Maintaining Provenance throughout the Additive Manufacturing Process

Nawfal F. Fadhel, Richard M. Crowder, Gary B. Wills
ECS, University of Southampton, UK

Abstract

The introduction of affordable 3D printers made a significant impact on personal fabrication artistic designs that may or may not be covered by Intellectual Property Rights (IPR). Therefore copyright holders or creators of 3D objects have a legitimate concern about sharing 3D objects. This work presents a model for signing printable 3D objects to address the IPR issue. 3D files contain object geometry plus a number of attributes however it lacks security attributes when it comes to provenance procedures as it uses inherited security protocols for digital documents, digital media that are not intended for 3D objects. This paper reviews security principles of signing of objects in digital form, and the metrics for assessing digital signatures, then illustrate the shortcoming of digital signing principles and current provenance procedures for 3D printed object from digital sources.. The proposed digital signing methodology aims to transition all the meta data associated with the digital 3D object to the physical 3D printed object The new model allows the transition of provenance between digital and physical form. At the same time it will follow archival principles to maintain accurate records and provide provenance.

Keywords; Digital Signing; 3D printing; 3D objects; provenance.

1. INTRODUCTION

Additive manufacturing (3D printing) has been used in engineering since the late 1970's [2]. However only recently has the technology become widely available at reasonable cost. Currently 3D printers can be purchased from approximately $600 (£400). The low cost of this technology has raised a number of concerns such as the lawsuit by the Game Workshop [1], in particular how can the provenance of 3D printed object be proven and guaranteed. Currently many 3D objects that are produced by architects, designers and engineers are unpublished due to intellectual property concerns. These objects are frequently used to illustrate and share designs or ideas. The problems associated with breaches of copyright etc., could have severe implications on the culture of open access and sharing of 3D objects. Currently it is difficult to prove authorships or identity once an object is fabricated using a personal 3D printer unlike organizations who have legal obligations not to infringe copyright. The public does not have the same legal obligation as companies as it defined in law [1]

The digital document from which the object is printed is either acquired through digital capture devices, produced by a CAD system. Some of these 3D designs (digital documents) are protected by publishing them under Creative Commons Licenses[2] or making them available only to certain individuals. This work proposes a framework to achieving provenance for printable 3D objects fabricated using 3D printers.

The paper reviews a number of attempts to solve the issue of secure signing either directly or indirectly; such as creating a standard to covering it under the definition of a secure system as in ISO7498 standard for trusted hardware [2], using digital watermarking [3] or secure transmission for digital files that has the potential to be streamed directly to the 3D printer [4].

The proposed framework is intended for sharing information about 3D objects securely using signing methods, such that when the object is printed the following attributes are also transferred to the printed object:

- Authentication: we need to authenticate an object with a trusted party.
- Integrity: we need to track visible changes and ensures the object has not been tampered with.
- Non-Repudiation: we need to prove that the object belongs to a certain party within reasonable doubt.

This paper provided a framework to sign 3D printed object and to understand this framework we start a background on additive manufacturing and 3D object in section 2. Then explain the current protocols and legal framework to protect 3D content in section 3 and explain their shortcoming in section 4. Current literature discussing provenance and security procedures for 3D objects are explained along with the existing solutions for 3D objects in section 5. The foundation for our framework examines both the digital and physical requirements for 3D object because of it uniqueness of having a versatile state (Digital/Physical) in sections 6 and 7. The framework is explained in section 8 with a scenario to show how this framework would work. Lastly a discussion and conclusions is presented in section 9.

[1] News Article: C. Thompson, "3D printing's forthcoming legal morass," 2012.

[2] Organization: http://creativecommons.org

2. ADDITIVE MANUFACTURING

The additive manufacturing process can be effectively considered to consist of two distinct phases, the digitization of an object and then its manufacture by 3D printing, as summarized in Figure 1.

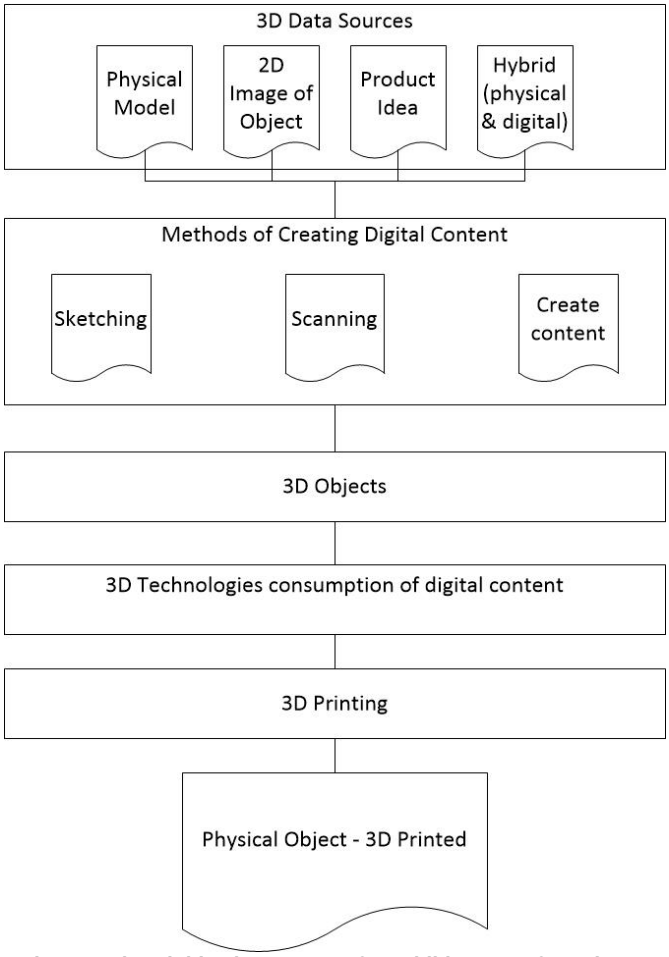

Figure 1 The Digitization process for Additive Manufacturing objects from concepts or existing product to fabricated objects or replicas

Figure 1 shows the steps required to convert a digital design to a digital object, and can be considered to require four steps:

- A digital representation of the object is firstly generated from a number of sources, ranging from scanning a model to a CAD drawing.
- The digital representation is cleaned by removing all the undesirable data and noise. The design is allocated physical data storage and the 3D object is stored in a digital state.
- The digital representation of the 3D object is fed into a slicing program that separate the object into layers, in preparation for fabrication.
- The fabrication process using an additive manufacturing machine to print out the object.

The 3D object contains the object's geometry and additional information, for example material, texture and color [6], this forms part of the meta-data if the digital data type is a STL file - or it's new derivative STL 2.0 [5]. The replacement for the STL format, AMF (Additive Manufacturing File) is defined in [6].

Once the digital information contained in the file has been processed into *slices*, the artifact can printed using additive manufacturing system. This process allows the artifact to be manufactured in wide range of materials including plastic, metal and ceramic.

The technology for 3D printing depends on the function of the fabricated object, in addition to its complexity and whether it will have movable parts. The final quality of the surface finish of a 3D printed artifact is dependent on the resolution capability of the printer used, the material used, and the method of printing. Currently available technologies for 3D printing include molten polymer deposition, granular material binding and photo-polymerization.

- Molten polymer deposition developed by Stratasys in 1988, is based on Fused Deposition Modeling (FDM) technology [7] and uses an ABS or PLA filament, which is heated to melting point and then deposited using a robotic head capable of moving three dimensions. Currently this is the technology that the low cost printers use.
- Granular material binding is a technology where a material powder (either a metal or polymer) is sprayed onto the object being printed and are heated with a laser to solidify, then another layer is added incrementally and this process will continue from until completion. The time to completion will depend on the detail level and accuracy required [7]. The unfused material also serves as a support for the layers that are being printed.
- Photo-polymerization is a 3D printing technique that exploits the property of certain liquid chemicals that changes state to a solid when exposed to UV light. The UV light is projected on a surface that is positioned on top of a liquid container with the surface is in contact with the plate; Then the UV light is displayed selectively on the plate initially then it start to build up on the layers of hardened material incrementally [5].

In these processes the additive manufacturing process builds an artifact using incremental layers of material typically 0.1mm in thickness.

2.1. Generating the 3D Objects

Development of 3D file types and digitization technologies is driven by a requirement for creating 3D content that also require special features such as colour, constellation, metadata and other features. Constructing 3D digital objects started with the development of the OBJ file format, which was followed a

number of file formats to accommodate different industrial or commercial needs which eventually lead to the adaptation of STL file format which was primarily designed to be used with stereolithography 3D printing technology designed by Hull [8].

2.2. Digitization principles

Acquiring a 3D representation can take place using one of four types of sources [9]:

- A digital copy of an object with the exact measurement being taken by a 3D scanner or similar system. The printed result is considered replica.
- **A** digital copy of the object is based on the object's fragments and document description of the missing areas of the original object, the printed result is considered to be a reconstructed replica.
- **A** digital copy of an artistic representation based on a description that documented in the archaeological records. The printed result is considered to be a dictated realization of the object.
- **A** digital copy of an artistic presentation based on description of an object that was mentioned in historical records the printed result is considered to be a inspired realization of the original design.

The 3D objects, can be acquired or created from a singular or multiple sources such is the case in reconstruction projects [9]. The generation of the content is also dependent on the application domain for example; in engineering and medical domains, the measurement systems needs to be precise and under controlled conditions for accurate results. On the other hand in archeology, when we have a number of viewpoints, either the actual physical objects or a description or artistic visualization of an object as described in texts etc. The selection of the digitization tool is important, as one expedition is different than the next one. Amico, Ronzino, & Iannone [10] discussed a specific benchmarking process that defines the technology for generating 3D content under harsh conditions discussed by Schafer in [11], which can affect the quality of the digitization but is compliant with the requirement for digitization. Furthermore the London Charter proposes a number of guidelines to be considered [12] when creating 3D objects for use in academia and museums.

At the end of the process of digitization regardless the results will in all probability exist as either a 3D CAD model or as drawings that contains the object geometry and a number of descriptors can be used as the input to the printing process.

3. OWNERSHIP AND DIGITAL RIGHTS OF A 3D OBJECT (PROVENANCE)

Attempts in the commercial and academic sectors regarding IPR have been considered at two levels, and are considered to be complex.

- The first, the content holder have the right to print the object but not own it and the object can either be viewed remotely via secure streaming like the attempt describe by Engel and Sommer [13] and Koller and Levoy [4]; It is unknown if this method would be widely adopted because of similar cases where Amazon deleted content from users Kindles claiming the users only had the right to rent them but not own [14].
- The second approach is you can possess the object but in order to secure it, it is provided with a watermark or similar feature that has to be incorporated. The watermarking procedure removes, modify or change a part of the object, and therefor can impinge on the purpose or quality of the object [3] reviews a number of these watermarking techniques.

Related to this we need to consider the Berne Convention for the protection of literary and artistic works (WIPO)[3] which states the copying procedure of artistic and literary works must be "*...substantial copied...*" to infringe its copyrights. In other words if forgers or illegal copyholders of 3D objects watermarks an object and removes part of it, the clam of ownership from the original author will be harder to prove because a substantial copying must occur and removing part of the object will only make it harder. This definition is somewhat different from the protection a patent or the implementation of a trade secret that can be invoked in the case of manufacturing.

Provenances of physical objects are addressed by a number of intellectual property laws, trademark and hallmarks. Investigating four scenarios that a 3D printed object can infringe on copyrights but in very specific conditions as explained in details by Bradshaw, Bowyer, and P. Haufe [1] these four areas are:

- Design protection, which protects the products that cannot be protected using copyright law or patent.
- Copyright protection, which protects creative works, which mostly cover literary and artistic works.
- Patent protection, which protects an inventor's invention for (normally 20 years) from remanufacturing without permission.
- Trade Mark protection, which protect the registered right of a company to indicate the origin of goods.

Watermarking present itsself as viable solution for providing provenance for 3D content but in reality the resulted object ceases to be a replica if the watermarking substantially affects the quality of the copy. In adding a signature to the 3D copy of object instead of subtracting or changing the information of a copy as in the case of watermarking we can retain *substantial copying* of the original.

Organization: [3] "Berne Convention for the Protection of Literary and Artistic Works", WIPO

4. SHORTCOMMING OWNERSHIP AND DIGITAL RIGHTS OF A 3D OBJECT (PROVENANCE)

As a result of the introduction of new digital file formats like AMF which is still in the drafting stages and existing formats such as (STL or STereoLithography) used in additive manufacturing to reproduce an object, the digital signing process needs to be reconsidered, because traditional signing methodologies' were not designed for 3D printing. The objective of the proposed framework (section 10) being to allow for the capability of proving the legitimately of any 3D object whether it is in a digital or physical state.

It is important to note that a 3D printed artifact do not currently have an identity or method of tracking; after the digital object is printed as it loses all of its digital security identifiers, and hence is effectively impossible to validate it authenticity, particular given the rapidly improving quality of the 3D printing process [1]. Hence the concern in both engineering (e.g. manufacture of out of specification components), or humanities (illegal copying of an object of significant historical content [15]).

5. PROTECTING 3D OBJECTS

The problem facing creators of 3D content is the issue of provenance, working with the issue of provenance of digital object is addressed through a number of solutions such as watermarking and digital signing. However Steganography is a suitable approach to hide information in physical objects and is defined as a covert measure of protecting information within information such as hiding images inside images or messages inside messages. Steganography and Watermarking are similar in the philosophy of hiding the information, as both uses parts of the same object they are protecting. Currently 3D printed object have no measurement of provenance but instrumental solutions such as hallmarking and Steganography from outside the digital domain could provide a viable solution.

5.1. Steganography

Steganography is the art of hiding information in ways that prevent the detection of hidden messages.[16]. This is the most common definition for. The existence of the message itself is kept hidden, however with the current techniques for cryptanalysis we can prove with acceptable accuracy that the cover medium has been exposed to manipulation and by cover medium we mean the data carrier for the hidden message [16]. Steganography can also be used for digital linkage and storage that can be achieved by embedding information into digital media, for example we can insert information such as personal or medical records into that persons digital image.

5.2. Digital Watermarking

Digital Watermarking: is a process of adding or embedding information into a digital media to prove its origin and protect the intellectual property. Watermarking is a provenance measure that is similar to digital signing, but the difference to signing is; signing is adding additional information to the object while watermarking subtracts a part of the object and alter it and place it back with the modification resulting in a altered version that is less similar to the original. This has been explored to proving provenance of 3D objects by using watermarking that are described by Alface and Macq [3] Watermarking is method where a part of the digital data is altered to imbed data containing information about the author of the object proving intellectual property claim [3], alteration such as changing the least significant bit in a digital image [17] or partial of physical geometry in the case of 3D watermarking [3].

5.3. Content Streaming

3D objects can be securely streamed using secure protocols such as HTTPS, the 3D data stream can be only viewed [4], it cannot be downloaded nor edited, some companies propose a new solution to streaming 3D content for 3D printers by streaming the content directly to the machine with the user downloading a copy, this method allows to the user to have a 3D printed copy but not own the digital file. For example a user commissions an artist to produce a piece of art although the user can print a copy, the user cannot download the original 3D data file that he/she commissioned to make. So this technology allows for licensing content but not ownership.

6. PHYSICAL REQUIREMNTS

As the provenance of 3D objects becomes more of a significant issue as more content is created, whether the native state of the object is native digital or natively physical, IPR remains in the hands of the creator of the object (engineer, artist, etc.).

For example, according to the aims of London Charter [12], where the digitization of cultural heritage artifacts is performed only when required, as result we are establishing two objects and one identity linking the original artifact with the replica.

6.1. Archiving and preservation of objects

In the field of archiving, it is common for archivist to use metrics such as Kipling's approach known as the 5W's and the H of journalism which are; *when* the record was appraised, *what* was appraised, *why* is was appraised, *how* were records appraised. *Who* and *where* are not mentioned but are implied.

Bantin [18] notes while archivist would have liked more semantics that describe the object to assist the archivist in proving maintenance of records, archaeologists practice a similar attitude as they study of materials when handling physical objects.

The requirements mentioned by Bantin [18], described the archiving of electronic records using Kipling method, which align in principle with *authentication, integrity* and *non-repudiation,* used by the Internet Engineering Task Force requirements for secure digital signing [19]

6.2. Provenance of objects

Within artistic communities, artists place the highest priority on proving provenance of an artistic work is given, taking precedence in the digitization process of artifacts or sharing a digital designs more widely [21] It is our view that for the provenance of physical objects we can use semantics in an identical mechanism to that used for the signing of the digital document.

The semantics can include the author of a document, acknowledgment of the reception of a document by a second party, witnessing the document signature and lastly agreement that the document is genuine.

For scholarly publication and the identity of data sets prior to digital publishing [20], it was noted that authorship in the academic circles serves a number of purposes. Firstly it provides individual ownership for the academic work to each of the contributor. Secondly it assigns credit to an academic(s) for their new discovery and finally it promotes academic reputation in a particular field of research.

Relating to this paper, we are looking at the transition of the identity of an object from the state where its claim of identity is proven in digital state to proving its claim of identity in an artifact after is has been 3D printed, by achieving the same three criteria; confidentiality, integrity and availability, which also makes our framework agnostic.

It has been suggested that cryptographers disregarded semantics about the object's origin and background and focus more on the security between participating partners in a transaction; The public key infrastructure and the information used in the signing process as constructed by cryptographic community currently can falls short in describing a 3D objects from a archival prospective. It can be concluded that by considering the material and meta-data of an object would benefit from using semantics when describing 3D printed objects.

7. DIGITAL REQUIREMENTS

Security principles have three main components, the information security, the information authenticity and the information transmission [33]. But first we need to establish a digital identity

7.1. Digital Identity

There is a general acceptance for the current signing principles and roles followed in the digital and physical domain, implementation of signing principles on additive manufacturing objects or 3D objects will contribute to digital identity using the uniqueness of the signed objects [22] Using the framework presented in Figure 2 Digital identity can be established by assigning a unique identifier to a data set using the signing data [23]. Currently unique identification numbers are assigned to physical object such as in packaging products, we can produce uniqueness in a 3D printed object by adding to signature to the 3D design rather than removing a part like in the case of watermarking 3D objects where the least significant bit is manipulated to imbed information [3]. Our model insures the integrity of a 3D object because we do not remove from the object only add to it.

7.2. Information security

The first element regarding the technology more precisely is physical Security, which has the following components:

- Confidentiality: is a property where information is only disclosed to authorized individuals, parties or processes [2].
- Integrity: In computer science data integrity is defined as the process where data is maintained to achieve a high level of accuracy and consistency over its life cycle [24].
- Availability: is a property where authorized access is provided upon request from a trusted individual, party or process [2].

7.3. Information authenticity

The principles for digital signing have not change since its introduction in electronic exchange; Digital signing, is the authenticity of electronic mail is proved genuine by providing evidence that the message has not changed and the sender is identified [22]. Digital signature holds the same value of a hand signature but is constructed using digital means to render it immune to counterfeiting; Digital Signature is used in signing confidential document and is an undeniable by the originator and receiver of the message.

The First element regarding securing the information using digital signing has the following components [22], [25]:

- Authentication: Is a property where a claim of identity is verified, The term authentication is used in conjunction with integrity, which is defined according the British standards as a property in which the data has not been altered or destroyed in unauthorized procedure [19].
- Integrity: same definition that is used in physical security component as data integrity but only for digital component and does not extend to the hardware [24].
- Non-repudiation: While Non-repudiation is a state where the entity involved in a communication with other entities is unable to deny involvement in the communication between parties [2].

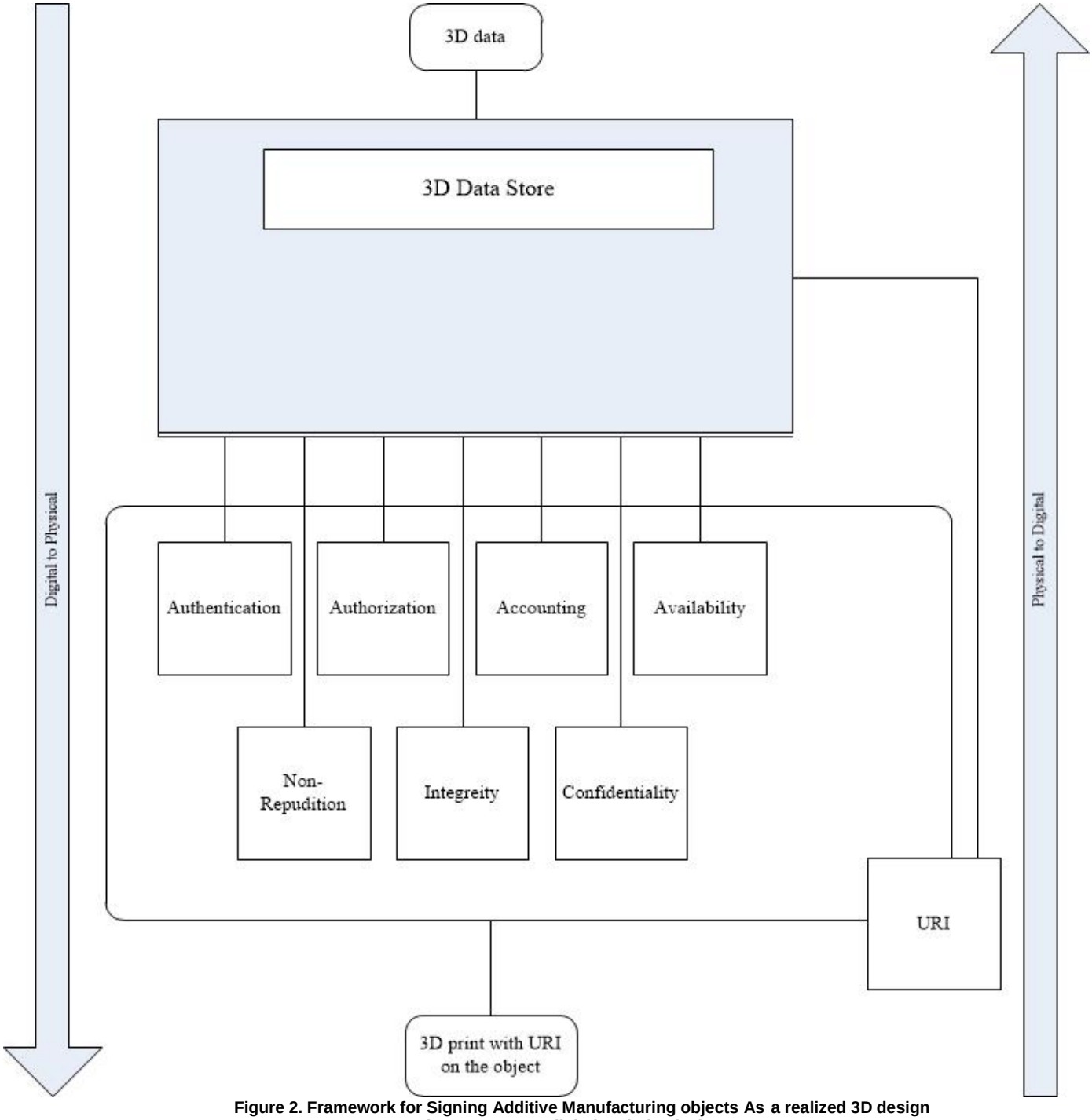

Figure 2. Framework for Signing Additive Manufacturing objects As a realized 3D design has two states, digital and physical.

The Second element for digital signing is to fill full some basic elements as described in [22], [25]

1. In digital signing a party of at least three is needed and that's why a signing authority is called a third party.
2. When signed information is stored and accessed a transmission occurs because provenance is achieved using a third party.
3. The signature contains the information about the signed material and that's the message.

7.4. Information transmission

The third element regarding the transmission of information has the following components:

- Authentication: same definition that is used in digital security component.
- Authorization: is a property where access is granted to resources based on access rights [2].
- Accounting: is a property where actions and interaction can be uniquely identified and traced [2].

Based on these definitions and our understanding of the problem we can combine the digital security attributes described above with the physical provenance methods. If the object was created in digital state then it can be recreated in a physical state via 3D printing and if the object is in physical state it can be digital scanned and becomes a digital object. The framework in **Error! Reference source not found.** is tailored to enable the transition of properties from the digital object to the physical 3D printed object.

8. THE PROPOSED SECURITY FRAMEWORK

Constructing a proposed framework for digital signing 3D objects requires us to place the logical semantics of signing methods in the digital domain and the claim of providence in the physical domain in one framework so they are linked. We have to go back to the basics of authentication and digital signing, although they are not design for use with 3D object, they can provide us with the metrics and semantics that were used to build the digital signing models. In **Error! Reference source not found.** a framework for signing additive manufacturing objects is presented where three attributes (authentication, integrity and non-repudiation) reside within the digital domain, and three attributes (confidentiality, physical integrity and availability) are placed in the physical world.

If the object was created in digital state then it can transition to a physical state via 3D printing and if the object is in physical state it can be digital scanned and becomes a digital object, hence the framework is domain agnostic. In Figure 2 the signing principles for the digital and physical objects the state of the object determines the signing methodology.

In summarizing the logic and need for the new signing framework for additive manufacturing objects we need to consider five points:

- According to the definition by NSTISS security system model acknowledges information not technology [21]. BSI standard of 1989 extend to the technology to establish trust outside the OSI model, which by definition can include trusted hardware.
- Digital artifacts have significant applications, For example, as an educational and learning tool in humanities or as a product in the engineering design process [12].
- XML format of the additive manufacturing file format has room for future amendment [6].
- According the draft ISO 52915 x.2.1.6 [6] lists provisions for future copyright protection and water marking but does not mention digital signing.
- Watermarking remove part of the object this process disrupts substantial copying of original artifacts [1].

These five points illustrate valid reasons and technological ability for creating a transitional signing model where the provenance is transferable from digital to physical form.

8.1. Scenario for creating and protecting printable 3D content

Consider the following scenario using the framework in Figure 2, an artist designs a lamp that has certain aesthetic qualities and shares it with friends and colleagues online. The artist would like to put a unique identifier on the object to protect the intellectual property of the digital design, when the object is 3D printed; the unique identifier is printed with the object. When the artist wants to establish provenance of the 3D printed object, a scan of the unique identifier will provide all the information and security attributes about the object.

Let us retell the scenario from the system point of view, an object is created in a digital state, this object has good amount of information about the object such as author, size creation date, access logs an other digital attributes. The system would attach a unique identifier to this object to point at all of these attributes, when the object is 3D printed with the unique identifier all the information about the object can tracked to the original digital object. The system can identify the 3D printed object through the unique identifier and retain its identity.

This research has investigated a solution using a new signing framework method to protect provenance of 3D content. This framework operates with or without steganographic methods for adding signature that could be extracted digitally from the 3D printed object.

The new signing methodology could be also employed in the manufacturing sector, such that a company would be able to sign an object from the inside or outside to establish provenance.

8.2. Digital Creation and Signing Scenario

The scenario in **Error! Reference source not found.** represents a provenance scenario to address the concerns of intellectual property holders when publishing 3D digital content, including safe delivery and transferring ownership of the digital content when the object is purchased, can also provide licensed prints if the creator wishes to retain ownership of the intellectual property.

1. Digital content creator whether a designer, engineering or digitizer creates the content. A digitizer is an individual who is scans a physical object.
2. 3D file is created in a digital file format (ST, PLY, AMF, ect).
3. 3D file is converted to AMF. The file is converted to AMF because AMF has support for security metadata.
4. A digital object identifier is generated and attached to the AMF file.
5. The AMF file is published where information about the object is catalogued and stored.

6. The content providers store the secured AMF files available for free or purchased download.
7. User Searches for an object that fill full his requirement.
8. User purchases the object then they download it.
9. User 3D Prints the object from the AMF file.
10. The physical object is created with a physical object identifier on it that is readable using the naked eye or hidden steganographically that can only be read through special digital scanning method.

8.3. Read and Retrieve Scenario

Error! Reference source not found. is a scenario-proving claim of ownership or simply investigating the object origin, the authenticity and rights for 3D printed objects and rights associated with it can be extrapolated from the physical object identifier

.

1. A 3D object is scanned for POI or read by naked eye if it was printed on the surface of the object.
2. The POI is searched for with content provider to find the object.
3. The data is fetched and access rights and privileges for that specific unique POI.
4. The original 3D file information is provided also the file it self if the user purchased multiple access or owner of the content.

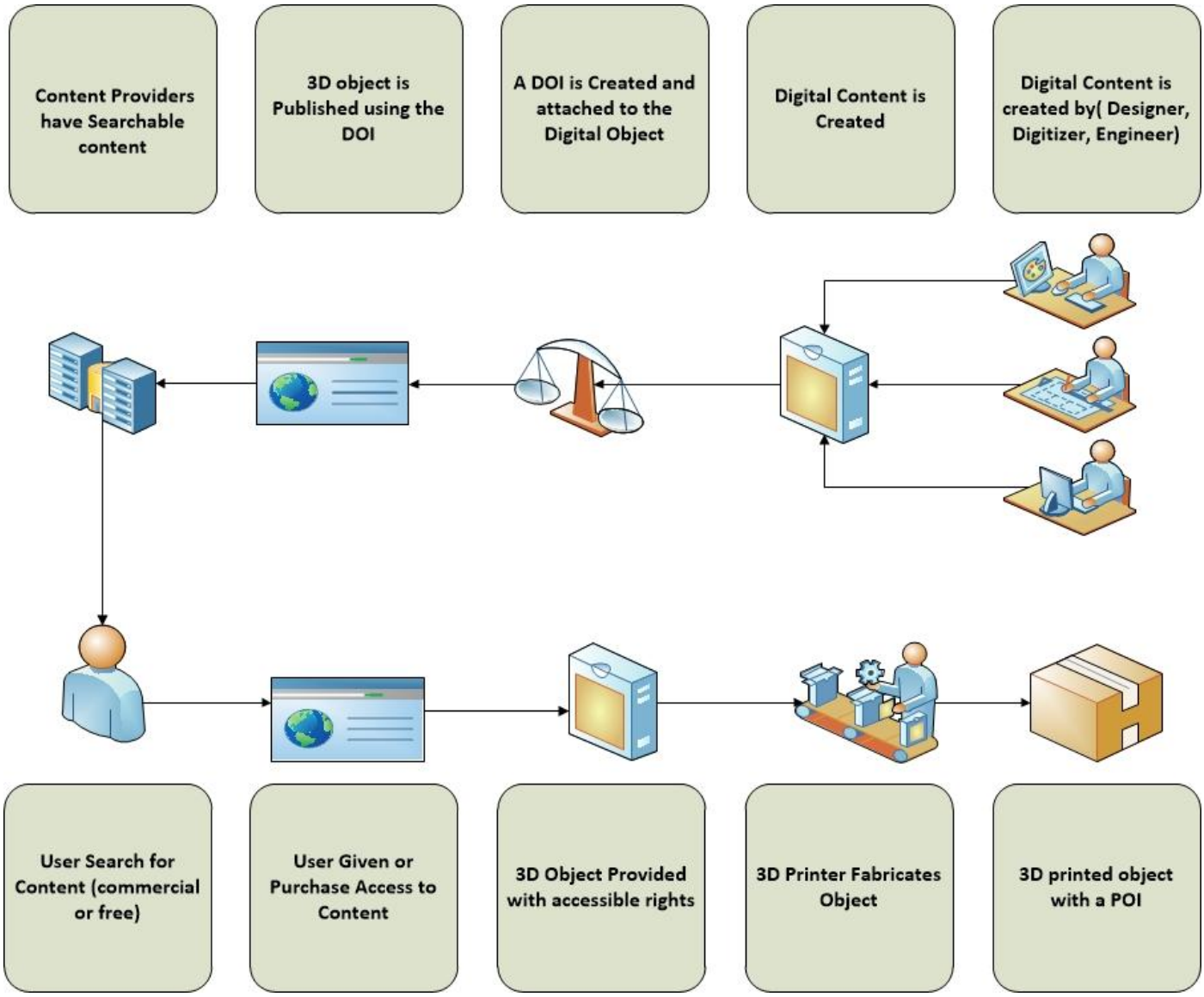

Figure 3. Digital Data creation to content provider then to users for 3D printing

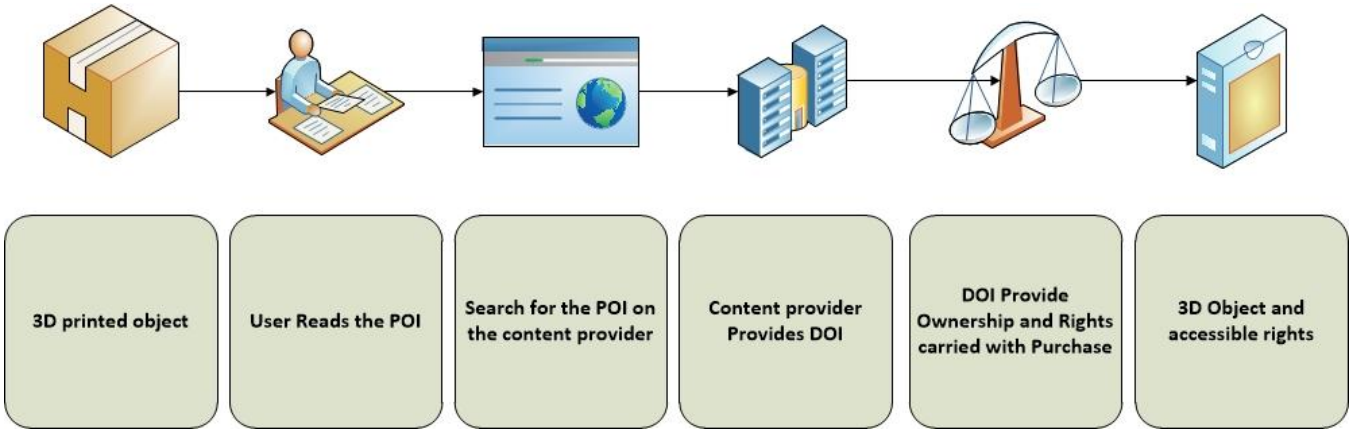

Figure 4. User checking physical object identifier to provide authenticity and digital object if rights owned

9. DISSCUSSION AND CONCLUSION

The basis for the designing a provenance framework that can be applied to any additive manufacturing objects has its roots in digital signature and could be further explored to incorporate semantics of 3D objects used to describe cultural heritage 3D object or printable copies of artifacts.

However due to public adaptation and demand for customized 3D printed products such as prosthetics or artistic object designs of household objects and jewelry, 3D object can also be referred as genuine 3D objects with a native digital state. After the additive manufacturing the object constructed is referred to as prototype, replica and often that's the case.

Intellectual copyright protection on 3D object and additive manufacturing according to [1] for the UK and [8] in the US, private owners of 3D printers are vastly exempt from the majority of intellectual property constraints when making 3D objects for non-personal gain, also less restricted commercial usage. As private owners of 3D printers are vastly exempt from the majority of intellectual property constraints when making 3D objects and currently there is no mechanism for audit, secure and track these 3D printed objects

Therefore there is a need for a secure technical process for transition of security attributes that establish the IPR of 3D objects from digital to physical state and back again. Technologies that back up the Intellectual copyright property for 3D objects are watermarking as illustrated survey by [3] and secure transmission using HTTPS using in the Michelangelo project [4].

Within the current literature attempts to enforce digital right management invariably discuses the use of watermarking, which has negative implication on the copying process. The use of digital signing introduces uniqueness to the objects, which contributes to the digital identity of additive manufacturing objects. It is our contention that we have established a need for the framework since there is no method of provenance transition between physical and digital objects. In this paper we have demonstrated that both the standard and the technology have the capability of accommodating the new model. We have explained shortcomings in the current state of proving claim of ownership in 3D printed object as also reviewed by Bradshaw [1]. We will continue apply the framework extension to copies of copies; such as scanning a finished additive manufacturing object with its signature in physical form and produce a digital model again. We will also investigate if the signatures on a 3D printed object produced using our model is transferable when captured digitally using scanning methods.

10. REFERENCES

[1] S. Bradshaw, A. Bowyer, and P. Haufe, "The intellectual property implications of low-cost 3D printing," ScriptEd, vol. 7, no. 1, pp. 5–31, Apr. 2010.

[2] I. ISO, "7498: Information Processing Systems, Open Systems Interconnection, Basic Reference Model," Int. Stand. Organ. Geneva, Switz., 1984.

[3] P. Alface and B. Macq, "From 3D mesh data hiding to 3D shape blind and robust watermarking: a survey," Trans. data hiding Multimed. Secur. II, pp. 91–115, 2007.

[4] D. Koller and M. Levoy, "Protecting 3d graphics content," Commun. ACM, vol. 48, no. 6, p. 74, Jun. 2005.

[5] J. Hiller and H. Lipson, "STL 2.0: A Proposal for a Universal Multi-Material Additive Manufacturing File Format," Proc. Solid Free. Fabr. …, no. 1, pp. 266–278, 2009.

[6] "Draft BS ISO DIS 52915 Additive manufacturing file format (AMF) Version 1.1," vol. 44, no. 0, 2013.

[7] R. a. Buswell, R. Soar, A. Gibb, and A. Thorpe, "Freeform Construction: mega-scale rapid manufacturing for construction," Autom. Constr., vol. 16, no. 2, pp. 224–231, Mar. 2007.

[8] Connor M. McNulty, Neyla Arnas and and T. A. Campbell, "Toward the Printed World: Additive Manufacturing and Implications for National Security," no. 73, 2012.

[9] C. Neamtu and S. Popescu, "Using reverse engineering in archaeology: ceramic pottery reconstruction," J. Autom. Mob. Robot. Intell. Syst., vol. 6, pp. 55–59, 2012.

[10] N. Amico, P. Ronzino, and G. Iannone, "Developing an 'Archaeological' Benchmarking Procedure," Proceeding 39th Conf. Comput. Appl. Quant. Methods Archaeol., 2011.

[11] B. B. and H.-G. B. Anja Schäfer, Hubert Mara, Julia Freudenreich, Christiane Bathow, "Large Scale Angkor Style Reliefs: High Definition 3D Acquisition and Improved Visualization using Local Feature Estimation," in Proc. of 39th Annual Conference of Computer Applications and Quantitative Methods in Archaeology (CAA), 2011.

[12] H. Denard, "The London Charter for the computer-based visualisation of cultural heritage," no. February, pp. 1–13, 2009.

[13] K. Engel and O. Sommer, "Remote 3d visualization using image-streaming techniques," ISIMADE-11 TH Int. Conf. Syst. Res. Informatics Cybern., 1999.

[14] M. Belanger, "Amazon. com's Orwellian Gaffe: The Legal Implications of Sending E-Books Down the Memory Holy," Set. Hall L. Rev., vol. 1, 2011.

[15] R. K. Jr, "Uniform Commercial Code Warranty Provisions and the Theory of Strict Liability in Tort as Solutions to Art Counterfeiting in Painting: A Critical Analysis, The," . Louis ULJ, vol. 1, 1975.

[16] H. Wang and S. Wang, "Cyber warfare: steganography vs. steganalysis," Commun. ACM, vol. 47, no. 10, pp. 76–82, Oct. 2004.

[17] W.-N. Lie and L. C. Chang, "Data hiding in images with adaptive numbers of least significant bits based on the human visual system," in Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on, 1999, vol. 1, pp. 286 –290 vol.1.

[18] P. Bantin, "Strategies for managing electronic records: a new archival paradigm? An affirmation of our archival traditions?," Arch. issues, pp. 1–22, 1998.

[19] C. Cullen, P. Hirtle, D. Levy, C. Lynch, and J. Rothenberg, Authenticity in a Digital Environment., no. May. 2000.

[20] J. Birnholtz, "What does it mean to be an author? The intersection of credit, contribution, and collaboration in science," J. Am. Soc. Inf. Sci. Technol., vol. 57, no. 13, pp. 1758–1770, 2006.

[21] J. McConnell, "National Training Standard for Information Systems Security (INFOSEC) professionals," no. 4011, 1994.

[22] D. Davies, "Applying the RSA digital signature to electronic mail," Computer (Long. Beach. Calif)., vol. 16, no. 2, pp. 55–62, 1983.

[23] L. Wynholds, "Linking to scientific data: Identity problems of unruly and poorly bounded digital objects," Int. J. Digit. Curation, vol. 6, no. 1, pp. 214–225, 2011.

[24] J. E. Boritz, "IS practitioners' views on core concepts of information integrity," Int. J. Account. Inf. Syst., vol. 6, no. 4, pp. 260–279, Dec. 2005.

[25] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

