

Revision 1, June 21, 2007: Clarification around version of Internet Explorer has been added as outlined in communication <http://www.ieso.ca/imoweb/news/newsItem.asp?newsItemID=3527>

Revision 2, September 6, 2007: Update to reflect current schedule, testing of Internet Explorer version 7 and comments received from Stakeholders

I. Introduction

The IESO certificate authority, [Cybertrust](#) is changing their current digital certificates from [Entrust](#) version 6 to Entrust version 7. This change is resulting in a need to replace all current users' certificates that access the market participant interface (MPI) with new ones. There is no requirement for new certificates, for market participants who only access the transmission rights auction market. Version 7 certificates are already in place.

The current version 6 certificates will continue to be supported by Cybertrust during the migration period.

The migration schedule will include the testing and verification period for the new version 7 certificates. Once participants have completed their user acceptance testing during this period, the actual conversion will proceed.

Key Issues

1. All active versions 6 certificates will be replaced over the following months. The IESO will develop a migration schedule and will work individually with participants to ensure business continuity. The IESO will work with a pre-assigned contact of the participant for the certificate replacement process.
2. As each individual conversion is completed, the operation of the version 6 certificate will be removed. The IESO will request confirmation from participants that version 7 certificate is working without any known issues prior to removing operation of version 6.
3. Version 7 certificates require Internet Explorer (IE) browser version 6 and beyond. This applies to higher versions of IE 6 (for example, IE 6.0 SP1 & SP2) **as well as IE 7.0**. Users of version 7 certificates will not be able to access the MPI using earlier version of Internet Explorer or Netscape navigator.
4. Version 7 certificates can be configured to be used in both the production and the sandbox (testing) environments. The previous practice of participants obtaining separate test certificates for use in

the sandbox is not required. Participants can however request certificates for use exclusively on the sandbox system if required.

5. Users of accounts that have not been activated in the last 6 months will be notified of such and prompted to confirm the retention of these accounts. If no confirmation is received the IESO will disable and revoke the account.

Background

The IESO uses digital certificates to ensure that the information you exchange with us over the internet is secure. You must use a digital certificate when you use the Market Participant Interface (MPI) or your company's own software to:

- Submit bids, offers, schedules or forecasts.
- Submit physical bilateral contract data.
- Retrieve metering data.
- Review your company information in our Registration system.
- To access the Transmission Rights Auction through the IESO web portal.

The IESO operates on a 'third party trust' basis. Third party trust refers to two parties being able to trust each other even if they don't know each other, because they both have a relationship with a mutual, trusted third party. The third party acts to ensure the trustworthiness of the other parties. In the case of digital certificates, a 'certification authority' is this trusted third party and in the IESO case this is Cybertrust.

The certification authority certifies the authenticity of the users, and assures us that information coming from a market participant is coming from a valid source. At the same time, our use of server certificates from a certification authority assures you that your data is going to the right place, i.e., that you are logged on to a secure server operated by the IESO.

For more information on digital certificates please refer to the Step by Step [Guide to Digital Certificates](#)

II. Stakeholders

All [current market participants](#) need digital certificate to transact in the IESO markets, to download settlement statements and invoices, and to access metering data. This impacts approximately 2000 individual users within the IESO authorised market participants.

III. Stakeholder Engagement Goals and Objectives

Goal

The goal of this plan is to present a schedule that would be acceptable to participants in replacing their certificates and meet the November , 2007 migration period deadline.

Objectives

1. To provide participants the opportunity to provide feedback to the IESO on time frames for re-issuing the digital certificates that will have the least impact on their business.
2. To verify with participants that the impacts of using Internet Explorer browser version 6 and beyond are manageable within the time periods allocated and that the elimination of Netscape navigator does not create any issues.

IV. Stakeholder Engagement Approach and Methods

The implementation of this stakeholder engagement plan will be in accordance with the IESO's approved [stakeholder engagement principles](#). The stakeholder plan will be subject to review and update as the process evolves and stakeholder comments are incorporated, and as revisions are warranted.

The stakeholder engagement approach will be feedback — with request for stakeholder review and written feedback.

The stakeholder engagement method to be employed will be a [web-based posting](#) with a request for written comments via e-mail. An e-mail communication will be sent to those authorised market participants who are in possession of a digital certificate to advise them of this stakeholder plan and the opportunity for feedback on the plan and schedule.

Web-based postings provide all interested stakeholders with an efficient low-cost method to be informed of the proposed changes with the opportunity to communicate their views via e-mail to the IESO (stakeholder.engagement@ieso.ca). All stakeholder input, including dissenting views, will be posted on the IESO website.

All feedback from stakeholders will be considered prior to implementation of the final schedule for roll out on the replacement certificates. This stakeholder plan provides all stakeholders with the opportunity to communicate their views and positions directly to the IESO in advance of any implementation.

Feedback will be provided on all stakeholder comments and how this input was considered, and the results of the consultation will be posted on the IESO website. All public manuals and technical documents would be updated to reflect any changes. Changes to these documents will follow the usual change control practices.

Updating on the implementation phase will be done via the [Information Technology Standing Committee \(ITSC\)](#)

V. Decision Making Steps and Schedule of Activities

Stakeholder Engagement Schedule	
Activity	Target Date
1. Posting of draft stakeholder plan and e mail communication to solicit feedback on the plan.	June 7, 2007
2. Deadline for stakeholder feedback on the plan.	June 27, 2007
3. Post final stakeholder plan and begin implementation phase.	July 3, 2007
4. Participants contacted individually to arrange suitable time frames for replacement certificates.	June to October
5. Update IT Standing Committee on status of implementation.	September 11, 2007
6. Completion of implementation phase.	November, 2007

Process Evaluation

Stakeholders will be provided the opportunity to provide feedback on the effectiveness of the process in achieving stated objectives.