

**NAESB PKI Standards for OASIS. AP Item 4 (a).**

**Comments provided by the NYISO**

**Elliot Gordon**

**October 08, 2012**

**002-5.1.1 Secured Access to OASIS Information**

Public access to OASIS information using the HTTP protocol shall be limited to only that information contained on the Transmission Provider’s OASIS Home Page that is deemed required to be made publically available, e.g., registration procedures, tariffs, etc. Access to all other OASIS information provided by the OASIS template interfaces or the associated browser-based interactive user interface as specified in Business Practice Standards WEQ-002-4 and WEQ-002-101 shall be secured using HTTPS with SSL/TLS.

All secured data exchange between a registered user (client) and OASIS Node (server) shall be established through mutual authentication using the SSL/TLS protocol and x.509 v3 Certificates issued in accordance with the NAESB Business Practice Standard WEQ-012.

The minimum assurance level that must be expressed and verified in the client and server Certificates used for SSL/TLS secured connections with OASIS shall be Basic assurance; use of certificates expressing a higher level assurance as specified in Business Practice Standard WEQ-012 shall be accepted as meeting the Basic assurance level.

In addition to the Relying Party Obligations specified in Business Practice Standard WEQ-012-1.4.4, OASIS Nodes shall be responsible for verifying:

* The client Certificate used to establish the secured connection to OASIS meets or exceeds the minimum assurance level specified in this Business Practice Standard, and

**Identity proofing assurance levels specified in NAESB Accreditation Requirements for Certification Authorities pertain to the ACAs overall confidence in the end user’s identity: (Appropriate Certificate Uses 1.3.1). In essence, assurance levels provide a method to increase confidence in the identity verification process. Increased threats to the identity proofing process call for higher levels of assurance; which then result in increased protection from fraudulent registrations.**

**“Real time” assurance level checks by a relying party at the OASIS Application level do little to increase or enhance the ACA’s (or the relying parties’) ability to determine the identity of the end-user. In actuality it reduces the security of the system by providing a false sense of validation. Once an identity is checked, regardless of assurance level, and a certificate is issued, rechecking the certificate’s assurance level at the time of application access provides no additional value with regard to validating identities on the other end of the transaction.**

**If differing assurance levels are mandated and necessary then perhaps a better use of resources would be stronger authentication checks commensurate to the identity proofing assurance levels. Stronger authentication protocols and methods would provide greater value in assuring the identity of the end user, process or machine in contrast to checking assurance levels on a certificate every time the certificate is presented.**

**However, given the importance of the security of the Electric Industry another solution to consider would be eliminating all but one assurance level in the identity proofing process. The highest level, which currently demands individuals present themselves in-person seems a very unlikely and impractical scenario. On the other side, Rudimentary does not appear as a commensurate check given critical infrastructure protection standards put into place within the past five years. A single assurance level check requiring verification of an individual’s identity by a trusted third party would go a long way to both strengthening and simplifying the assurance level checking process. A single level removes the need to check levels at the time of application access and removes the burden of selecting assurance levels for different applications; the recent discussions for Oasis and e-Tagging illustrate this dilemma.**

**10/11/12 - Currently the standard requires a minimum of Basic or higher. The check is required to assure that the certificate presented meets the requirements of the Transmission Provider.**

* The client Certificate is associated with a valid registered user account on the OASIS Node.

OASIS clients (users) should verify:

* The server Certificate used to establish the secured connection to OASIS meets or exceeds the minimum assurance level specified in this Business Practice Standard, and
* **Please provide technical implementation details on how clients could perform these checks.**

**10/11/12 – It is not the responsibility of the subcommittee or the Business Practice Standards to specify implementation of the product. Need to contact your OASIS tech support for implementation.**