



**INFORMATION SECURITY ASSURANCE:**

FORUM SYSTEMS' FEDERAL INFORMATION ASSURANCE SOLUTION





## INTRODUCTION

With security concerns being brought to the forefront, and the increasing use of the Internet to vend content to the public, information needs to be shared and integrated in a highly efficient manner throughout various agencies of the federal government. With this ever-increasing flow of information, comes a growing challenge for federal agencies to protect the integrity, confidentiality, and availability of the content they maintain. No longer can security and privacy issues be addressed on a system-by-system basis. These security and privacy issues are key components in how federal agencies will work together on critical cross-government initiatives such as Homeland Security and e-Gov.

## E-GOVERNMENT MANDATES

As an example of the federal government's emphasis on streamlined information sharing, The Bush administration has recommended the spending of \$700 million to "improve intelligence-gathering and information-sharing between agencies and throughout all levels of government" as a function of the newly created Department of Homeland Security (DHS). Recent legislation also indicates the government's desire to embrace the electronic exchange of information in an efficient and secure manner. Examples include:

- ▶ Clinger-Cohen Act of 1996, designed to streamline IT acquisitions and emphasize life cycle management of IT as a capital investment
- ▶ Health Insurance Portability and Accountability Act of 1996 ("HIPPA"), which safeguards the electronic transmission of private medical data
- ▶ Gramm-Leach-Bliley Act of 1999, which provides privacy protections against the sale of private financial information
- ▶ Electronic Signatures in Global and National Commerce Act of 2000 ("E-Sign"), which encourages the exchange of information via the Internet through the use of electronic signatures
- ▶ e-Gov Act of 2002, which seeks to provide a one-stop-shop approach for the private sector to obtain public sector information via the Internet
- ▶ Sarbanes-Oxley Act of 2002, which deals with corporate governance and related information security and privacy controls

Of course, there is a price to pay with the increase in information flow within the federal government. This content must remain secure as it travels between agencies and is vended to the private sector and the public. Without adequate security and efficient flow of information between government agencies, millions of dollars can be lost and lives can be endangered.

## THE PILLARS OF SECURITY: THREAT PROTECTION & TRUST MANAGEMENT

Recent security breaches and attacks to government computer systems, as well as systems in the private sector, are constant reminders of the need for safe and secure transmission of content over the Internet. These lapses in security can result in lost access to servers, applications, and networks, and can be very expensive. This expense can be measured in terms of lost productivity, the cost to repair an organization's system(s), and the system's credibility – which has no accurate measure.

Information Assurance is primarily concerned with the following issues:

- ▶ Persistent security that spans time and the location of content – including content that is in-transit, stored in a database, or being processed by an application.
- ▶ Protection of information in a mixed workflow environment – including e-mail, file transfers, EDI, mobile applications, and Web Services.

<sup>1</sup>[www.whitehouse.gov](http://www.whitehouse.gov)





Information Assurance is enabled by using content security mechanisms that can be broken into two major categories, Threat Protection and Trust Management.

**THREAT PROTECTION** is primarily focused on protecting an organization's information content from vulnerability to attacks. Initiatives like e-Gov have led to an increased use of the Internet by the federal government to exchange and vend content to the public. As a result, there is ever-increasing exposure to potential external security attacks. DoS attacks prevent the exchange of critical information between systems and agencies. Attacks not only compromise the confidentiality of content, but also its integrity. **INTRUSION DETECTION AND PREVENTION** focuses on threat protection capabilities that can mitigate the damage caused by these security breaches.

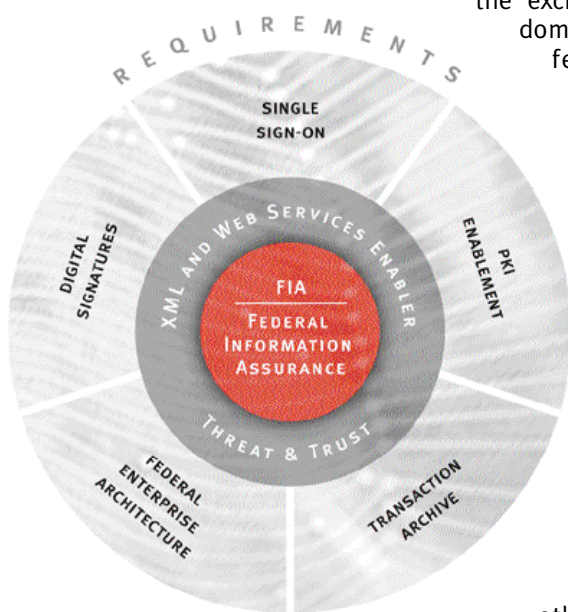
**TRUST MANAGEMENT** deals with the question, "Can someone be trusted to perform a particular action on a specific object?" It unifies the notions of properly identifying an individual via **AUTHENTICATION**, providing access control through the process of granting or denying use of network resources via **AUTHORIZATION**, preserving the integrity of content (through **NON-REPUDIATION**) by ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message, establishing an audit trail by recording the history of transactions in an **TRANSACTION ARCHIVE**, and protecting the confidentiality of content through **ENCRYPTION**.

## GOVERNMENT INFORMATION ASSURANCE REQUIREMENTS

While each of the federal government's various agencies has developed its own Security Policy, there are several common technologies, standards, and architectures that span agencies. These include:

### SINGLE SIGN-ON (SSO)

SSO is a method of identification and authorization that permits the user to access all information systems, to which he or she is authorized, in a single, transparent manner. The *Organization for the Advancement of Structured Information Standards* (OASIS) has defined an *Extensible Markup Language* (XML) standard, the *Security Assertion Markup Language* (SAML), to make SSO possible. SAML enables the exchange of authentication and authorization information between domains. SSO is being deployed throughout the various agencies of the federal government. As an example, the United States Army has created a portal with SSO, called Army Knowledge Online, to provide it's 1.2 million users, at locations around the world, with a single access point for information. This functionality is also crucial to the use of federated systems that span multiple government agencies, like those employed by the Department of Homeland Security.



### DIGITAL SIGNATURES

Digital Signatures are digital codes that can be attached to an electronic transmission, or document, that uniquely identify the sender. The *Electronic Signatures in Global and National Commerce Act of 2000* ("E-SIGN") was passed to encourage the exchange of information via the Internet through the use of electronic signatures. Digital signatures are essential to secure transmission of content over intranets, or over the Internet.

### PUBLIC-KEY INFRASTRUCTURE (PKI) ENABLEMENT

PKI is a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Federal agencies, like the Department of Defense (DoD), have fully embraced the use of PKI to securely communicate electronically within and between branches of the military. PKI is so crucial to this arm of the federal government that they have declared, "All DoD unclassified networks that authenticate





users.... shall be PK-enabled...”<sup>2</sup> . Support for key standards, such as *DoD PKI X.509 Certificate Support and FIPS-140 Level II Specification for Private Key Lifecycle Management*, are requirements for vendors of “Commercial-Off-the Shelf (COTS)” technology to be considered by the DoD. Furthermore, support for Common Access Cards (CAC), which allows a user to store their private key(s) on a removable/portable smart card, is a requirement of the DoD.

### **FEDERAL ENTERPRISE ARCHITECTURE (FEA)**

The FEA is an initiative of the federal government (led by the White House’s Office of Management and Budget (OMB)) to identify, “duplicative investments, gaps, and opportunities for collaboration within and across Federal Agencies.”<sup>3</sup> The FEA is a framework designed to transform the federal government into being more citizen-centered, results-oriented, and market-based. It is comprised of five reference models that define technologies (and their capabilities), industry-standards, and emerging technologies to be used in federal IT projects. Upon implementation, the federal government will be able to improve communication flow, and efficiency, via integration of disparate systems. It will also be able to enhance cost savings through reuse of technology and components.

### **TRANSACTION ARCHIVE**

A Transaction Archive is a repository for recording the history of XML, and non-XML, transactions and storing them in an external database. Government agencies must continuously record and audit their mission-critical electronic business transactions to support regular security reviews of all programs and systems per the Government Information Security Reform Act of 2000 (a.k.a. The Security Act). By archiving XML transactions, and other content, it is possible to analyze security breaches, maximize operational performance, and maintain regulatory compliance.

### **XML & WEB SERVICES: FACILITATING INFORMATION EXCHANGE**

Web Services and XML are key technologies that will enable the federal government to efficiently share and integrate content between it’s multiple agencies and systems. According to a General Accounting Office (GAO) report, “XML has the potential to help the federal government significantly streamline the process of identifying, integrating, and processing information from widely dispersed systems and organizations.”<sup>4</sup> XML is a platform independent, universal language, developed by the World Wide Web Consortium (W3C), that is used to support the structuring and integration of documents and content on the web. It enables the definition, transmission, validation, and interpretation of content between applications and between organizations.

The federal government is mandating XML and Web Services as the primary technologies for the integration of content across its many agencies. According to Robert Haycock, manager of the OMB’s E-Gov Office, these technologies are “enabling cornerstones [of the] transformation in the way the federal government does business and communicates with citizens.”<sup>5</sup>

### **SECURITY**

XML’s greatest strength and weakness is that it describes a great deal about the content that’s represented in a document. On one hand, this feature simplifies programming and facilitates interoperability among systems and disparate applications. On the other hand, XML’s openness makes it easy for those interested in breaching security to see where crucial content ‘lives’. The exposed nature of XML elevates security issues from the TCP/IP stack to the application layer of the OSI model.

Security technologies, like SSL, which were designed to protect peer-to-peer transmissions, are unable to handle

<sup>2</sup> Department of Defense Memorandum: Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense, May 17, 2001

<sup>3</sup> The Federal Enterprise Architecture: An Overview of Vision and Progress, Robert Haycock; XML Conference & Exposition, December 2002

<sup>4</sup> GAO-02-327 Electronic Government

<sup>5</sup> The Federal Enterprise Architecture: An Overview of Vision and Progress, Robert Haycock; XML Conference & Exposition, December 2002





multi-hop data exchange, across secure and non-secure transport protocols, and across varying security domains. As more information moves between applications that are not in the immediate control of the originator, it becomes essential to guarantee that only the intended recipients are given appropriate access privileges to the information – where ver it resides. Assurances need to be made that information is not only tamper-proof and confidential during transit but also upon arrival, in-storage, and during processing.

## **FORUM SYSTEMS' FEDERAL INFORMATION ASSURANCE SOLUTION**

Forum Systems addresses *THREAT PROTECTION AND TRUST MANAGEMENT* for the federal government with its *FEDERAL INFORMATION ASSURANCE SOLUTION (FIAS)*. Forum Systems has developed a content security infrastructure that actively guards mission-critical content as it moves between, and within, federal agencies. The FIAS allows for automated and centrally managed security policies that allow sharing and dissemination of protected information across multiple content exchange points that span multiple systems, and government agencies.

### **THREAT PROTECTION**

While traditional firewalls do a good job of monitoring and recognizing malicious network-level attacks and intrusions, they are not able to view the content of messages in order to detect and prevent security breaches at the application level. This allows hackers to embed harmful instructions and application data into XML messages, which are then able to flow undetected into an internal network or directly into an application. Forum Systems' FIAS offers XML-specific Intrusion Prevention (XIP™) at “the edge” of the network to prevent such an attack from occurring. It also provides vulnerability isolation and monitoring capabilities to ensure that critical systems, and applications, stay on-line.

### **TRUST MANAGEMENT**

There are four essential elements critical to comprehensive XML and Web Services trust management:

- ▶ Identity Authentication
- ▶ Access Control (Authorization)
- ▶ Content Integrity
- ▶ Confidentiality and Privacy

If you don't have these layers of defense, your Web Services will be open to anyone who wants to access and manipulate content. Forum Systems' FIAS addresses the question, “Can someone be trusted to perform a particular action on a specific object?” by making it possible for security designers to gain control of policy variability across these four essential elements.

Forum Systems' solution provides a number of paths to establishing a digital user/entity identity and enforcement of access rights and privileges, including support for SSO via SAML, as well as X.509 certificate support. It supports the integrity of the content being transmitted, via non-repudiation, by externally archiving an entire document and/or selected elements (including Digital Signatures) of a document to a relational database. Forum Systems' also offers support for asymmetric and symmetric encryption algorithms for both SSL and XML security operations.

### **STANDARDS SUPPORT**

Forum Systems has been at the forefront of XML-based security technologies with in-depth “know-how” of XML technologies and the implementation of Web Services security specifications. Forum Systems is heavily involved with numerous Web Services security standard's bodies, including W3C, OASIS, IETF, and NIST to help guide and determine the most appropriate security guidelines.





## CONCLUSION

The federal government's push to transform its numerous agencies into being more citizen-centered, results-oriented, and market-based is underway. Current events dictate that it is inevitable that the various disparate federal agencies must improve information flow – both intra-agency and between agencies. This all must be accomplished at a reasonable cost, and in a relatively short time period. The power and flexibility of Web Services and XML will play a central role in making this a reality. The challenge of ensuring that federal agencies protect the integrity, confidentiality, and availability of the content they maintain will depend largely on the functionality present in offerings like Forum Systems' *FEDERAL INFORMATION ASSURANCE SOLUTION*.

