## http://www.jsequeira.com/projects/sevis\_batch/howto.html

## Summary

Exchanging data with the SEVIS batch processing servers has not been a very transparent process for universities to-date. The specifications released by EDS have been moving targets, and the documents' emphasis has definitely been on completeness and accuracy over brevity or simplicity. This tutorial takes a different approach, walking you through just what you need to know to begin sending files to the INS using free, cross-platform software. The first part of the tutorial, dealing with digital certificate preparation, will be of interest to IT departments who are planning on implementing vendor-provided SEVIS software. The second part of the tutorial, concerning the actual transfer process, will be more of interest to institutions that plan on implementing the batch method on their own.

## Introduction

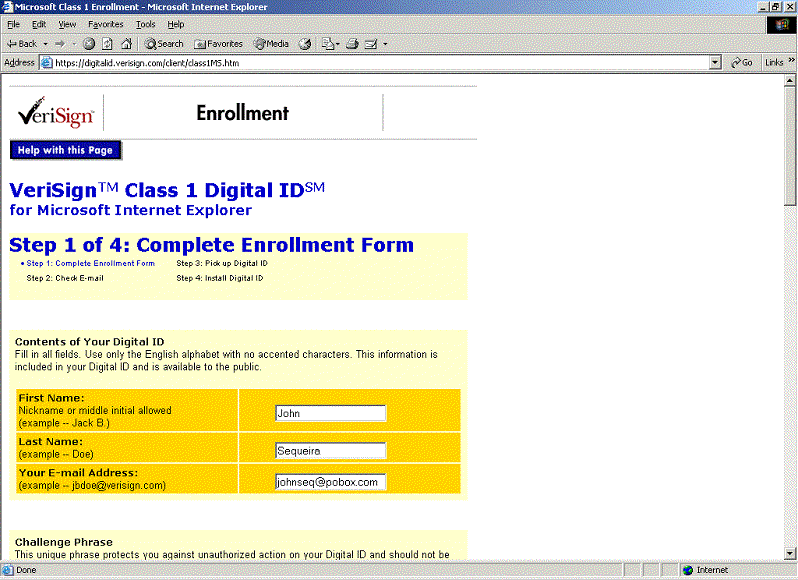
Digital Certificates. XML. PKI. PDF. SEVIS batch implementation involves a short list of technologies that may be new to your campus, but there's a decent amount of complexity in each. This document is going to assume you know what all of the pieces of the puzzle are, and just help in putting them together. Part I will cover obtaining the digital certificate you'll need to authenticate the document transfer, and Part II will cover actually sending the file and receiving a response from the INS using free HTTP communications software cURL and free encryption software openssl.

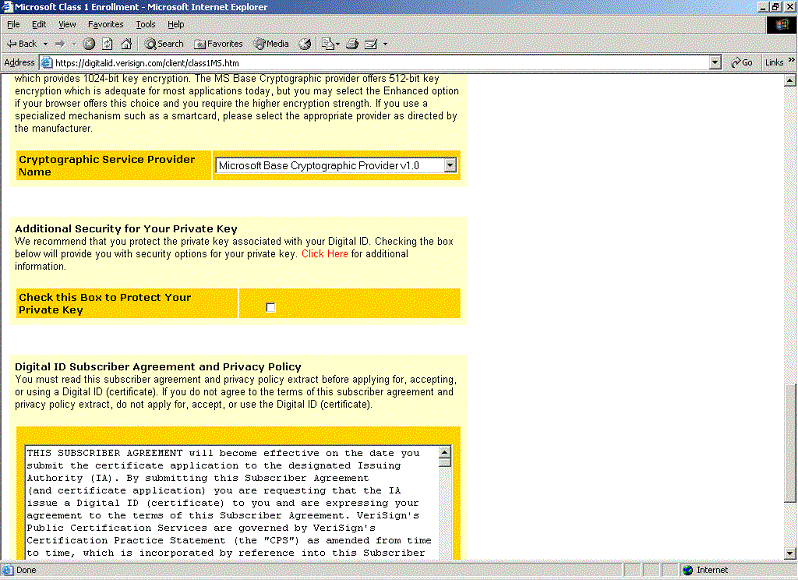
## Part I: You'll need to be Certified

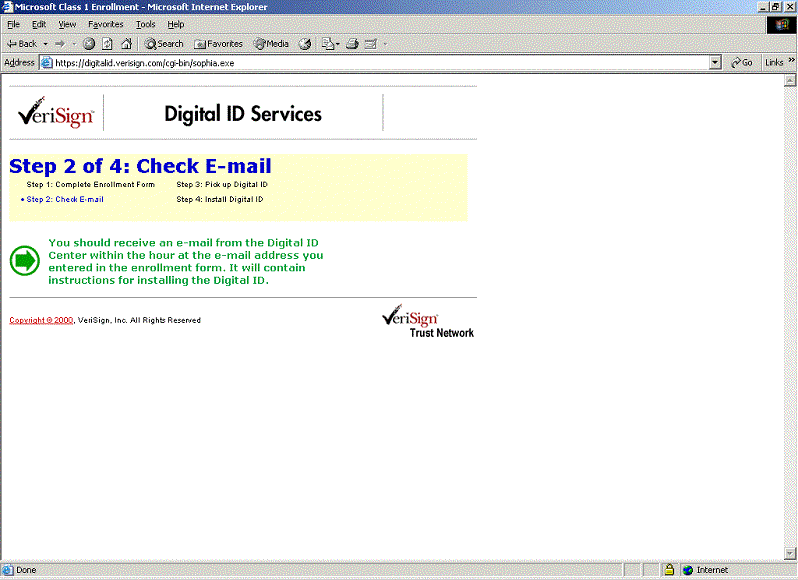
There's been a lot of confusion on the SEVIS Readiness mailing list as to what type of certificate you'll need to communicate with SEVIS. Server certificates are relatively expensive at close to $700/year and client certificates go for a paltry $14.95/yr. The good news is, you can get the client certificate. The bad news is, ... actually there is no bad news. It's pretty simple.

* Click this link: <http://www.verisign.com/products/class1/index.html>
* Follow the signup process.

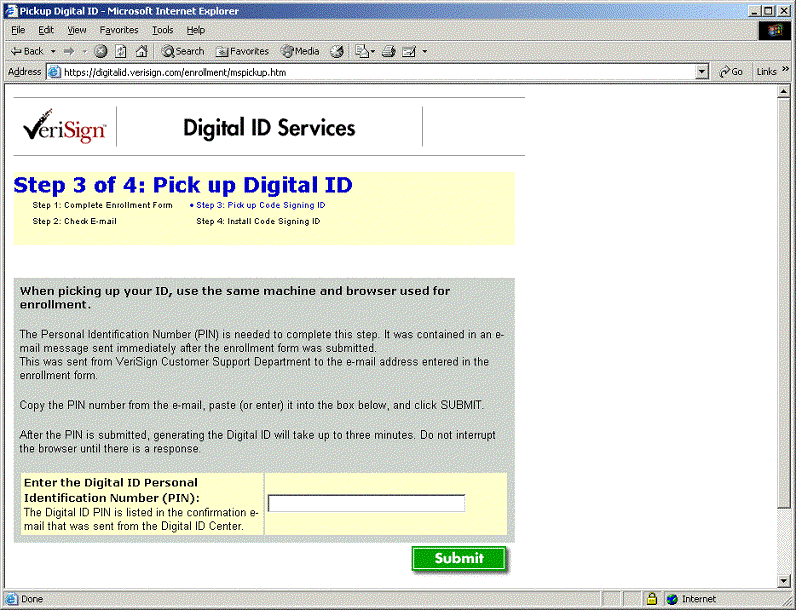
Like any other online purchase, Verisign will ask for your contact information and credit card information, then send you a confirmation email to make sure you are who you say you are.



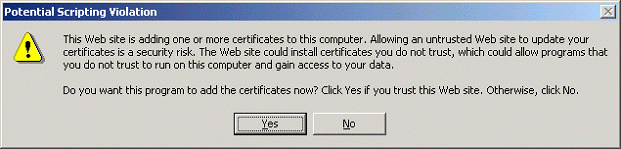




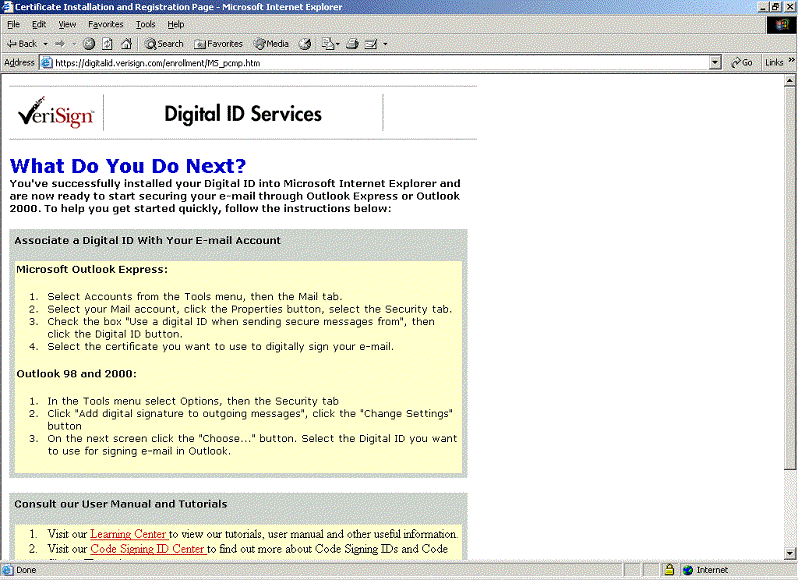
After you receive the confirmation email, you return to the Verisign web site and enter in a PIN code included in the email.



At this point you're ready to install the certificate. If you're using Internet Explorer, it will 'grab' the certificate from the Verisign web site and install it in it's internal certificate list. Before doing so, you'll see the warning below.



Click okay and you've got a certificate.

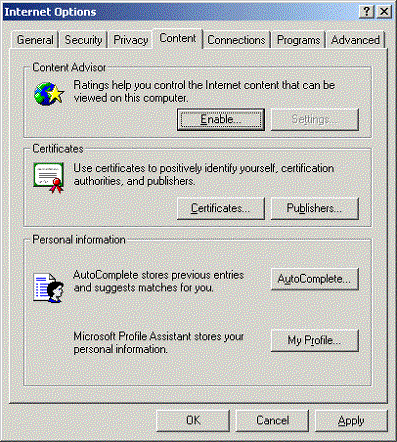


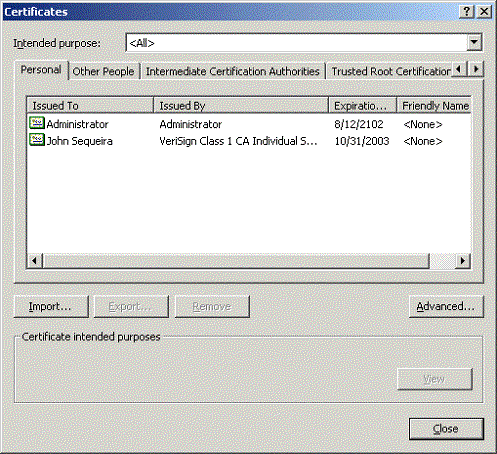
## What do you mean my ID's no good?

Congratulations - you've got the certificate. With it, you can encrypt and digitally sign files uploaded by your browser or sent by your email program. The recipient of the file will be able to verify that you are who you say you are and know that Verisign vouches for you.

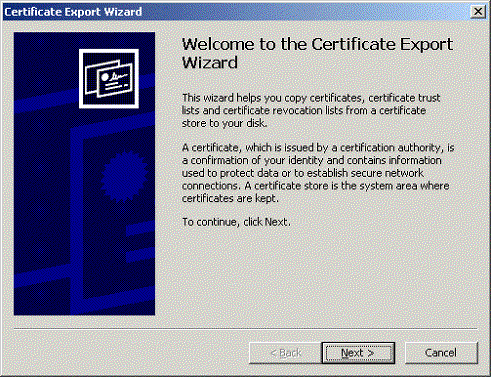
While I'm sure that sounds terribly thrilling, it's not something we care about right now. Instead, we want to programmatically communicate with the INS SEVIS batch server without going through a browser or an email client. To do that, we'll have to export the certificate stored in Internet Explorer's browser certificate vault, and convert it to the format understandable by our upload program.

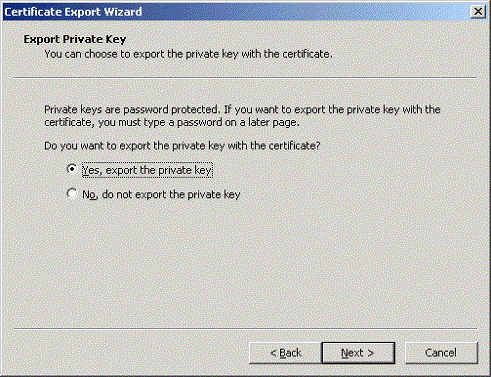
In Internet Explorer, select the menu option *Tools->Internet Options->Content->Certificates*, highlight your new Verisign certificate and click *Export*.



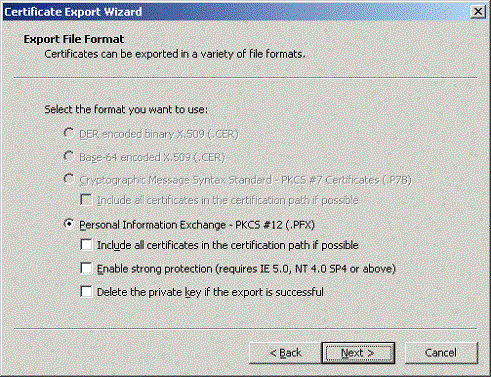


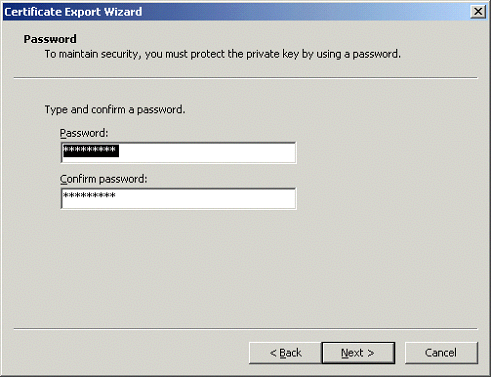
Proceed through the export wizard, as shown in the screenshots below.

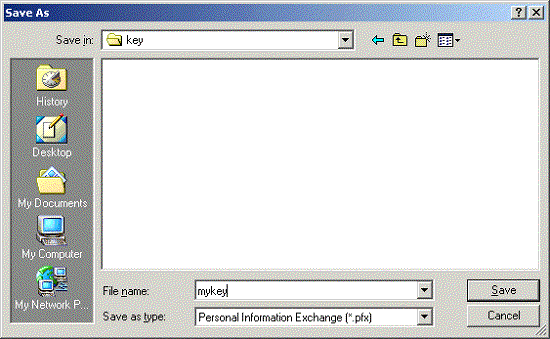


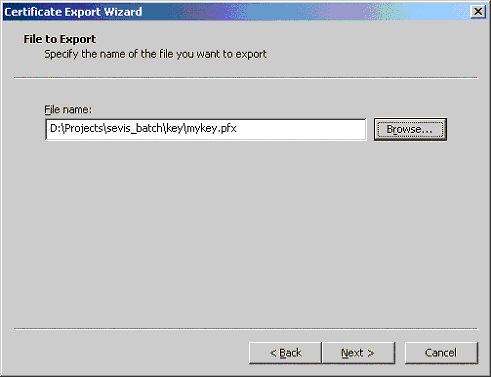


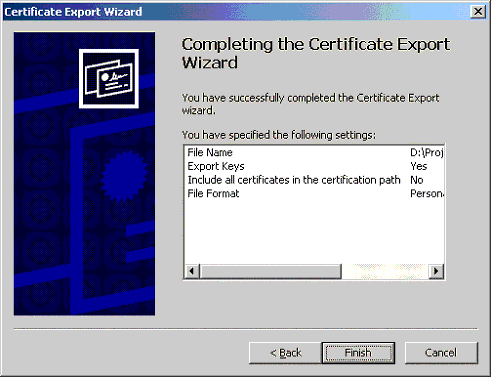
Make sure you export it in the "Personal Information Exchange" .pfx format, and don't forget your password.









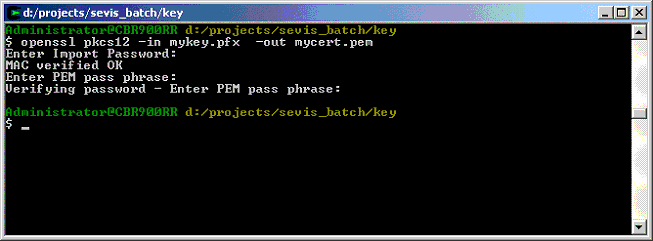


We'll be encrypting the files we send to SEVIS with a free software called openssl, and it needs a certificate in the .pem format. The next step therefore is to install and use our trusty free encryption utility *openssl* to convert our certificate into the right format. There are many ways to get openssl, depending on whether you're using Windows or Unix. We'll assume you've got it installed and working, but check out [Appendix A](http://www.jsequeira.com/projects/sevis_batch/3.html#Appendix%20A) if you need some advice.

Okay, now that you have openssl installed, the command you want to execute is :

openssl pkcs12 -in mykey.pfx -out mycert.pem

For the Import password, use the password you chose when exporting the file from IE. You'll also need to add a pass phrase to the PEM file. I just used the same phrase for convenience.



## Yes, you do need HELP

Next we need to gain access to the SEVIS system, so that we can tell them about the new certificate we'll be using to sign our batch files. Call the SEVIS Help Desk at 1-800-892-4829, hit the "Batch Issues" phone tree option, and ask the friendly HELP Desk personel for access to the system.

I was emailed out my username, password and school code within an hour or two, and I was pretty impressed with the responsiveness. There was a problem that I discovered later in this rapid reply, but for now let's assume everything worked as planned and you've got access.

* Go to the URL for SEVIS testing:

<https://egov2.ins.usdoj.gov/sevis>

* Click on the link for your school (e.g. Test School 106 F) under "Name of School" heading.
* Locate the "Register for Batch Processing" link in the upper right hand corner.
* Accept the terms

## Part II: Talking to SEVIS

Talking to SEVIS involved several steps:

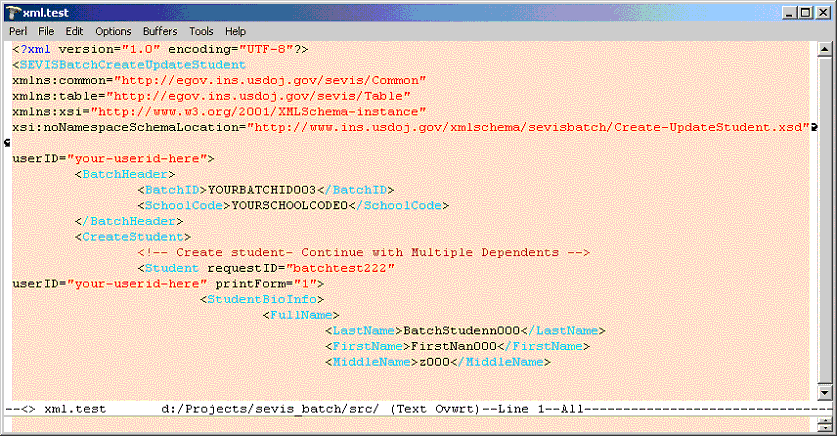
* sending batches of XML to the INS server,
* waiting awhile (currently ~ 1 hr, but will be 1 day in production)
* then downloading a gzipped archive of the processed batch. The archive will include an XML log and possibly PDF files if you've requested them.

SEVIS accepts certificate-encrypted HTTPS uploads of XML files and downloads of gzipped files. While there are definitely straightforward ways to achieve this functionality using .NET, Java, and/or Perl, the least complicated method is definitely with a mature, cross-platform and free command line utility like cURL.

By selecting cURL, we've reduced the problem to selecting the right command line switches.

I'm going to assume that you either have a sample XML file, or you've taken the one I've provided in references at the end of the article. If you're using my XML file, you'll need to make sure that all userid="" attributes, and that the batchid and schoolcode are accurate. For good measure, you should change the name and identifying characteristics of the student (SSN, license, name, remarks), because SEVIS is beginning to implement de-duping functionality and your batch might get kicked out if it looks too much like my sample.

Here's what the top part of the XML file looks like before modification:



Yours should look something like mine. Now, we invoke curl and pass in our pem file, give the pass-phrase we defined early, and then pass in the form variables:

* schoolcode
* batchid
* xml (actually the batch file's XML)

It looks like this:

d:\Projects\sevis\_batch\src>curl -E mycert.pem:"secretphrase" -F schoolcode=SEA214F00076000 -F batchid=00000000000003 -F xml=@20021104.xml https://egov2.ins.usdoj.gov/sevisbatchtest/action/batchUpload

% Total % Received % Xferd Average Speed Time Curr.

Dload Upload Total Current Left Speed

100 5066 100 142 100 4924 33 1148 0:00:04 0:00:04 0:00:00 0

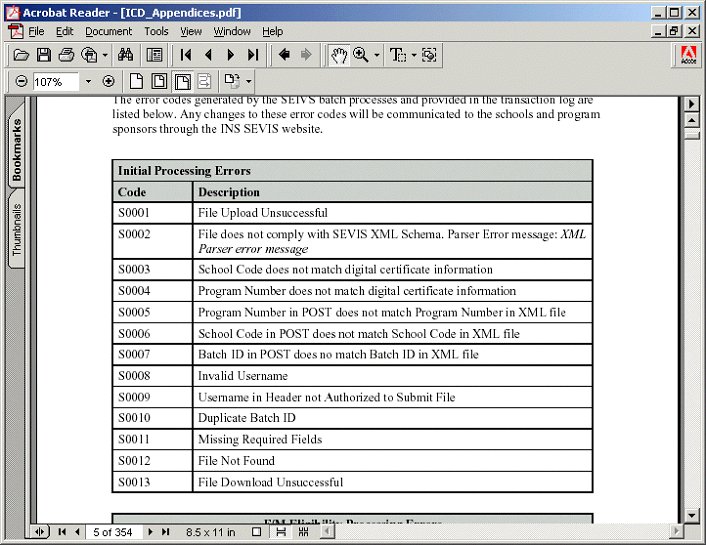
<?xml version="1.0" encoding="UTF-8"?>

<UPLOAD\_RESULT batchID="00000000000003" dateTimeStamp="2002-11-04T18:35:13.687-05:00" accepted="true"/>

bash-2.05b$

The accepted="true" attribute is the key to knowing you have succeeded in sending the file.

I don't want to lead you to believe that the first time through this I was successful. Actually, I kept getting errors messages kicked back, and don't be surprised if you have the same issue. In my case, each of the error messages I received was clearly documented in the ICD Appendix B, as shown below.



After working through the error messages (typos in the schoolCode, not having the curl batchid match my XML file etc.) I still couldn't get it to work. It turns out I was given the wrong username to the SEVIS system, or rather there was a typo in the one I was given. A quick call to the SEVIS help desk cleared that up, and I was able to post successfully.

Now that SEVIS has your data, what are you supposed to do? Take a break. Really - it takes about an hour for batch files to be processed on the test servers, and until then you can't really do much. On the production servers, INS has indicated a turnaround of more like 1 day.

When the batch file is ready to download, invoke curl by passing in

* schoolcode
* batchid
* destination for results

bash-2.05b$ ./sevis\_get20021104.bat

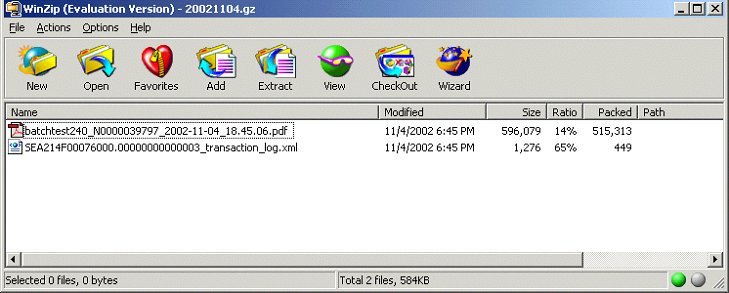
d:\Projects\sevis\_batch\src>curl -E mycert.pem:"secretphase" -o results/20021104.gz -F schoolcode=SEA214F00076000 -F batchid=00000000000003 https://egov2.ins.usdoj.gov/sevisbatchtest/action/batchDownload

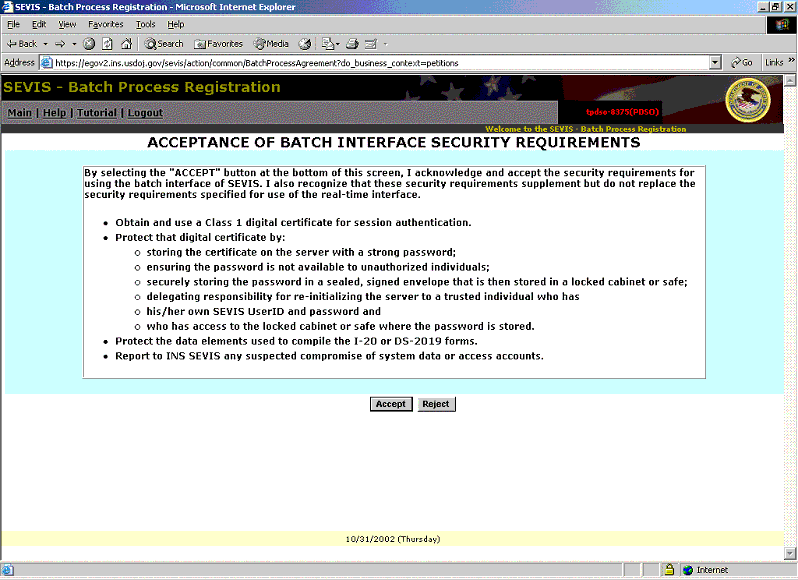
% Total % Received % Xferd Average Speed Time Curr.

Dload Upload Total Current Left Speed

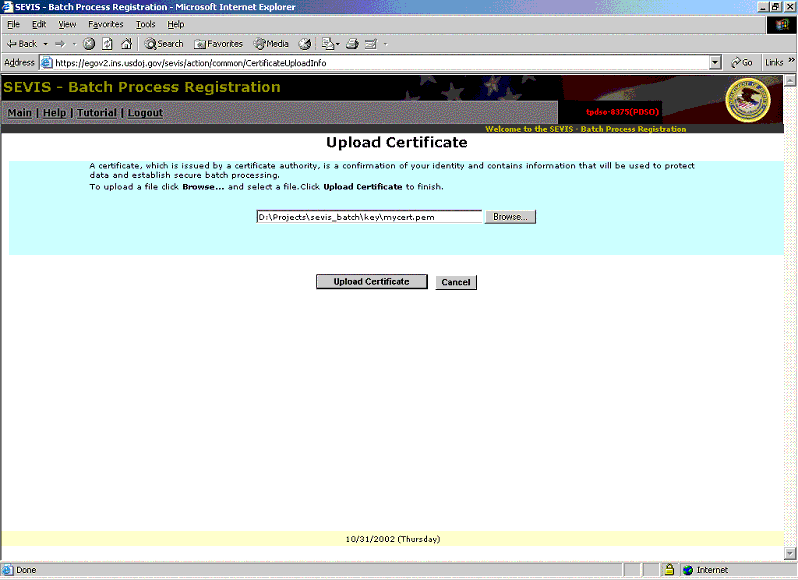
100 504k 0 504k 100 243 52482 24 0:00:09 0:00:09 0:00:00 84461

When we open up the file that came back to us, we see that we received a PDF file and an XML log of the transfer. Success!





Then upload your newly created .pem certificate



You should see the the confirmation screen.

That's it - you're all set to send files to the INS. On to Part II!

## Appendix A: Installing Free Software for Windows

If you're running the example code above on the Unix platform, both the cURL and the OpenSSL website have source code or binary distributions that are easily installed. If you're on the Windows platform, your best bet is to download the Cygwin set of tools at <http://www.cygwin.com>. If you click on the "Setup" link, you'll download a program that will allow you to clikc on the command-line utilities you'd like to install. It's a pretty painless, Installshield-like procedure.

## Conclusion

We've covered one example of sending data to SEVIS, and hopefully that's enough to bootstrap your campus' efforts. While it might not necessarily go this smoothly for you, I don't performing the batch transfer process to be much more difficult than tweaking an XML attribute or two, and a few calls to the HELP desk. Once you've got batch under your belt, there's plenty more to learn. If you look at the whole SEVIS solution you'll see that the batch file management, data warehousing/consolidatioon, workflow and change management issues will be far more challenging than sending and receiving an XML file to INS over the internet. Even so, my hope is that by digesting this tutorial you'll have more time to spend on the bigger issues.

## Resources

* [Source Code and utilities for this tutorial](http://www.jsequeira.com/projects/sevis_batch/download.zip)
* [Versign Client Certificate](http://www.verisign.com/products/class1/index.html)
* [Newfront Software's SEVIS Readiness Mailing List](mailto:sevislist-subscribe@newfrontsoftware.com)
* [Cygwin](http://www.cygwin.com/) - With Cygwin, you can get both curl and openssl, along with many other handy Unix tools
* [curl](http://curl.haxx.se/) - cURL web site
* [OpenSSL Website](http://www.openssl.org)
* [openssl Certificates How-To](http://www.openssl.org/docs/HOWTO/certificates.txt)

TroubleShooting  
  
**Error: Windows does not have enough information to verify this certificate**

How to install the Class 1 Digital ID Intermediate CA Certificate for Internet Explorer (VeriSign Class 1 individual Subscriber CA - G2)?

Resolution

1.  Download the Class 1 Intermediate CA Certificate [here](https://knowledge.verisign.com/resources/sites/VERISIGN/content/live/SOLUTION/6000/SO6052/en_US/Class1_Intermediate_CA.cer)  
     **Note:** Firefox users may need to right click and select **Save Link As**  
2.  Double click on the certificate file  
3.  Under the General tab, click **Install Certificate**  
4.  A Certificate Import wizard will appear > click **Next**  
5.  Select **Place all certificate in the following store**  
6.  Click **Browse**  
7.  Select **Intermediate Certification Authorities**  
8.  Click **OK** > **Next**  
9.  Click **Finish**

To verify that the intermediate certificate is installed correctly, please follow these instructions:  
  
1.  Open Internet Explorer  
2.  From the menu bar, click **Tools** > **Internet Options** > **Content** > **Certificates**  
3.  Under **Personal** tab, select **Issued to: <The\_name\_of\_your\_certificate>**  
4.  Click **View**  
5.  Select **Certification Path** tab

You will see the following Path:

**VeriSign Class 1 Public Primary CA  
VeriSign Class 1 individual Subscriber CA - G2  
<The\_name\_of\_your\_certificate>**