Innovative Solutions for the Deregulated Energy Industry

webCARES

Security Officer

Newsletter

Volume 1, Issue 2 Winter 2002

FAQ's For the Certificate Renewal Process

Can you believe it? For many companies it is already digital certificate renewal time. Over the past few months I have guided many Security Officers (SO's) through the renewal process and below are answers to their most frequently asked questions.

As always, OATI and the webCARES™ (web Certificate Administration, Renewal, and Enrolment Service) team strive to provide the absolute best level of support. If you have additional questions on certificate renewals please let us know at webCARES@oati.net.

Q. Why do I have to renew certificates each year? Can't renewal be done every 2 or 3 years?

A. The policies and procedures implemented by OATI, including certificate validity periods of one year, are based on NERC's *Energy Market Access and Reliability Certificates* (e-MARC) Policy. This policy has been under review since last summer and is expected to be adopted sometime in 2003. We at OATI empathize with the increased burden yearly certificate renewals place on SO's and therefore have designed the webCARES™ renewal process to be extremely simple and straightforward. In addition, our conformance to e-MARC standards, such as renewing certificates and private keys every year, ensures a higher level of security for the entire industry.

Q. What is the easiest way to renew my certificates?

Continued on page 2

INSIDE THIS ISSUE

NERC Sanctioned Certificate Authorities and Certificates?

In previous e-mails and newsletters OATI has attempted to keep you abreast on NERC's march towards a standard Public Key Infrastructure (PKI) which would ensure safe, secure certificates across all of NERC's applications. This is the latest information.

Note: Much of the information below was obtained from presentations and minutes found on the official NERC PKI site: http://www.nerc.com/~filez/pkisc.html

The NERC PKI initiative started with the e-MARC (Energy Market Access and Reliability Certificates) Certificate Policy draft document and will hopefully end by achieving the goal of creating "a trusted environment in which energy industry participants can conduct business". The OASIS Standards Collaborative (OSC) created the e-MARC Certificate Policy with the intent that it would form the basis for an open, standard, secure mechanism to communicate with OASIS nodes, and also be used to secure electronic tagging communications. The OSC hoped that once established the e-MARC Policy would be adopted to form the basis for secured data communication across the entire energy industry.

The OSC sought the input and expertise of the NERC Critical Infrastructure Protection Advisory Group (CIPAG) in April, 2001 to 1) review, extend, and adopt the e-MARC Certificate Policy, and 2) to establish a process by which Certificate Authorities (such as OATI webCARES™) would be "certified" as compliant with the e-MARC Policy. In June 2002 the NERC Board of Trustees approved a PKI project based on e-MARC. The CIPAG selected an outside consultant, MITRE Corporation (www.mitre.org), and formed a PKI Steering Committee (PKISC) to define, design, develop, and roll out a comprehensive PKI infrastructure to secure access to NERC cyber-assets (e.g., IDC, SDX, etc.) and for use by the industry as a whole.

Of the major decisions the PKISC will face, those which may be very important to you, are:

- What Certificate Authorities will be used and how will they be chosen? The final choice may, or may not include the Certificate Authority you are currently using.
- Will one certificate be used to encrypt and sign data (i.e. your current webCARES™ certificates) or will each user be required to have two separate certificates (one for encryption

Continued on page 4

Continued from page 1

A. If the certificate *Subject* will not change (i.e. the certificate owner's information like name, e-mail, organization, location, state, etc.), simply sign onto webCARES™, from the *Management* section click on the *Common Name* of the certificate and click the *Renew* button. You then click the *Confirm to create certificate* button and click the link to *Install the certificate.* This installs a new certificate in your browser (the old certificate remains) which you then export and install onto the certificate owner's computer (following the exact same export/import procedures used for the original certificate). To avoid confusion during the import process, and during certificate use, be sure to delete the old certificate from the end user's browser.

Q. Do I have to re-register the renewed certificates with OATI's ETS (Tagging) or webOASIS systems?

A. No. Recognizing the fact that the certificate renewal process is labor intensive, and that certificate serial numbers change for each new certificate, OATI designed ETS and it's webOASIS system to save you work by using the certificate's subject field. Therefore, as long as the certificate's *Subject* remains the same you do NOT have to re-register a renewed certificate on OATI's ETS (tagging) or webOASIS web sites. If the subject information DOES change, you WILL have to re-register the user's certificate.

Q. Do I have to re-register the renewed certificates with non-OATI OASIS nodes?

A. Yes. Most OASIS nodes choose to register your username with your certificate serial number (referred to as a JTSIN OASIS ID number). Since serial numbers change during the renewal process you will have to re-register the new serial number with each OASIS node. However, once you have renewed the appropriate certificates you can click *View JTSIN OASIS ID Number* within the *Management* section of webCARES™ and easily create a table which can be e-mailed to each OASIS node. Please consult each node administrator for the exact registration process. If you only plan to query information you do not need to re-register as "anonymous" access is granted "view" privileges by most nodes.

Q. How do I renew a certificate where the certificate name has changed or the owner has been replaced?

A. You must create a new certificate with the new name and either let the existing certificate expire or revoke it. If you do not have available certificates then the old certificate must be revoked before the new one can be created. Remember, revoking a certificate will prevent the certificate owner from using that certificate. Because the certificate name has changed, the renewed certificate will have to be re-registered on all OASIS and OATI systems. For assistance with re-registering your renewed certificates on OATI systems please send an email to support@oati.net.

Q. How do I renew a certificate where only the certificate e-mail address has changed?

OATI calls this "reissuing" instead of "renewing". You can either revoke the certificate and reissue it, or e-mail webCARES@oati.net and request an "Allow Reissue" (which prevents you from having to revoke the certificate). The *Reissue* button is located on the certificate *Details* page just below the *Revocation Details* section. The "reissued" certificate must be installed into the end user's browser and re-registered on all OATI and OASIS systems. For assistance with re-registering your renewed certificates please send an email to support@oati.net.

Q. Can I renew *expired* certificates?

A. Yes. On the certificate *Details* page click the *Reissue* button. This is possible because a new key pair is generated.

Q. Is it true that ALL renewed certificates have to be re-registered with OATI's webSweep?

A. Yes. If the certificate owner needs to create reservations then you must perform OASIS certificate registration with the renewed certificate within webSweep. From the webSweep *Options* page click *OASIS Certificate Registration,* click the appropriate OASIS node button, and follow the directions. The *Certificate Password* is the password created during exporting the certificate to a .pfx file.

Q. I have a lot of certificates to reinstall on a lot of different computers. Is there any way to automate the certificate installation process?

A. OATI recommends installing each certificate yourself. This ensures they are installed correctly, the private keys are not compromised, and the certificate owner's questions are answered. However, to be realistic, we provide the following list of "options" we have used to help other companies automate the install process.

1) Use *Microsoft Roaming Profiles.* This allows you to install a certificate once and have it be available to that user from any machine they log onto. Follow the appropriate article below to set up *Roaming Profiles.* Then logon as the user and install their certificates. When you log off, the certificate information will be copied to a logon server and be available to the user from any machine they log into. For additional information see:

Windows 2000:
http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q302082&
Windows .NET:
http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q324749&

There are a couple of caveats. 1.) Certificates become part of the *Windows* User Profile they are installed into and thus only available for use when the machine is logged on with the associated *Windows* user id. Using a *Windows* user id "shared" between multiple users (i.e. an AM and PM shift) simplifies the process as all certificates can be installed into the "shared" *Windows* user ids. 2.) *Roaming Profiles* can become quite large, consume network bandwidth and drive space, and may slow down the logon process. 3.) Do not use *Mandatory Profiles* as private key material is prevented from being encrypted and distributed correctly.

2.) *Use Login Scripts.* A login script is set up per user and runs every time a user logs in. A simple version would prompt the user to answer the *Certificate Import* Wizard questions to install their certificate. This would require very

careful communication of each certificate's installation password. A more advanced script would automate the complete install process using a scripting tool like KiXtart™ which ships with the Windows NT4/2000 Resource Kit (http://www.kixtart.org/). Remember, logon scripts must be stored in a Domain Controller folder with the share name of *Netlogon*, or in subfolders of the *Netlogon* folder. This folder should exist by default but if not you must create it.

For more information on the above options, or for sample scripts, e-mail webCARES@oati.net. ❖

One Click Security Upgrade

You have experienced the ease at which you can create, renew, and revoke digital certificates using OATI's webCARES™ web site. You have also become familiar with the somewhat more challenging task of installing the certificates.

Now it is possible for you, or your IT department, to upgrade the security of sensitive in-house web sites with as little as one click! Microsoft's web server features a *Require Client Certificates* option which can be used to increase security on highly sensitive web sites (see Figure 2). Sensitive sites typically include extranets, intranets, web based e-mail, and industry wide sites like FRCC's FTMS or WECC's EHV site.

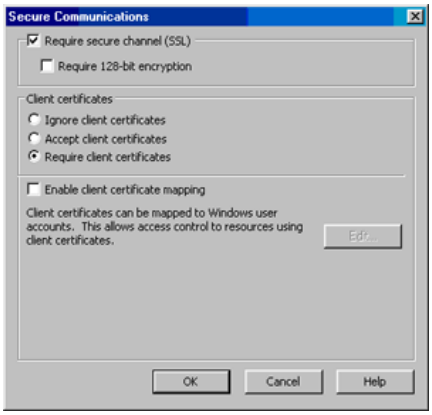

Figure 2

Web sites using the *Require Client Certificates* option prompt users to select a valid client certificate before they are allowed access into the site. This prevents unauthorized access by individuals who have unlawfully obtained access to a user's work area, computer, or Internet connection and "discovered" a valid username and password or secret IP address/URL.

This type of increased security is called "dual factor authentication" because it requires users to have "something they know" (i.e. their username and password) and "something they possess" (i.e. their digital certificate).

The *Require client certificates* radio button can be set at any level within a web site by starting the *IIS Management Console,* choosing the *Properties* of any web site, directory, or file, selecting the *Directory|File Security* tab and clicking *Edit* within the *Secure Communications* section.

A web server certificate (which can also be created on webCARES™) must be installed before the *Edit* button will be accessible. As you can see from Figure 2, client certificates can be mapped to *Windows* user accounts. This makes it incredibly easy to determine which resources a user can, or cannot, access.

For information on this "One Click Security Upgrade" or more advanced security upgrades like mapping certificates to usernames, or single sign-on, please contact webCARES™ Support at webCARES@oati.net. ❖

NEW webCARES™ Version 2.0: A Single Source for Your Digital Certificates

Have you or your IT department ever needed to increase security on a web site? How about hiding sensitive e-mail from co-workers or competitors? Or maybe encrypting files on your laptop or digitally signing source code?

webCARES™ 2.0 will allow you to produce digital certificates for all these needs and more! Version 2 of webCARES™ was released on Dec. 9th and has some exciting changes. Most importantly, you are no longer confined to creating only client authentication (i.e. SSL) certificates. Through the same simple interface, the certificates created can now be used throughout your enterprise for securing access to web sites, encrypting e-mail and files, and digitally signing e-mail, documents and source code. Just as before, enter the certificate name, e-mail address, and organizational unit and click *Submit Request*. It's that easy. Behind the scenes we have added the appropriate *key usages* to allow your certificates to work seamlessly with any in-house application. The management of these certificates remains as simple as always so backups, installations, renewals, and revocations are a breeze.

We also make the JTSIN OASIS node certificate renewal/re-registration process easier by allowing you to conveniently view your certificate's *JTSIN OASIS ID Numbers* from within the webCARES™ *Management* section. Once you have renewed your certificates, you can copy and paste your certificate information (including the *JTSIN OASIS ID Numbers*) into a spreadsheet or use the *Certificate Report* button to send your information to each OASIS node administrator.

webCARES™ 2.0 can also be used to create web server certificates for sensitive in-house or industry web sites. A webCARES™ representative will assist you in generating a web server certificate request. Once the request is submitted to OATI a server certificate is returned which can be installed onto your in-house web servers. These server certificates allow your sensitive web sites, directories, or files, to be protected in the exact same way as the popular B2B or B2C web sites. Many other changes are included so watch for the upcoming press release and remember…

If you need to protect a sensitive web site, hide e-mails and files, digitally sign e-mail, documents and source code, or get rid of all those usernames and passwords…why install and pay for certificates twice? Use webCARES™!! ❖

Continued from page 1

and one for digital signatures)? As you can probably guess, one certificate per user is easier to manage but two certificates are more secure (i.e. a malicious user would need to steal one certificate to decrypt your data and a different certificate to impersonate you.).

- How long will your certificates be valid for? The current generally accepted validity period is one year but we all know how frustrating it is to deal with certificate renewals and re-registration every year.

In addition to the activities by CIPAG and the PKISC, the North American Energy Standards Board (NAESB) Wholesale Electric Quadrant (WEQ) has identified in their approved 2003 Annual Plan an action item to "Review activities of NERC CIPAG in light of NERC-NAESB MOU regarding cyber security requirements and their business practice and system communication standards implications." NAESB has been named in prior FERC rulings as being the single standards setting body for the electric industry. To date, many of the activities undertaken by the CIPAG have not been well communicated nor open for comment by the industry at large. We sincerely hope that the NAESB WEQ's interest and involvement in the CIPAG and PKISC will illuminate the issues confronting our industry and its users.

OATI strongly supports the spirit and necessity of e-MARC and filed comments to that effect with the FERC in response to the SMD NOPR. However, to be successful any such initiative must consider the overall impacts to each of our companies and users and not be an overly burdensome or costly endeavor. The PKISC is just starting their work, and OATI hopes to be a part of the process and solution to bring a unified security model to the energy industry. We would encourage you, as an OATI Security Officer, to offer your thoughts, comments and experiences (of managing and operating in the front line PKI trenches) to the members of the PKISC (see ftp://www.nerc.com/pub/sys/all_updl/cip/pkisc/Roster.pdf).

I know they would be glad to hear from you! ❖

Security Cube Notes & News

- Tri-State G&T Association, Inc (TSGT) has joined the OATI webOASIS node as the newest transmission provider.
- webCARES™ can be purchased as a delivered in-house Certificate Authority replacing the need for other more expensive or complicated systems. Please contact webCARES@oati.net for additional information.
- The NEW Security Officer User's Manual can be downloaded from a link on the webCARES™ main page. The new manual has been updated and now includes information on certificate renewal procedures, troubleshooting certificate issues, and using certificates with in-house applications, web sites, and e-mail.
- ***webCARES Certificate and PKI Consulting Service*** is now available. Whether you are implementing a PKI, rolling out additional certificates, upgrading security on a web site, or eliminating your plethora of usernames and passwords with a single sign-on solution, the webCARES consulting team has the answers. If you, or your IT department, are interested please contact webCARES@oati.net for a free consultation.
- Digitally sign your source code using Microsoft's *SignCode.exe.* OATI signs its web browser applets to allow them to run in the correct internet security zone and would gladly share our experience with you.
- Use your webCARES certificates (i.e. Digital ID's) to secure your e-mails from the rest of the world and to prove that they actually came from you. Please contact webCARES@oati.net or visit the following links for more information: **Note**: Ignore the references to *Get a Digital ID for sending secure messages* as you already have your webCARES Digital ID's (i.e. certificates).
  - **Outlook 98**: http://support.microsoft.com/default.aspx?scid=KB;en-us;182356
  - **Outlook 2000**: http://support.microsoft.com/default.aspx?scid=kb;en-us;195477
  - **Outlook 2002 (XP)**: http://support.microsoft.com/default.aspx?scid=kb;en-us;286159
- Microsoft has released an updated *Certificate Enrollment Control* (xenroll.dll) which prevents unauthorized deletion of certificates. The updated control generates two new *Potential Scripting Violation* messages which alert the user to what is happening in the background. webCARES uses the new control and thus you will see these two new messages during the certificate request and creation process. Please choose "Yes" when prompted. For more information visit http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-048.asp

Additional Info & Feedback… 763-201-2000 or webCARES@oati.net