



## “Putting your new X.509 digital certificates to work”

*Securing applications with digital certificates can seem daunting at first, especially with the lack of support for existing products. However, if you break the process into phases, and have each phase handled by an expert in that area, the aspects of securing your applications with digital certificates are easier to comprehend and less daunting.*

### **Patrick Tronnier**

Principal Security Architect,  
Open Access Technology International Inc.

Most of you gave a sigh of relief after rolling out X.509 digital certificates to encrypt and protect your companies' access to the Tagging (ETS) system. Many of you will give an even bigger sigh of relief once your digital certificates have replaced the Trade Agent system for securely accessing OASIS systems. The “sighs of relief” are most likely from implementing a technology you are not 100% familiar with and having it actually work!

Well, let me tell you, there are many more “sighs of relief”s” down the wire as more applications and systems are forced to migrate from an unsecured environment to digital certificates. If you thought Tagging and OASIS were the end of the applications needing certificates-- think again!

*Continued on page 2*

## Which is more secure...You decide?

*It is acceptable that a company Security Officer (SO) or End User (EU) could control and secure certificates and their private keys. Each method is legitimate (based on Internet RFC's) and when done correctly, each is secure. Here we clearly present both methods and let you decide.*

### **Ben Porath**

Project Manager,  
Open Access Technology International Inc.

A digital certificate, like a driver's license, is used to prove the owners identity. However, unlike a driver's license, a digital certificate comes with a private key that is mainly used to prove that no information in the certificate has changed. The verification process is called Digitally Signing, and the result is a Digital Signature, or encrypted thumbprint, of the information contained in the certificate.

As you can guess, if a private key is compromised it would be fairly easy for an imposter to assume the identity of the true certificate owner. Therefore, secure methods of private key transfer, backup, and recovery are paramount to the secure, effective use of digital certificates.

An important concept when dealing with private keys is whether a certificate's private key is *exportable* or *non-exportable*. *Exportable* means the certificate's private key can be copied to a file and thus transferred and installed on any number of computers. This is the type that some Certificate Authorities distribute to each end user. *Non-exportable* signifies the certificate's private key cannot be exported, or removed, and thus cannot be used outside of the browser it was installed into. This is the type OATI webCARES company security officers are encouraged to distribute to their end users.

Which is right for your company?

OATI webCARES was designed to provide local company Security Officers (SO's) with access to certificates and private keys for each end user within their company. Once an SO is dual or triple authenticated/verified they can download

*Continued on page 3*

### **INSIDE THIS ISSUE**

- 1 “Putting your new X.509 digital certificates to work”
- 1 Which is more secure...You Decide?
- 2 Using OATI certificates on OASIS nodes
- 3 Certificate Troubleshooting
- 4 Security Officer Survey results
- 5 Security Cube Notes and News

Migrating applications to certificates can seem daunting at first, especially if there is lack of support for existing products. However, if you break the migration down into phases, and have each phase handled by an expert in that area, the aspects of migration are easier to comprehend and less daunting.

A great example of a successful migration to certificates is the Western Electricity Coordinating Council or WECC (formally WSCC). They were forced to upgrade their EHV (extra high voltage) application to use digital certificates due to the discontinuation of support for Trade Agent.

OATI assisted with this conversion and broke it down into 3 phases: 1) distribution of certificates to end users and end user support, 2) server changes, and 3) application code changes.

Phase 1: The first phase is typically the toughest and most time consuming as it involves distribution and support of end user certificates. However, most WECC/EHV users already had OATI certificates. Therefore, the few that didn't were directed to the OATI webCARES web site ([www.oaticerts.com/repository](http://www.oaticerts.com/repository)) where they registered and were verified, and then able to download their certificates. Bill Comish, WECC Director of Operations and Training, who directed the overall operations of the migration, stated "I greatly appreciated how willing OATI was to step in and help us in the conversion to digital certificates on very short notice. The customer service they provide, as our users make the transition, is outstanding."

Phase 2: Phase two consisted of server changes that entailed requesting and installing a server certificate, installing a root certificate, turning on CRL (Certificate Revocation List) checking, choosing a secure protocol and port to operate over, (the default protocol is SSL/TLS and the default port is 443. Both of these are allowed through most firewalls) and if needed, uninstalling the previous product. In the case of WECC, the application servers were hosted at a remote location and OATI worked with the administrator there to make the changes mentioned above.

Phase 3: The third phase, application code changes, can be further broken down into changing links or tags to point to the secured content, editing and populating the database with certificate related fields and data, implementing a method for caching or storing certificate credentials, and

optionally using SSL to secure connections to remote content or database servers. For example, Karen Holdren, the lead developer at Hardy Software, worked with OATI to make the following changes to the WECC/EHV application. First, all of the hyperlinks, bookmarks and source tags had to be switched to use https instead of http. (For example change SRC=http:// to SRC=https://) Secondly, certificate issuer, subject and credential access type fields (i.e. username/ password /certificate) were added to the database to store certificate and logon type information. Thirdly, when an end user accesses the EHV application, WECC chose to store the certificate credentials in the built in ASP *Client Certificate* object. The EHV database and web site were on the same machine so no changes were made to the ODBC connection object. However, if your content or database is not located on the application server, remember to use certificates and SSL to make your remote connections secure.

From initial conference call to final testing, the migration of the WECC/EHV application to certificates took only 15 days, and is a testament to benefit of dividing the migration into phases and working with experts who will support you every step of the way. ❖

## Using OATI Certificates on OASIS Nodes

In response to the tremendous interest in using OATI certificates on OASIS nodes we would like to update you on the status of each node.

OASIS Node	Accepting OATI Certificates?
AEP	Yes
MAIN	Yes
MAPP	Yes
MISO	Yes
NEPOOL	Yes
New Brunswick	Yes
Northwest	Yes
Rocky Mountain	Yes
SWPP	Yes
VACAR	Yes

The most effective way to persuade an OASIS node Administrator into accepting your certificates is for you to contact them and express your support for using your existing OATI digital certificates. For a list of OASIS Nodes and contacts, please visit the following URL: <http://mapp.oasis.mapp.org/documents/nodeacc.html>. ❖



certificates for each of their End Users (EU's). It becomes the SO's responsibility to securely export, transfer, and archive ALL certificates and private keys. The EU never has access to his or her private key. In support of this method, an SO User's Manual is provided detailing the importance keeping private keys secure and offers suggestions on optimal private key management (i.e. export to a floppy disk and place the disk in a secure location).

An obvious advantage of this method is having a trustworthy and knowledgeable security person in charge of a company's certificates and private keys. The main disadvantage is an SO can masquerade as an EU or distribute private keys to unauthorized individuals. (See "You decide..." sidebar for a more thorough list of advantages and disadvantages)

---

***"The obvious advantage of this method is having a trustworthy and knowledgeable security person in charge of a company's certificates and private keys."***

---

An alternate methodology is to allow each End User to have control of their certificate and private key. This process involves downloading an "exportable" certificate and private key directly into the EU's browser. A company SO isn't initially involved in the process and thus initially the SO does not have access to the EU's private key.

The EU is responsible for the secure use, transfer and backup of their certificate and private key. This includes transferring them onto a computer shared with others or a home computer. It also includes securely backing up the certificate and private key and recovering it in the event of disk failure.

The primary difference in this method is there's no third party access to an EU's certificate and private key. The main disadvantage is no control over the mass proliferation of private keys, which can lead to unauthorized individuals masquerading as a valid EU.

If you have strong beliefs in regards to the securest way to control your company's certificates and private keys, and don't want to be mandated into one method or the other, you may want to consider contacting NERC's PKI/e-MARC "steering committee". They are implementing a PKI project that covers this exact point and currently leans towards End User control of certificates and private keys. I am sure they would welcome input from concerned, knowledgeable industry participants who deal with these types of issues on a daily basis. ❖

## **Certificate Troubleshooting**

*Below is the first part in a continuing series on troubleshooting certificate related issues.*

In general it is best to troubleshoot from what you control outwards. This means start your troubleshooting at the certificate level and work outwards to your computer, LAN,

## **YOU DECIDE...**

This table highlights the differences between each of the private key control methodologies:

### **Security Officer (SO) Method:**

- Knowledgeable "Security" person is in charge
- One safe central location of all private keys at each Company
- Control over the proliferation of "exportable" certificates (this can be very important at certificate renewal time)
- Single entity accountability for certificates and their renewal
- SO installs certificates on machines shared by multiple users
- SO acts as knowledgebase for troubleshooting certificate issues (single source for help)
- SO knowledge can easily be upgraded or passed to others
- Gov. access to encrypted data during emergencies
- SO can decrypt EU's encrypted data (this can be important after an employee leaves the company)

### **End User (EU) Method:**

- Each EU learns to manage and secure private key
- Private keys are not centrally located at each company
- Certificate renewal can often be difficult because certificates may
- Each EU is accountable for certificate and its' renewal
- The default certificate installation is exportable
- Exportable certificates installed on machines shared by multiple users
- Each EU must be trained on safe certificate handling procedures and troubleshooting skills
- Each EU must be updated when new knowledge regarding certificates and private keys becomes available
- EU must approve Gov. access to encrypted data during emergencies
- Only EU can decrypt his/her encrypted data



WAN, the Internet, and eventually the destination web or application servers. With this in mind, here are some ideas for troubleshooting certificate issues.

**1) Turn OFF browser “Friendly Error Messages”.** So-called “friendly” error messages potentially mask more helpful error messages. To do this uncheck the “Show Friendly Error Messages” item towards the bottom of the “Browsing” category on the “Advanced” tab of Internet Explorer’s “Internet Options”.

A common “non-friendly” error message is:

#### 403.7 Forbidden: Client certificate required

This error occurs when the web page you are trying to access requires that your browser have a client certificate that the web server recognizes or “trusts”. There are several possible causes of this problem:

- The root certificate, of the Certificate Authority who issued your client certificate, is not installed on the web server and thus is not part of the Certificate Trust List the web server sends back to the browser.

- The client certificate has expired or its effective time has not been reached yet. Time zones can be a factor here as certificates can be issued and installed before their validity period starts.

- The certificate’s link to its private key is broken.

**2) View the certificate to insure it is still valid, has a private key associated with it, and links, or “chains” back to the Root Certificate Authority who issued it.** Certificates will be listed under the “Personal” certificate store and can be viewed by double clicking on the certificate in question. To open the “Personal” certificate store choose “Tools” > “Internet Options” > “Content” tab > and click the “Certificates” button from within Internet Explorer. Valid certificates should satisfy the following:

- Be within the validity period that is listed on both the “General” and “Details” tab.

- “You have a private key that corresponds to this certificate” will be listed at the bottom of the “General” tab.

- The “Certificate Status”, which is listed at the bottom of the “Certification Path” tab, should display “This certificate is OK” for each certificate listed in the “Certification Path”.

**3) Check to see if the certificate has been revoked.** On the “Details” tab of each certificate should be listed a “CRL Distribution Point” or CDP entry. To download the latest Certificate Revocation List, (CRL) copy this value and paste it into your browser. (Note: The OATI CDP is <http://www.oaticerts.com/repository/ial.crl>) Once downloaded, check to make sure the serial number of your certificate is NOT on the CRL list.

In the next newsletter we will dig deeper into troubleshooting certificate export, import, renewal, and private key issues. Remember; contact OATI at 763-201-2020 for help with ALL certificate related issues! ❖

## Security Officer Survey Results

Thanks to everyone who responded to the “OATI webCARES Appreciation and Feedback” survey emailed on May 15. Below are a few of the interesting observations culled from the results of the survey. If your response contained detailed suggestions or comments, please be assured we are evaluating them and will use your feedback to enhance our products and services.

- 100% of respondents believed it's better for company Security Officers, rather than end users, to have control of company’s certificates and corresponding private keys!
- An overwhelming majority of respondents were pleased and had only positive comments on the first two questions which asked what improvements, if any, would be recommended to the webCARES web site or certificate delivery processes.
- In 90% of the responses a newsletter was thought to be useful while less than half thought “security related classes” would be beneficial at this time.

If you would like to complete the survey, or comment on this newsletter, please email us at [webCARES@oatiinc.com](mailto:webCARES@oatiinc.com). ❖

## Security Cube Notes & News

- For programmatic access to OASIS web sites, or any web site protected with X.509 certificates, check out webFetch.exe. WebFetch is called from existing code and sets up an SSL session that can then be used to return data to either the browser or a file. It can also post data to a secure web site and takes parameters similar to TAAPI.exe.
- OATI has been selected to assist the Florida Regional Coordinating Council with the enhancement of the Florida Transaction Management System (FTMS) by incorporating advanced security mechanisms including X.509 digital client certificates.
- webCARES Certificate Integration Toolkit is now available for those companies who wish to use OATI digital certificates to enhance the security of an in-house or third party application. This toolkit includes FAQ’s, presentations, sample code, etc. and illustrates how easy it is to secure your application with digital certificates. It simplifies the process of migrating away from less secure username/password scenarios to true Client Aor too complicated solutions, and is backed by OATI’s knowledgeable and responsive support staff.

**Additional info ... 763-201-2020**

