RESPONSE TO NAESB REQUEST FOR INDUSTRY COMMENTS

From: Dominion Resources Services, Inc
Greg Dodson (greg_dodson@dom.com)
120 Tredegar Street
Richmond, VA. 23219
Date: April 28, 2004

Dominion Resources Services, Inc. would like to propose some minor changes to references relevant to Public Keys within the Internet ET standards.

We believe that Email should be acceptable for the exchange of **Public** keys. In two separate areas of the document there are two recommended methods (courier mail and postal mail) for key exchange, but the document does not distinguish between Public and Private Keys.

The following is from the proposed standard,

"[10].3.17 Encryption keys should be self-certified. The exchange of keys should be done in a secure manner such as via postal mail. Key policies, including key exchange policies should be communicated to trading partners."

AND

"Each company must generate its Public Key and Private Key pair. The RSA key generation algorithm should be chosen for versions of PGP which offer alternatives. Implementers of OpenPGP should choose DSA and El Gamal when creating their key pair. The Public Keys should be distributed using a secure method (e.g., courier mail) to the company's trading partners.."

The nature of PUBLIC keys lend themselves to a method of key exchange which is not intended to be secure. The EDI group would recommend EMAIL and suggest the following changes to the proposed standard,

We propose the following changes to the respective sections of the document:

[10].3.17 Encryption keys should be self-certified. The exchange of Public keys should be completed electronically such as via email. The exchange of Private keys, if applicable, should be done in a secure manner such as via postal or courier mail. Key policies, including key exchange policies should be communicated to trading partners.

AND

Each company must generate its Public Key and Private Key pair. The RSA key generation algorithm should be chosen for versions of PGP that offer alternatives. Implementers of OpenPGP should choose DSA and El Gamal when creating their key pair. The Public Key should be distributed electronically to the company's trading partners. Private keys are not typically exchanged with trading partners. In the event that a Private key needs to be exchanged, the exchange should occur in a secure manner such as postal or courier mail.