WoT model for authenticity contents in virtual learning platforms

Paulo A. Gaona-Garcia[1], Jesús Soto-Carrión[2],
[1] *Engineering Faculty, Distrital University, Bogotá, Colombia.*
[2]*Artificial Intelligence Department, Pontifical University of Salamanca, Madrid Campus, Spain*

***Abstract* — The following research proposal seeks to bring a model of security software on virtual learning platforms LCMS under all SCORM specifications to ensure the authenticity of content created under concepts of digital signature and identification of protocols and mechanisms to ensure such activities.**

***KeyWords* —** Security, authenticity mechanisms, virtual learning platforms, LCMS, SCORM, digital signatures, certificates of authentication.

I. Introduction

IN the schemes of software security the representation of the authenticity is one of the principles of this line of work. In this way, it is seen in the future, in the area of digital certificates, as one of the basis to guarantee the sent documents validity through a Web of communications between client-computer and of course taking into account internet. This principle of security is the base to propose common models and alternatives of works to multiple businesses. Thus, there are going to be a lot of mechanisms to achieve the authenticity of information that is managed, day by day, for each one of the communication systems in all the computers. In the research that will show this project we can summarize that to implement the virtual objectives of learning (LO) to guaranty the use of the content under all SCORM specifications there must exist three elements: adaptability, usability, and accessibility. Although, adaptability is not for all systems according to reference [6]. In this case, the Moodle platform is one of the best CLMS to have a good adaptation [9]. For this reason, this is the most important element to analyze the security to get to information and contents through SCORM.

II. The real security about LCMS platforms

A. About LCMS

LCMS (Learning Content Management System) have been an evolution for the systems based on contents CMS (Content Management System). These systems were created to manage and control the users' information in a corporative level. From the moment it appeared, this has been a product of integration of different kind of groups. These groups have permitted, in a global way, to support the initiative of standardizing the development processes of platforms. According to reference [17] these platforms have represented an important factor to facilitate some methodologies to study different from the traditional ones based on just training CBT (Computer Based Training), IBT (Internet Based Training) y WBT (Web Based Training). The view in relation to software security and the use of tools and platforms that have been developed to support learning is not encouraging.

It is clear that exist a lot of mechanisms and are useful for this kind of activities. The grade of confidence to identify the authority and creation of academic contents in this kind of platforms is not totally controlled by any technological devise. This gives some academic instructions and represents a fundamental topic in the process of formation and evaluation in learning. All the previous ideas want to reinforce the previous facts through the results of the analysis in relation to software authentications in more that 300 companies. There are some very important companies that deal with health, financial areas and education. This analysis was made by the CSI (Computer Security Institute) helped by its director Richardson [26] at the end of 2008. This analysis presents that the improper use of the information is one of the most important factors in the use of software applications. For this reason education represents the second vulnerable area to be attacked by the use of tools of communication and learning. In this way, education is in the virtual platforms of learning LCMS. In the figure number 1, it is possible to notice that the most important problems are the viruses on internet, but the improper use of information (Insider Abuse) and the financial

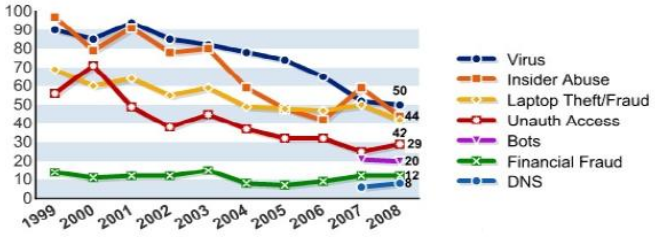

Fig. 1. Number of problems in the ten last years in areas such as government, business, help, and education. Source [26]

This article is part of the thesis research project mentored Ph.D. program in Computer Engineering from the Pontifical University of Salamanca. Director: Dr. Jesús Soto Carrión. Tbe researcher, *Paulo A. Gaona-García*. is the head of the Investigation Group GIIRA at Distrital University.

frauds are problems are impossible to control with companies' security rules.

Therefore, we can identify that most of the software answers, in the security area, are focused on diminishing problems dealing with issues like authentication and access controls. But, the part of data certifications shows that the results are not rewarding. Consequently, security is not clear. In the marketing it will always exists methods to attack the weak areas of computer systems.

III. SECURITY SCHEMES ABOUT SOFTWARE APPLICATIONS.

One of the elements that are important to take into account, before taking about the area of security in software technologies in relation to the Authenticity of Contents, is to know the condition and model of security representation that is in the market therefore, to talk about the whole contents Authenticity. We will base on a software security model proposed by [3]. This model is located in a telematic context. It says that to guarantee a software service there must be a model of representation to identify the security elements to apply. For this reason, the next model allows locating us in a global context to represent the kind of security that it is necessary to determine in relation to informatics applications

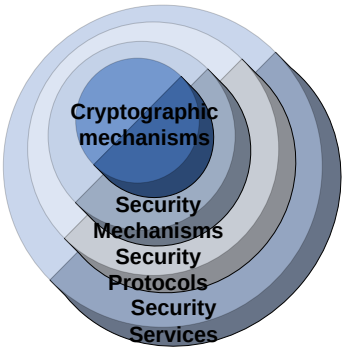

Fig. 2 Elements to provide security mechanisms. Source: [3]

and at the same time it helps us to be in the authenticity of contents.

The previous model represents the base that locates the security in the communication system. This model locates each security according to the elements that are important to its appliance. It begins with cryptographic mechanisms and mechanisms of security to write in code the information and authenticate the same mechanisms. It continues with some protocols of communication to send data and finally, the security service that is all the structure that guaranties the contents authenticity on a LCMS platform taking into account all the SCORM specifications.

A. Authenticity Services

The concept of authenticity is in relation to the principle of Confidentiality. It is also known as confidential levels and another principle that is confidentiality of contents in a communication context. The word "*Confidentiality*" in software world has a lot of elements that have been treated by a lot of authors to give them a different view to apply. This is because Confidentiality, Authenticity, Integrity, Acceptance and Controls of Access have been considered as important elements of a sure communication. This is a topic that we are going to discuss from an academic and scientific point of view with help of some technological areas.

From the academic point of view some authors [7] work this concept under the possibility of "the transmitter and receiver must be able to understand the content of the message". For this reason it is important to certificate the encryption and decoding of the message through a number of clues that are used in a process of communication between two entities. On the other hand, [5] talks about confidentiality as the base of privacy. So, "the information that has been received for the web will not be intercepted and read by any other entity". This ensures the origin of the information. The reference [3] affirms that confidentiality does not have to be related with privacy, because these words are similar but have a different meaning. The use of these words, in a context of software security, change a lot taking into account "the coordinate use of judgments and security services that are available." To implement this concept it is necessary to think about its fundamental state that is in relation to the cryptographic principles that are mentioned bellow.

B. Cryptographic systems

A Cryptographic System is a security mechanism that assures information between two entities that want to hold a communication canal. The process of hiding a message is considered the how and has a particular characteristic. This is both clues and algorithms are used to hide the secret message. In this sense, we can find that the components of a cryptographic system are:

1. Original message ***M***
2. Message written in code ***C***
3. Secret key ***K***
4. Operation to write the code ***Ek***
5. Operation to decode ***Dk***

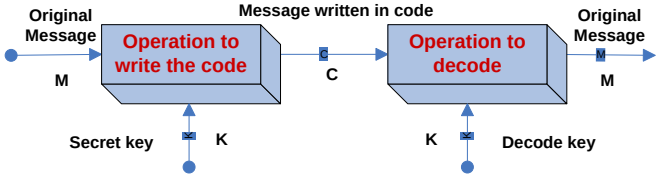

Fig 3 Classic cryptographic system

The previous figure represents a normal operation to write messages in code. This process represents the Classic Cryptographic scheme. One of the cryptographic characteristics is that it is composed by two branches. These ones are used depending on the conditions of the system that is going to be used. These branches are known as

cryptosystems of private key or symmetric and cryptosystems of public key or asymmetric.

C. Systems of private key – Symmetric

Cryptosystems of private key are known as Symmetric Systems. They are characterized by managing an operation to write from a code ***Ek*** to a message m to be sent and a process of decoding ***Dk***. Another characteristic is the privilege to share a private ***K*** that is just known by the transmitter and the receiver. The success of the well development of these kinds of systems depends on the security of the private key. It is important to assure keys for both the transmitter and the receiver and not to focus on the cryptographic algorithm security. This one develops the process of writing in codes and decoding of the message that could be public.

D. Systems of public key -– asymmetric

Cryptographic systems of public key, known as asymmetric systems, have the five elements of a normal cryptosystem. But the difference between these two systems is based on the creation and distribution of the keys that are the result of the process of writing in codes and decoding of the messages between the transmitter and the receiver. Another characteristic supported by many authors is that it is not possible for a computer to deduce the private key. This is because the purpose is to work with a unidirectional system that does not allow getting the original message m from the encrypted message ***C***. This is guaranteed by encrypted mechanisms.

IV. Techniques to Verify Authenticity

There are a lot of mechanisms and algorithms that prove the authenticity of digital documents in the available techniques. In this point, it is important to highlight the most representative mechanisms that are used for most of the companies.

A. Digital Certifications

Digital certifications are known as one part of the information that is in relation to a digital document. To get a digital certification the information must be an "entity". This is in charge of creating the couple of public keys and its assignment of the private key to guarantee it during a specific period. This process creates a "*Digital Certification*". This is given by an unknown agent called TTP (Trusted Third Parties). This certification is generated through a CA (Autority Certification) under the name of Certification authority. The presence of a certification authority guarantees a good environment for communications. These ones have to work under a structure known as PKI (Public Keys Infraestructure) or infrastructure of certification to fulfill all the requirements and TIPs through a certification authority in a model of shared safety by many users.

B. Digital Signature

A signature is in general the cryptographic process to write a message in private code. In a textual way, [3] defines it as "a piece of information added to a unity of data. This is the result of a cryptographic transformation of a person who signs private transformation. This allows a receptor entity proving the authenticity of the origin and integrity of the received data". For this reason, the generated sign is considered a part of the original message that is sent to an addressee. For addressee's part, he or she has to do some basic operations to verify and to acquire the enough author's intellectual warranties of the document and the message. This concept of digital sing has been accepted in the telematic area because it generates mechanisms, techniques and algorithms that ratify the proper development, and at the same time, the generation of new specifications to determine the evolution of this concept in informatics areas. This gives it a position of mechanism to affirm validity of an author's document (Authentication), to verify that the document is not manipulated or changed (Integrity) and to avoid author's authority through negation (No negation). The last one is helped by the validation of the author's public key, so he is related to the document with the sign.

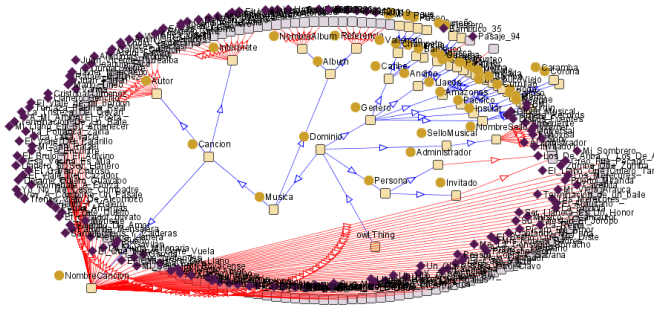

Fig. 4. Example of a Web of Trust. Source (Author)

C. Model and process of digital sign

Hash function is a fundamental part in the algorithms structure of digital sign utilizing unidirectional functions in the authentication of the messages. This guarantees that once a message is written in code it is not possible to go back. This function guarantees the "fingerprint" of the document. Consequently, these kinds of functions create a great value in the software and telecommucations world. Next, there is a graphic representation of the digital sign known as generic in whatever kind of specification, mechanism and cryptographic algorithms used for this purpose:

In this sense, the Digital Sign represents one of the most important characteristics to develop the contents authenticity. This authenticity is one of the most important values to work in relation to informatics nets known as Web of Trust that are going to be explained next.

V. Web of Trust and Social Networks.

WoT "*Web of Trust*" is a concept that has been worked from the creation of the mechanism PGP "Pretty Good Privacy" for e-mails security through its creator [15]. This

mechanism states the idea to allow and accept user's identity in a communication system when the user is known by another user of the system that guarantees some minimal conditions of confidence to accept him in the communication scheme of the platform that they are sharing. Under these circumstances, there is a new concept that allows the interaction of users about social nets and it is in relation to the project SIF (Social Interaction, Framework) [10] In this framework an agent evaluates another agent's reputation based directly on observations of some witnesses that are participating in the same system. It was different for the traditional electronic systems because participants have to use external mechanisms that were used as intermediary between the people that were holding a communicative process. One technological issue that was used from some years ago is in relation to browsers. In this case, the most common browser because of its characteristics is Firefox through the WOT component. It is possible to download this component to the user's computer. This avoids problems in relation to internet such as: advices that are not sure or necessary, steeled identities, no trusted commercial web pages, problems with link security before clicking on them, a so forth. There are some prototypes that are developed with this model of web of trust. They are reflected in the model of reference [13] a web of trust and some prototypes worked by reference [14]. These prototypes need users to give a qualification of them and in this way it is possible to have a central organism (direct punctuations) to other trusted users (collaborative punctuations). Therefore, central system pursuits users that do punctuations of each one and utilizes this punctuation to create a reputation in relation to a specific user. These systems need previous social relations between the users of an electronic community. It is not clear the way relations are established and how qualifications are spread through this community. These previous characteristics have created some projects that allow us reinforcing the proposal to find a trusted system with digital contents about a LCMS based on a series of specifications through SCORM. This is going to be discussed in the next point.

VI. MODEL TO PACK DATA

When virtual platforms of learning began to be stronger in the academic community as one of the available and valid alternatives to control non presential activities there was a study that allowed stating some rules in order to generate contents and different functions from the platform of work. For this reason, a lot of international groups appeared. This allows determining a group of rules to deal with the contents. In this case, we can base on works developed like SCORM through ADL [16], IMS Content Packaging [18] for the definition of the structure of contents, IMS Simple Sequencing [23] for the structure of contents of learning and the evaluation of these ones through Learning Design [21] and giving them through IMS Model Data [22] with the objective of the creation of a data structure in a representation of different stages for its application with different pedagogical points of view and elements proposed by [2].

A. Objectives and representation of contents

In the model to pack data to contents on virtual platforms of learning LCMS, there are some references that are a base to determine each function of content. In this way, we can base on works developed by [1] to draw the most important specifications in IMS through [19]. It is important to base on works developed by SCORM through [16] and the works developed by reference [8]. The last one presents some characteristics and specifications that are in the market and that were mentioned before. To identify some functional parts of any specification it is important to highlight the concept of learning objective from the point of view of programming. This one, mentioned by [8] in his works, exalts the idea of the relation of the contents to their creation. For this reason, he says that the concept has changed so as to work with RLO (Reusable Learning Object). This topic was developed under IEEE specifications with [25] by the author [10] to define the metadata and the elements to define the contents. Any way, these ones adapt the E-learning world to offer a paradigm focusing on the objectives in the use of components with the definition of most of the specifications.

According to [8] "The RLO objective is to have a lot of learning material pieces to combine each other and reutilize them in different contexts. Although, the reutilization of learning objectives have more problems that the reutilization of software objectives". These problems are in relation to the identification of a standard to use; under these circumstances they are important in the creation of contents.

B. A group of SCORM specifications

SCORM (Shareable Content Object Reference Model) was an idea supported by defense departments of the United States in 1997. The critical proposal of this entity is to support itself on the previous initiatives to form its own group of specifications. This group is formed by IMS, IEEE through LOM, AICC specifications, but there are more.

C. SCORM Operative Model

The second version for 2004 is been prepared. It has [16] some important differences from the first version in the marketing. Content Aggregation Model (CAM). According to the specification [16] of this model, it defines the way to join, ticket, and pack content. As SCORM objective is focused on objects, it is necessary a good description of how these objects can be connected. Run-Time Environment (RTE). RTE describes the process and development for a CLMS with a SCO and the process of communication between them. A student just has an active SCO in a moment. Sequencing and Navegation (SN). SCORM model describes the sequence and interaction with RTE. Although, the description of the process and the sequence is made using IMS (Simple Sequencing) specifications described in [24]. Therefore, the model [24] is oriented to the relation and purpose of the pedagogical models used and the use of methodological strategies in relation to instructions. In this way, the process of learning is going to be

guarantee for the student with guidance. The objective of SCORM, under platforms LCMS, is to be a local storage to pack contents. This is to use the content in the platform as a manager of services of content. In this way, a user is going to use the content by watching it. In SCORM specifications for LCMS, it is necessary an architecture based on the browser and with boundaries to the use of contents used by an user so as to learn. Therefore, a learning process is guaranteed through a SCORM sequence. In this way, there are a lot of

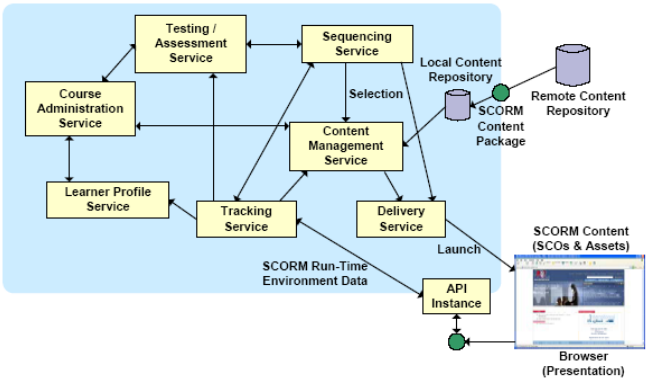

Fig. 5. SCORM model in LCMS platforms source: [16]

rules to specify and use the content in a sequence following the students' process of learning.

D. Looking at security in standards

There must be three elements to state virtual objectives of learning to guarantee the use of content by following some specifications. These are: Adaptability, reusability, and accessibility. Adaptability is here, but there are many systems that are not compatible with it reference [6]. On the other hand, reusability, and accessibility are analyzed by [6] in terms of bases for standards. He concludes that the platform LRN bears a variety of standards next to educative level such as the SCORM model, the IMS specifications and the Moodle platform. All of these are helped to guarantee requirements for accessibility to some content resources. In the SCORM specifications there are some elements that are used to work in a strategic way and to adapt the content to authenticity through packing it. This is going to be a guideline to analyze. It depends on the language used to develop authenticity through Digital Sign and for this case the definitions given by XML that are commented below.

VII. XML-Security

XML was proposed by W3C (World Wide Web Consortium) (originally known as the consortium for editorial revision of SGML proposed by IBM) in 1996. In 1998 it became a standard and it has been one of the most important contributions for software to manage, import, and export data on internet and on any kind of platform. This has showed new alternatives for the distribution of information in a clear and organized way for software systems. This is a standard for this kind of process. For this case, this paragraph is focused on the analysis of this standard and it is related to the qualities of security to support the XML Security project activities of authenticity. This project has three important elements that allow the identification of appropriated formats to manage digital signs in a communication system. On one hand, there are some characteristics given by XML-Signature [30] for digital signs of documents. On the other hand, there is the encryption operation through XML-Encryption Syntax and Processing [28]. Finally, it is the distribution of keys through XML-Key Management [29].

A. XML- Signature

The specification given by XML Digital Signature according to [30] uses some technologies for encryption of contents. In this process we can find some asymmetric algorithms and a generation of keys through HASH functions using alternatives such as SHA1, RSA and others. Under these guidelines for encryption it is necessary a structure for the distribution of public keys to provide the elements for this mechanism in relation to identity and no negation. In a general way, we can find some elements in the Digital Sign that define three fundamental guidelines:

- The following image represents an example of digital sign for the acquisition of a product on internet.
- Enveloping Signature: the sign XML involve the content that is signed.
- Detached Signature: The signed object is separated from XML sign.

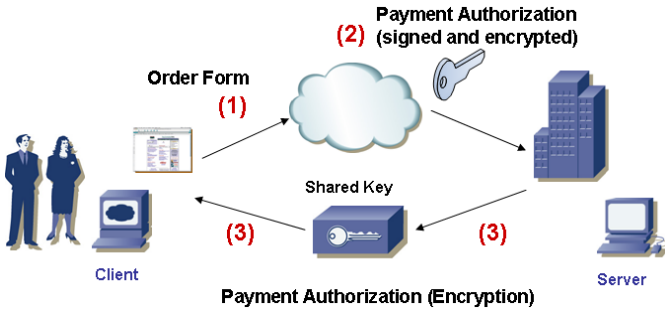

Fig. 7. Example of a digital sign for a transaction on the Web.

- Enveloped Signature: the signed content involves the sign.

In this case there is a banking transaction to ask for products on internet. This transaction is made with a credit card:

1. The client makes his demand through a form given by a bank.
2. When the form is filled, the client send it and it is encrypted with a key that is shared by the client and the bank. Therefore, the form is singed by the client and it is sent to the bank.
3. The bank processes the form and confirms the client's information (identity card, last name, etc.) then, the credit card encrypted information is processed to confirm the data and the clients demand continues its process.

B. XML-Encryption

XML-ENCRYPTION according to [28], describes the way in which singed data have to be written in code by the Web. This is with the objective to avoid the easy detection by external agents in the process of communication. In the encryption and decode process defined by [28] it is possible to identify the following roles:

- ***Application:*** the demand makes an application of encryption XML through giving enough data and guidelines for the process.
- ***Encryption:*** this is an implementation of the XML encryption to encrypt data.
- ***Decode:*** implementation of the XML encryption to decode data.

VIII. METHODOLOGY TO WORK

To develop the statement of the model we will base on security standards proposed in the market. In our case, the international standard given by ISO/IEC 27002 and proposed for the year 2007 for the use of information including international standards about requirements, risk analysis, measures and guidelines for the implementation of the software security that is an important element is what we want to assure in LCMS platform through authenticity mechanisms.

How to assure information with ISO/IEC 27002 in SCORM specifications To think about the model it is necessary to take into account some ISO/IEC 27002 considerations in relation to the classification from the legal point of view through these

```
<EncryptedData Id? Type? MimeType? Encoding?>
    <EncryptionMethod/>?
    <ds:KeyInfo>
      <EncryptedKey>?
      <AgreementMethod>?
      <ds:KeyName>?
      <ds:RetrievalMethod>?
      <ds:*>?
    </ds:KeyInfo>?
    <CipherData>
      <CipherValue>?
      <CipherReference URI?>?
    </CipherData>
    <EncryptionProperties>?
</EncryptedData>
```

Code 1. Representation of XML-Encryption. Source:[28].

three elements:

A. Data protection and privacy of personal information

In the strategy that will be proposed about authenticity it is important to have a mechanism that assures protection and privacy of information through a group of rules defined by XML-ENCRYPTION. This is to have the protection of:

- Person's information that creates the environment to work.
- Person's information that creates that creates the virtual instruction resource.
- Person's information that uses the shared resource in the virtual instruction.

B. Protection of the organization record

For the protection of the organization record some enterprises are going to be taken into account because they make digital certifications that mention a particular academic institution. This is with the objective of legalizing all the contents in the institution.

C. Intelectual property Wright.

To valid people's data in a process of communication it is important to highlight wrights and intellectual property of the created content. In this case, it is important to use XML-SIGNATURE to identify their validity. The cases to evaluate are:

- Person's information that creates the environment to work.
- Person's information that creates that creates the virtual instruction resource.
- Person's information that use the shared resource in the virtual instruction.

D. Security proposal about SCORM evident archive

To follow these three elements it will implement XML-SECURITY through XML-SIGNATURE and XML-ENCRYPTION to try to counteract these problems.

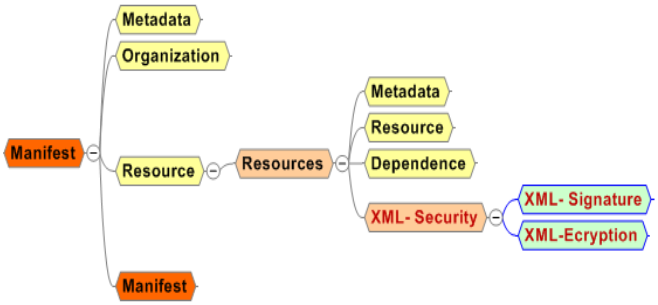

Fig. 8 Archive evident with security guidelines about the authenticity of content

To follow these characteristics it is important to highlight the idea that the most important archive to develop the process with the SCORM specifications is known as evident through the following representation:

This evident archive has an important role in the creation, opening, and search process of the learning objective on a LCMS platform under SCORM specifications.

This allows a connection to get all learning object characteristics. Therefore, it represents the element that is going to make easy the identification and ticketing on the content with the LOM standard security.

E. Security proposal about LOM

LOM work is to identify, in the ticket called Wrights, the sing characteristics that is add to the content. To do this, XML-SECURITY is based on the standard for this proposal that is represented in figure 9.

LOM will be the base for authenticity content process. The

standard for this is just mentioned, as it was mentioned in the previous chapters, and security guidelines are not included to strengthen the authenticity of the author's content.

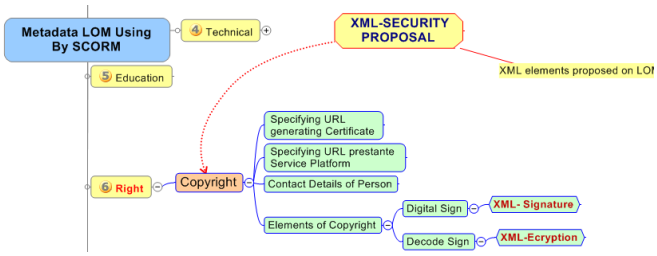

Figure 9 - Proposal of security ticket about author's Wright elements

F. Proposal of Security model for contents

The proposed model is based on toll and elements functional representation that are in a group of guidelines to defined contents by SCORM. Bellow, there is a model of the proposal to be developed and it has to the fig 11. This model must be framed in a plan of security through the use of ISO/IEC 27002 standard already discussed. Thus, it must be based on a company security mechanisms. This will generate sings about contents under SCORM specifications and at the same time, it is based on a LCMS virtual platform for learning. To state the previous proposal it is necessary to understand the creation of the model from the representation of each one of the identified roles in a communication process (Manager, Teacher, Student, and Guest).

In a general way, we can say that the model wants to get the following cases:

Therefore, the proposal is a software prototype to establish an architecture for the generation of digital certifications through PKI infrastructures. This is going to allow the LCMS virtual learning platform to manage the content authenticity through user manager, teacher, student, and guest's activities on SCORM specifications.

IX. Conclusion

We can say that there are a lot of organizations, in the market, based on research groups that work on standard components about software applications through security Web architectures. These groups emphasize the importance of

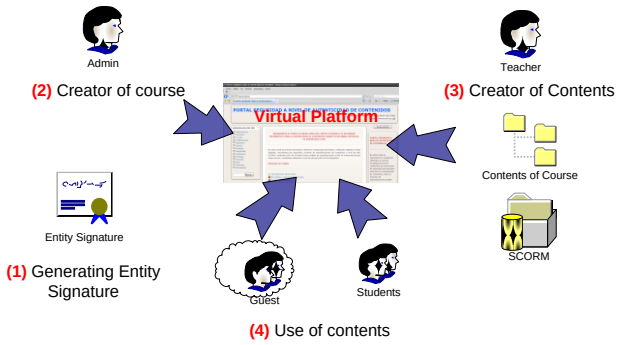

Fig. 10 - Kinds of sings created on LCMS platforms

XML language as one of the critical elements to guarantee the communication process in a Web environment. Therefore, the importance of [25], IETF, W3C and other contributions by some authors on a research level as [1], [5] is exalted. Many other highlight the idea of facilities offered by XML to create a secure environment for communication and to assure the integrity of information. This is connected with the SCORM specifications, realizing an adaptation to the model that works on the creation of content on LCMS platforms.

About security to guarantee the authenticity of generation of contents there is not any specification because security is focused on administrative issues to ticket content, generation of content, and from the pedagogical point of view the case of each one of the previous activities already discussed. The IMS consortium has worked on security too. But, it gives no relevant proposals in relation to authenticity for users and mechanisms to access to different kind of LCMS platforms under communications models focused on the WEB. All this is possible through protocol communication support and help from mechanisms such as: SSL, SLT VPN systems, among other alternatives, with reference [23] specifications. For communication between platforms it gives an authentication proposal. In its characteristics it is considered a new specification to deal with security of contents on a level of metadata. LOM, in a particular way, has a ticket in which there is a reference to the use of intellectual property of learning. This is known as Wrights. It describes property intellectual wrights and the conditions to use the object of learning that is used. But, as the standard says, these conditions have been proposed without taking into account security of the object that is used. In this case, it is a strong candidate to implement mechanisms of authenticity.

For our particular case, SCORM seems to have a lot of important advantages in relation to the analyzed specifications. In SCORM structure is the LOM standard. This standard, as it was mentioned before, has a metadata known as Wrights and it deals with object intellectual wrights for learning. This is not deep, but it works as a beginning for the objectives of this project, that will be valid in SCORM specifications. In these ones, we find some elements that are used to work in a strategic way to adapt the packing of content to the learning objectives authenticity. At the same time, this is going to be an analysis guideline that depends on the language that is going to be managed to work authenticity through Digital Sign. In this case we have the definitions by XML-Security. In the stated software security model it is important to highlight its well development on a confident structure through the WOT concept. At the same time, it is important to highlight its keys use and distribution through PKI with a known institution support that will let the generation of each one of the certifications for the user's access to the platform. This allows managing a group of SCORM specifications to create a virtual space and contents by a manager or a teacher. But, LCMS platform needs security mechanisms to deal with user's profile for each particular situation. This is what guarantee an authenticity model security of contents with SCORM specifications and

based at the same time, on external mechanisms to guarantee a good development through each one of the participants in a communication process. This one is formed by: managers, designers, teachers, students, guests, staff, etc.

Finally, we can determine that a plan for authenticity security mechanisms of contents on LCMS platforms depends on a group of specifications that is in the market. But the problem is that the plan is new and it is not able to state all the specifications. For this reason, it is important to determine that just a digital sign is not going to be taken into account, in a LCMS environment, but people's content validity to create a virtual space. These people are the ones in charge of the creation of the content for the teachers and the generation of a sign for the ones who use the material. This will create a high security level of the available contents in a LCMS. In this way, it is possible to state a concept about the kind of platforms that are used in social nets known as Web of Trust WOT. This will allow the generation of a more confident environment to work with an available material in these learning environments.

REFERENCES

[1] Burgos, D. Doctoral Thesis. Estudio de la estructura y del comportamiento de las comunidades virtuales de aprendizaje no formal sobre estandarización del e-learning. Madrid, España: Tesis Doctoral. Universidad Europea de Madrid. (2006)

[2] Burgos, D., Tattersall, C., & Koper, R. How to represent adaptation in eLearning with IMS Learning Design. Interactive Learning Environments, 15(2), 161-170. (2007)

[3] Carracedo, J. Seguridad en Redes Telemáticas. Ed. McGraw-Hill. ISBN: 84-481-4157-1. Pág. 549. (2004).

[4] González MJ. "B-Learning utilizando software libre, una alternativa viable en Educación Superior", Revista Complutense de Educación, Vol. 17, Nro. 1, pp. 121-133. Spain. (2006).

[5] Halsall, F. Redes de Computadores e Internet. Ed. Quinta Edición. Pearson – Addison Wesley. ISBN 10: 84-7829-083-5. Pág. 858.(2006)

[6] Kareal, F & Klema, J, Adaptivity in e-learning. In A. Méndez-Vilas, A. Solano, J. Mesa and J. A. Mesa: Current Developments in Technology-Assisted Education, Vol. 1, pp. 260-264. (2006)

[7] Kurose, J, & Ross, K, Redes de Computadores un Enfoque Descendente Basado en Internet. Ed. Pearson - Addison Wesley. ISBN: 84-7829-061-3. Pág. 768. (2004)

[8] Marquez, J. Estado del arte del eLearning. Ideas para la definición de una plataforma Universal. Trabajo de Investigación Doctoral. Universidad de Sevilla. Departamento de Lenguajes y Sistemas Informáticos. Marzo (2007)

[9] Santos, O.C. Technology Enhanced Life Long eLearning for All. In K. Maillet and R. Klamma: Proceedings for the 1st Doctoral Consortium on Technology Enhanced Learning. European Conference on Technology Enhanced Learning, p.66-71, (2006).

[10] Schillo, M., & Funk P. Who can you trust: Dealing with deception. In Proceedings of the workshop Deception, Fraud and trust in Agent Societies at the Autonomous Agents Conference, pages 95-106. (1999)

[11] Vélez, J. Arquitectura para la Integración de las Dimensiones de Adaptación en un Sistema Hipermedia Adaptativo. Trabajo de Investigación Doctoral. Universitat de Girona. Departament de Electrònica, Informàtica i Automàtica. Marzo (2007)

[12] Wiley D. & Edwards K. Online self-organizing social systems: The decentralized future of online learning. Quarterly Review of Distance Education, 3:33–46. (2002)

[13] Yenta, L, & Foner 1997, A multi-agent, referral-based matchmaking system. In Proceedings of the 1st International Conference on Autonomous Agents, pages 301-307.

[14] Yu, B 2000, Mahadevan Venkatraman, Munindar P. Singh. An adaptive social network for information access: Theoretical and experimental results.

[15] Zimmermann, H 1980, OSI: Open System Interconnection, IEEE Transactions on Communications, vol. 28, no. 4, pp. 425 - 432.(1980)

[16] ADL, [2004], Advanced Distributed Learning. SCORM 2004 Sharable Content Object Reference Model. [Viewed April 2009], <http://www.adlnet.org/Pages/Default.aspx>

[17] Boneu, J. (2007), "Plataformas abiertas de e-learning para el soporte de contenidos educativos abiertos". Revista de Universidad y Sociedad del Conocimiento (RUSC). Universidad Oberta de Catalunya. 1698-580X. Vol. 4 Nro. I. pg. 36-47, [Viewed April 2009], <http://www.uoc.edu/rusc/4/1/dt/esp/boneu.pdf>

[18] IMS-CP, 2005, Global Learning Consortium. IMS Content Package. Version 1.2. Public Draft Specification, Viewed April 2009, <http://www.imsglobal.org/content/packaging/index.html>

[19] IMS-GC, (2009), Global Learning Consortium. [Viewed April 2009], <http://www.imsglobal.org>

[20] IMS-GWS, (2005), Global Learning Consortium. IMS General Web Service [Viewed April 2009], <http://www.imsglobal.org>

[21] IMS-LD, (2003), Global Learning Consortium. IMS Learning Design. Version 1. [Viewed April 2009], <http://www.imsglobal.org/learningdesign/index.cfm>

[22] IMS-MD, (2006), Global Learning Consortium. IMS Meta Data. Version 1.3 Final. [Viewed April 2009], <http://www.imsglobal.org/metadata/index.html>

[23] IMS-SS, (2003), Global Learning Consortium. IMS Simple Sequence. Version 1.0 Final Specification, [Viewed April 2009], <http://www.imsglobal.org/simplesequencing/index.html>

[24] LTSC. (2002). Learning Technology Standards Committee. Draft Standard for Learning Object Metadata. IEEE Standard 1484.12.1, New York: Institute of Electrical and Electronics Engineers, [Viewed April 2009] <http://ltsc.ieee.org/wg12/20020612-Final-LOM-Draft.html>

[25] OASIS,(2009), Advancing Open Standards for the information society, [Viewed May 2009] <http://www.oasis-open.org/home/index.php>

[26] Richardson, (2008). CSI: Computer, Crime & Security Survey. Computer Security Institute. Thirteen Annual. Published by Computer Secure Institute. [Viewed May 2009] <http://www.gocsi.com/>

[27] W3C-ARCH. (2004).Web Services Architecture W3C Working Group Note 11 February 2004. [Viewed May 2009], < http://www.w3.org/TR/ws-arch/ >

[28] W3C-ENC. (2002). XML Encryption Syntax and Processing. W3C Recommendation 10 December 2002 Viewed May 2009, <http://www.w3.org/TR/xmlenc-core/>

[29] W3C-KEY, (2001). XML Key Management Specification (XKMS). W3C Note 30 March 2001 [Viewed May 2009]. <http://www.w3.org/2001/XKMS/>

[30] W3C- SIGN. (2008). XML Signature Syntax and Processing (Second Edition). W3C Recommendation 10 June 2008. Viewed May 2009, <http://www.w3.org/TR/xmldsig-core/>