OATI
Innovative Solutions for the Deregulated Energy Industry
webCARES
Security Officer
Newsletter
web Certificate Administration, Renewal, & Enrollment System
Volume 1, Issue 4
Summer 2003

NERC's PKI Steering Committee (PKISC) has made tremendous progress towards a unified digital certificate policy for the entire energy industry.

NOTICE: Please forward this article to all IT and Security staff who may be affected by NERC's PKI initiative.

As stated in previous newsletters, the "Energy Market Access & Reliability Certificates" policy or "e-MARC" lays out strict criteria for who can issue digital certificates, what the digital certificates can be used for, and exactly how each digital certificate will be issued, renewed, and revoked. According to the latest e-MARC draft, the items most affecting Security Officers are:

* There will be a minimum of two types of certificates, one for encryption and one for digital signing. You will be allowed to backup the encryption certificates, but not the digital signing certificates.

Continued on page 2

A Cyber Security Technical Forum will be presented at the OATI Customer Meeting in Orlando, FL on October 15th – 17th

NOTICE: Please forward this article to all IT and Security staff who may be interested in attending the Cyber Security Technical Forum.

DON'T MISS THIS!! The purpose of the forum is to update Security Officers and IT staff on fulfilling the technical aspects of upcoming FERC and NERC Cyber Security initiatives.

* The first part of the forum will cover how you, as a Security Officer or IT person, will be affected by the upcoming FERC and NERC Cyber Security initiatives.

* The second part of the forum will use detailed demonstrations to show exactly how you can implement the most important initiatives including securing shared workstations and encrypting and/or digitally signing sensitive documents and data (i.e. e-mail, audit logs, event logs, etc.).

* For a complete agenda please email webCARES@oati.net. ❖

Inside This Issue

Continued from page 1

* Role certificates, (i.e. a certificate shared by more than one user) which are used in typical control room or marketing areas, will need to be created and stored on a smart card or equivalent hardware device.

* The NERC PKISC is asking for public comment on the latest draft of the e-MARC Certificate Policy which can be found at https://www.nerc.net/comments/.

* The above items are covered in detail at OATI's Cyber Security Technical Forum (see page 1). ❖

Details for requesting a Server certificate from webCARES^{SM} for interacting with the MISO Market Initiative web site.

You can save your company time and money with a Server certificate from webCARES^{SM} which can be used to interact with the MISO Market Initiative web site.

Here are the steps:

1. Email webCARES@oati.net stating your intention to create a Server/Application certificate. OATI will email you back all the necessary verification information including the exact information to place in the CN=, O=, OU=, L=, and S=, of your actual certificate request file.
2. Use your web or application server to generate the certificate request file, using the information received in step 1, and email the certificate request file to webCARES@oati.net.
3. Within 48 hours you will receive your Server/Application certificate which can be immediately installed into your web or application server.
4. The Server certificate can be managed within webCARES^{SM} just like any of your other certificates.
5. webCARES^{SM} Server/Application certificates are used to connect to MISO's Market Initiative web site and also have been used to secure E-mail servers, Instant Messaging Gateways, VPN servers/devices, Corporate Extranets, and sensitive web sites within HR and Accounting. ❖

MISO Market Initiative Trials requires companies with non-alphanumeric characters in their name to reissue their testing certificates.

If your company has non-alphanumeric characters (including ampersands, hyphens, underscores, periods, etc.) in the organization name within your certificates, and you plan on using them for the MISO Market Initiative trials, you will be required to reissue the certificates.

Although non-alphanumeric characters are valid X509 characters, the issue was too deeply integrated to be fixed before the MMI trials start. Thus MISO is asking that any certificates used for testing on their MMI site contain ONLY alphanumeric characters in the company name.

Here are the steps to reissue certificates.

1. Email webCARES@oati.net asking to remove the non-alphanumeric characters from your company name and listing which certificates will be used FOR TESTING on the MISO Market Initiative web site.
2. OATI will perform the name change and will allow a reissue of the corresponding testing certificates.
3. From within the webCARES(SM) Certificate Management area, click on the affected certificate and click "reissue". Follow the prompts to create and download the new certificate.
4. Install the new certificate into the end users computer and delete the old one.
5. Since the company name will have changed, you will need to re-register the certificate for use on the ETS (Tagging) site and on any OASIS node it will be used to access. To re-register ETS (Tagging) certificates please send an email to support@oati.net and include the name of the certificate's which need to be re-registered. ❖

DON'T FORGET TO …

Register

GROSVENOR Resort IN THE WALT DISNEY WORLD® RESORT

OATI Customer Meeting, October 15-17, Grosvenor Resort, Lake Buena Vista, Florida

http://www.oatiinc.com/workshop/documents/Customer2003Registration1.pdf

Fix & FAQ's for certificates configured with an expired "OATI Issuing Authority" certificate in their path.

Below are steps to fix this issue and some frequently asked questions which deal with OATI's Issuing Authority certificate.

Certificates which show an expired "OATI Issuing Authority" certificate in their certification path were exported with the "Include all certificates in the certification path if possible" option NOT checked. Thus, when they were installed they chained to the old "OATI Issuing Authority" certificate (which was valid for two years and expired 9/13/03).

* To fix this, re-export the end users certificate from the Security Officer's browser and check the box "Include all certificates in the certification path if possible". Also check "Yes" to export the private key. Then install the new certificate.

OR,

* Download the current "OATI Issuing Authority" certificate from http://www.oaticerts.com/repository/ia1(2).crt.

* Install it by right clicking on it and choosing "Install Certificate". Then click "Next" to accept all the defaults and click "Finish".

Why does the OATI Issuing Authority Certificate show as expired?

When certificates were created or renewed over the past year they were installed WITHOUT a copy of the latest "OATI Issuing Authority" certificate (i.e. the box "Include all certificates in the certification path if possible" was not checked during the export/import process). Since Microsoft will create a certificate chain based on name only, when the new or renewed certificates were installed Microsoft could not find the exact issuer of the certificate (i.e. the latest OATI Issuing Authority certificate) so it linked them to the OLD OATI Issuing Authority certificate. This certificate was valid for two years and expired on 9/13/03.

In general, if all certificates would have been installed with the OATI recommended "Include all certificates in the certification path if possible" option, or if Microsoft automatically built certificate chains by certificate key identifiers, we would not have any issue with an expired OATI Issuing Authority Certificate.

How was it fixed?

If a web site is protected by an OATI server certificate, (i.e. all OATI applications) then Microsoft's certificate validation engine will use the server's valid OATI Issuing Authority certificate, instead of any expired certificate, and both server and client certificates should chain correctly.

If a web site is NOT protected by an OATI server certificate, then each client experiencing this issue will need to install the valid OATI Issuing Authority certificate. The easiest way to do this is to follow the fix suggested in the first part of this article.

If installing the new OATI Issuing Authority certificate does not fix the issue, what then?

Reboot the computer. Internet Explorer will cache certificate chains and keep them in memory even when the browser is closed. Rebooting the computer forces Internet Explorer to build a new chain and the current OATI Issuing Authority certificate will be discovered. ❖

Links to the form used to change Security Officers and previous webCARES℠ Security Officer Newsletters.

Here are URL's to the form needed to change Security Officers and to all previous Security Officer Newsletters:

Change Security Officers:
www.oaticerts.com/repository/webCARES-AppForm-BusRep.pdf

Previous Security Officer Newsletters:

Summer 2002:
www.oaticerts.com/repository/SONewsletterv1i1.pdf
Winter 2002:
www.oaticerts.com/repository/SONewsletterv1i2.pdf
Summer 2003:
www.oaticerts.com/repository/SONewsletterv1i3.pdf
❖