Claims-Based Authentication for a Web-Based Enterprise

Coimbatore Chandersekaran and William R. Simpson

***Abstract*— Authentication is the process of determining whether someone or something is, in fact, who or what they are declared to be. The authentication process uses credentials (claims) containing authentication information within one of many possible authentication protocols to establish the identities of the parties that wish to collaborate. Claims are representations that are provided by a trusted entity and can be verified and validated. Of the many authentication protocols, including self-attestation, username/password and presentation of credentials, only the latter can be treated as claims. This is a key aspect of our enterprise solution, in that all active entities (persons, machines, and services) are credentialed and the authentication is bi-lateral, that is, each entity makes a claim to the other entity in every communication session initiated. This paper describes authentication that uses the TLS protocols primarily since these are the dominant protocols above the transport layer on the Internet. Other higher layer protocols, such as WS-Security, WS-Federation and WS-Trust, that use a Public Key Infrastructure credential for authentication, integrate via middleware. This authentication is claims based and is a part of an enterprise level security solution that has been piloted and is undergoing operational standup.**

Keywords- authentication; Public Key Infrastructure; Claims-based Identity; Web services; Transport Layer Security; Bi-lateral authentication.

I. Introduction

Authentication is a system function that establishes a level of confidence in the truth of a claim (e.g., a user's identity or the source and integrity of data). The authentication process includes the presentation of a credential, validation of the credential, proof of the claimed binding, determination of authentication assurance level (includes multiple factors), and the completion of the authentication decision by the establishment of a communications channel with the identity.

II. Active Entities in the Enterprise Context

Entities within the enterprise environment may be active or passive. Passive entities include information packages, static files, and reference data structures. They are the target of activities. They do not initiate activities and cannot provide the role of requestor or provider. Active entities are those entities that change or modify passive entities, request or provide services, or participate in communication flows. Active entities are users, hardware, and services. All active entities in the enterprise have DoD certificates, and their private keys are stored in tamper-proof, threat-mitigating storage. Communication between active entities in the enterprise requires full bi-lateral, Public Key Infrastructure (PKI), end-to-end authentication [2, 4a, 6b].

Manuscript received February 11, 2013; revised March 26, 2013. 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 US DoD 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, Va. 22311 USA and is the corresponding author phone: 703-845-6637, FAX: 703-845-6848 (e-mail: rsimpson@ida.org)

Active entities must be named in accordance with DoD Naming instruction [1]. Authentication in the enterprise environment is implemented as a verifiable claims-based attestation process. Figure 1 displays two active entities performing authentication and Active Entity B retrieving content from a passive entity.

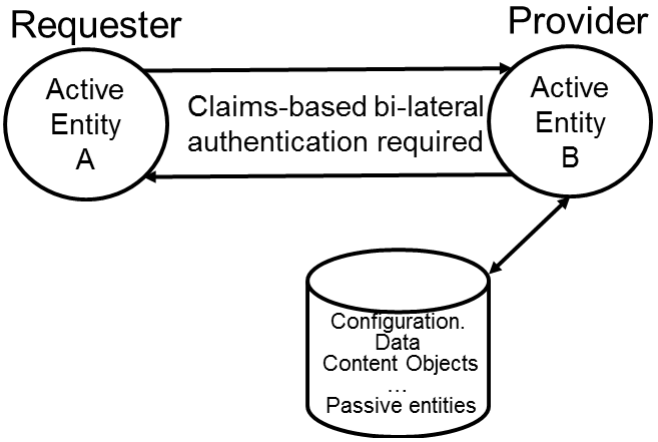

Figure 1 Communication between Active Entities

III. Credentialing in the Enterprise Context

A credential is a claim (in this case of identity) that can be verified as accurate and current. Credentials must be provided for all active entities that are established in the enterprise in order to perform authentication. Prior registration as an active entity with a confirmable entity name is required. The forms of credentials in use include certificates, Kerberos tickets, and hardware tokens. The details of generating, escrowing/retrieval, distributing, validating, and revoking certificates are discussed in specifications for DoD Certificates. Users are issued hardware tokens (Common Access Cards [CAC]) that have DoD Certificates stored on them with the private keys stored in hardware on the card. Machines and services are issued software certificates that contain the public key with the private key generated and remaining in hardware storage modules.

IV. Authentication in the Enterprise Context

Authentication is responsible for establishing the identity of an entity. Authentication is achieved by receiving, validating, and verifying the identity credential. For certificates, validation is achieved by encrypting a message with the private key of the requester and transmitting it to the provider. The provider can then validate that it was sent by the requester by decrypting it with the requester's public key. This assures that the requester is the holder of the private key. Verification is achieved by verifying the trusted agent that issued the certificate, this authentication is two-way (the requestor authenticates the provider and the provider authenticates the requestor).

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

A. *Certificate Credentials*

The required credential for enterprise personnel is an enterprise-issued X.509 (currently version 2.1), RSA-based certificate. X.509 certificates are used to bind an entity name to a public key in the PKI and to hold additional attributes (such as organizational unit data, and other data encoded in the distinguished name (DN)). They are used by authentication and authorization services, digital signing, and other cryptographic functions. Enterprise certificate credentials for users must be obtained through designated trusted Certificate Authorities (CAs). The CA provides the enterprise PKI credentials for users, devices, and services. Certificate credentials contain non-secret (publicly available) information. A hardware token that contains the certificate is preferred to software-only certificates. For enterprise users, the method of credential storage is an enterprise-issued card with a highly secure tamper-proof hardware store, which is FIPS 140-2 level 2 validated for cryptographic tokens.

Software certificates (used in addition to hardware tokens) are in the PKCS#12 [2] formats and must be installed in certificate storage associated with the entity that owns the certificate or its host device (which must also be credentialed). A user may have a software certificate issued by a designated CA that is installed in certificate storage in the user's host device. For devices and services that are established in the enterprise, a software certificate is acquired from a designated CA and is installed in certificate storage on the device itself and on the host device. [For hardware elements outside the enterprise, PKCS#12 files may be maintained as backup offline - but, in general, should not be stored on the hardware device attached to the network.] The certificate credential for an entity must contain the enterprise-unique and persistent identifier in the certificate subject DN field; for users this is the extended common name; for devices and services this is the Universally Unique Identifier (UUID) in accordance with the enterprise naming standard.

B. *Registration*

The registration function is a service that creates and maintains the information about the identities of entities in the enterprise. There are three main issues to consider as discussed below:

1) Kerberos Tickets

Kerberos is a network authentication protocol originally developed by the Massachusetts Institute of Technology, and now documented in several Internet Engineering Task Force (IETF) Internet Drafts and RFCs [6f]. Kerberos tickets are used with enterprise Active Directory (AD) forests.

2) Authentication and Attribute Assertion Tokens

Once authentication is established, the attributes of the identities are used to produce authorization claims. The primary method for expressing authorization claims in the enterprise uses derived credentials based on attribute assertion tokens at the message layer. These tokens contain security assertions and are obtained from a Security Token Service (STS). These tokens are based on the Security Assertion Markup Language (SAML) (current version) standard [3f]. The use of SAML tokens in this context is discussed in [21]. Although the standard allows for authentication elements in the SAML token, they are not used in this formulation. SAML is used only for authorization, and the only link to authentication is the binding to the requester by a holder-of-key (HOK) check (see [22] for the definition of this check and how it is performed).

3) Interoperability of Credentials

Public key cryptography depends on the ability to validate certificates against a trusted source. The use of PKI is discussed in [9]. External information sharing includes authentication based upon a federation agreement that specifies approved primary and derived credentials. The credentials will be configured for such federations.

C. *Authentication*

The enterprise supports two general methods for authentication: Kerberos-based and Direct PKI. Authentication relies on certificates.

1) Devices and Services Authentication PKI

Devices and Services are configured to authenticate themselves to the identity provider of the enterprise using bi-lateral Transport Layer Security (TLS) [6a]. The authentication relies on enterprise-issued PKI certificates

2) User Initial Authentication to the Domain

The user authenticates using the PKI-enabled logon program, which asks the user for a passcode that is, in turn, used as an index to a Kerberos key. This is a hybrid approach where the hardware token is read and user ownership is sought by presenting an input screen for the passcode associated with the hardware token. PKINIT is invoked, completing the authentication by PKI (Kerberos supports both password based user authentication and PKI based principal authentication with the PKINIT extension) using the certificate stored on the card. The Kerberos-based authentication uses the PKINIT and Kerberos protocols. For enterprise operations, users authenticate to the Identity Manager with the enterprise hardware token.

The hardware token credential is only used by human users, and either soft certificates or certificates stored in hardware storage modules are used for other entities. The user authenticates to the domain controller using a smartcard logon program such as the CAC or another approved active card and authenticates using the hardware token and a user-supplied PIN. The PKI Initiation program is invoked completing the authentication by PKI**.** External users (users communicating from outside the enterprise) are then provided a virtual private network (VPN) tunnel and treated as if they were within the domain. Kerberos supports both password-based user authentication and PKI-based principal authentication (with the PKINIT extension). Successful completion of the logon procedure signifies successful authentication of the user to the domain controller (a timeout will occur at pre-configured period more details are provided in [2]).

3) User Authentication to Services Using PKI

It is assumed at this point that the user has successfully authenticated to the Identity Manager using PKI. If the user wishes to access any other web service through the web

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

browser, he does so using HTTPS. All entity drivers will be configured to use TLS client authentication. This additionally provides Transport Layer Confidentiality for subsequent message layer traffic over https. This validates the user's certificate and passes the certificate to the web service being accessed.

4) Service-to-Service Authentications

Requesters make requests for capabilities from Web services. In all cases, any capability request is preceded by TLS client authentication. Services may request other web services for capabilities (service providers). Services may include web services, utility services, and others.

V. Infrastructure Security Component Interaction

Figure 2 shows the basic authentication flows required prior to all interactions. This flow is the basic TLS setup.

When a requester wishes to use another service, there are four active entities that come into play. Details are provided in Figures 3 and 4 - the active entities are listed below.

1. a. For a user:
   The user (Requester) web browser -- This is a standard web browser that can use the HTTP and HTTPS drivers (including the TLS driver) on the platform.
   b. For a service:
   The requester host platform
2. The Security Token Service (STS) in the requester's domain
3. The Enterprise Attribute Store
4. The requested service (application server) in the resource application environment.

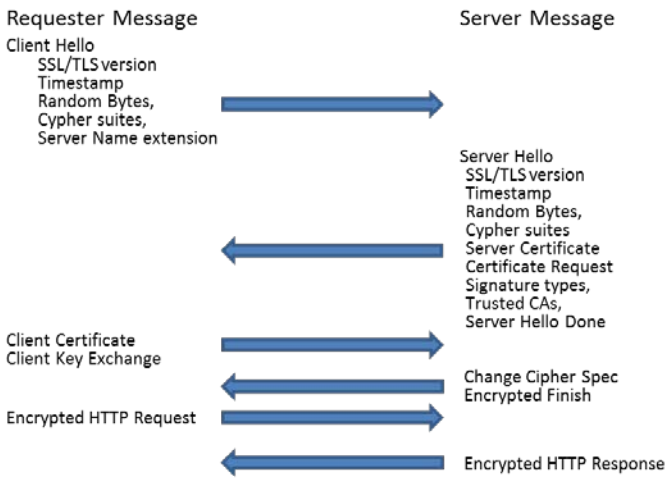

Figure 2 Authentication Flows

A. *Interactions Triggered by a User Request for Service*

The user first makes a request to STS. Included in that request is an identifier (the Uniform Resource Identifier (URI) [6c]) or a token referring to this identifier of the target service. The STS will generate the SAML credentials and return them to the browser with instructions to redirect to the service and post the SAML in this request to the application server (see Figure 3). If HTTPS messages are used, then bi-lateral authentication takes place based on configuration of the servers and the web browsers.

B. *Interactions Triggered by a Service Request for Service*

The web service (1) will send a service request to the web service (2) as shown in figure 4. All communications shown in this figure are preceded by a bi-lateral authentication triggered by an HTTPS message.

VI. Compliance Testing

Authentication testing verifies that the bi-lateral PKI-based authentication is working properly in the enterprise. This includes testing TLS on every connection in the security flows. Packet captures are done on nodes in the flow and then TLS traffic is checked for certificate exchanges and encryption. Checks for OCSP (the Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate). calls and returns verify that certificate status is being checked correctly. The packet captures are executed for a request to the STS. Authentication testing covers revoked and expired certificates. Captures will show OCSP traffic for the revoked certificate.

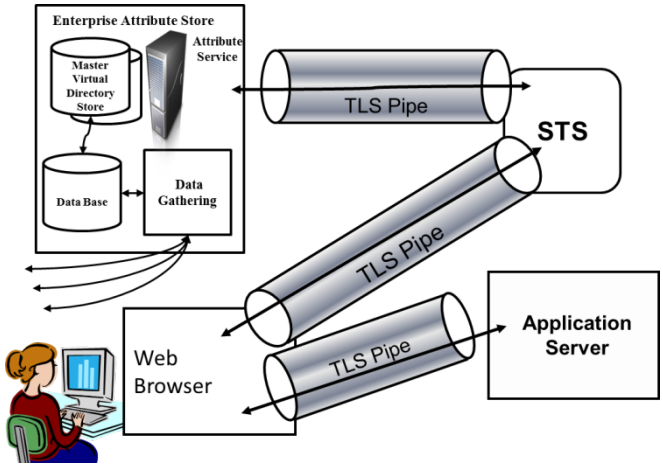

Figure 3 Web Browser Request for Service Message Flows

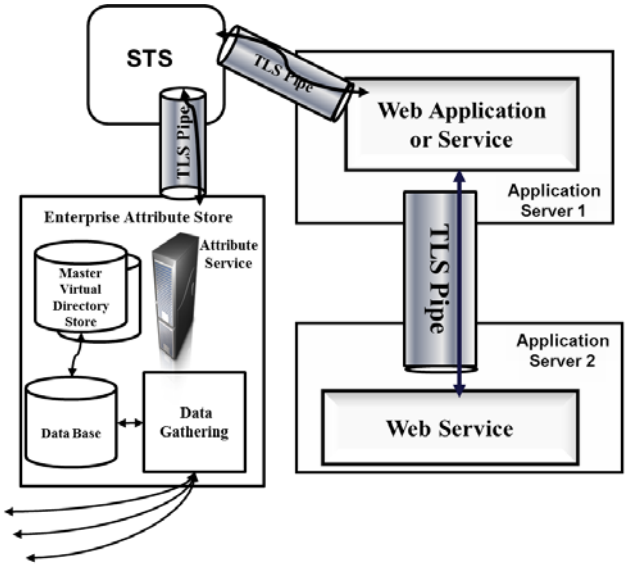

Figure 4 Web Service Request for Service Message Flows

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

VII. Federated Authentication

Federated communications must meet all of the enterprise requirements, including:

- Naming PKI certificates,
- Certificates issued by a recognized certificate issuer,
- Valid, not-revoked, dates,
- TLS MutualAuth authentication, and
- SAML tokens from designated authorized STSs that meet all of the above requirements.

A. *Naming and Identity*

Identity is established by the enterprise or the requesting agency as agreed to in the federation agreement. In the enterprise, this is primarily through the enterprise naming contained in the enterprise-issued X.509. These names should be standardized throughout the enterprise and satisfy the property of uniqueness over space and time. For people, this name is the enterprise standardized name, but for other certificate authorities, their naming schemes are accepted based on federation agreements. The identity used by all federated exchanges is the Distinguished Name as it appears on the primary credential provided by the certificate authority. If there is a collision, mapping of federation names will be required.

Credentials

Credentials are an integral part of the federation model. Each identity requiring access is credentialed by a trusted credentialing authority. Further, the STS used for generating SAML [4a-h] tokens, is also credentialed (as are all active entities in the enterprise). The primary exchange medium for setting up authentication of identities and setting up cryptographic flows is the PKI embodied in an X.509 certificate. The certificate authority must use known and registered (or in specific cases defined) certificate revocation and currency-checking software.

B. *Translation of Claims or Identities*

Identities are translated as indicated in the federation agreement. For simple federation, where requests are across the enterprise domains, there is no mapping, as the identities are in the appropriate form already.

C. *Other Issues*

The registering of recognized STS and claim mapping must be promulgated in an an enterprise policy memorandum after ratification of the federation agreement. The federation agreement may be an attachment to such a policy memorandum. This memorandum must be distributed to the appropriate organization for implementation by the Enterprise Attribute Store (EAS) and STS Administrators for incorporation in the trusted STS store. This maintains the lines of authority. A more complete discussion of federation, including a sample federation agreement is provided in [20].

VIII. Maturing Guidance

Related changes to OASIS, W3C, and IETF standards will necessarily be cause to reconsider and possibly modify these processes when appropriate. Because these standards tend to be backward compatible, or allow appropriate sunset periods, it can be assumed that phased-in implementation of changes will take place.

IX. Summary

We have presented an authentication process for identity management and bi-lateral authentication between requesters and providers in an enterprise environment. The enterprise environment providers include web application and web services. The authentication is the beginning of a claims-based process that will include SAML claims for authorization. The content delivery process is part of an enterprise architecture for high assurance that is web-service based and driven by commercial standards. Portions of this architecture are described in references [18 – 31].

X. Acknowlegements

The authors would like to acknowledge our debt of gratitude for the comprehensive and detailed review provided by Dr. Margaret Myers and Dr. Kevin Foltz of the Institute for Defense Analyses. There contributions added significantly to the clarity and accuracy of the material presented herein.

References

[1] Standard for Naming Active Entities on DoD IT Networks, Version 3.5 (or current), Sept. 23, 2010.

[2] Public Key Cryptography Standard, PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002

[3] OASIS open set of Standards

a. N. Ragouzis et al., *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. OASIS Committee Draft, March 2008.
b. P. Madsen et al., *SAML V2.0 Executive Overview*. OASIS Committee Draft, April 2005.
c. P. Mishra et al. *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005.
d. S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005.
e. S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005.
f. S. Cantor et al. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005.
g. S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005.
h. F. Hirsch et al. *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005
i. J. Hodges et al. *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005.

[4] National Institute of Standards, Gaithersburg, Md:

a. FIPS PUB 196, Federal Information Processing Standards Publication. “Entity Authentication Using Public Key Cryptography”, February 18, 1997
b. FIPS 197, Advanced Encryption Standard (AES), November 2001.
c. Publication 800-38, *Recommendation for Block Cipher Modes of Operation:* 38A, *Methods and Techniques, December 2001;* 38B, *The RMAC Authentication Mode, November 5 2002 draft; 38C,*

The CCM Mode for Authentication and Confidentiality, May 2004.
d. Federal Information Processing Standards Publication, Special Publication 800-67, Version 1.2 , Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised January 2012

[5] Common Criteria for Information Technology Security Evaluation:
a. Version 3.1, revision 3, July 2009. Part 1: Introduction and general model.
b. Version 3.1, revision 3, July 2009. Part 2: Functional security components.
c. Version 3.1, revision 3, July 2009. Part 3: Assurance security components.
d. Common Methodology for Information Technology Security Evaluation, Version 3.1, revision 3, July 2009

[6] Internet Engineering Task Force (IETF) Standards:
a. RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2", August 2008.
b. RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.
c. STD 66 (RFC3986) Uniform Resource Identifier (URI): Generic Syntax, T. Berners-Lee, R. Fielding, L. Masinter, January 2005
d. STD 9 (RFC0959) File Transfer Protocol, J. Postel, J. Reynolds, October 1985.
e. STD 5 (RFC0791) Internet Protocol, J. Postel, September 1981, and subsequent RFCs 791/950/919/922/792/1112.
f. RFC 4120: The Kerberos Network Authentication Service V5), updated by RFC 4537 and 5021
g. RFC 4510 Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006
h. Authentication Methods for LDAP. M. Wahl, H. Alvestrand, J. Hodges, R.L. Morgan. IETF RFC 2829, May 2000.

[7] United States Department of Defense, X.509 Certificate Policy, Version 10 , 2 March 2009.

[8] DoDI 8500.2 DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.

[9] FPKI-Prof Federal PKI X.509 Certificate and CRL Extensions Profile, Version 6, 12 October 2005.

[10] KRP Key Recovery Policy for the United States Department of Defense, Version 3.0, 31 August 2003.

[11] PKCS 1 RSA Cryptography Standard, RSA Laboratories, 14 June 2002.

[12] SDN 702 Abstract Syntax for Utilization with Common Security Protocol (CSP), Version 3 X.509 Certificates, and Version 2 CRLs, Revision C, 12 May 1999.

[13] SDN 706 X.509 Certificate and Certification Revocation List Profiles and Certification Path Processing Rules for MISSI Revision D, 12 May 1999.

[14] DoD Directive 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense," June 21, 2005

[15] DoD 5200.1-R "Information Security Program," January 1997

[16] National Security Telecommunications and Information Systems Security Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," June 2003

[17] 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.

[18] 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.*

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[27] Coimbatore Chandersekaran and William R. Simpson, Lecture Notes in Engineering and Computer Science, Proceedings World Congress on Engineering 2012, The 2012 International Conference of Information Security and Internet Engineering, Volume I, *"Claims-Based Enterprise-Wide Access Control"*, pp. 524-529, London, July 2012.

[28] William R. Simpson and Coimbatore Chandersekaran, Lecture Notes in Engineering and Computer Science, Proceedings World Congress on Engineering 2012, The 2012 International Conference of Information Security and Internet Engineering, Volume I, *"Assured Content Delivery in the Enterprise"*, pp. 555-560, London, July 2012.

[29] Coimbatore Chandersekaran and William R. Simpson, Springer Science+Business Media Dordrecht 2012, Book Chapter, *IAENG Transactions on Engineering Technologies* - Special Edition of the World Congress on Engineering and Computer Science 2011, Lecture Notes in Electrical Engineering 170, DOI: 10.1007/978-94-007-4786-9_16, ISBN: 978-94-007-4785-2, Chapter 16, "*Co-Existence of High Assurance and Cloud-Based Computing*", 14pp. May 2012.

[30] William R. Simpson and Coimbatore Chandersekaran, Lecture Notes in Engineering and Computer Science, Proceedings World Congress on Engineering and Computer Science 2012, Volume 1, *"Enterprise High Assurance Scale-up"*, pp. 54-59, San Francisco, October 2012.

[31] Coimbatore Chandersekaran and William R. Simpson, International Journal of Scientific Computing, Vol. 6, No. 2, *"A Uniform Claims-Based Access Control for the Enterprise"*, December 2012, ISSN: 0973-578X, pp. 1-23.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)