer-supplier relationship [10] [11].

The rest of the article is structured as follows. Section 2 and 3 describes the theoretical concepts used along the present paper and development methodology used for de creation of the web application, respectively. Then, Section 4 describes the justification and importance of the present work. Later, Section 5 describes the development of the web application of timestamping, as well as the adaptation of the process of signing and timestamp in the Electronic Factoring process of the company BIGDATA C.A. Then, Section 6 and 7 describes the used development tools and obtained results. Finally, section 8 presents the conclusions of the results obtained and future works.

2. THEORETICAL BACKGROUND

2.1 Electronic Factoring

Factoring is a financial transaction and a type of debtor finance in which a business sells its accounts receivable (i.e., invoices) to a third party at a discount [11]. Electronic Factoring is a modality of conventional factoring, in which, electronic invoices are used instead of physical invoices. The actors involved in an electronic factoring process are the following:

- **Seller (company issuing the invoice):** The person or entity that uploads the invoice to the system to be sold.
- **Confirmer (debtor of the invoice):** The person or entity who confirms his/her willingness to pay the invoice that have been loaded by the seller.
- **Buyer (company buying the invoice):** The person or entity that purchases the uploaded invoice with a considerable discount.

2.2 Timestamping

Timestamping is a mechanism used to guarantee that the information has not been modified from the moment when the stamp was generated [12]. The timestamping service is requested to a Time Stamping Authority (TSA) by sending a summary (hash) of the information to be stamped. This service become necessary because electronic documents need to be preserved for long period of time due to legal requirements, and they also require a proof of no-modification of their content from a date they have been signed [13].

3. METHODOLOGY: UML-BASED WEB ENGINEERING

UML-based Web Engineering (UWE) is a methodology for the development of web applications and it is founded on Unified Process [15] and UML. This is characterized to be an object oriented, iterative and incremental methodology [15]. The UWE design strategy is based on models that are constructed during the analysis phase being the most important the conceptual and process models [16].

This methodology was chosen for this paper taking into account the results obtained by Maria Escalona and Nora Koch in a comparative study of web development methodologies such as: WSDM, W2000, RNA, NDT, UWA, among others [17]. Such paper indicates that UWE stands out mainly for its process orientation, obtaining of requirements, and CASE tools support allowing development of applications of better quality.

UWE uses UML notations and its method consists of five main models i.e. Requirements, Content, Navigation, Presentation and Processes models. Each of those models are developed in a different scenario during the software development process [17].

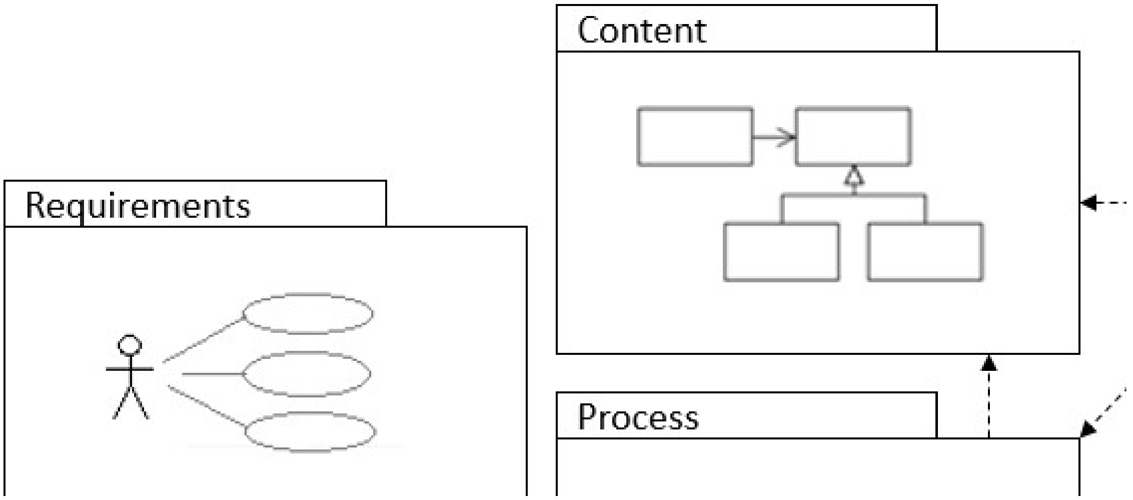


Figure 1: Main Models of the UWE Methodology

4. RELATED WORKS AND JUSTIFICATION OF THE PRESENT WORK

Currently, the Electronic Factoring system developed by the company BIGDATA CA does not have a security mechanism that guarantees the integrity of the documents generated in the Factoring process. This situation can undoubtedly generate complications in cases where such documents have to be used as evidence in judicial proceedings. This is the reason why the Company has seen the need to provide an Electronic Factoring System with greater confidence and legal security.

For the reason stated above, the Company has decided to incorporate the use of electronic signatures and timestamps for the signing process to provide greater legal security to the documents. This solution will ensure the non-repudiation of the generated documents and at the same time ensure the date and time of its creation/modification by using the timestamp obtained from reliable source i.e. Time Stamping Authority (TSA).

Generally, the timestamping service is contracted through a TSA, however there are other interesting alternatives, such as the one proposed by Yuefei Gao and Hajime Nobuhara in their project called "A Decentralized Trusted Timestamping Based on Blockchains" [19]. In such work, the authors provide a timestamping system in a decentralized way, to guarantee the integrity and reliability of the information.

There are also other previous works with improvements to the use of the timestamp service, such as that proposed by Stavrou and Voas [20], who propose a decentralized time stamp consumption solution, based on usage of multiple TSAs and digital cryptocurrency systems (blockchain), in order to mitigate possible risks related to the consumption of time stamps. However, these improvements are not totally viable, because, although the use of blockchain protocols has the advantage of having multiple parts for validation of time stamps, this represents a high computational cost and requires numerous network interactions. In addition, there is no direct incentive for mutually reliable independent parties to cooperate with each other, which has undoubtedly limited the adoption of decentralized time-stamping approaches.

Due to mentioned reasons, it is important to create a simple timestamping system, but that satisfies all the requirements of companies and users. The intention of the present work is to provide this simple, but secure system that allow organization to sign documents with timestamps; and this system will be implemented in the aforementioned real company i.e. BIGDATA CA. The results obtained in this project will also benefit other people or companies that have similar systems or processes, where they wish to guarantee the validity of the documents generated over time.

5. DEVELOPMENT OF THE PROPOSED TIMESTAMPING WEB APPLICATION

5.1 Overview

The implemented electronic factoring process is based on the conventional factoring. The main difference is that it makes use of electronic invoices (in XML format) instead of physical (paper based) invoices. However, some improvements have been implemented to its process in order to provide greater confidence in terms of legal issues. The most important improvements applied to the factoring process were: (a) willingness of payment done by the debtor of the invoice (which details of the commitment to pay the invoice on a given date) and (b) usage of electronic signatures with timestamps of generated documents (process implemented in the web application of timestamping).

Figure 2 shows the general electronic factoring process; it also indicates the steps where the electronic signature and timestamp process was adapted. It is important to mention that this solution was implemented in a real company called BIGDATA C.A.

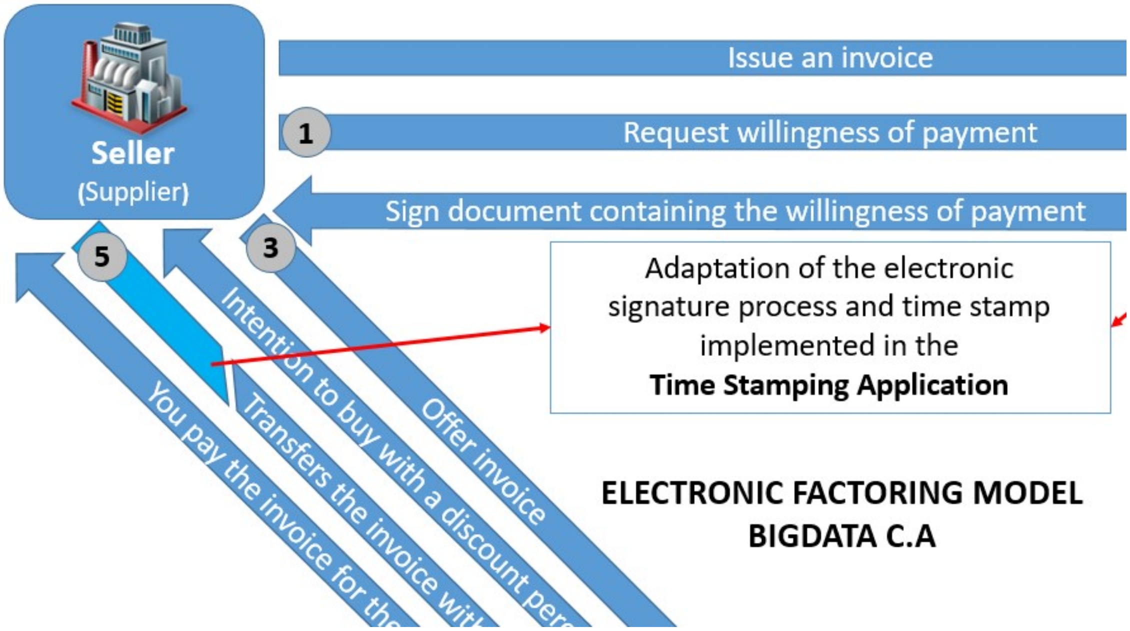

Seller
(Supplier)
Issue an invoice
1
Request willingness of payment
Sign document containing the willingness of payment
3
5
Adaptation of the electronic signature process and time stamp implemented in the
Time Stamping Application
Offer invoice
Intention to buy with a discount perc
Transfers the invoice with
You pay the invoice for the
ELECTRONIC FACTORING MODEL
BIGDATA C.A

***Figure 2:** Electronic Factoring Process of The Company BIGDATA C.A*

As an initial requirement to begin the electronic factoring process, the seller must have issued an electronic invoice to one of its customers (debtor), and then the following steps have to be executed:

1) The seller requests to the debtor to confirm his/her willingness to pay the invoice.
2) The debtor gives this confirmation of willingness of payment sending a document signed electronically with timestamp. Such document indicates the deadline until when the payment must be done.
3) Once the signed willingness of payment has been received, the seller initiates a negotiation of the invoice with a buyer previously registered in the electronic factoring system.
4) The buyer evaluates the characteristics of the invoice and makes a purchase offer including a discount over the total value of the invoice based on different conditions such as the value of the invoice and the remaining days for payment.
5) The seller accepts the purchase offer of the buyer and reassigns the invoice to the buyer by signing the electronic document with timestamp and indicating that the new owner is the buyer.
6) Once received the reassigned invoice from the seller, the buyer makes the payment to the seller. After payment, the system automatically notifies to the debtor the transference of the invoice to the new owner. The debtor must pay to the buyer the total value of the invoice until the deadline stipulated in the document.
7) Finally, the debtor pays the total value of the invoice to the buyer until the deadline.

The electronic signature with timestamp process was implemented in steps 2 and 5 through the web application.

5.2 Assumptions

It is assumed that the Company that will use the application has a current electronic signature certificate and has hired the Time Stamping service with a reliable TSA.

It is assumed that the equipment or device where the Time Stamping Web application is going to be used, has a stable internet connection when carrying out the signature and time stamp process.

5.3 Requirements

Prior to the development of the application, the actors involved in the system were defined: (a) general user who represents any person who uses of the Timestamping application, and (b) administrator user who represents the entity that implements the Time sealing service of TSA and who will be responsible for the administration of the application (see Figure 3).

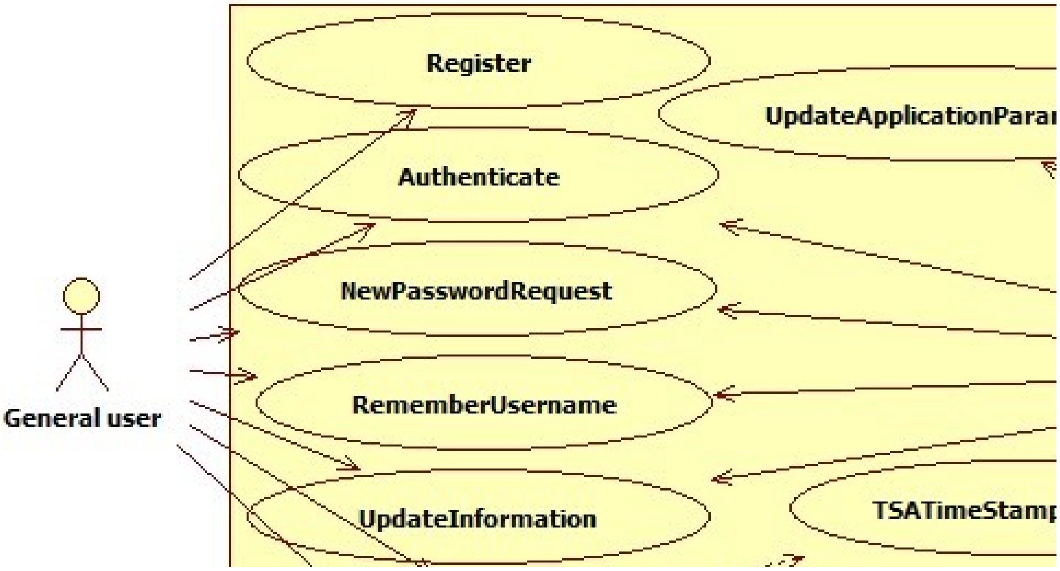


Figure 3: General Purpose Use Case Diagram

In the following, the description of each use case obtained based on the requirements.

- **Register:** The application allows general users to perform the registration process. For this process, the user must provide different data such as identity card number, given names, surnames, electronic signature certificate (optional), e-mail, username, and password.
- **Authenticate:** The application will allow the access of any previously registered user by using his/her username and password combination.
- **New password request:** When a user does not remember his password, he can request a new password.
- **Remember username:** When a user does not remember the username to access the system, you can select the "Remember username" option.
- **Update information:** Users must be able to update their information when required, as long as they are authenticated in the application.
- **Sign and stamp XML:** Users must be able to sign and stamp XML documents with their electronic signature certificate.
- **Documents Repository:** Users must be able to search, delete, or download previously signed/stamped documents. Users must indicate the range of dates of the desired documents.
- **Update application parameters**: The administrator user must be able to update the parameters of the application. The updateable parameters will be the following: TSA url, user name and authentication password.

5.4 Database Model

The database model was created based on the specified requirements and use cases (see Figure 4). The model has the following tables.

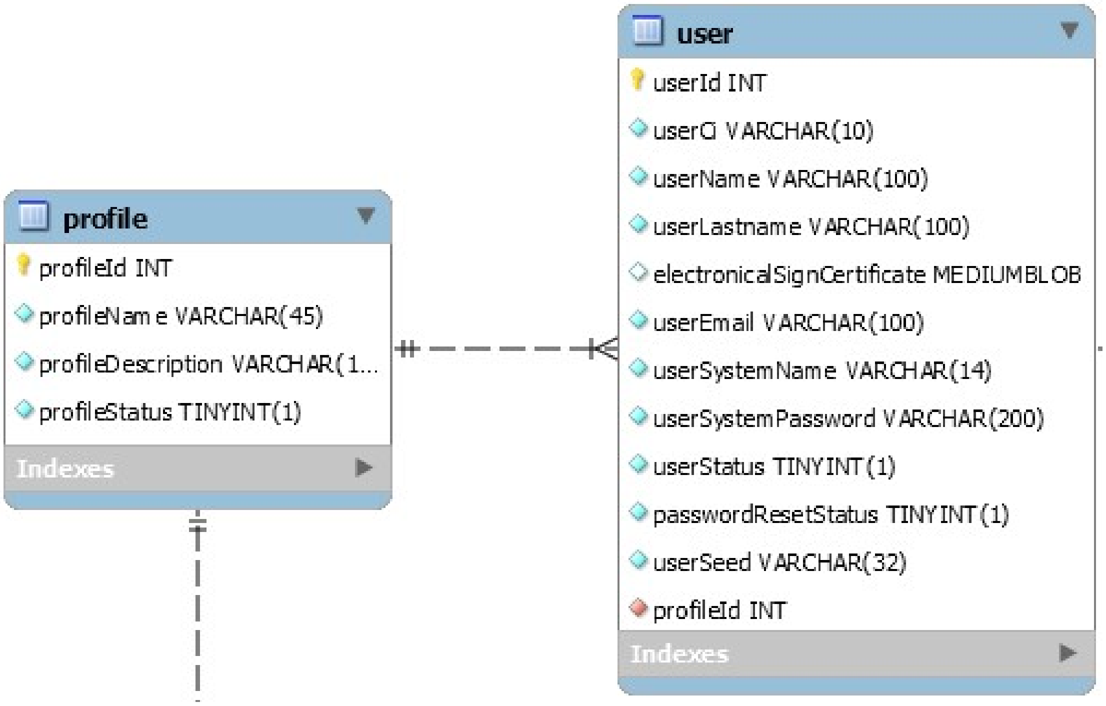


Figure 4: Conceptual Database Model

- **User:** Stores the information of users and their certificates.
- **Profile:** Contains the profiles of existing users of the system. The profile indicates the level of access to the system (access to different options of the system).
- **Permission:** Specifies the permissions or options that a profile can access.
- **Page:** Stores the URL of pages of the web application. This information is used to build the menu of the system based on the permissions associated with the profile of a user.
- **Signed documents:** This is where XML documents are stored and electronically sealed.
- **Parameters:** This table is where the connection parameters of the TSA are stored in order to consume the timestamping service.

5.5 Deployment Diagram

Figure 5 shows the relationship between the client, the web server, the TSA, and the database. Each of the parties involved is described below:

- **Client:** user who wants to perform the process of signing and timestamping of an XML document.
- **Web Server:** conformed by the Web Application containing the Timestamping process and the Interface with the TSA.
- **TSA:** The entity that attends the timestamping requests made by the application.
- **Database:** this is where the user information and documents that have been signed/sealed by the application are stored.

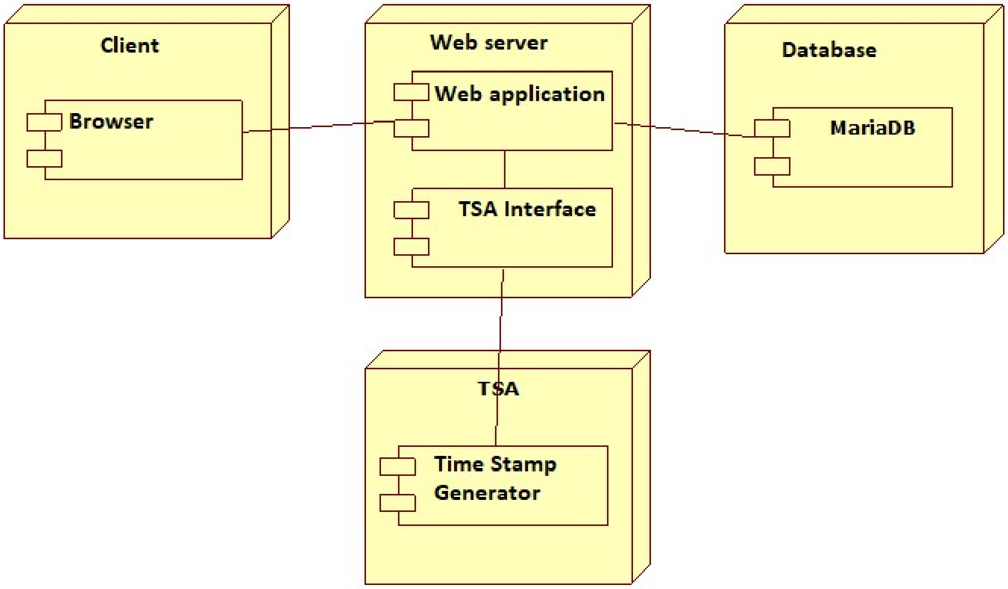


Figure 5: Deployment Diagram

5.6 Navigation Diagrams

5.6.1 General user

From the main page, users with the role of "general user" can: request a new password, authenticate to enter the application, remember their username. A new user can request his/her registration. Once authenticated, the system displays the internal home page, where authenticated users can: update their information, sign and seal documents, and access the repository of signed documents (see Figure 6).

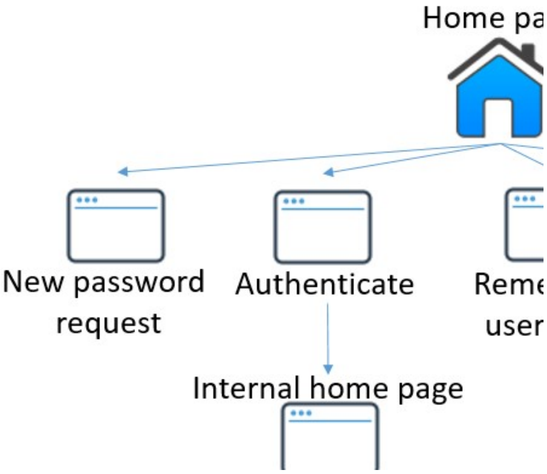


Figure 6: General User Navigation Diagram

5.6.2 Admin user

From the main page, users with the role of "admin user" can: request a new password, authenticate to enter the application, and remember their username. Once authenticated to the system, the users get access to the internal home page, where they can: update their information and update the application parameters (TSA Url and password for consumption of timestamps) (see Figure 7).

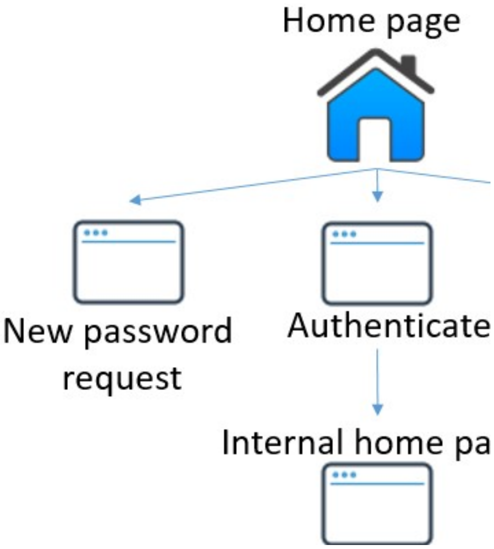


Figure 7: Administrator User Navigation Diagram

5.7 Process Diagram

Figure 8 shows the process diagram of the "Signing and stamp XML documents" use case. It starts when the users loads the XML file to be signed and his/her signature certificate and inputs his/her pin/key. If the loaded information is wrong, an informative message will be displayed to the user and he/she will not be able to continue until provision of the correct information. On the other hand, if the provided information is correct, the loaded XML document will be signed without any issue. While the document is signed, the corresponding timestamp is also added. The system also allows the possibility of store the signed document in the database.

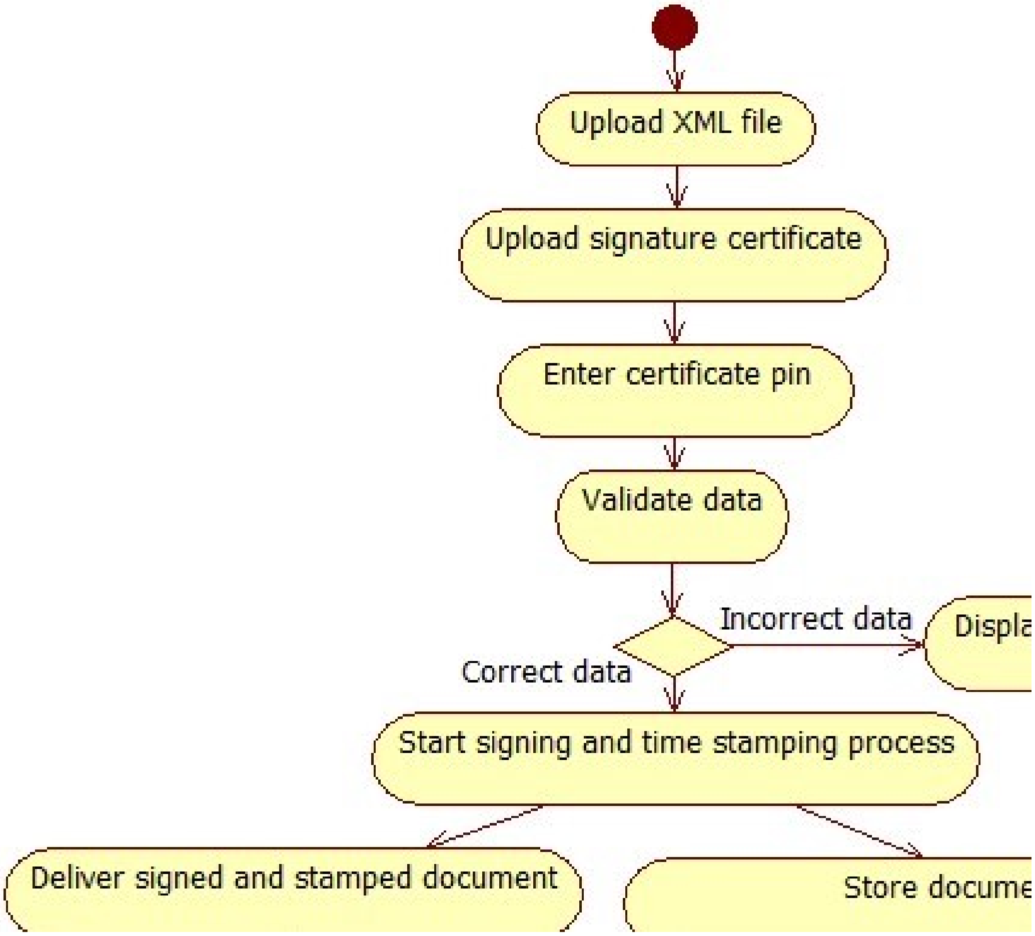

Upload XML file
Upload signature certificate
Enter certificate pin
Validate data
Incorrect data
Displa
Correct data
Start signing and time stamping process
Deliver signed and stamped document
Store docume

Figure 8: Diagram of Signing and Timestamping the XML Document

5.8 Construction of the application

5.8.1 Definition of the main process of the application

Taking into account the process to make an electronic signature with timestamp and the systems requirements, the main process is executed as follows.

1) The user uploads a document in XML format to the application and initiates the process of electronic signature and timestamp by entering the key of the electronic signature certificate.
2) The electronic signature process is performed on the hash summary of the original document, resulting in a signed document.
3) A new hash summary of the signed document is obtained and sent to the TSA with a timestamp request.
4) The TSA attends the timestamp request by associating the date and time in which the request was made and generating a new hash summary with the new information and it is electronically signed by the TSA.
5) The TSA returns the generated timestamp.
6) The application generates a new document, which contains the electronically signed original document in conjunction with the timestamp returned by the TSA.
7) The application return the signed and timestamped document to the user.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

It should be noted that all this process is done in a transparent way for the user in a time no longer than a few seconds.

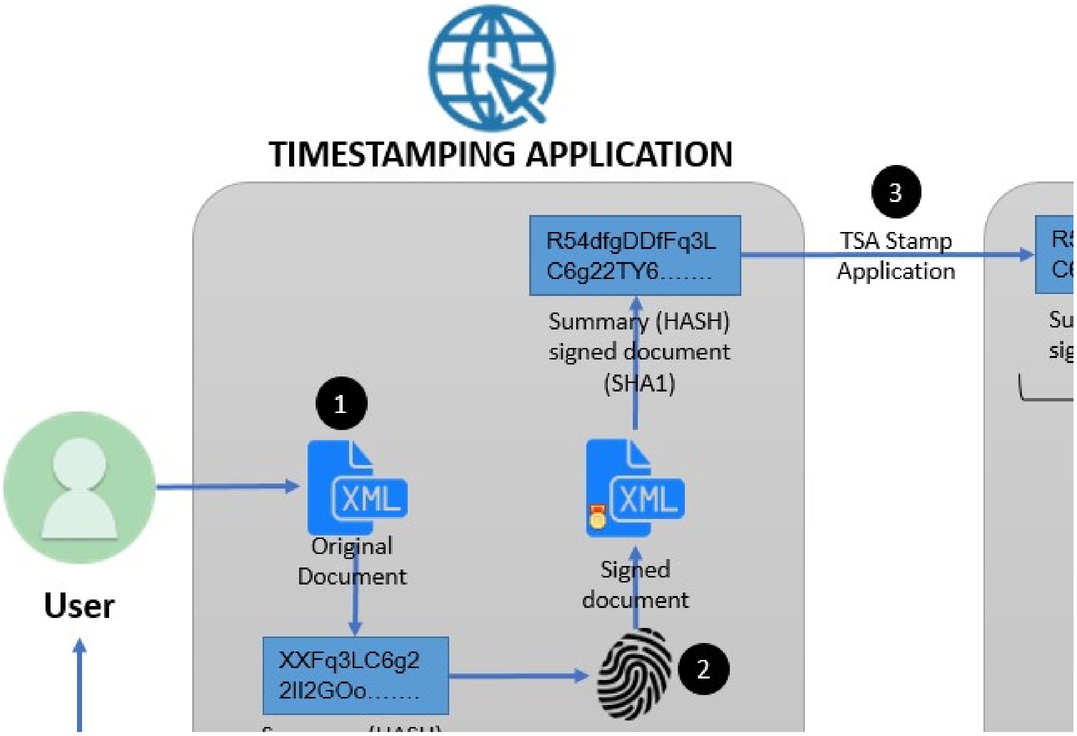

TIMESTAMPING APPLICATION
3
TSA Stamp Application
R54dfgDDfFq3L C6g22TY6.......
Summary (HASH) signed document (SHA1)
1
User
XML
Original Document
XML
Signed document
XXFq3LC6g2 2Il2GOo.......
2

Figure 9: Timestamping Web Application Process

1

5.8.2 Packages and classes

For the implementation of the Web Application, the following packages and classes were created (See Figure 10):

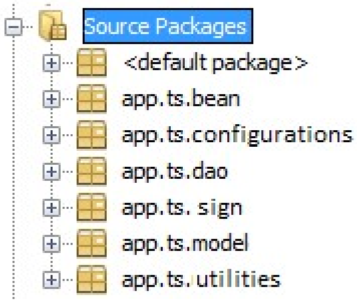


Figure 10: Packages Created For The Application

The following describes each package and its contents:

- **app.ts.bean:** Contains the classes that handle the pages of the application: SignStampBean.java, LoginBean.java, MenuBean.java, ParametersBean.java, RepositoryBean.java, UsersBean.java.
- **app.ts.configurations:** Contains the classes that load the initial configurations for the application: LoadParameter.java, InitializeApplication.java, Parameters.java.
- **app.ts.dao:** Contains the accesses to the objects (Data Access Object) corresponding to the entities, to interact with the database: DocumentDao.java, PageDao.java, ParameterDao.java, Profile.Dao.java, PermissionDao.java, UserDao.java.
- **app.ts.sign:** Contains the necessary classes to carry out the signing process and timestamp, these classes use the "PolygonESL-2.0" libraries provided by the TSA: SignFileo.java, SignDocument.java.
- **app.ts.model:** It contains the models of the entities: SignedDocuments.java, Page.java, Parameter.java, Profile.java, Permission.java, User.java.
- **app.ts.utilities:** Contains additional classes that integrate with the libraries "PolygonESL-2.0" for the signing process, in addition to several methods in common with other classes that help reuse code: ConsolePrivateKeySelector.java, PrivateKySelector.java, Utilities.java.

6. DEVELOPMENT TOOLS

Figure 11 shows the architecture diagram of the developed application. It shows how the different development tools are related. The tools used for the implementation of the process of electronic signature, consumption, and use of timestamps were Java and JSF programming language in conjunction with the PolygonESL 2.0 libraries [3] provided by the TSA. On the other hand, for the storage of the signed XML documents, user information and system parameters and the database manager MariaDB was used. For the interaction of the application with the DB, the relational mapping tool Hibernate was used. Finally, for the deployment of the application the Apache Tomcat application container was used, so that users can make use of the application from any device with an internet connection and a web browser.

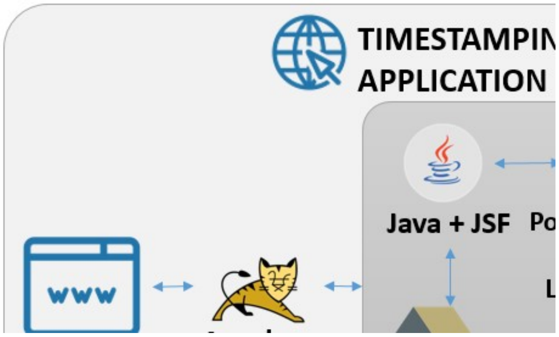


Figure 11: Architecture Diagram

Figure 12, 13 and 14 shows the screenshots of the implemented system. Figure 12 shows the application login page, Figure 13 shows the application home page after accessing the system, and Figure 14 shows the interface where the signature and timestamp process is performed, where the user loads the information needed to perform this process.

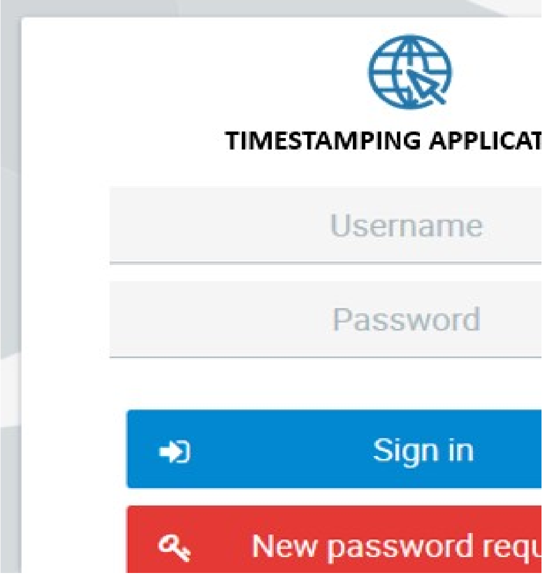
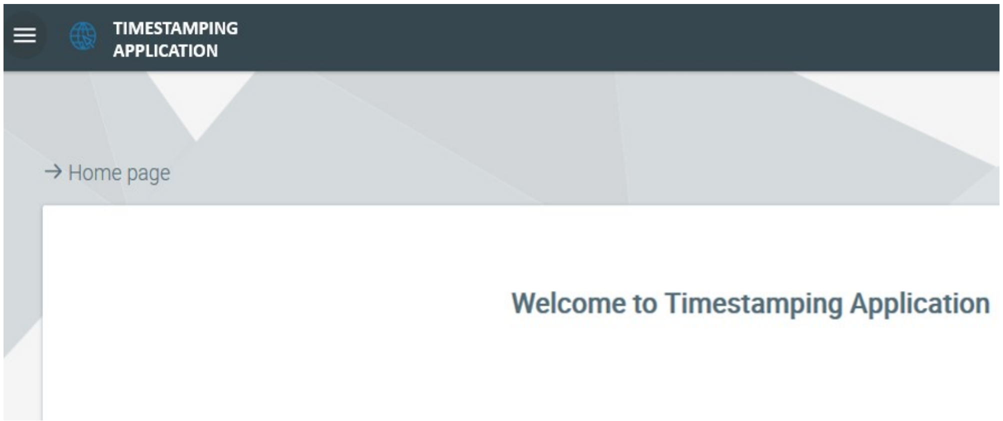
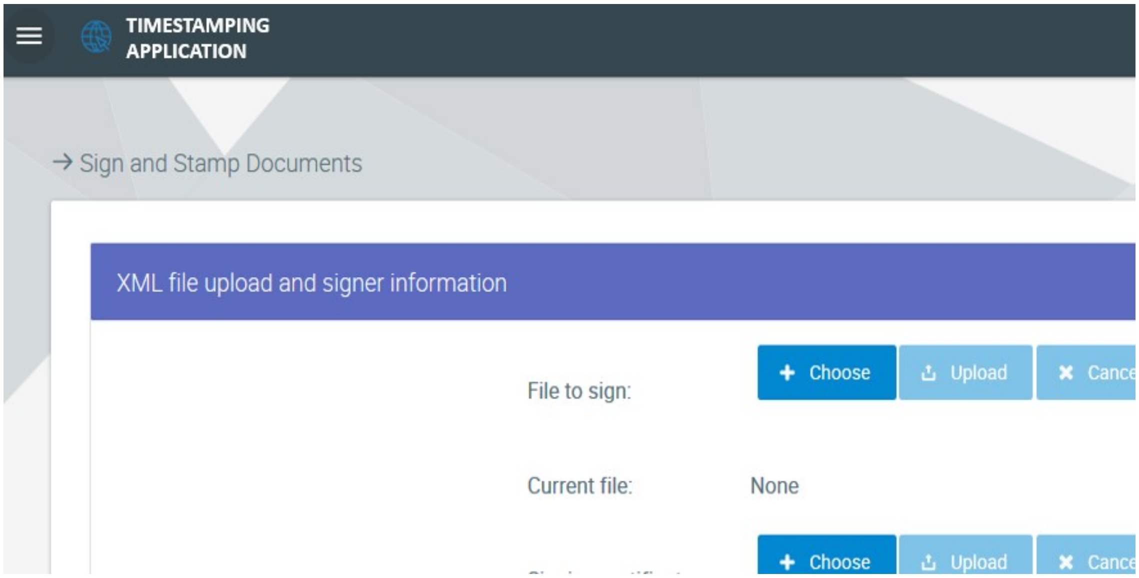


Figure 12: Login Page



Welcome to Timestamping Application

Figure 13: Application's Home Page



File to sign:

Current file: None

Figure 14: Signing and Timestamping Page

7. RESULTS

Through the implementation of the Application, it was to be able to have a greater legal validity and integrity to the information contained in the documents. The following table shows a comparison between the XML file without signature, only with signature, and signature with timestamp.

Table 1: Comparison Of Unsigned, Signed, And Timestamp Signed XML Documents.

	Unsigned XML	Signed XML	Signed XML + timestamp
Integrity of information	NO	YES	YES
Confidence of the signature	NO	YES	YES
Reliability of the signature's date and time	NO	NO	YES

Having implemented the timestamping application to the Electronic Factoring system developed by the company BIGDATA CA, it was possible to give greater confidence, security and agility to the factoring process. It is important to remember that the use of electronic signatures in conjunction with timestamps allowed to ensure that the information contained in documents are kept intact over time, giving more solids evidence of integrity, allowing those documents usable even in judicial proceedings.

8. CONCLUSIONS AND FUTURE WORK

In this paper, we have shared our experience in developing a web application of Timestamping using an appropriate signature format that adjusted the Electronic Factoring system. The access to the source code of its Electronic Factoring system of the company BIGDATA C.A facilitated the integration of the timestamping application. The use of the PolygonESL-2.0 libraries provided by the TSA of the Banco Central del Ecuador (Central Bank of Ecuador) for the consumption of the timestamping service allowed a considerable reduction in the development time of the application.

It is important to remember that the use of electronic signatures in conjunction with timestamps allowed to ensure that the information contained in documents are kept intact over time, giving more solids evidence of integrity, allowing those documents usable even in judicial proceedings.

The models suggested by the UWE methodology allowed to develop the application in an agile way, focusing on the functional part of the same one. Since the illustrations proposed by the methodology are easy to understand, they facilitated the communication between the developer and the client, allowing to elicit in better way the requirements of the application.

At the moment, the timestamps is used only in the Electronic Factoring process, but its use can be extended to other processes of the Company such as: email signing, signing of contracts and documents in other formats such as PDF, OOXML and ODF. In addition, it is expected to be able to implement the signature and time-stamp functionality in an automatic or unassisted way, eliminating the need for the entire process to be carried out by a person.

REFERENCES:

[1] Brzica, Hrvoje, Boris Herceg, and Hrvoje Stančić, "Long-term Preservation of Validity of Electronically Signed Records", *INFuture2013: Information Governance*, 2013, pp. 147-158.

[2] Diego Patricio Muñoz Guerrero, "Tributación en comercio electrónico en el Ecuador", Quito - Ecuador, 2013.

[3] ECIBCE, "Certificación Electrónica Banco Central del Ecuador", September 16, 2016, https://www.eci.bce.ec/preguntas-frecuentes#21.

[4] Ahto Buldas, Peeter Laud, Helger Lipmaa and Jan Villemson, "Time-stamping with binary linking schemes", *Advances in Cryptology—CRYPTO'98. Springer Berlin/Heidelberg*, 1998, pp. 486-501.

[5] Wallace Carl, Ulrich Pordesch, and Ralf Brandner, "Long-term archive service requirements", *No. RFC*, 2007.

[6] Díaz Francisco Javier, Macia Nicolás, Molinari Lía, Venosa Paula and Sabolansky Alejandro Javier, "Importancia de contar con un servicio de sellado digital de tiempo en una PKI", *XII Workshop de Investigadores en Ciencias de la Computación*, 2010.

[7] Yoo, Sang Guun, Keun Young Park, and Juho Kim. "A security-performance-balanced user authentication scheme for wireless sensor networks", *International journal of distributed sensor networks 8.3*, 2012, 382810.

[8] Yoo, Sang Guun, Hyukjun Lee, and Juho Kim. "A performance and usability aware secure two-factor user authentication scheme for wireless sensor networks", *International Journal of Distributed Sensor Networks 9.5*, 2013, 543950.

[9] Yoo, Sang Guun. "5G-VRSec: Secure Video Reporting Service in 5G Enabled Vehicular Networks", *Wireless Communications and Mobile Computing 2017*, 2017.

[10] Cámara de comercio de Ambato, "Cámara de Comercio de Ambato", September 03, 2016, http://www.cca.org.ec/informativo/blog/160-%C2%BFque-es-el-factoring.

[11] Çela, Shpresa, and Anila Bani. "Economic Factoring Role and its Advantages Compared with Debt Collectors and Bank Credit to SMEs in Albania", *International Journal of Management and Business Economics (IJMBE)*, Vol.4, Number 4, 2015.

[12] Milinković, Stevan, et al. "Evaluation of some time-stamping authority software", *6th International Conference on Methodologies, Technologies and Tools enabling e-Government, Belgrade*, Serbia, 2012.

[13] Martin Vigil, Chistian Weinert, Denise Demeriel and Johannes Buchmann, "An efficient time-stamping solution for long-term digital archiving", *Performance Computing and Communications Conference (IPCCC)*, 2014 IEEE International. IEEE, 2014.

[14] Jacobson, Ivar, et al. "The unified software development process", vol. 1. Reading: Addison-wesley, 1999.

[15] Escalona María José and Nora Koch, "Ingeniería de Requisitos en Aplicaciones para la Web–Un estudio comparativo", *Universidad de Sevilla*, 2002.

[16] Rivero José Matías, Julián Gustavo Rossi, Esteban Robles Luna and Nora Koch, "Improving Agility in Model-Driven Web Engineering", *CAiSE Forum*, vol. *734*, 2011.

[17] Koch Nora and Andreas Kraus, "The expressive power of uml-based web engineering", *Second International Workshop on Web-oriented Software Technology (IWWOST02)*, Vol. 16. CYTED, 2002.

[18] Liu Jun and Zhen-duo WANG, "Application of XML Digital Signature to Electronic Order System [J]", *Computer Security 8*, 2012.

[19] Yuefei Gao and Hajime Nobuhara, "A Decentralized Trusted Timestamping Based on Blockchains", *IEEJ Journal of Industry Applications, vol. 6, no. 4, pp. 252-257, 2016.*