NATIONAL ENTERPRISE ARCHITECTURE FRAMEWORK
KINGDOM OF BAHRAIN

Technology Standards and Guidelines

Security Domain

Kingdom of Bahrain
eGovernment Towards a Better Life

DOCUMENT INFORMATION AND HISTORY

Document Reference Number: ETS-SEC-02.01		Title: Security Domain
Document Type: Enterprise Technology Standards		**Category:** Security
Approver: ICT Governance Committee (ICTGC)		**Approval Date:** 04/12/2013
Effective Date: 04/12/2013	**Last Review Date:** 02/12/2013	**Next Review Date:** As Required
SPOC for Change: NEAF Chief Architect – Email ID: neaf@ega.gov.bh		
Synopsis: Establishes technology standards and guidelines in Security Domain for Information Systems interoperability and information exchange		

Document History

Version Number	Date (dd/mm/yyyy)	Author	Remarks
1.0	06/12/2010	NEAF Team	Baseline version
2.0	02/12/2013	NEAF Team	Updated and incorporated review comments from ICTGC

Review and Approval History

Version Number	Date (dd/mm/yyyy)	Reviewer / Approver	Remarks
2.0	04/12/2013	ICTGC	Formal approval by ICTGC

TABLE OF CONTENTS

1. Introduction 5
2. Summary of Technology Standards/Specifications and Tools 6
   2.1. Public Key Infrastructure (Certificate Security) 6
   2.2. Transport Security 6
   2.3. Encapsulation security 7
   2.4. Timestamp token 7
   2.5. Secure Shell 8
   2.6. Email Security 8
   2.7. IP Security 8
   2.8. Encryption 9
   2.9. XML Security 9
   2.10. Web Services Security 10
   2.11. Identity Management System 10
   2.12. Authentication, Authorization and Accounting 11
   2.13. Access Management 11
   2.14. Anti-virus and Anti-spyware 12
   2.15. Anti-Spam 12
   2.16. Desktop Firewalls 12
   2.17. Enterprise Perimeter Firewalls 13
   2.18. Proxy Server 13
   2.19. Intrusion detection system 14
3. Details of Standards / Specifications and Associated Guidelines 15
   3.1. ESP 15
   3.2. TLS 1.2 15
   3.3. CMS 16
   3.4. TSP 16
   3.5. SSH 17
   3.6. RFC 3207 17
   3.7. S/MIME v3 18
   3.8. WS-TRUST 18
   3.9. WS-I Basic Security Profile 19
   3.10. WS-I Security 19
   3.11. WS-Secure Conversation 20
   3.12. WS-Federation 21
   3.13. WS-Policy 21
   3.14. WS-SecurityPolicy 22
   3.15. SAML 23
   3.16. 3DES 23
   3.17. RSA 24
   3.18. MD-5, SHA 24
   3.19. XML-Signature Syntax and Processing, XML-DSS 25
   3.20. XMLenc 26
   3.21. Decryption Transform for XML Signature as defined by W3C 26
   3.22. XKMS 2.0 26
   3.23. SAML token profile 27
   3.24. SAML 2.0 28
   3.25. XACML 28
   3.26. X.509 29
   3.27. PKCS 29

3.28. IPSec....30
3.29. SSL....30
4. Details of Tools Supporting Recommended Standards....32
4.1. IBM Tivoli Federated Identity Manager (TFIM) & Tivoli Access Manager for e-business (TAMeb)....32
4.2. Oracle Access Management solutions....32
4.3. CA Access Management solutions....33
4.4. RADIUS....33
4.5. Diameter....34
4.6. TACACS+....34
4.7. IBM Tivoli Identity Manager....35
4.8. Oracle Identity Management Solution....35
4.9. TrendMicro....36
4.10. Symantec....36
4.11. McAfee....36
4.12. Cisco IronPort....37
4.13. Microsoft Forefront....37
4.14. Kaspersky....37
4.15. CA Inc.....38
4.16. Microsoft Windows Defender....38
4.17. Microsoft Windows Firewall....39
4.18. IPTables....39
4.19. CISCO Firewall....39
4.20. Juniper Firewall....40
4.21. Checkpoint Firewall....40
4.22. Fortinet Firewall....41
4.23. McAfee (Secure Computing Corporation) Firewall....41
4.24. Cisco Intrusion Detection Systems....41
4.25. Tipping Point Intrusion Detection Systems....42
4.26. Sourcefire Intrusion Detection Systems....42
4.27. ISS Intrusion Detection Systems....42
4.28. Juniper Intrusion Detection Systems....43
4.29. Microsoft Internet Security and Acceleration Server (ISA Server)....43
4.30. Blue Coat Proxy Server....44
4.31. WebSense Server....44
5. Appendices....45
5.1. Appendix a: Abbreviations and Acronyms....45
5.2. Appendix B: Related Documents / Links....46

1. INTRODUCTION

This document covers tools, technologies and standards used in the Security domain. The process of arriving at these standards has been outlined in the NEAF - Technology Standards Methodology & Process document in Section 3 - Methodology and Approach. The following standards have been base lined after considering their acceptance across ministries. Some of the tools, technologies and standards have been identified as potential requirements and hence been incorporated in this document. These may be considered as recommendations for current and future use.

This document shall be considered for revision in conjunction with the NEAF - Technology Standards Methodology & Process document at appropriate intervals of time as decided by the ICT Governance Committee. Any addition or upgrade to these tools and standards may be incorporated by following the process described in the NEAF - Technology Standards Methodology & Process document in Section 6 - Review and Maintenance of Technology Standards and Guidelines.

2. Summary of Technology Standards/Specifications and Tools

This section contains a summary of standards and tools applicable to the Secuirty domain. These have been grouped into sub-sections (categories), with each category addressing one aspect of the related standards and tools. Further details and links to these standards and tools have been provided in the following sections of this document.

The rationale for selection of these standards and tools are :

- Based on the usage across ministries as captured in the internal survey.
- Technology best practices.
- References from international standards bodies.

2.1. Public Key Infrastructure (Certificate Security)

Introduction to Sub-Category	▪ The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. Digital certificate is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. ▪ PKI initiatives must interoperate with other PKI solutions, utilize a Kingdom wide approach, and conform to any relevant laws and policies.
Applicable Standard(s)	▪ X.509 – (Details) ▪ PKCS - For PKI (such as Certification Request, Certificate Profile) – (Details)
Remarks	
Exceptions	

2.2. Transport Security

Introduction to Sub-Category	▪ Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security and data integrity for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.
Applicable Standard(s)	▪ TLS 1.2 – (Details) ▪ SSL – (Details)

Remarks	
Exceptions	

2.3. ENCAPSULATION SECURITY	
Introduction to Sub-Category	▪ The Encapsulating Security Payload (ESP) header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with the IP Authentication Header (AH), or in a nested fashion, e.g., through the use of tunnel mode. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. For more details on how to use ESP and AH in various network environments, see the Security Architecture document.
Applicable Standard(s)	▪ CMS - Encapsulation security – (Details)
Remarks	
Exceptions	

2.4. TIMESTAMP TOKEN	
Introduction to Sub-Category	▪ The ANS X9.95 standard for trusted timestamps expands on the widely used RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol by adding data-level security requirements that can ensure data integrity against a reliable time source that is provable to any third party. Applicable to both unsigned and digitally signed data, this newer standard has been used by financial institutions and regulatory bodies to create trustworthy timestamps that cannot be altered without detection and to sustain an evidentiary trail of authenticity. ▪ Timestamps based on the X9.95 standard can be used to provide: • Authenticity: Trusted, non-refutable time when data was digitally signed. • Integrity: Protection of the timestamp from tampering without detection. • Timeliness: Proof that the time of the digital signature was in fact the actual time. • An evidentiary trail of authenticity for legal sufficiency.
Applicable Standard(s)	▪ TSP - Timestamp token – (Details)

Remarks	
Exceptions	

2.5. SECURE SHELL	
Introduction to Sub-Category	▪ Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plaintext, rendering them susceptible to packet analysis.[2] The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.
Applicable Standard(s)	▪ SSH - Secure Shell – (Details)
Remarks	
Exceptions	

2.6. EMAIL SECURITY	
Introduction to Sub-Category	▪ As email becomes more prevalent in the market, the importance of email security becomes more significant. In particular, the security implications associated with the management of email storage, policy enforcement, auditing, archiving and data recovery.
Applicable Standard(s)	▪ RFC 3207 - E-mail transport security – (Details) ▪ S/MIME v3 - E-mail content security – (Details)
Remarks	
Exceptions	

2.7. IP SECURITY	
Introduction to Sub-Category	▪ IP Security provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. ▪ IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer.

Applicable Standard(s)	▪ IPSec - IP security (Authenticated header) – (Details) ▪ ESP - IP encapsulation security (for VPN requirements) – (Details)
Remarks	
Exceptions	

2.8. ENCRYPTION	
Introduction to Sub-Category	▪ Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. ▪ The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).
Applicable Standard(s)	▪ 3DES - Encryption algorithms – (Details) ▪ RSA - Encryption algorithms For signing – (Details) ▪ RSA - Encryption algorithms For key transport – (Details) ▪ MD-5, SHA - Encryption algorithms For hashing – (Details)
Remarks	
Exceptions	

2.9. XML SECURITY	
Introduction to Sub-Category	▪ The XML Security standards define XML vocabularies and processing rules in order to meet security requirements. ▪ These standards use legacy cryptographic and security technologies, as well as emerging XML technologies, to provide a flexible, extensible and practical solution toward meeting security requirements.
Applicable Standard(s)	▪ XML-Signature Syntax and Processing, XML-DSS - XML signatures – (Details) ▪ XMLenc - XML encryption – (Details) ▪ Decryption Transform for XML Signature as defined by W3C - XML signature and encryption – (Details)

	▪ XKMS 2.0 - XML key management where a PKI environment is used – (Details) ▪ SAML - XML security assertion mark-up – (Details) ▪ XACML - XML access control – (Details)
Remarks	
Exceptions	

2.10. WEB SERVICES SECURITY	
Introduction to Sub-Category	▪ WS-Security (Web Services Security, short WSS) is a flexible and feature-rich extension to SOAP to apply security to Web services. It is a member of the WS family of web service specifications and was published by OASIS. ▪ The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security.
Applicable Standard(s)	▪ WS-TRUST - Web Services Security – (Details) ▪ WS-I Security - Web Services Security – (Details) ▪ WS-I Basic Security Profile – (Details) ▪ SAML Token Profile - Web services security – (Details) ▪ SAML - WS-Access Control profiles, WS-Security mark-up profiles – (Details) ▪ WS-Policy – (Details) ▪ WS-Security Policy – (Details) ▪ WS-Federation – (Details) ▪ WS-Secure Conversation – (Details)
Remarks	
Exceptions	

2.11. IDENTITY MANAGEMENT SYSTEM	
Introduction to Sub-Category	▪ An identity management system refers to an information system, or to a set of technologies that can be used to support the management of identities in an organization. Identity management systems provide facilities for managing lifecycle of identities from establishment to destruction.
Applicable Standard(s)	▪ IBM Tivoli Identity Manager (Version 5.0 or higher) (Details)

	▪ Oracle Identity Manager (Version 10gR3 or higher) (Details) ▪ Sun Identity Manager (Version 8.0 or higher) (Details)
Remarks	
Exceptions	

2.12. AUTHENTICATION, AUTHORIZATION AND ACCOUNTING	
Introduction to Sub-Category	▪ "Authentication, Authorization and Accounting" (AAA), are the three primary services that provide a network security and a record of user activity by identifying who the user is, what the user can access, and what services and resources the user is using when they make a connection with a server. Examples of the services a user may be trying to access are dial up access to Internet, e-commerce, or mobile internet devices. The authentication part tells who the user is and authorization is what the user is allowed to do while on the server. Authentication can be valid without authorization but authorization is not valid without authentication. The last part, accounting, tracks what the user did while on the system.
Applicable Standard(s)	▪ RADIUS (Details) ▪ Diameter (Details) ▪ TACACS+ (Details)
Remarks	
Exceptions	

2.13. ACCESS MANAGEMENT	
Introduction to Sub-Category	▪ Access management refers to the use of access control engines that provide centralized authentication and authorization capabilities for applications. Access management products may include identity administration, role/rule life cycle management, and audit and federation capabilities. They frequently incorporate some level of user-provisioning functionality or integration with a user-provisioning tool.
Applicable Standard(s)	▪ IBM Tivoli Federated Identity Manager (Version 6.2) – (Details) ▪ IBM Tivoli Access Manager for e-business (Version 6.1) – (Details) ▪ Oracle Access Manager (Version 10.1.4.3.0) – (Details) ▪ Sun Open SSO Enterprise (Version 8.0) – (Details) ▪ CA SiteMinder – (Details)
Remarks	
Exceptions	

2.14. ANTI-VIRUS AND ANTI-SPYWARE	
Introduction to Sub-Category	▪ Anti-virus software is used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware. Spyware is a type of malware that is installed on computers and that collects information about users without their knowledge.
Applicable Standard(s)	▪ Trend Micro (Details) ▪ Symantec (Norton) (Details) ▪ McAfee (Details) ▪ Kaspersky Lab (Details) ▪ CA (Details) ▪ Windows Defender (Details) ▪ Microsoft Forefront (Details)
Remarks	
Exceptions	

2.15. ANTI-SPAM	
Introduction to Sub-Category	▪ E-mail spam, also known as junk e-mail, is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. To prevent e-mail spam, both end users and administrators of e-mail systems use various anti-spam techniques. Some of these techniques have been embedded in products, services and software to ease the burden on users and administrators.
Applicable Standard(s)	▪ Trend Micro (Details) ▪ Symantec (Details) ▪ McAfee (Details) ▪ Cisco IronPort (Details) ▪ Microsoft Forefront (Details)
Remarks	
Exceptions	

2.16. DESKTOP FIREWALLS	
Introduction to Sub-Category	▪ A desktop firewall is a software application used to protect a network connected computer from intruders. Desktop firewalls work in the background at the device (link layer) level to protect the integrity of the system from malicious computer code by controlling network connections to and from a user's computer, filtering inbound and outbound traffic, and alerting the user to attempted intrusions.

Applicable Standard(s)	▪ Microsoft Windows Firewall (Details) ▪ Trend Micro (Details) ▪ Symantec Norton (Details) ▪ Kaspersky Lab (Details) ▪ iptables (Details)
Remarks	
Exceptions	

2.17. Enterprise Perimeter Firewalls

Introduction to Sub-Category	▪ A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.
Applicable Standard(s)	▪ Cisco ASA (Details) ▪ Juniper Firewalls (Details) ▪ Check Point Firewalls (Details) ▪ Fortinet FortiGate Firewalls (Details) ▪ McAfee Firewall Enterprise (Secure Computing Firewall) (Details)
Remarks	
Exceptions	

2.18. Proxy Server

Introduction to Sub-Category	▪ In computer networks, a proxy server is a server (a computer system or an application program) that acts as a go-between for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules.
Applicable Standard(s)	▪ Microsoft ISA Server 2006 (Details) ▪ Blue Coat (Details) ▪ Websense (Details)
Remarks	▪
Exceptions	

2.19. INTRUSION DETECTION SYSTEM	
Introduction to Sub-Category	▪ An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. In a passive system, the intrusion detection system (IDS) sensor detects a potential security breach, logs the information and signals an alert on the console and or owner. In a reactive system, also known as an intrusion prevention system (IPS), the IPS responds to the suspicious activity by resetting the connection or by reprogramming the firewall to block network traffic from the suspected malicious source.
Applicable Standard(s)	▪ Cisco 6500 IDS Module (Details) ▪ Cisco IPS (Details) ▪ Cisco ASA (Details) ▪ TippingPoint IPS (Details) ▪ Sourcefire 3D System (Details) ▪ IBM ISS RealSecure and Proventia (Details) ▪ Juniper Intrusion Detection and Prevention Appliances (Details)
Remarks	
Exceptions	

3. Details of Standards / Specifications and Associated Guidelines

This section provides a brief description of the relevant standards listed in section 2 along with links for references to these standards.

3.1. ESP	
Description	▪ Encapsulating Security Payload (ESP) provides confidentiality, in addition to authentication, integrity, and anti-replay. ESP can be used alone, or in combination with AH. ▪ ESP does not normally sign the entire packet unless it is being tunnelled—ordinarily, just the IP data payload is protected, not the IP header.
Applicable to	▪ IP Security
Reference(s)	▪ http://www.ietf.org/rfc/rfc2406.txt
Remarks	▪ Encapsulating Security Payload (ESP) is a member of the IPSec protocol suite. In IPSec it provides origin authenticity, integrity, and confidentiality protection of packets. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure. ▪ Unlike Authentication Header (AH), ESP does not protect the IP packet header. However, in Tunnel Mode, where the entire original IP packet is encapsulated with a new packet header added, ESP protection is afforded to the whole inner IP packet (including the inner header) while the outer header remains unprotected. ESP operates directly on top of IP, using IP protocol number 50.

3.2. TLS 1.2	
Description	▪ The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. ▪ At the lowest level, layered on top of some reliable transport protocol (e.g., TCP [TCP]), is the TLS Record Protocol.
Applicable to	▪ Transport Security

Reference(s)	▪ http://tools.ietf.org/html/rfc5246 ▪ http://tools.ietf.org/html/rfc5746 ▪ http://tools.ietf.org/html/rfc5878 ▪ http://tools.ietf.org/html/rfc6176 ▪
Remarks	The TLS Record Protocol provides connection security that has two basic properties: ▪ The connection is private. Symmetric cryptography is used for data encryption (e.g., AES [AES], RC4 [SCH], etc.). The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record Protocol can also be used without encryption. ▪ The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA-1, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.

3.3. CMS	
Description	▪ This syntax is used to digitally sign, digest, authenticate, or encrypt arbitrary messages. The Cryptographic Message Syntax describes encapsulation syntax for data protection. ▪ It supports digital signatures, message authentication codes, and encryption. The syntax allows multiple encapsulation, so one capsulation envelope can be nested inside another
Applicable to	▪ Transport Security
Reference(s)	▪ http://www.ietf.org/rfc/rfc3370.txt
Remarks	▪ The Cryptographic Message Syntax can support a variety of architectures for certificate-based key management, such as the one defined by the PKIX working group

3.4. TSP	
Description	▪ Timestamp tokens are issued by Timestamp authorities for long lived signatures. Such time-stamps prove that what was time-stamped actually existed at the time indicated,

	whereas any other time indication is only a claim by the signer and is less useful in dispute resolution. Time-Stamp Protocol, RFC 3161 [RFC3161], describes the use of a time stamp authority to establish evidence that a signature existed before a given time, useful in applications where dispute resolution may be necessary
Applicable to	▪ Transport Security
Reference(s)	▪ http://www.w3.org/TR/xmldsig-bestpractices/#timestamp-authorities
Remarks	▪ This can be used to verify that a digital signature was applied to a message before the corresponding certificate was revoked thus allowing a revoked public key certificate to be used for verifying signatures created prior to the time of revocation. This is an important public key infrastructure operation

3.5. SSH	
Description	▪ Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network. All of these channels are multiplexed into a single encrypted tunnel. The SSH Connection Protocol has been designed to run on top of the SSH transport layer and user authentication protocols
Applicable to	▪ Transport Security
Reference(s)	▪ http://www.ietf.org/rfc/rfc4254.txt
Remarks	▪ It provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections

3.6. RFC 3207	
Description	▪ This is SMTP Service extension considered to be secure when compared to TLS. service that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet
Applicable to	▪ Email Security

Reference(s)	▪ http://www.rfc-editor.org/rfc/rfc3207.txt
Remarks	▪ This protocol is mostly preferred as it gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

3.7. S/MIME v3	
Description	▪ S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send and receive secure MIME data. ▪ Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).
Applicable to	▪ Email Security
Reference(s)	▪ http://www.ietf.org/rfc/rfc2633.txt
Remarks	▪ S/MIME has the advantage of the object-based features of MIME and allows secure messages to be exchanged in mixed-transport systems. ▪ S/MIME can be used in automated message transfer agents that use cryptographic security services that do not require any human intervention, such as the signing of software-generated documents and the encryption of FAX messages sent over the Internet.

3.8. WS-TRUST	
Description	▪ From the perspective of web security, there are three fundamental concepts related to security: the resources that must be secured; the mechanisms by which these resources are secured (i.e., policy guards); and policies, which are machine-processable documents describing constraints on these resources. ▪ Policies can be logically broken down into two main types: permission policies and obligatory policies. A permission policy concerns those actions and accesses that entities are permitted to perform and an obligation policy concerns those actions and states that

	entities are required to perform. ▪ These are closely related, and dependent: it is not consistent to be obliged to perform some action that one does not have permission to perform. A given policy document is likely to contain a mix of obligation and permission policy statements.
Applicable to	▪ Web Services Security
Reference(s)	▪ http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss ▪ http://www.oasis-open.org/standards
Remarks	

3.9. WS-I Basic Security Profile	
Description	▪ Industry-wide, the WS-I Basic Security Profile is an interoperability policy that addresses transport security, SOAP messaging integrity and many other related security considerations for WS-I's Basic Profile v1.1 and v1.2, Simple SOAP Binding Profile 1.0 and Attachments Profile 1.0.
Applicable to	▪ Web Services Security
Reference(s)	▪ http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html ▪ http://www.oasis-open.org/standards ▪
Remarks	▪ The WS-I Basic Profile (official abbreviation is BP), a specification from the Web Services Interoperability industry consortium (WS-I), provides interoperability guidance for core Web Services specifications such as SOAP, WSDL, and UDDI. The profile uses Web Services Description Language (WSDL) to enable the description of services as sets of endpoints operating on messages.

3.10. WS-I Security	
Description	▪ WS-Security (Web Services Security, short WSS) is a flexible and feature-rich extension to SOAP to apply security to Web services. It is a member of the WS-* family of web service specifications and was published by OASIS. ▪ The protocol specifies how integrity and confidentiality can be enforced on messages and

	allows the communication of various security token formats, such as SAML, Kerberos, and X.509. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security.
Applicable to	▪ Web Services Security
Reference(s)	▪ http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss ▪ http://www.oasis-open.org/standards
Remarks	▪ WS-Security adds significant overhead to SOAP-processing due to the increased size of the message on the wire, XML and cryptographic processing, requiring faster CPUs and more memory and bandwidth. • Encryption was faster than signing • Encryption and signing together were 2-7 times slower than signing alone and produced significantly bigger documents. • Depending on the type of message, WS-SecureConversation either made no difference or reduced processing time by half in the best case. • It took less than 10 milliseconds to sign or encrypt up to an array of 100 kilo bytes, but it took about 100~200 to perform the security operations for SOAP.

3.11. WS-SECURE CONVERSATION	
Description	▪ WS-SecureConversation by itself does not provide a complete security solution for Web services. ▪ WS-SecureConversation is a building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of security models
Applicable to	▪ Web Services Security
Reference(s)	▪ http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/os/ws-secureconversation-1.4-spec-os.doc. ▪ http://oasis-open.org/committees/tc_home.php?wg_abbrev=ws-sx ▪ http://www.oasis-open.org/standards
Remarks	▪ A feature of Windows Communication Foundation (WCF) is the ability to establish secure sessions between two endpoints that authenticate each other and agree upon an

	encryption and digital signature process. ▪ Establishing this secure session enables the set of messages that are exchanged between the two endpoints to be more efficient, because the SCT (Security Context Token) has a symmetric key.

3.12. WS-FEDERATION	
Description	▪ The Web Services Federation specification is another component of the Web Services Security model that defines mechanisms to allow different security realms to federate by allowing and brokering trust of identities, attributes, authentication between participating Web services. The mechanisms defined in this specification can be used by passive and active requestors. The Web service requestors are assumed to understand the new security mechanisms and be capable of interacting with Web service providers.
Applicable to	▪ Web Services Security
Reference(s)	▪ http://www.ibm.com/developerworks/library/specification/ws-fed/ ▪ http://msdn.microsoft.com/en-us/library/bb498017.aspx#wsfedver1_topic1 ▪ http://www.oasis-open.org/standards
Remarks	▪ It is a well documented method for exchanging federation metadata makes it easy to bootstrap trust relationships and also to determine policies for obtaining services. ▪ Cross organizational identity mapping and distributed sign-out improve the utility and overall security of accessing federated service providers by minimizing the user's need to manage many identifiers and tokens. It also helps us in making the interactions between the participants easy.

3.13. WS-POLICY	
Description	▪ WS-Policy is a specification that allows web services to use XML to advertise their policies (on security, Quality of Service, etc.) and for web service consumers to specify their policy requirements. ▪ WS-Policy is now a W3C recommendation since September 2007. ▪ WS-Policy represents a set of specifications that describe the capabilities and constraints of the security (and other business) policies on intermediaries and end points (for

	example, required security tokens, supported encryption algorithms, and privacy rules) and how to associate policies with services and end points.
Applicable to	▪ Web Services Security
Reference(s)	▪ http://www.w3.org/2007/07/wspolicy-testimonial ▪ http://www.w3.org/TR/ws-policy/
Remarks	▪ WS-Policy is now a W3C recommendation since September 2007. ▪ WS-Policy represents a set of specifications that describe the capabilities and constraints of the security (and other business) policies on intermediaries and end points (for example, required security tokens, supported encryption algorithms, and privacy rules) and how to associate policies with services and end points.

3.14. WS-SECURITYPOLICY	
Description	▪ WS-SecurityPolicy is a WS* specification, created by IBM and 12 co-authors, that has become an OASIS standard as of version 1.2. ▪ It extents the fundamental security protocols specified by the WS-Security, WS-Trust and WS-SecureConversation by offering mechanisms to represent the capabilities and requirements of web services as policies. Security policy assertions are based on the WS-Policy framework.
Applicable to	▪ Web Services Security
Reference(s)	▪ http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html ▪ http://www.oasis-open.org/standards
Remarks	▪ Most policy assertion can be found in following categories: • Protection assertions identify the elements of a message that are required to be signed, encrypted or existent. • Token assertions specify allowed token formats (SAML, X509, Username etc.). • Security binding assertions control basic security safeguards like transport and

	message level security, cryptographic algorithm suite and required timestamps. • Supporting token assertions add functions like user sign-on using a username token. ▪ Policies can be used to drive development tools to generate code with certain capabilities, or may be used at runtime to negotiate the security aspects of web service communication. Policies may be attached to WSDL elements such as service, port, operation and message, as defined in WS Policy Attachment.

3.15. SAML	
Description	▪ The WS Security package contains a SAML Token generated by the Security Token Server in the requestor's forest. The signature on this package may not be recognized in the application Forest. ▪ The signature may be from a federated partner or within the enterprise. Service cannot be granted under these circumstances, and in fact the SAML package will not be examined for assertions.
Applicable to	
Reference(s)	▪ http://www.w3.org/2008/security-ws/papers/Delegated_SAML_Assertion_Pruning-b.pdf ▪ http://www.oasis-open.org/standards ▪ http://www.oasis-open.org/standards#samlv2.0
Remarks	▪ It will mainly improve the comprehensibility of writing that deals with Internet security, particularly Internet Standards documents (ISDs). To avoid confusion, ISDs should use the same term or definition whenever the same concept is mentioned.

3.16. 3DES	
Description	▪ The XML Encryption specification must describe how to use XML to represent a digitally encrypted Web resource (including XML itself). The XML representation of the encrypted resource must be a first class object (i.e., referenceable and consequently describable, signable, etc.) and represented by a distinct element type. ▪ The specification must provide for the encryption of a part or totality of an XML document. The mechanisms of encryption must be simple: describe how to encrypt/decrypt digital content.
Applicable to	▪ Encryption

Reference(s)	▪ http://www.w3.org/TR/xml-encryption-req#sec-Intro ▪ http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37972
Remarks	▪ In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. ▪ Because the key size of the original DES cipher was becoming problematically short, Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against brute force attacks, without designing a completely new block cipher algorithm.

3.17. RSA	
Description	▪ RSA is a public-key cryptosystem for both encryption and authentication. RSA is combined with the SHA hashing function to sign a message in this signature suite. ▪ It must be infeasible for anyone to either find a message that hashes to a given value or to find two messages that hash to the same value. If either were feasible, an intruder could attach a false message onto the signature.
Applicable to	▪ Encryption
Reference(s)	▪ http://en.wikipedia.org/wiki/SHA-2 ▪ http://en.wikipedia.org/wiki/SHA-3 ▪ http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html ▪ http://tools.ietf.org/html/rfc6234 ▪ http://www.css-security.com/tag/secure-hash-algorithm/ ▪ http://www.w3.org/PICS/DSig/RSA-SHA1_1_0.html ▪
Remarks	▪ SHA-1 has been replaced by SHA-2 ▪ Currently SHA-3 is being finalized. ▪ The hash functions SHA1 has been designed specifically to have the property that finding a match is infeasible, and is therefore considered suitable for use in this role.

3.18. MD-5, SHA	
Description	▪ SHA is a cryptographic message digest algorithm similar to the MD4 family of hash

	functions. It differs in that it adds an additional expansion operation, an extra round and the whole transformation was designed to accommodate the DSS block size for efficiency
Applicable to	▪ Encryption
Reference(s)	▪ http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html ▪ http://tools.ietf.org/html/rfc6234 ▪ http://www.css-security.com/tag/secure-hash-algorithm/ ▪ http://www.itl.nist.gov/fipspubs/fip180-1.htm ▪ http://csrc.nist.gov./publications/fips/fips180-3/fips180-3_final.pdf ▪ http://en.wikipedia.org/wiki/SHA-2 ▪ http://en.wikipedia.org/wiki/SHA-3 ▪ http://www.w3.org/PICS/DSig/SHA1_1_0.html ▪
Remarks	▪ The Secure Hash Algorithm takes a message of less than 264 bits in length and produces a 160-bit message digest which is designed so that it should be computationally expensive to find a text which matches a given hash. i.e. if you have a hash for document A, H(A), it is difficult to find a document B which has the same hash, and even more difficult to arrange that document B says what you want it to say.

3.19. XML-SIGNATURE SYNTAX AND PROCESSING, XML-DSS

Description	▪ The XML Signature is a method of associating a key with referenced data (octets); it does not normatively specify how keys are associated with persons or institutions, nor the meaning of the data being referenced and signed. ▪ Consequently, while this specification is an important component of secure XML applications, it itself is not sufficient to address all application security/trust concerns, particularly with respect to using signed XML (or other data formats) as a basis of human-to-human communication and agreement.
Applicable to	▪ XML Security
Reference(s)	▪ http://www.w3.org/TR/xmldsig-core/ ▪ http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/
Remarks	▪ XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.

3.20. XMLENC	
Description	▪ The XML Recommendation specifies the syntax of a class of resources called XML documents. The specification provides requirements for a XML syntax and processing for encrypting digital content, including portions of XML documents and protocol messages.
Applicable to	▪ XML Security
Reference(s)	▪ http://www.w3.org/TR/xml-encryption-req ▪ http://www.w3.org/TR/#tr_XML_Encryption
Remarks	▪ Encryption is one of the secure ways of sending messages through the internet. It can provide varied levels of security depending upon the security levels. It helps almost all the docs to be transferred securely over the internet.

3.21. DECRYPTION TRANSFORM FOR XML SIGNATURE AS DEFINED BY W3C	
Description	▪ It is an XML Syntax for the creation of digital signatures. An XML Signature can sign part of the same XML document which contains the signature enveloped another XML document, referenced through an URI detached.
Applicable to	▪ XML Security
Reference(s)	▪ http://www.w3.org/Consortium/Offices/Presentations/XML_Signatures/#[5]
Remarks	▪ Digital signatures give much security to the report. There will be a need where we need to share the resources by providing limited access to the reader so that they can't edit the data. It's a way of securing information from unauthorised access

3.22. XKMS 2.0	
Description	▪ This specifies protocols for distributing and registering public keys, suitable for use in conjunction with the standard for XML Signatures.

	▪ The XML Key Management Specification (XKMS) comprises two parts -- the XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS).
Applicable to	▪ XML Security
Reference(s)	▪ http://www.w3.org/TR/xkms2-bindings/#XKMS_2_0_Section_1 ▪ http://www.w3.org/TR/xkms2-req ▪ http://www.w3.org/TR/xkms/
Remarks	Open XKMS is an open source implementation of the W3C Recommendation of the XML Key Management Specification 2.0 (XKMS 2.0). ▪ A Client API providing access to the XKMS server in different ways: Apache SOAP, JAX-WS, HTTP. ▪ A Server Side Web service providing an access point to a PKI (including a demo PKI for testing purposes). ▪ A Test Suite to check the correctness of the server implementation and the interoperability with others implementations. ▪ A XKMS Library providing the base functionalities for dealing with XKMS 2. Used by the Client API, the Web service and the Test Suite. ▪ A Graphical Demo Client named Oxien using the Client API to demonstrate some base functionality (using the Client API but only Windows compatible).

3.23. SAML TOKEN PROFILE	
Description	• WS-Security offers a general-purpose mechanism for associating security tokens with message content. The specification defines the below approved token type: • SAML (Security Assertion Markup Language) Token Profile
Applicable to	▪ XML Security
Reference(s)	▪ http://www.ws-i.org/Profiles/SAMLTokenProfile-1.0.html ▪ http://www.oasis-open.org/standards#wssprofilesv1.0 ▪ http://www.oasis-open.org/standards
Remarks	▪ These profiles defines how to use its token type within the WS-Security specification. For example, the UsernameToken Profile describes how a Web service client can supply a

	UsernameToken as a way to identify the requestor by a username and optionally by supplying a password.

3.24. SAML 2.0	
Description	▪ Security Assertion Markup Language 2.0 (SAML 2.0) is a version of the SAML OASIS standard for exchanging authentication and authorization data between security domains. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end-user) between an identity provider and a web service. SAML 2.0 enables web-based authentication and authorization scenarios including single sign-on (SSO).
Applicable to	▪ XML Security
Reference(s)	▪ http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf ▪ http://www.oasis-open.org/standards
Remarks	▪ SAML 2.0 was ratified as an OASIS Standard in March 2005, replacing SAML 1.1. The critical aspects of SAML 2.0 are covered in detail in the official documents SAMLConform, SAMLCore, SAMLBind, and SAMLProf.

3.25. XACML	
Description	• eXtensible Access ControlMarkup Language (XACML), which is the most significant and emerging solution for controlling access in an interoperable and flexible way, to make it easily deployable and suitable for open Web-based systems.
Applicable to	▪ XML Security
Reference(s)	• http://www.w3.org/2009/policy-ws/papers/Samarati.pdf • http://lists.w3.org/Archives/Public/public-device-apis/2010Jun/0247.html
Remarks	• XACML standard allows the possibility to define new functions, data types, and policy combination methods, thus exploiting the language's flexibility to adapt it to several different needs.

3.26. X.509	
Description	▪ In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) for single sign-on (SSO) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
Applicable to	▪ Certificate Security
Reference(s)	▪ (obsolete)http://tools.ietf.org/html/rfc4210
Remarks	▪ X.509 also includes standards for certificate revocation list (CRL) implementations, an often neglected aspect of PKI systems. The IETF-approved way of checking a certificate's validity is the Online Certificate Status Protocol (OCSP). Firefox 3 enables OCSP checking by default along with versions of Windows including Vista and later.

3.27. PKCS	
Description	• The Public-Key Cryptography Standards are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. • First published in 1991 as a result of meetings with a small group of early adopters of public-key technology, the PKCS documents have become widely referenced and implemented. Contributions from the PKCS series have become part of many formal and de facto standards, including ANSI X9 documents, PKIX, SET, S/MIME, and SSL.
Applicable to	▪ Certificate Security
Reference(s)	▪ http://www.rsa.com/rsalabs/node.asp?id=2129 ▪ http://www.rsa.com/rsalabs/node.asp?id=2124
Remarks	▪ This standard describes general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

3.28. IPSec	
Description	▪ Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. ▪ IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host.
Applicable to	▪ IP Security
Reference(s)	▪ (Obsolete)http://tools.ietf.org/html/rfc5998
Remarks:	▪ The IPSec suite is a framework of open standards. IPsec uses the following protocols to perform various functions: • A security association (SA) is set up by Internet Key Exchange (IKE and IKEv2) or Kerberized Internet Negotiation of Keys (KINK) by handling negotiation of protocols and algorithms and to generate the encryption and authentication keys to be used by IPsec. • Authentication Header (AH) to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replay attacks. • Encapsulating Security Payload (ESP) to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

3.29. SSL	
Description	▪ Secure Socket Layer (SSL), are cryptographic protocols that provide security for communications over networks such as the Internet. SSL encrypt the segments of network connections at the Transport Layer end-to-end.

	▪ Several versions of the protocols are in widespread use in applications like web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).
Applicable to	▪ Transport Security
Reference(s)	▪ http://tools.ietf.org/html/rfc5246 ▪ http://tools.ietf.org/html/rfc5746 ▪ http://tools.ietf.org/html/rfc5878 ▪ http://tools.ietf.org/html/rfc6176
Remarks	▪ It is mainly used to ensure authenticity and integrity to communications

4. Details of Tools Supporting Recommended Standards

This section provides a brief description of the relevant tools listed in section 2 along with links for references to these tools.

4.1. IBM Tivoli Federated Identity Manager (TFIM) & Tivoli Access Manager for e-business (TAMeb)

Description	▪ IBM considers Tivoli Federated Identity Manager (TFIM) as its main access management offering, with Tivoli Access Manager for e-business (TAMeb) merely a stripped-down, low-cost alternative (TAMeb is bundled with TFIM). TFIM is a highly sophisticated offering, with built-in capabilities for simple, federated provisioning and Web services security, as well as versatile identity federation capabilities.
Applicable to	▪ Access Management
Reference(s)	▪ IBM Tivoli Federated Identity Manager http://www-01.ibm.com/software/tivoli/products/federated-identity-mgr/ ▪ IBM Tivoli Access Manager for e-business http://www-01.ibm.com/software/tivoli/products/access-mgr-e-bus/
Remarks	▪ These are mainly used to provide centralized authentication and authorization capabilities for applications. ▪ Access management products may include identity administration, role/rule life cycle management, and audit and federation capabilities. ▪ They also incorporate some level of user-provisioning functionality or integration with a user-provisioning tool.

4.2. Oracle Access Management solutions

Description	▪ Oracle Access Manager is the access management product from Oracle that couples the capabilities for access management and identity administration. ▪ Sun OpenSSO Enterprise Sun OpenSSO Enterprise (formerly Sun Access Manager and Sun Federation Manager) is the single solution for access management, federation, and Web services security.
Applicable to	▪ Access Management
Reference(s)	▪ Oracle Access Manager ▪ http://www.oracle.com/technology/products/id_mgmt/coreid_acc/index.html ▪ http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index.html ▪ Sun OpenSSO Enterprise

	▪ http://www.sun.com/software/products/opensso_enterprise/index.xml ▪ http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index.html
Remarks	▪ These are mainly used to provide centralized authentication and authorization capabilities for applications. ▪ Access management products may include identity administration, role/rule life cycle management, and audit and federation capabilities. ▪ They also incorporate some level of user-provisioning functionality or integration with a user-provisioning tool.

4.3. CA ACCESS MANAGEMENT SOLUTIONS	
Description	▪ CA SiteMinder is a centralized Web access management system that enables user authentication and single sign-on, authentication management, policy-based authorization, identity federation and auditing of access to Web applications and portals.
Applicable to	▪ Access Management
Reference(s)	▪ CA SiteMinder http://www.ca.com/us/internet-access-control.aspx
Remarks	▪ These are mainly used to provide centralized authentication and authorization capabilities for applications. ▪ Access management products may include identity administration, role/rule life cycle management, and audit and federation capabilities. ▪ They also incorporate some level of user-provisioning functionality or integration with a user-provisioning tool.

4.4. RADIUS	
Description	▪ Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. Because of the broad support and the ubiquitous nature of the RADIUS protocol it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.
Applicable to	▪ Authentication, Authorization and Accounting
Reference(s)	▪ RADIUS http://tools.ietf.org/html/rfc2865

	Further Reading ▪ AAA protocol at Wikipedia http://en.wikipedia.org/wiki/AAA_protocol
Remarks	▪ "Authentication, Authorization and Accounting" (AAA), are the three primary services that provide a network security and a record of user activity by identifying who the user is, what the user can access, and what services and resources the user is using when they make a connection with a server.

4.5. DIAMETER	
Description	▪ Diameter is a computer networking protocol for AAA (authentication, authorization and accounting). It is a successor to RADIUS. Diameter is not directly backwards compatible, but provides an upgrade path for RADIUS.
Applicable to	▪ Authentication, Authorization and Accounting
Reference(s)	▪ Diameter http://tools.ietf.org/html/rfc3588 Further Reading ▪ AAA protocol at Wikipedia http://en.wikipedia.org/wiki/AAA_protocol
Remarks	▪ "Authentication, Authorization and Accounting" (AAA), are the three primary services that provide a network security and a record of user activity by identifying who the user is, what the user can access, and what services and resources the user is using when they make a connection with a server.

4.6. TACACS+	
Description	▪ Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.
Applicable to	▪ Identity Management
Reference(s)	▪ TACACS+ http://tools.ietf.org/html/draft-grant-tacacs-02 Further Reading ▪ AAA protocol at Wikipedia http://en.wikipedia.org/wiki/AAA_protocol

Remarks	▪ "Authentication, Authorization and Accounting" (AAA), are the three primary services that provide a network security and a record of user activity by identifying who the user is, what the user can access, and what services and resources the user is using when they make a connection with a server.

4.7. IBM Tivoli Identity Manager	
Description	▪ IBM Tivoli Identity Manager, also known as TIM, is an identity lifecycle management product from IBM. TIM provides centralized identity lifecycle management.
Applicable to	▪ Identity Management
Reference(s)	▪ IBM Tivoli Identity Manager http://www-01.ibm.com/software/tivoli/products/identity-mgr/
Remarks	▪ Identity management systems provide facilities for managing lifecycle of identities from establishment to destruction.

4.8. Oracle Identity Management Solution	
Description	▪ Oracle Identity Management (OIM) is an enterprise infrastructure, which leverages Oracle's technology. ▪ Sun Identity Manager is the user provisioning software to truly provide role-based user provisioning.
Applicable to	▪ Identity Management
Reference(s)	Oracle Identity Manager ▪ http://www.oracle.com/technology/products/id_mgmt/oxp/index.html ▪ http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index.html Sun Identity Manager ▪ http://www.sun.com/software/products/identity_mgr/index.xml ▪ http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index.html
Remarks	▪ Identity management systems provide facilities for managing lifecycle of identities from establishment to destruction.

4.9. TrendMicro	
Description	▪ Trend Micro is a computer company that develops software and services to protect against computer viruses, malware, spam, and Web-based threats. Trend Micro is the anti-spam system predominantly utilized by ministries/agencies.
Applicable to	▪ Protection from email spam, computer viruses, malware and Web-based threats ▪ Desktop Firewall
Reference(s)	▪ Trend Micro http://emea.trendmicro.com/emea/home/index.html
Remarks	▪ To provide a unified solution for protection from e-mail spam, computer viruses, malware, spam, and Web-based threats.

4.10. Symantec	
Description	▪ Symantec includes a family of software and services to protect against computer spam, web-based threats, computer viruses and malware.
Applicable to	▪ Protection from email spam, computer viruses, malware and Web-based threats ▪ Desktop Firewall
Reference(s)	▪ Symantec http://www.symantec.com/business/products/family.jsp?familyid=brightmail ▪ Symantec (Norton) http://www.symantec.com/norton/index.jsp
Remarks	▪ To provide a unified solution for protection from e-mail spam, computer viruses, malware, spam, and Web-based threats.

4.11. McAfee	
Description	▪ McAfee, Inc. is an computer security company that markets leading anti-spam solutions. ▪ McAfee, Inc. Also has antivirus software and computer security company that markets McAfee VirusScan and related security products and services, including the IntruShield, Entercept, and Foundstone brands
Applicable to	▪ Protection from email spam, computer viruses, malware and Web-based threats
Reference(s)	▪ McAfee http://www.mcafee.com/us/enterprise/products/email_and_web_security/index.html

	▪ www.mcafee.com
Remarks	▪ To provide a unified solution for protection from e-mail spam, computer viruses, malware, spam, and Web-based threats.

4.12. CISCO IRONPORT	
Description	▪ IronPort designed and sold products and services that protect enterprises against Internet threats. It was best known for IronPort AntiSpam, the SenderBase email reputation service, and email security appliances. It was acquired by Cisco Systems.
Applicable to	▪ Email Spam protection
Reference(s)	▪ Cisco IronPort http://www.ironport.com/products/email_security_appliances.html
Remarks	▪ To protect from e-mail spam, both end users and administrators of e-mail systems use various anti-spam techniques which have been embedded in some of these anti-spam products.

4.13. MICROSOFT FOREFRONT	
Description	▪ Microsoft Forefront is a line of comprehensive security products. According to Microsoft, the Forefront line will provide companies with multiple layers of defense against threats.
Applicable to	▪ Protection from email spam, computer viruses, malware and Web-based threats
Reference(s)	▪ Microsoft Forefront http://www.microsoft.com/en-us/server-cloud/forefront/default.aspx
Remarks	▪ To provide a unified solution for protection from e-mail spam, computer viruses, malware, spam, and Web-based threats.

4.14. KASPERSKY	
Description	▪ Kaspersky Lab is a computer security company offering anti-virus, anti-spyware, anti-spam, and anti-intrusion products.

Applicable to	▪ Protection from computer viruses, malware and Web-based threats ▪ Desktop Firewall
Reference(s)	▪ Kaspersky Lab http://www.kaspersky.com ▪ Kaspersky Labs http://www.kaspersky.com/kaspersky_internet_security
Remarks	▪ To provide a unified solution for protection from computer viruses, malware, spam, and Web-based threats.

4.15. CA INC.	
Description	▪ CA Inc., formerly, Computer Associates Inc. provides anti-virus and internet security programs for consumer personal computers.
Applicable to	▪ Protection from computer viruses, malware and Web-based threats
Reference(s)	▪ CA http://www.ca.com/us/it-security-solutions.aspx
Remarks	▪ To provide a unified solution for protection from computer viruses, malware, spam, and Web-based threats.

4.16. MICROSOFT WINDOWS DEFENDER	
Description	▪ Windows Defender, formerly known as Microsoft AntiSpyware, is a software product from Microsoft to prevent, remove and quarantine spyware in Microsoft Windows. It is included and enabled by default in Windows Vista and Windows 7, and is available as a free download for Windows XP and Windows Server 2003
Applicable to	▪ Protection from computer viruses, malware and Web-based threats
Reference(s)	▪ Windows Defender http://www.microsoft.com/windows/products/winfamily/defender/default.mspx
Remarks	▪ To provide a unified solution for protection from computer viruses, malware, spam, and Web-based threats.

4.17. Microsoft Windows Firewall	
Description	▪ Windows Firewall is the firewall service included with desktop and server releases of Microsoft Windows from Windows XP and Windows Server 2003 onwards.
Applicable to	▪ Desktop Firewall
Reference(s)	▪ Microsoft Windows Firewall http://www.microsoft.com/windowsxp/using/security/Internet/sp2_wfintro.mspx and http://www.microsoft.com/windows/windows-vista/features/firewall.aspx
Remarks	▪ To provide a solution for protection from computer viruses, malware, spam, and Web-based threats.

4.18. IPTables	
Description	▪ iptables is a user space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall and the chains and rules it stores. Different kernel modules and programs are currently used for different protocols.
Applicable to	▪ Desktop Firewall
Reference(s)	▪ iptables http://www.netfilter.org
Remarks	▪ To provide a solution for protection from computer viruses, malware, spam, and Web-based threats.

4.19. CISCO Firewall	
Description	▪ Cisco Adaptive Security Appliance 5500 Series, or simply Cisco ASA, is Cisco's line of network security devices introduced in 2005, that succeeded existing lines of popular Cisco products viz. Cisco PIX, Cisco IDP 4200 and Cisco VPN 3000 Series Concentrators. ▪ Cisco PIX (Private Internet eXchange) is a popular IP firewall and network address translation (NAT) appliance. Cisco announced the end-of-sale and end-of-life dates for all Cisco PIX Security Appliances, software, accessories, and licenses. Cisco will continue to support Cisco PIX Security Appliance customers through July, 2013.
Applicable to	▪ Enterprise Firewall

Reference(s)	▪ Cisco ASA http://www.cisco.com/en/US/products/ps6120/index.html ▪ Cisco PIX http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/
Remarks	▪ To provide a solution for protection from unauthorized access while permitting authorized computer traffic between different security domains based upon a set of rules and other criteria.

4.20. JUNIPER FIREWALL	
Description	▪ Juniper products are widely used in the large networks around the world and it is a leader in high-performance networking. Juniper Netscreen products has largely been announced for end of sales by Juniper.
Applicable to	▪ Enterprise Firewall
Reference(s)	▪ Juniper Firewalls http://www.juniper.net/us/en/products-services/security/
Remarks	▪ To provide a solution for protection from unauthorized access while permitting authorized computer traffic between different security domains based upon a set of rules and other criteria.

4.21. CHECKPOINT FIREWALL	
Description	▪ Check Point Software Technologies Ltd. is a hardware and software company that is best known for its firewall and VPN products.
Applicable to	▪ Enterprise Firewall
Reference(s)	▪ Gartner Magic Quadrant for Enterprise Network Firewalls http://mediaproducts.gartner.com/reprints/juniper/vol4/article1/article1.html ▪ Checkpoint Solutions http://www.checkpoint.com ▪ http://www.checkpoint.com/products/firewall-software-blade/index.html
Remarks	▪ To provide a solution for protection from unauthorized access while permitting authorized computer traffic between different security domains based upon a set of rules and other criteria.

4.22. Fortinet Firewall	
Description	▪ Fortinet is a private company that specializes in consolidated network security appliances. Fortinet's flagship product line is sold under the brand name of FortiGate.
Applicable to	▪ Enterprise Firewall
Reference(s)	▪ Fortinet Fortigate http://www.fortinet.com/products/fortigate/
Remarks	▪ To provide a solution for protection from unauthorized access while permitting authorized computer traffic between different security domains based upon a set of rules and other criteria.

4.23. McAfee (Secure Computing Corporation) Firewall	
Description	▪ Secure Computing Corporation developed and sold computer security appliances and hosted services to protect users and data. McAfee acquired the company in 2008. Secure Computing Firewall has been developed as McAfee Firewall Enterprise.
Applicable to	▪ Enterprise Firewall
Reference(s)	▪ McAfee Secure Computing http://www.securecomputing.com/
Remarks	▪ To provide a solution for protection from unauthorized access while permitting authorized computer traffic between different security domains based upon a set of rules and other criteria.

4.24. Cisco Intrusion Detection Systems	
Description	▪ Cisco provides holistic network security through its IDS integrated switch/router services, ASA Adaptive Security Appliance and 4200 series IPS sensor.
Applicable to	▪ Intrusion Detection Systems
Reference(s)	▪ Cisco Security Products and Services http://www.cisco.com/en/US/products/hw/vpndevc/index.html

Remarks	▪ To provide protection from unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet.

4.25. TIPPING POINT INTRUSION DETECTION SYSTEMS	
Description	▪ TippingPoint is a leading vendor for Intrusion Prevention Systems.
Applicable to	▪ Intrusion Detection Systems
Reference(s)	▪ TippingPoint http://www.tippingpoint.com, http://www.tippingpoint.com/technology_tse.html
Remarks	▪ To provide protection from unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet.

4.26. SOURCEFIRE INTRUSION DETECTION SYSTEMS	
Description	▪ Sourcefire, Inc develops network security hardware and software. The Sourcefire 3D System is based on Snort, an open-source intrusion detection engine. The Sourcefire 3D System is an intrusion prevention solution that can be divided into three customer protection phases—IPS, Adaptive IPS, and Enterprise Threat Management (ETM).
Applicable to	▪ Intrusion Detection Systems
Reference(s)	▪ Sourcefire 3D System http://www.sourcefire.com/products/3D
Remarks	▪ To provide protection from unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet.

4.27. ISS INTRUSION DETECTION SYSTEMS	
Description	▪ Internet Security Systems (ISS) is a security software provider that was acquired by IBM in 2006. Proventia and RealSecure are leading intrusion detection and prevention systems from ISS.

Applicable to	▪ Intrusion Detection Systems
Reference(s)	▪ IBM Internet Security Systems (ISS) http://www.iss.net/
Remarks	▪ To provide protection from unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet.

4.28. JUNIPER INTRUSION DETECTION SYSTEMS	
Description	▪ Juniper Networks intrusion detection and prevention products provide comprehensive inline protection from worms, Trojans, spyware, keyloggers, and other malware. By accurately identifying application traffic, they ensure continuous availability of business-critical applications.
Applicable to	▪ Intrusion Detection Systems
Reference(s)	▪ Juniper Intrusion Detection and Prevention Appliances http://www.juniper.net/us/en/products-services/security/idp-series/
Remarks	▪ To provide protection from unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet.

4.29. MICROSOFT INTERNET SECURITY AND ACCELERATION SERVER (ISA SERVER)	
Description	▪ Microsoft Internet Security and Acceleration Server (ISA Server) is a Firewalling & Security product based on Microsoft Windows. Primarily designed to securely publish web servers and other server systems, provide Stateful, Application-Layer Firewalling, act as a VPN endpoint, and provide Internet Access for client systems in a Business Networking environment.
Applicable to	▪ Proxy Server
Reference(s)	▪ Microsoft ISA http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/default.aspx
Remarks:	▪ The proxy server evaluates the request according to its filtering rules and provides a level

	of protect from the incoming requests to the systems..

4.30. BLUE COAT PROXY SERVER	
Description	▪ Blue Coat secures Web communications and accelerates business applications across the distributed enterprise. Blue Coat's family of appliances and client-based solutions – deployed in branch offices, Internet gateways, end points, and data centers – provide intelligent points of policy-based control
Applicable to	▪ Proxy Server
Reference(s)	▪ Blue Coat http://www.bluecoat.com/products/overview
Remarks	▪ The proxy server evaluates the request according to its filtering rules and provides a level of protect from the incoming requests to the systems..

4.31. WEBSENSE SERVER	
Description	▪ Websense is a San Diego-based company specializing in Web security gateway software. It enables clients (businesses and governments) to block access to chosen categories of website
Applicable to	▪ Proxy Server
Reference(s)	▪ Web Sense http://www.websense.com, http://www.websense.com/content/WebFilter.aspx
Remarks	▪ The proxy server evaluates the request according to its filtering rules and provides a level of protect from the incoming requests to the systems..

5. APPENDICES

5.1. APPENDIX A: ABBREVIATIONS AND ACRONYMS

Abbreviation / Acronym	Security
TLS	Transport Layer Security
S/MIME	Secure Multipurpose Internet Mail Extension
IPSec	Internet Protocol Security
SSL	Secure Socket Layer
CMS	Content Management System
TSP	Time Stamp Protocol
SSH	Secure Shell
3DES	Triple Data Encryption standards
RSA	Random Sequential Adsorption
RSAES	Random System Algorithm Encryption Scheme
OAEP	Optimal Asymmetric Encryption Padding
MD-5	Message-Digest algorithm 5
SHA	Secure Hash Algorithm
SAML	Security Assertion Markup Language
DSS	Digital Signature Service
SSO	Single Sign-on
RADIUS	Remote Authentication Dial In User Service
TACACS	Terminal Access Controller Access-Control System
ASA	Adaptive Security Appliance
IPS	Intrusion Prevention Systems
IDS	Intrusion Detection Systems
ISS	Internet Security Systems
ISA Server	Internet Security and Acceleration Server

5.2. APPENDIX B: RELATED DOCUMENTS / LINKS

Acknowledgement of major references for international technology standards and Specifications:

- Internet Engineering Task Force (IETF)
  http://www.ietf.org
- International Standards Organization (ISO)
  http://www.iso.org
- World Wide Web Consortium (W3C)
  http://www.w3c.org

Acknowledgement of other references for international technology standards and specifications:

- American National Standards Institute (ANSI)
  http://www.ansi.org
- ECMA International
  http://www.ecma-international.org
- Institute of Electrical and Electronics Engineers (IEEE)
  http://www.ieee.org
- National Institute of Standards and Technology (NIST)
  http://www.nist.gov
- Object Management Group (OMG)
  http://www.omg.org
- Open Mobile Alliance (OMA) and WAP Forum
  http://www.openmobilealliance.org
  http://www.wapforum.org
- Organization for the Advancement of Structured Information Standards (OASIS)
  http://www.oasis-open.org
- Unicode, Inc.
  http://www.unicode.org