



Innovative Solutions for the
Deregulated Energy Industry

webCARES

Security Officer

Newsletter

web Certificate Administration, Renewal, & Enrollment System

Volume 1, Issue 3

Summer 2003

MISO Secures Midwest Market Initiative with Single Sign-On Digital Certificate Solution

In a move seen by many as an example of what the future holds for security and electronic access in the energy industry, the Midwest Independent System Operator (MISO) has elected to use digital certificates as the sole authentication mechanism for accessing its Midwest Market Initiative (MMI) system.

In essence this frees the users from remembering, and their support staff from supporting, usernames and passwords.

The single sign on concept is simple and straightforward as it relies on a trusted third party Certificate Authority (CA) to validate an individual's real-world identity and issue a digital certificate linked or "bound" to that identity. The CA's reputation is built on this "binding" process and thus the individual's certificate can safely be substituted for any other forms of authentication (i.e. username and password).

Continued on page 2

Granting Your Applications Access to Digital Certificates via Winhttpcertcfg.exe

NOTICE: Please forward this article to all IT staff and application developers as it could save hours in programming and troubleshooting certificate issues.

If your company is like OATI, digital certificates are slowly infiltrating deeper and deeper into your daily operations. Many common operations like accessing a web page and sending e-mail now implement the increased security of digital certificates. The underlying Public Key Infrastructure (PKI) technology has been available for years but wide spread use of digital certificates only came about after browser and e-mail user interfaces were upgraded to make it easy and intuitive for a user to use their digital certificates.

The same has to happen to your internal applications. Intranets, extranets, web services, document signing, and single sign-on solutions will eventually all need to easily, elegantly, and unobtrusively use digital certificates.

A tool from Microsoft™ makes this job much easier; Winhttpcertcfg.exe.

Winhttpcertcfg.exe is used to give Windows user accounts permission to an existing or newly imported certificate. Typically, certificates used by multiple users or applications are kept in the *Local Machine* certificate store and by default only administrators or the user who installed the certificate have access to this store. Since services and web applications run under their unique *Windows* user accounts they would not have access to these certificates.

For example, a web site may query information from a third party web server that requires client certificates. The results returned from the query are based on which user

Continued on page 4

INSIDE THIS ISSUE	
1	MISO Secures Midwest Market Initiative with Single Sign-On Digital Certificate Solution
1	Granting Your Applications Access to Digital Certificates via Winhttpcertcfg.exe
2	Entergy & MISO MMI Accept OATI Digital Certificates
3	WebCARES™ FAQ's
4	Security Cube Notes and News

Accept OATI Digital Certificates

Reasonable due diligence is required before trusting any CA. Therefore, before accepting OATI's webCARES as a trusted CA, MISO staff interviewed OATI's staff, reviewed OATI's processes, examined OATI's secure Data Center, and were confident OATI's CA could not be compromised (i.e. triple access to server rooms, simultaneous dual access to CA server cages and dual access to the CA's private keys, etc).

Once trust is established in any CA, web servers can be set up to accept certificates issued from that trusted CA and reject all non-trusted certificates. The challenging step can be getting certificates from the trusted CA to the end users. However, this was not an issue as many of the MMI users already had OATI webCARES™ certificates for tagging and OASIS access.

But here is where single sign-on systems and its users really begin to reap benefits. When users access the MMI system all they will need is their certificate. No usernames, no passwords, and nothing to remember! If a user has only one valid certificate in the browser the single sign-on system will allow access without even prompting to choose a certificate. It can't get any easier. Imagine how nice it will be for the IT department and support staff not to have to deal with username "confirmations" or password "resets"!

The user's certificate is checked by the MMI web server (i.e. to ensure it is not expired, revoked, or tampered with) and then to the MMI role-based access management system. Although a detailed description of the MMI access management system is outside the scope of this article, the user's Local Security Officer can easily set the user to have different rights for different sections of the MMI portal based on the roles linked to the certificate. The user may have the ability to submit bids for the Day Ahead market, but have read-only privileges for the Real Time market.

If a user leaves a company or their private key is compromised (i.e. lost or stolen), the certificate is simply revoked and thus cannot be used to access the MMI system. No usernames to delete or disable, no complicated re-registration procedure, and no lengthy username/password distribution process. The Local Security Officer just links a different certificate to existing roles and the new user is off and running.

At any company where both customer service and security are paramount, it is easy to see why single sign-on solutions may be the road map to the future for security and electronic access in the energy industry. ❖

The Entergy OASIS node and MISO's Midwest Market Initiative have added OATI webCARES™ to their trusted list of Certificate Authorities and access to their systems can now be done using OATI digital certificates.

In a customer friendly move designed to save certificate costs for its customers, allow easy integration and use of existing certificates across all major NERC applications, and eliminate end user confusion, Entergy and MISO are now allowing access to their systems using OATI digital certificates. This comes as a relief to customers who up until now had to pay for certificates issued from alternate certificate providers but can now rely solely on their OATI certificates.

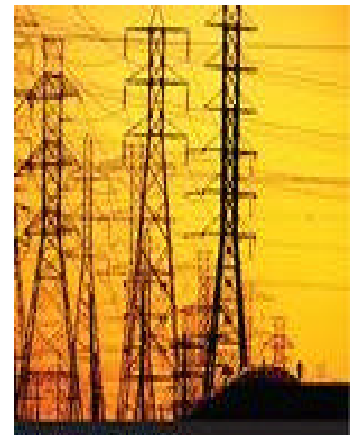
Patrick Tronnier, webCARES™ Principal Security Architect, thinks the decision may also be based on the philosophy of choosing "industry specific" CA's like OATI webCARES™ instead of the large "baked-in" CA's. "From the beginning we have made substantial investments in time and energy to make sure our personnel and processes reflect the unique needs of energy market participants and our physical and cyber security are the best in the energy industry. General market CA's just can't get this specialized. Nor can they provide the quick response times to support requests."

Any company using non-OATI certificates to access the Entergy OASIS node or MISO's MMI system can contact webCARES@oati.net to get procedures on how to use the same webCARES™ certificate for ETS (Tagging) and all OASIS nodes, including Entergy.

Here is an updated list of OASIS nodes that accept OATI digital certificates.

OASIS Node

AEP
Entergy
MAIN
MAPP
MISO
NEPOOL
New Brunswick
Northwest
OATI webOASIS
Rocky Mountain
SWPP
VCAR ❖



webCARES™ FAQ's

Below are some frequently asked questions of the webCARES™ staff over the past few months.

Q. How do I change Security Officer's for my company? How can I reflect a company name change on our existing digital certificates? How do I change e-mail addresses on existing certificates? How do I change contact information for our existing Security Officers?

A. Completely fill out, sign, and return to OATI the *Business Representative Application Form* located at: <http://www.oaticerts.com/repository/webCARES-AppForm-BusRep.pdf>. You can email or fax the form but OATI must receive the signed original before any changes can be completed. Once OATI receives the form and has verified the changes, all company SO's will be notified via email. The normal turnaround is 4-5 business days from when OATI receives the original form.

Q. Why does OATI recommend we choose a SO from the IT or Security Department?

A. Digital certificates will become central to all company IT and Security functions and thus it makes sense to use the same certificates throughout the organization and to coordinate the enrollment, issuance, revocation, renewal, and archive of digital certificates with a knowledgeable expert in the IT or security department.

Q. My SO certificate has expired and I can't get into webCARES™. What should I do?

A. If your SO certificate has expired you must call the OATI Helpdesk support staff to have them re-verify you. Once this is done you must delete your old SO certificate from all browsers (if appropriate) and sign-on to webCARES™ to get your new SO certificate. When you initially sign-on to webCARES™ your username and password will remain the same however you must hit *Cancel* to the initial *Client Authentication* window to allow webCARES™ to issue you a new certificate.

Q. My SO certificate has been lost, deleted, or corrupted and I can't get into webCARES™. What should I do?

A. You must call the OATI Helpdesk support staff to have them re-verify you and follow the steps in the previous answer to sign-on to webCARES™ and download your new Security Officer certificate. Once you have your new certificate, follow company procedures to insure it is backed up to a secure location.

Q. Can I revoke or let expire un-needed certificates to increase or make room for additional certificates?

A. Yes. Revoked or expired certificates will add to your total certificates available. Remember to delete the revoked or expired certificates from the end users browser.

Q. I can't log into webCARES™.

A. Here are some things to remember:

- webCARES™ (www.oaticerts.com) has a completely different web address than ETS/Tagging (www.oati.net).

- Your webCARES™ username and possibly your password is different than your ETS/Tagging username and password.

- The SO certificate you use to access webCARES™ may or may not be the same certificate you would use to access ETS/Tagging.

- Usernames and passwords in all OATI systems are case sensitive.

- Passwords used to gain access to webCARES™ are not necessarily the same as the passwords used when exporting/importing the webCARES™ certificates.

Q. If I purchase additional ETS/Tagging ID's do they come with certificates?

A. Yes. Additional ETS/Tagging ID's are purchased in minimum quantities of 5 and include one digital certificate for each ETS/Tagging ID. Please contact the OATI Helpdesk for additional information, including pricing.

Q. How do I purchase additional webCARES™ certificates?

A. Send an email to webCARES@oati.net to request the *Amendment to the OATI ETS Agreement* (Tagging customers) or the *Amendment to the webCARES Agreement* (all other customers).

Q. I have created the end user's certificate but he/she is unable to log into any of the OATI applications.

A. Once you create the end user certificate you must request to have it linked to either an existing OATI user account or a new one. To create this linking send an email to the OATI Helpdesk support staff @ support@oati.net and tell them the Common Name of the new certificate and the OATI user account to link it to. If the new certificate is to be linked to a new OATI user account then the email should also contain the requested user name, password, and e-mail address. With this information the new certificate can be successfully linked and the end user can use his/her certificate, user account, and password to get into the OATI applications. ❖

runs the query and thus the web server must have permission to use the appropriate user's certificate each time it runs a query (i.e. a client side SSL session is set up with the end users certificate).

Below is an example showing how to import a certificate and give the web server *IWAM* account the appropriate permissions it will need to run a query based on the *Patrick Henry* certificate. Here is a description of each parameter.

```
C:\winhttpcertcfg -i patrickhenry.pfx -p xyz {line wrapped}
-c LOCAL_MACHINE\MY {line wrapped}
-a IWAM_PATRICK3@TRONNIER.ORG
```

Imported certificate:
CN=Patrick Henry
OU=OATI
O=Open Access Technology International Inc
L=Minneapolis
S=MN
C=US
E=patrick.tronnier@oatiinc.com

Granting private key access for account:
TRONNIER\IWAM_PATRICK3

-i patrickhenry.pfx -p xyz (This is the end user certificate file to be imported and its password)

-c LOCAL_MACHINE\MY (This is the certificate store the certificate is imported into. Certificates in the *MY* store are available to web server applications regardless of who is logged onto the machine)

-a IWAM_PATRICK3 (Windows account used by the web service which needs access to the certificate)

@TRONNIER.ORG (Windows domain name. To use a local machine user name use MACHINE\Username)

If the certificate has already been imported you can substitute the following command:

```
winhttpcertcfg.exe {line wrapped}
-g -c LOCAL_MACHINE\MY {line wrapped}
-s "Patrick Henry" {line wrapped}
-a IWAM_PATRICK3@TRONNIER.ORG
```

For additional information please contact webCARES@oati.net. ❖

Security Cube Notes & News

- The NERC PKI initiative is moving forward at full steam and the chances are good that all NERC applications will require e-MARC certificates by the end of the year. OATI attended a PKI Vendor Forum, which was held by NERC's PKI Steering Committee on May 19th to educate potential PKI vendors on the direction e-MARC is heading. OATI is strongly recommending the Security Officer Model and multiple Root Certificate Authorities as part of the final e-MARC requirements. We continue to believe the best security for the industry would be to use existing Root Certificate Authorities (instead of creating a single NERC Root CA) and to keep certificates and private keys in the hands of knowledgeable SO's (instead of end users).
- Saskatchewan Power (SPC), CLECO, and Duquesne Energy (DLCO) have joined the OATI webOASIS node as the newest transmission providers.
- FREE SMART CARDS & READERS with each certificate purchased! Receive a free smart card and reader with the purchase of each additional webCARES™ digital certificate as part of our bulk purchase program. Minimum of 50 certificates. Does not apply to replacement of existing certificates or certificates distributed as part of any OATI product. Offer expires July 31, 2003.
- Save your company thousands of dollars! Recommend webCARES™ as a replacement to your expensive, complicated, non e-MARC compliant, existing enterprise PKI/digital certificate solution and receive a free OATI shirt. Recommendation must be a qualified Senior IT staff person responsible for purchasing decisions.
- Please be advised that Microsoft's Cumulative Patch for Internet Information Service (MS03-018), released May 28th, requires the patch from Microsoft Security Bulletin MS02-050 to be installed immediately before, or directly after applying MS03-018. If patch MS03-018 is installed and MS02-050 is not present, IIS will reject client side certificates. To restore acceptance of client side certificates install the MS02-050 patch.
- Did you know how easy it is to accept webCARES certificates on your web servers? Contact webCARES@oati.net for additional details.

Additional info... webCARES@oati.net

