PKI Implementation Plan for Electronic Tagging

Overview

NERC Electronic Tagging has been on-line since September, 1999. The functional specifications for Electronic Tagging may be downloaded from the NERC website.

The Electronic Tagging - Functional Specification Version 1.7.095 document provides a detailed specification for the communication of tagging information among the various services. Strict guidelines concerning security architecture are enforced, both directly and indirectly, throughout the specification.

NERC, the DoE and NAESB have joined together to create the e-MARC PKI[1]. 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 data communicated between E-Tagging services
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.

All data communicated between Electronic Tagging services should be considered sensitive and must therefore be encrypted.

To achieve data encryption between services, all E-Tag services must implement server-side SSL for http communication. The certificate used must be an X.509 certificate issued by a trusted vendor[2].

- This means that every E-Tag service that receives E-Tag messages must require that every E-Tag message be sent on an SSL-encrypted socket connection, and must use an X.509 server certificate issued by a trusted vendor[2] to establish that connection.

[1] Energy Market Access and Reliability Certificates Public Key Infrastructure

[2] Definitions and registration procedures for trusted pre-"e-MARC" SSL certificate vendors must be developed.

- No E-Tag service can, at this time, require a client certificate from the sender of an E-Tag message. As the E-MARC implementation plan advances, client certificates will be required, but at this time they can not be required.
- All E-Tag messages must be sent using port 443, the standard SSL HTTP socket port, instead of port 80, which is the standard non-encrypted HTTP socket port.

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 Electronic Tagging service implementation does not use a web server that supports SSL, the costs will be greater.

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 and 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 clients across the industry, clients will not have to work with so many varying security implementations.

The implementation of SSL on all Electronic Tagging services will lay the foundation for e-MARC by ensuring that all services are already communicating using SSL and X.509 server certificates. The next steps become 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 clients to e-MARC certificates
5. The re-design of systems to implement a new client security architecture
6. Registration of server and client certificates so that E-Tag services can verify the identity of the other services with which they are communicating

Plan Recommendation

The steps needed to ensure the implementation of SSL with X.509 certificates on all Electronic Tagging services include, but are not limited to:

1. Applicable modifications to the functional specification and approval of those modifications
2. Establishing a recommended timeline for the implementation of SSL for all service communications within Electronic Tagging
3. Monitoring the status of SSL implementation

Note that this recommendation does not apply to the GUI's or user interfaces offered by vendors. However, vendors are strongly encouraged to implement SSL on user interfaces that utilize public networks if they have not done so already.

The recommended timeline is as follows:

June 1, 2004	All services governed by the functional specification may offer clients the ability to communicate sensitive data using http over SSL (https). A service must continue to offer interactions as before until the specification can be modified. However, all clients will be strongly encouraged to interact with these services using SSL. Every E-Tag service offering SSL service will be required to accept connections on both ports 80 and 443. Connections on port 80 will be unencrypted, as today. Connections on port 443 will be encrypted using SSL and server-side certificates.
Fall, 2004	All services must support client communications using http over SSL (https); unencrypted client connections to E-Tag services will no longer be supported. All modifications to the E-Tag Functional Specification required to support the client-side use of SSL and X.509 certificates for encryption of all communications between tag services must be approved. A phased implementation plan will be developed for the integration of client-side X.509 certificates and mutual authentication for all communications governed by the E-Tag Functional Specification.
Future	All services must communicate using e-MARC server and client certificates.