Assured Content Delivery in the Enterprise

Coimbatore Chandersekaran, and William R Simpson

***Abstract*— In the era of wikileaks and the sensitivity of information assets in an enterprise system at all classification levels, there exists a need for assured content delivery. The promise of Digital Rights Management (DRM) has yet to be realized and knowledgeable analysts opine that it may never be achievable. It will certainly need copious amounts of specialized software and maybe even specialized hardware before information assurance can be satisfied. We do not rely on DRM technologies at this point, but reserve the right to review future developments in this area. None-the-less, there exists a need for an assured content delivery process for enterprise authoritative documentation. We propose a process of culling the authoritative information and placing it in an authoritative content repository. Content in this repository is available only through a service request and "browsing" of the content is not permitted. The existence of the information asset and related information assets may be obtained from search engines or other references. The content store has a librarian that is a collection of software and manual processes, and a retrieval service. These two aspects provide for the authenticity and authority of the content. In an environment of trusted individuals we place our loss of control mitigation in the notification of restrictions and the diligence of the users. This enterprise solution is part of a larger enterprise architecture that is web-service based and driven by commercial standards and includes naming, certificates issuance for identity and Public Key Infrastructure (PKI), mutual authentication and confidentiality through transport layer security, and digital signatures for integrity among other concepts. These are described in several of the references and are currently undergoing initial operational capability standup.**

***Index Terms*—** Digital Rights Management, Content Protection, Access Control, Authorization, Record Management

I. INTRODUCTION

Content or information assets will include documents, spreadsheets, web pages, presentations and other complete or incomplete sets of information. All information assets will be considered authoritative and be under rights management. The rights management will be an integral part of the development of these contents. As much as is possible, the workings of the rights management system should be transparent to the user. This is as much for records keeping as well as control.

Manuscript received December 15, 2011; revised March 3, 2012. This work was supported in part by the U.S. Secretary of the Air Force and The Institute for Defense Analyses. The publication of this paper does not indicate endorsement by the Department of Defense or IDA, nor should the contents be construed as reflecting the official position of these organizations

Coimbatore Chandersekaran is with the Institute for Defense Analyses.(email: cchander@ida.org)
William R. Simpson is with the Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, Virginia 22311 USA and is the corresponding author phone: 703-845-6637, FAX: 703-845-6848 (e-mail: rsimpson@ida.org)

Several concepts are reviewed in the next sections that apply to content delivery, before getting into the details of distributing assured content:

a. The concept of Digital Rights Management.
b. Mandatory Access Control
c. Metadata and Metacards
d. Creation of an information asset in an authoritative data store.

II. *CONTENT DELIVERY AND DIGITAL RIGHTS MANAGEMENT (DRM)*

DRM technologies attempt to control use of digital media by preventing access, copying or conversion to other formats by end users. Long before the arrival of digital or even electronic media, copyright holders, content producers, or other financially or artistically interested parties had an interest in controlling access and copying technologies. Examples include: player piano rolls early in the 20th century [1], and video tape recording [2]. The advent of digital media and analog/digital conversion technologies, especially those that are usable on mass-market general-purpose personal computers, has vastly increased the concerns of copyright-dependent individuals and organizations, especially within the music and movie industries, because these individuals and organizations are partly or wholly dependent on the revenue generated from such works.

The advent of personal computers as household appliances has made it convenient for consumers to convert media (which may or may not be copyrighted) originally in a physical/analog form or a broadcast form into a universal, digital form (this process is called ripping) for location- or time-shifting. This, combined with the Internet and popular file sharing tools, has made unauthorized distribution of copies of copyrighted digital media (digital piracy) much easier. DRM technologies have enabled publishers to enforce access policies that disallow copyright infringements. DRM is most commonly used by the entertainment industry (e.g., film and recording). Many online music stores, such as Apple Inc.'s iTunes Store, as well as many e-book publishers have implemented DRM [3]. In recent years, a number of television producers have implemented DRM on consumer electronic devices to control access to the freely-broadcast content of their shows, in response to the rising popularity of time-shifting digital video recorder systems such as TiVo [4].

Common DRM techniques include:

- Embedding of a tag(s) (This technology is designed to control access, distribution and reproduction of accessed information) [5],
- Encryption [6], and
- Scrambling of expressive material [7].

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Many DRM schemes use encrypted media which requires purpose-built hardware to hear or see the content. This appears to ensure that only authorized users (those with the hardware) can access the content. Additionally, purpose built software for the content can enforce restrictions on saving or modifying content, and dates of applicable use, etc. It additionally tries to protect a secret decryption key from the users of the system. While this in principle can work, it is extremely difficult to build the hardware to protect the secret key against a sufficiently determined adversary. Many such systems have failed in the field. Once the secret key is known, building a version of the hardware that performs no checks is often relatively straightforward. In addition user verification provisions are frequently subject to attack, pirate decryption being among the most frequented ones. A common real-world example can be found in commercial direct broadcast satellite television systems such as DirecTV and Malaysia's Astro. The company uses tamper-resistant smart cards to store decryption keys so that they are hidden from the user and the satellite receiver. However, the system has been compromised in the past, and DirecTV has been forced to roll out periodic updates and replacements for its smart cards.

DRM within defense enterprises is of paramount importance for both protection of assets from wiki-leaks type incidents, and in records management. DRM in the defense enterprise context – is the restriction of access and movement of information within the defense enterprise and the release of the information outside of the defense enterprise.

A. *Mandatory Access Control*

Mandatory Access Control (MAC) is a system of access control that assigns security labels or classifications to system resources and allows access only to entities (people, processes, devices) with distinct levels of authorization or clearance. These controls are enforced by the content delivery system. For example, the delivery system should not deliver a NATO only information asset to a requester without NATO claims. These principles also apply to delivery of classified information assets to holders of the appropriate security clearances. With content delivery, changes to authoritative data are not allowed and MAC consists of four basic elements:

a. Enforcing Access control, including read/ copy/ print/ store/, etc.
b. Labeling the information asset and content parts and restrictions within an information asset.
c. Conveying the restrictions to the requestor including screen displays where appropriate
d. Enforcing restrictions or obtaining acknowledgement of these restrictions from the requestor.

B. *Enforcing Access Control*

Enforcing access control is through the discretionary access control process. After bi-lateral authentication, the requester presents claims in the form of a Security Assertion Markup Language (SAML)[1] token [8]. Claims in the SAML token are compared to Access Control Lists (ACLs) in the information asset. In certain cases, in order to promote information sharing, the requester may have the right to override the hardware and software requirements, but this is not available for classified information. The claims are used to limit the authority over the data as shown in the list below:

Claim 1: read, copy, retain the information asset.
Claim 2: read only on screen, may print the information asset but not cut and paste any parts of the information asset, cannot save to user environment in electronic form read only on screen With MAC displays present, no other privileges.

The details of these claims and their names are part of the use cases. However, some additional considerations for the MAC control include the hardware and software compatibility. In a “compliant” environment as discussed above, and with the separation of classified and unclassified, standard hardware and software will be enforced.

C. *Labeling of Content and Information Assets*

Labeling, when combined with ACLs based upon use cases, and claims presented by requesters provides a tightly coupled combination of mandatory access control and discretionary access control. Since labeling is the basis for access, the labeling system must be uniform and trusted. Uniformity is achieved by standardized approaches and criteria. Standards exist for use by the enterprise. [9-11]. Labeling also carries restrictions for reproduction or usage of portions of the material provided and what attributions and labeling must be made upon such usage, if permitted.

D. *Conveying Restrictions to the Requester*

Depending upon the level of access granted, there are multiple ways to convey the restrictions to the requester. Restrictions include modification (any modification causes the signature check to fail), reproduction and storage (including which stores are appropriate), distribution restrictions, and required receipts (if any), and re-use of content whole or in part. These restrictions are store with the MAC displays. The following factors apply:

If the requester is an individual viewing the information asset without the ability to save or extract information, the display can be tailored to provide the restrictions in prominent form (usually banners at the top and/or bottom of the screen). Classified banners are Red with white lettering; unclassified banners are blue with white lettering.

If the requestor is an individual with the permission to store and save the information, or the requester is not an individual, the entity must be provided the restrictions placed upon the material.

Requesters who are individuals may get the banners when the information is displayed, but also get the restrictions again when storing or saving the information.

In any of these scenarios, the labeling must stay with the information asset and the information asset may not be edited and returned to the authoritative content store, except

[1] S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005.

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

by changing the version number and submitting it to the librarian for rework.

E. *Enforcing or Obtaining Acknowledgement of Restrictions*

Information sharing must be logged as an event in the logging format of the enterprise web services, and periodically reviewed. Abuse of such sharing treated as a disciplinary problem and possible suspension access. Saving of the file, printing or cutting segments to memory can only be done by authorized individuals and does not proceed until an acknowledgement of the distribution and access restrictions is obtained. These acknowledgements must be logged as a special event in the logging format of the enterprise web services, and periodically reviewed.

F. *Metadata Cards*

Metadata (metacontent) is traditionally found in the card catalogs of libraries. Metadata is also used to describe digital data using metadata standards specific to a particular discipline. By describing the contents, key words, concepts, and context of data files, the quality of the original data/files is greatly increased. For example, an information asset may include metadata specifying what language it's written in, what tools were used to create it, key words and concepts that may be used by a search engine to discover which information assets relate to a specific subject or concept. The metacard is used to hold all of the meta content and its reference data for a subject information asset. The defense enterprise will use a metadata card that is based upon full text indexing with content as described below. This metacard will be used by search engines within the defense enterprise. This card may be converted to a DDMS Metacard where needed [12].

G. *Creating an Information Asset*

When an information asset has been through an appropriate level of review, and deemed to be useable for reference and/or the source of action or authority, it may be submitted to a librarian for inclusion in an authoritative content store.

III. The Rights Management Function

The Rights management is a collective concept that includes the automated and manual processes to accomplish the steps below:

a. The information asset must be labeled for access and distribution; this is done by the author. Defaults may be assigned absent author input and are defaulted to the most restrictive case. Such labeling may include classification, availability and distribution such as Unclassified NATO only or SECRET, FOUO, NOFORN. Communities of Interest (COI)s develop standard access use cases to compute claims, while others, such as GroupX ONLY, requires access use cases be developed and provide to the Enterprise Attribute Store (EAS)[2]. If a standard use case is not available, an access use case is dynamically generated based on defaults and user specifications. The information asset is also labeled by the author as "draft" or "final". When more than one signature is appended, this label can be changed to "approved" by the user if this is an officially approved/sanctioned information asset. These tags are part of the metadata that is recorded for the information asset.
b. Signed by the author for content integrity (additional signatures may be affixed for authority, see section below).
c. Generation of associated metadata.
d. Assignment of an identity (name) – defaulted by the system but can be changed by the user.
e. Author assignment of the actual storage location on the network and filing of the cross-reference between the location and the identity of the asset. The information asset is stored in an enterprise location and/or a personal location for author retrieval and further work.
f. Presentation of a rights information request page (defaulted to read/write/delete rights to the creator and read/delete rights to all others and signature. If additional group-level rights are required (e.g., COI group, special-access group), these are specified at this time. The rights information is stored in the ACL data store as well as in the EAS.
g. Examination of the MAC labels and where an information asset is not unclassified and not available to all (internal/external), encryption of the information asset and the attachment of an appliqué to the information asset which is used to communicate to the Rights Manager for access control. . If the information asset is not MAC labeled and is available to all internal and external, the information asset is not encrypted.
h. Both encrypted and unencrypted assets may be further distributed without consequence.

To access an information asset, the appliqué attached to the content program for the information asset examines the information asset and if it is encrypted communicates to the Rights Manager via a secure web session to verify claims. If a user is going to be out of communication, a local copy of the information asset with an associated Trust Package can be loaded onto the user's device. This copy triggers a message to the rights manager to add this storage location to the metacard. When the user connects to the network, the Trust package invokes the appliqué on the content program to set up a web session between the user and the Rights Manager for applying rights to the modified information asset. Retrieval of the encrypted information asset invokes the appliqué again and a session is initiated with the content retrieval service.

A. *The Components of a Stored Information Asset*

The components of a stored information asset are provide in Figure 1 and must be created in steps as described below:

Formatted Document Section a. Information Labeled

Provided by the rights management software with defaults based upon user COI memberships or by user from approved list, also includes "draft", "final", or Approved as previously described. Labels may be reviewed and modified by the author.

[2] The EAS is a special store that contains data and attributes of enterprise entities that are used to make access claims.

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

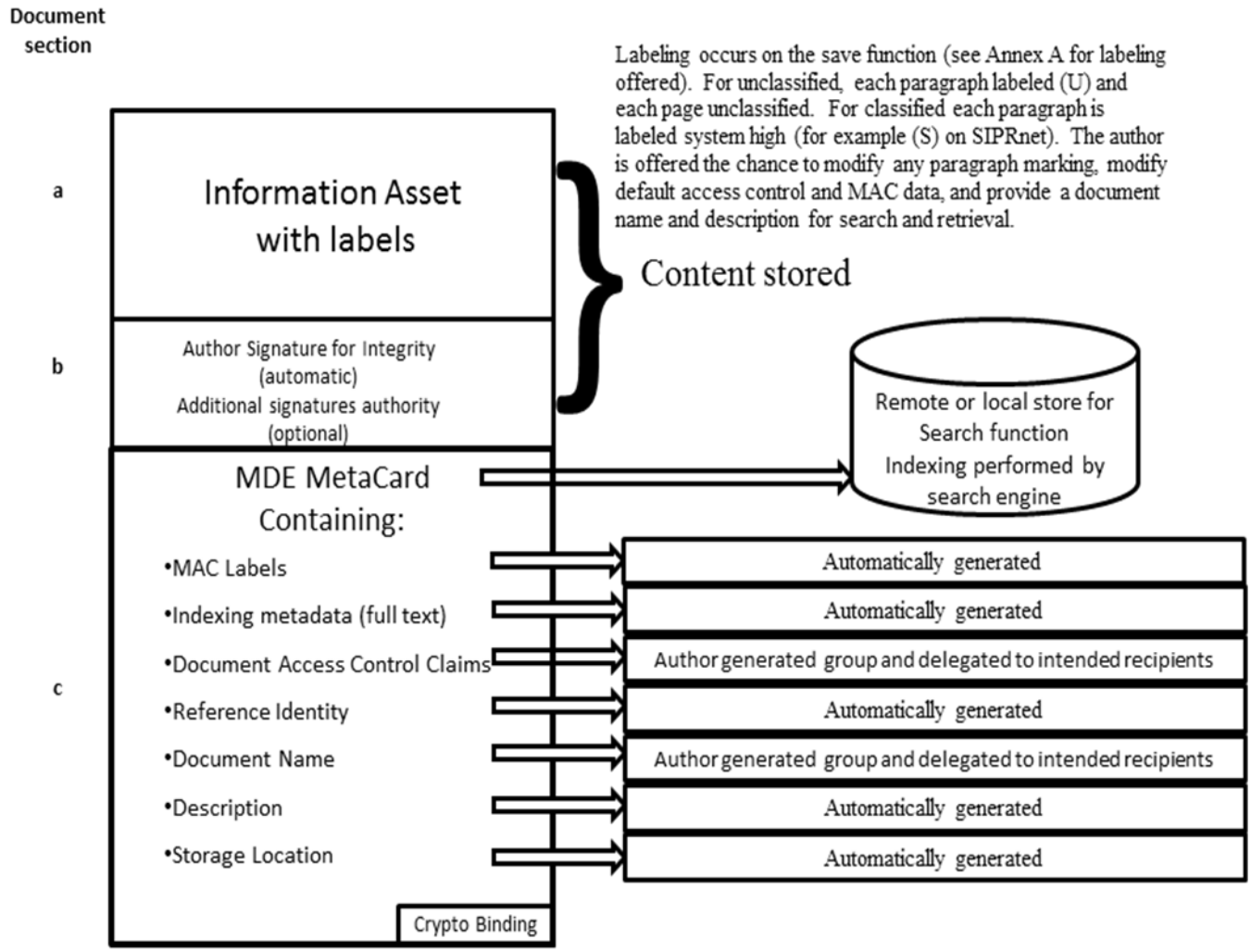

Figure 1 Authoritative Content Information Asset Format

Formatted Document Section b. Information Asset Signature(s)

The author's signature (and others) are added and further changes to the information asset at this point are prohibited. Revisions are treated as a new information asset with either name changes or versioning. Any changes required to get additional signatures, starts the process over again. The information asset may be retrieved (using the content retrieval software) by authorized users and additional signatures applied as long as the information asset is not revised.

External Information c. MDE Metacard

The Meta Data Environment (MDE) Metacard is prepared. This involves a number of items described below: It should be noted that most information assets are not directly retrievable and it must be retrieved by the content retrieval service for checking of ACLs, MAC issues and restricted authorities. The exception is unclassified, unlimited distribution.

- Mandatory Access Control Labels

These are taken directly from the trusted labeling of the information asset, and are for applying MAC screens and restrictions.

- Key Word MetaData

The key words are developed from full information asset text scan and/or can be manually entered.

- ACL Lists and Associated Data

The primary ACL is provided by the author (example, "MyGroup"). The rights manager must go to the EAS and verify that the claim does not already exist and ask for an alternate if it does. Once the label is chosen the rights manager inserts this as a delegatable claim of the author. The delegation service is then invoked and the claim may be delegated to individuals from the Global Access List (GAL). The author may also designate organizational units as having the claim.

- Reference Identity and Information asset Description

This is the mechanism for retrieval. The rights manager software defines the identity to prevent duplication, ambiguity or confusion in the information asset file keeping system.

- Information asset Name

The rights management software will provide a default name. It may be modified by the author.

- Information asset Description

The rights management software will suggest a description based upon a title or lead heading. It may be modified by the author.

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

- Storage Location(s)

This is the actual storage location of the information asset in network asset store. Each time an unmodified copy of the information asset is stored in a different location, the appliqué provides that location and the unique id of the information asset to the rights manager for updating the metacard. The metacard may contain any number of storage locations. This latter allows cleanup when archiving old content.

The content is encrypted (except when the information asset MAC indicates unclassified with no distribution limitations) with key management being maintained by the rights manager and available to the content retrieval software. A copy of the encrypted content may be store locally, together with key material for off-line usage for a time not to exceed one week. On next connection to the network, the information asset will be updated if changed, or eliminated from local storage if not. If the information asset is distributed, the content retrieval service will be triggered by the appliqué when the information asset is encrypted, and credentials/access will be checked.

B. Distribution or Retrieval of an Information Asset

Distribution may be made in a number of ways:

1. The information asset may be sent by the anyone in an email to anyone, but members of the groups indicated in the ACLs may decrypt controlled information assets. Any changes to the information asset are stored under a new name or version, and under the editor's signature. If the information asset is encrypted and invokes the appliqué on the content program to set up a web session between the user and the content retrieval software described below. If the information asset is not encrypted, it is simply displayed for the user.
2. The recipient may save it to his local store or transmit it further by e-mail system allows, but any enterprise holder of the information asset cannot access encrypted content until he is online with the content retrieval system to check the access control and get the package decrypted.
3. The author may also provide the reference location. The reference location is used in a normal method to retrieve the data, but if it is encrypted, the appliqué begins a dialogue with the content retrieval service described below.
4. A requestor may have discovered the information asset by search and can the request access as in 3. Any attempt to open the information asset triggers the appliqué if the information asset is encrypted, which invokes the appliqué on the content program to set up a web session between the user and the content retrieval software described below.
5. Users outside of the defense enterprise (and accepted extensions), or within the defense enterprise without success have an encrypted package of no value. The exception is that unclassified unlimited distribution packages have no encryption and may be opened by anyone. Users within the enclave (or access to the enclave) will go to the rights manager upon opening the information asset and have ACLs checked before decrypting.

C. Content Retrieval Service

The retrieval service is accessed as a web service. The web service may be invoked directly or by the content application appliqué on an attempt to open the information asset. In either case the normal process of web service invocation applies, beginning with the bi-lateral PKI authentication using TLS [13] and the presentation of a SAML. The requester then passes the reference identity of the information asset that the requester has independently determined. This may either be by search or prior knowledge. The passing of this reference identity may be as a parameter in the initial request or by a dialogue exchange with the retrieval service. The retrieval service then takes the following actions:

Retrieval Service Actions 1.
SAML is verified and validated; claims are stripped and saved for further examination. Access to the Content Retrieval program is granted to all authenticated users.

Retrieval Service Actions 2.
Retrieval information asset name requested is checked against the list of information assets in the content store.

- ✓ If information asset exists, storage location is retrieved.
- ✓ If information asset is not on this list, an error message is returned and activity is closed.

Retrieval Service Actions 3.
Information asset is retrieved; decrypted and overall author signature is validated for integrity.

Retrieval Service Actions 4.
ACL list and associated data are retrieved for the information asset.

Retrieval Service Actions 5.
Claims and/or distinguished name in the SAML token are compared to the ACL list

- ✓ If no match is found access is denied, and activity is closed.
- ✓ If a match is found, further processing is undertaken.

Retrieval Service Actions 6.
Depending upon privileges associated with ACL / Claims match.

- ✓ Decrypt the information asset for presentation and insert MAC controlled screens and transmit to user.
- ✓ Offer to save the information asset in the user's environment with time restrictions as noted above, post text box containing distribution restrictions and ask for acknowledgement, then acknowledgement is logged. Save always includes the information asset and the signature blocks and encryption of the package. A trust package will provide local access as described earlier.

Retrieval Service Actions 7.
Closing of presentation system terminates TLS connection.

D. Import or Export of Information Assets

Imported/Exported Information assets are processed through the Rights Management service. When information

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

assets are imported into the defense enterprise, saving of the assets triggers the Rights Management System as described above. The source of imported information assets can be the email (or similar communication) system or a removable storage device. For exported information assets, the appliqué attached to the encrypted information asset interfaces with the Rights Management service via a secure link to validate access rights. If the information asset can be accessed outside of the defense enterprise domain, the asset is decrypted and made available to the recipient. If not, the user is displayed a rejection notice. In order to support external accessing of information assets, a more restrictive ACL data store can be located at the boundary. A soft cert (software X.509) may be used for coalition and other federated partners.

IV. SUMMARY

We have presented a process for protecting the authenticity of content of critical information assets in an enterprise. This process provides a searchable data base and assured content delivery through the implementation of services that make access control decisions based upon use case definitions, policy, and attributes of the requestor. Mitigation is achieve by express notification or restrictions to the trusted user base through MAC presentation screens, and the explicit requirement for acknowledgment of assent and understanding which is logged and reviewed. Particularly sensitive information assets may be marked for tracking which will aid in post-incident forensics of insider malicious or careless behavior. The content delivery process is part of a more comprehensive enterprise architecture for high assurance that is web-service based and driven by commercial standards. Portions of this architecture are described in references [14 – 23].

REFERENCES

[1] Umeh, Jude, The World Beyond Digital Rights Management', British Computer Society, 2007, IBSN 978-I-902505-87-9.
[2] Rimmer, Mathew, Digital Copyright and the Consumer Revolution, Edward Elgar Publishing Limited, 2007, IBSN 978 –I -84542-948-5.
[3] Anonymous, How Apple is changing DRM, The Guardian, May 2008.
[4] Berlind, David, TiVo sits at nexus of DRM conundrum, ZDNet News and Blogs, Setemeber 2006.
[5] Wijering, Jeroen, W3C Web TV: Adaptive Streaming & Content Protection, Long Tail Community Blog, Feb 2011.
[6] Kundar, D., and Karthik, K., Video Fingerprinting and Encryption Principles for Digital Rights Management, Proceedings of the IEEE, Vol. 92, No. 6, June 2004.
[7] Safavi, R., and Yung, M. (eds), Digital Rights Management Technologies, Issues, Challenges and Systems, 1st International Conference, Sydney, Australia, November 2005.
[8] OASIS open set of Standards:
a. N. Ragouzis et al., *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, March 2008.
b. P. Madsen et al., *SAML V2.0 Executive Overview*, April 2005.
c. P. Mishra et al. *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.
d. S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.
e. S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.
f. S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.
g. F. Hirsch et al. *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.
[9] Federal Information Processing Standards Publication 188, 1994 September 6, Standard Security Label for Information Transfer, http://www.itl.nist.gov/fipspubs/ fip188.htm
[10] Authorized Classification and Control Markings Register**,** Director of National Intelligence (DNI) Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO) Washington, DC 20511, Volume 1, Edition 2 (Version 1.2): 12 May 2008.
[11] DoD 5200.1-PH, DoD Guide to Marking Classified Documents**,** April 1997, Assistant Secretary of Defense for, Command, Control, Communications and Intelligence, http://www.dtic.mil/dtic/pdf/customer/STINFOdata/DoD5200_1ph.pdf
[12] DDMS version 4.0 released, September 23, 2011, http://metadata.ces.mil/mdr/irs/DDMS/
[13] Internet Engineering Task Force (IETF) Standard, RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2", August 2008.
[14] William R. Simpson, Coimbatore Chandersekaran and Andrew Trice, Electronic Digest of the 2008 System and Software Technology Conference, *"A Persona-Based Framework for Flexible Delegation and Least Privilege*", Las Vegas, Nevada, May 2008.
[15] William R. Simpson, Coimbatore Chandersekaran and Andrew Trice, The 1st International Multi-Conference on Engineering and Technological Innovation: IMET2008, *"Cross-Domain Solutions in an Era of Information Sharing"*, Volume I, pp.313-318, *Orlando, FL., June 2008.*
[16] Coimbatore Chandersekaran and William R. Simpson, World Wide Web Consortium (W3C) Workshop on Security Models for Device APIs, *"The Case for Bi-lateral End-to-End Strong Authentication"*, 4 pp., London, England, December 2008.
[17] William R. Simpson and Coimbatore Chandersekaran, The 2nd International Multi-Conf.on Engineering and Technological Innovation: IMETI2009, Volume I, pp. 300-305, *"Information Sharing and Federation", Orlando, FL., July* 2009.
[18] Coimbatore Chandersekaran and William R. Simpson, The 3rd International Multi-Conf. on Engineering and Technological Innovation: IMETI2010, Volume 2, *"A SAML Framework for Delegation, Attribution and Least Privilege"*, pages 303-308, *Orlando, FL.*, July 2010.
[19] William R. Simpson and Coimbatore Chandersekaran, The 3rd International Multi-Conference on Engineering and Technological Innovation: IMETI2010, Volume 2, *"Use Case Based Access Control"*, pages 297-302, *Orlando, FL.*, July 2010.
[20] Coimbatore Chandersekaran and William R. Simpson, The First International Conference on Computer Science and Information Technology (CCSIT-2011), *"A Model for Delegation Based on Authentication and Authorization"*, Springer Verlag Berlin-Heildleberg, Lecture Notes in Computer Science 20 pp.
[21] William R. Simpson and Coimbatore Chandersekaran, The 16th International Command and Control Research and Technology Symposium: CCT2011**,** Volume II, pp. 84-89, *"An Agent Based Monitoring System for Web Services"*, Orlando, FL., April 2011.
[22] William R. Simpson and Coimbatore Chandersekaran, International Journal of Computer Technology and Application (IJCTA)**,** *"An Agent-Based Web-Services Monitoring System" Vol. 2, No. 9, September 2011*, page 675-685.
[23] William R. Simpson, Coimbatore Chandersekaran and Ryan Wagner, Lecture Notes in Engineering and Computer Science, Proceedings World Congress on Engineering and Computer Science 2011, Volume I, *"High Assurance Challenges for Cloud Computing"*, pp. 61-66, San Francisco, October 2011.

ISBN: 978-988-19251-3-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)