PKI Implementation Plan for OASIS

Overview

OASIS[1] has been on-line since January, 1997 to facilitate open communication of transmission information including information related to the purchasing and selling of transmission rights. Technical requirements and standards for OASIS are documented in the S&CP[2] Version 1.4 document and associated updates.

While the S&CP has created a common communication standard for OASIS, dramatically different security architecture implementations abound. OASIS systems are not by any means the only systems with differing security architectures. NERC E-Tagging systems and many industry support systems all have security architectures that are different or non-existent.

NERC, the DoE and NAESB have joined together to create the e-MARC PKI[3]. This infrastructure is designed to facilitate secure electronic communications between systems sharing sensitive energy related data and users accessing these systems. The e-MARC PKI is based on the *X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, Request for Comment (RFC) 2527 of the Internet Engineering Task Force (IETF).

This implementation plan document has been created to accomplish the following goals:

1. Implement data encryption for all sensitive OASIS data
2. Lay the foundation for e-MARC

Implementation of Data Encryption

The standard for data encryption for Internet-based communications is Secure Socket Layer (SSL). SSL is a protocol that is universally accepted for use in web browsers and web servers.

SSL uses PKI by allowing clients to encrypt data sent to a web server with that server's public key. The server, and only the server, can decrypt the data ensuring data confidentiality between the client and the server.

Section 5.1(g) of the S&CP requires that "Sophisticated data encryption techniques….shall be used to transfer sensitive data across the Internet and directly between OASIS nodes". Section 5.1(d) requires user registration and Section 5.1(e) requires passwords to authenticate the user if not using certificates as identified in Section 5.1(m).

---

[1] Open Access Same-Time Information System
[2] Standards and Communication Protocols for Open Access Same-Time Information System
[3] Energy Market Access and Reliability Certificates Public Key Infrastructure

The only transmission information on OASIS that is considered sensitive is the Source and Sink information associated with a pending request. Passwords associated with user accounts should also be considered sensitive and should never be passed unencrypted. Therefore, anytime a user communicates password information, that communication should be encrypted.

To achieve data encryption for sensitive OASIS data, all OASIS nodes should, at a minimum, implement SSL. The certificate used should be an X.509 certificate issued by a trusted ~~vender~~vendor. Because SSL does not alter http, but simply provides a "socket" for encrypting http traffic, the cost of implementation should be fairly low. If, however, an OASIS implementation does not use a web server that supports SSL, the costs will be greater.

[PRS: We will need to determine a definition for trusted vendor and a mechanism to communicate to all OASIS users the specific "trusted vendors" that are used by each OASIS node so they can be prepared if/when challenged with the "do you trust this certificate" dialog.]

Laying the Foundation for e-MARC

If implemented properly, a PKI such as e-MARC ensures the following security services:

- Confidentiality: The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended
- Authentication: The assurance to one entity that another entity is who he/she/it claims to be
- Integrity: The assurance to an entity that data has not been altered (intentionally or unintentionally) from sender to recipient and from time of transmission to time of receipt
- Technical Non-Repudiation: A party cannot deny having engaged in the transaction or having sent the electronic message

A PKI such as e-MARC makes use of X.509 digital certificates installed on the client end to perform the services listed above. Each server has a public key and a private key (i.e. SSL) AND each client has a public key and a private key. This allows data to be encrypted in both directions ensuring confidentiality while receiving or sending data. The presence of a unique digital certificate for each client ensures identity of the client. The use of digital signature to electronically "sign" the data ensures integrity. The fact that the digital signature uses the sender's private key (which only the sender possesses) ensures non-repudiation.

The e-MARC implementation, if widely accepted and implemented, can significantly aid in the management of identities across various industry systems. By providing one common identity for users across the industry, users will not have to work with so many varying security implementations.

The implementation of SSL on all OASIS nodes will lay the foundation for e-MARC by ensuring that all nodes are already communicating using SSL and X.509 server

certificates. The next step(s) becomes much more difficult due to the factors involved. The implementation of e-MARC client certificates depends on many factors including:

1. The approval of the e-MARC proposal.
2. The implementation of the root CA.
3. The accreditation of approved e-MARC vendors.
4. The migration of users to e-MARC certificates.
5. The re-design of OASIS security architectures that do not currently support X.509 certificates.

Plan Recommendation

The WEQ-IT should take the necessary steps to ensure the implementation of SSL with X.509 certificates across all OASIS nodes. These steps include, but are not limited to:

1. Ratifying a NAESB Standard recommendation for the WEQ defining the standard security requirements to be implemented in OASIS. This recommendation would establish the~~Establishing a~~ recommended timeline for the implementation of SSL for all sensitive communications with OASIS
2. Modifying the S&CP if necessary
3. Surveying the OASIS nodes concerning status

The recommended timeline is as follows:

June 1, 2004	All nodes must offer clients the ability to communicate sensitive data using http over SSL (https). A node may continue to offer interactions as before for an interim period.
Sept. 1, 2004	All nodes must communicate sensitive data using http over SSL (https) only.
e-MARC	Nodes may interact using e-MARC certificates
Future	Nodes must interact using e-MARC certificates

[PRS: I would hesitate at proposing an OASIS security standard that does not address full mutual authentication of both server-side and client-side certificates. While the above timeline might make some sense, to what degree does anyone feel the industry is in support of server-side encryption only? Since this must be a NAESB standard, I would recommend a full, comprehensive OASIS security standard. If there is support, this could be proposed as an interim OASIS Phase 1A standard, or deferred until OASIS II.]