Employment and Social Development Canada | Emploi et Développement social Canada

Canada Education Savings Program (CESP)

Data Interface Operations and Connectivity

Version Number: 7.0

Version Date: November 24, 2016

Latest Update: July 17, 2024

Canada

Canada Education Savings Program - Data Interface Operations and Connectivity

Large print, braille, MP3 (audio), e-text and DAISY formats are available on demand by ordering online or calling 1 800 O-Canada (1-800-622-6232). If you use a teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. No.: Em4-46/2024E-PDF
ISBN: 978-0-660-73100-1

Version History

Version	Release Date	Description
R 1.0	September 30, 1998	Initial version for HRSDC internal reviews.
D 2.0	March 15, 1999	Ongoing updates.
D 2.1	April 27, 1999	Ongoing updates.
D 2.2	May 27, 1999	Ongoing updates.
D 2.3	July 21, 1999	Ongoing updates.
D 2.4	October 10, 1999	Management review and update.
D 2.5	November 15, 1999	Review updates release.
R 2.0	December 15, 1999	Updates to contacts list
R 3.0.1	November 6, 2001	Ongoing updates.
R 4.0	April 27, 2005	Ongoing updates.
R 5.0	August 6, 2007	New LRA procedures and new version of ViaSafe.
D 6.0	October 6, 2015	Ongoing updates
R 7.0	November 24, 2016	Ongoing updates

Legend

D Draft

R Release

Comments and questions regarding this document may be addressed to:

Employment and Social Development Canada – ESDC

Electronic Services Section

Phase IV, Mailstop: Bag 4

40 Promenade du Portage

Gatineau QC K1A 0J9

Telephone: 1-888-276-3624

E-mail: cesp-pcee@hrsdc-rhdcc.gc.ca

Table of Contents

1 Introduction

Organizations of Registered Education Savings Plans (RESPs) must report all financial transactions including the Canada Learning Bond (CLB), the Canada Education Saving Grant (CESG) and any federally provincial administered incentives to the Canada Education Savings Program (CESP)under Employment and Social Development Canada (ESDC). The program accepts and returns electronic reporting through a dedicated, secure Internet-based, Public Key Infrastructure (PKI). No other means of information exchange is accepted.

1.1 Purpose

The purpose of this document is to provide detailed information on how to set up secure encrypted bi-directional telecommunications operations between organizations and the CESP.

1.2 Scope

This document describes the nature of and mechanisms for the transmission of information between organizations and the CESP. The *Data Interface and Connectivity* document provides the following information:

- how to obtain access to the Public Key Infrastructure (PKI)
- how organizations connect and transmit information to the CESP
- when organizations send and receive information
- who to contact for technical support concerning problems with information exchanges.

This document does not cover general business requirements of organizations managing RESP's or business rules surrounding the CESP. Business issues are covered in other documents, which include:

- Canada Education Savings Act
- Canada Education Savings Regulations
- Canada Education Savings Grant Interface Transaction Standards
- Trustee Agreements
- Promoter Agreements

2 Non-technical Connectivity Requirements

This section outlines non-technical requirements that must be arranged by organizations to transmit files to CESP.

2.1 Key players

Organization Business Contact: The Business Contact is the person responsible to inform the CESP of any organizational changes including all PKI granting/modifications related activities.

Certificate Custodian: The custodian is the person that assumes responsibility for the protection of any information following its decryption and must also protect the certificate and the password.

Local Registration Authority (LRA): Provides assistance to the Certificate Custodian of the External Device Certificate on behalf of Shared Services Canada (SSC).

Guarantor: Provides assistance to the LRA in the form of validating the identity of the Certificate Custodian in person.

2.2 Public Key Infrastructure (PKI) device certificate

Public Key Infrastructure (PKI) device certificate facilitates the transmission of secure, encrypted, and authenticated electronic mail over the Internet. PKI encrypted media ensures that no sensitive information is exposed during transmission between organizations and the CESP. All PKI transmissions receive acknowledgement in both directions.

The PKI device certificate and Managed Secure File Transfer (MSFT) account set-up must be completed prior to submitting any data files to the CESP. To obtain or make changes to an External Device Certificate, the request must be made by the organization's business contact by sending an email to the CESP. An External Device, Application, Group & Role Certificate Administration Form will be sent directly to the Certificate Custodian for completion to obtain a device certificate.

Completed form must be sent to the CESP authorized LRA for processing. Each organization is limited to 2 External Device Certificates. One Certificate Custodian (user account) should be designated as primary, and the second Certificate Custodian as a back-up. Once the External Device Certificate becomes activated, reports already received through the primary certificate should be deleted. Reports not retrieved or deleted after 3 months will be cleared to reduce network congestion. The back-up account should be activated at least once a month to ensure that it is functioning properly.

If an organizational change occurs and a Certificate Custodian must be replaced, the organization's business contact must advise the CESP that they wish to have the external device certificate revoked and name a replacement Certificate Custodian. The new Certificate Custodian must send the completed External Device Application, Group & Role Certificate Administration Form to the CESP for processing.

2.3 External device certificate application process

The LRA & Guarantor participates in the External Device Certificate application process in the following manner:

Certificate Custodian Initialization

The LRA and Guarantor are responsible for completing their specified sections of the External Device, Application, Group & Role Certificate Administration form. All Certificate Custodians must identify themselves to a Guarantor, showing 2 pieces of ID, 1 with a photograph, both with signatures and valid expiration dates, such as a driver's license or credit card. The Guarantor will complete and signed section 4 of the Form confirming the identity of the Certificate Custodian.

Once the completed form is received, the LRA provides the Certificate Custodian with half of the initialization codes (the authorization code) via video conference. The reference code, which is the other half, will be sent by email from Shared Services Canada (reference code). Both codes are required to activate the device and they become void after 12 days.

Key Recovery

Key recovery is necessary when the Certificate Custodian:

- fails to recall their password
- when the profile is compromised due to loss of their personal computer
- when there is suspected unauthorized access; or
- when one's common name changes

In order to request a key recovery, the Certificate Custodian must send their request by email to:

EDSC.NC.PCEE.TRANSFERT_SECURISE-SECURE_TRANSFER.CESP.NC.ESDC@HRSDC-RHDCC.GC.CA

The LRA will request Shared Services Canada to set up the Certificate Custodian for recovery. The LRA will provide the new authorization code for key recovery via video conference and Shared Services Canada will provide the reference code by email. Until key recovery is complete, Certificate Custodian cannot submit new files to the CESP or access the report files returned from them.

2.4 Contact information

If there is a problem, please contact the authorized LRA at the email address noted below:

EDSC.NC.PCEE.TRANSFERT_SECURISE-SECURE_TRANSFER.CESP.NC.ESDC@HRSDC-RHDCC.GC.CA

For all technical support, please contact Shared Services Canada at the email address below:

SSC.Sftsupport-SoutienSFT.SPC@Canada.ca

3 Technical Connectivity Requirements

This section outlines technical requirements that organizations must fulfill to establish telecommunications with the CESP.

3.1 Managed Secure File Transfer (MSFT) Service

Organizations must use MSFT software to send data to the CESP via the Internet. MSFT is Entrust enabled, and is recognized by ESDC as a secure method of data encryption. MSFT is the only file transmission technology that CESP accepts.

MSFT software is provided free to organizations by CESP. MSFT software and installation instructions are sent to organizations by SSC as part of the PKI subscription process, however, the PKI certification process must be complete prior to installation and use of MSFT.

The benefits of using MSFT include the following:

- data compression
- non-repudiation (proof services)
- simple execution
- information protection
- management and change tracking

3.2 Configuration Requirements

The MSFT Client software[1] works on any personal computer equipped with the following:

- at least 12 Mbytes of free disk space on the user's hard disk for software. Additional space is required for logs
- at least 5 times the disk space estimated for data files being transferred (for example, A 10MB file requires 50MB of free disk space to process through MSFT agent)
- client requires Java Runtime Environment:
    - minimum version of Java is Java 6 update 7
    - recommended version of Java is Java 8
- network Card or Dial-up Modem
- operating system: Any Windows version

The MSFT client software is also available as a standalone Java application and is configurable to run as a Windows service. Organizations are to contact SSC to discuss this feature.

[1] This is a Java based application but is launched using a web browser. The web link that launches the application runs a JNLP file that uses Java Web Start. Pop-ups should be enabled for this site.

3.3 Network Requirements

Organizations must have access to Internet service from the MSFT configured PC. Internet access enables the transmission of secure PKI Internet transmission to the SSC MSFT agent at one of the SSC Data Centers.

Note: Response time and service availability depends on the quality of the local Internet service acquired by the organization.

3.3.1 Access to SSC MSFT Services

Internet Protocol (IP) connectivity must exist from the MSFT Agent PC to the ITSB MSFT service. If the organization MSFT Agent is running behind any type of Firewall (application firewall, Router, etc.), the following ports must be open (outbound):

- TCP port 389 for Lightweight Directory Access Protocol (LDAP) connection. This port is used to connect to the LDAP servers
- TCP port 829 for Authority portion of the PKI key management portion. Required for maintenance of the user security profile with the PKI server
- TCP port 443 for Hypertext Transfer Protocol over Secure Socket Layer or HTTPS and TLS/SSL connections must be granted.