Canada Education Savings Program (CESP)

Data Interface Operations and Connectivity

Version Number: 7.0

Version Date: November 24, 2016

Canada

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

Table of Contents

1 Introduction

Organizations of Registered Education Savings Plans (RESPs) must report all financial transactions including the Canada Learning Bond, the Canada Education Saving Grant 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 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 CESP

- When organizations send and receive information

- Who to contact for technical support concerning problems with information exchanges with the CESP system

This document does not cover general business requirements of organizations managing RESPs 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 Agreement

- Promoter Agreement

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 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 in order 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 <u>organization's business contact</u> 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 registered mail. 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:

NC-INSCRIPTION_ENROLMENT-GD@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 registered mail 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.

Email : NC-INSCRIPTION_ENROLMENT-GD@hrsdc-rhdcc.gc.ca

For all technical support, please contact Shared Services at the email address noted below.

Email : SoutienSFT-SFTSupport@tpsgc-pwgsc.gc.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 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 (ie. A 10MB file requires 50MB of free disk space to process through MSFT agent)

- Client require 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

Note 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.

Note 2: 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.

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.

4   General Transmission Information

The CESP receives information from RESP organizations, in the electronic format defined by the specifications outlined in the *Interface Transaction Standards* (ITS).

Organizations submit encrypted data representing transactions within an RESP to Shared Services Canada (SSC). The data is decoded by SSC and transferred to the CESP for processing. The CESP returns reports, indicating transaction events and associated errors, to organizations by the same encrypted method.

4.1   Industry Testing

Organizations must submit data to the CESP Industry Testing Unit to be compliant with the current *Interface Transactions Standards* specifications.

Until organization test data is compliant, organization production data is not accepted by the CESP. This policy prevents format errors in organization data and increases data integrity.

The *Industry Testing Guide* provides detailed information on the guidelines for Industry Testing.

4.2   Standard Production Runs

The CESP receives files containing transaction information representing activities within a RESP and processes them monthly based on calendar year and processing period. A production run is typically the monthly timeframe within which the CESP processes organization data files.

4.3   Summary report transaction (Record Type "700")

Organizations must send records of Record Type "700" to the program once per processing period. The summary report transaction files are sent to the CESP in the same manner as standard production files. Details of the Record Type "700" can be found in the *Interface Transaction Standards*.

4.4   Processing Period

Organizations report all RESP activity that occurred during a processing period to the CESP by the production run cut-off date. Processing periods normally extend from the first day of the month to the last day of the same month. The cut-off date for organizations to submit a data file for a production run generally falls on the fourth business day following the processing period's end date.

For example: the February 2016 production run would have a processing period of January 1st, 2016 to January 31st, 2016. The production run cut-off date would be February 4th, 2016.

The summary reporting transaction (Record Type "700") must also be sent to the CESP on a monthly basis and in a separate file, however, the deadline to submit this information for a given processing period is delayed one month.

For example: For the processing period covering January 1st, 2016 to January 31st, 2016 the cut-off date for submitting summary reporting transaction (Record Type "700") would be the production run cut-off date for the February 2016 production run (February 4th, 2016).

Note: Any future transactions received in a file following the last day of the processing period will be rejected.

For Example: A transaction dated January 5th, 2016 received by the CESP on January 7th, 2016 for the December 1 to 31, 2015 processing period will be rejected.

4.5   Submission of transactions

The CESP system uses the Processing date and Transaction Date to determine a beneficiary's entitlement. Therefore, organizations should ensure that transactions which occur in a given processing period are reported to the CESP before the production run cut-off date for that particular processing period. Information contained in files received by the CESP system, after the production run cut-off date, is stored and processed in the next processing period unless the organization requests that the file be removed.

If transmission to the CESP is delayed due to CESP technical difficulty, deadline dates are extended and organizations are notified via ListServ notification.

4.6   Monthly Processing

The CESP system processes RESP transactions to calculate the amount of CLB, CES Grant and/or provincial incentives awarded by or owed to the CESP.

CLB, CES Grant and/or provincial incentives are awarded to a beneficiary based on the order the transactions occurred with the organization.

The CESP system uses the date of the transaction and not the date in which the CESP receives the transaction information. When processing the monthly CLB, CES Grant and/or provincial incentives amount, all transactions from all organizations are considered together during one production run. The single production run prohibits additional data from being collected and processed separately.

Transactions occurring on the same date receive grant amounts in proportion to the contribution amount. Therefore, it is important to transmit data within the prescribed period.

During processing there is an order in which certain transactions are processed. Non-financial transactions, which provide information on the RESP contract, beneficiary and subscriber, are processed first. Financial transactions (Record Type "400") such as contributions, withdrawals and transfers are processed after the non-financial transactions. Refer to the *Interface Transaction Standards* for details on all record and transaction types.

Files containing the summary report transaction (Record Type "700") are processed separate from, and do not have an impact on, the processing of standard financial and non-financial CLB, CES Grant and/or provincial incentives transactions.

4.7   Production Schedules

Organization transaction data is not processed until after the production run cut-off date. After the data is processed, payment of CLB, CES Grant and/or provincial incentives to the organization typically occurs on the last business day of the month.

Current production schedules for transaction processing and any other relevant information are issued periodically by the CESP via ListServ notification.