Ressources humaines et Développement des compétences Canada
Human Resources and Skills Development Canada

Canada Disability Savings Program

Data Interface Operations and Connectivity

Version Number: 1.1
Version Date: October 2008

Canada

Document Version History		
Version	**Date**	**Description**
1.0	July 11, 2008	Version 1.0 of the CDSP Data Interface Operations and Connectivity. This document covers all functionality for the set up of secure encrypted bi-directional telecommunications operations between an Issuer and CDSP.
1.1	Oct 16, 2008	Version 1.1 of the CDSP Data Interface Operations and Connectivity. This document covers all functionality for the set up of secure encrypted bi-directional telecommunications operations between an Issuer and CDSP.

Comments and questions regarding this document may be addressed to:

Canada Disability Savings Program
Human Resources and Skills Development Canada
140, Promenade du Portage, Phase IV Mailstop: Bag 4
Gatineau, Quebec
K1A 0J9

Telephone: 1-888-276-3632

Fax (819) 953-6500

E-mail: rdsp-reei@hrsdc-rhdcc.gc.ca

Table of Contents

1 Introduction ..... - 2 -
1.1 Purpose ..... - 2 -
1.2 Scope ..... - 2 -
1.3 Terms ..... - 3 -
2 Non-technical Connectivity Requirements ..... - 4 -
2.1 PKI Subscription Basics ..... - 4 -
2.2 The Guarantor Model ..... - 4 -
2.3 Local Registration Authority & the Guarantor ..... - 5 -
2.4 PKI User Requirements ..... - 5 -
2.5 LRA & PWGSC Contact Information ..... - 6 -
3 Technical Connectivity Requirements ..... - 7 -
3.1 PWGSC MSFT (Managed Secure File Transfer) Service ..... - 7 -
3.2 Configuration Requirements ..... - 7 -
3.3 Network Requirements ..... - 8 -
3.3.1 Access to ITSB MFST Services ..... - 8 -
4 General Transmission Information ..... - 8 -
4.1 Industry Testing ..... - 8 -
4.2 Standard Production Runs ..... - 9 -
4.3 Processing Period ..... - 9 -
4.4 Report Timing ..... - 9 -
4.5 Monthly Processing ..... - 9 -
4.6 Production Schedules ..... - 10 -

1 Introduction

An Issuer of the Registered Disability Savings Plan (RDSP) must report Canada Disability Savings Bond (Bond) and Canada Disability Savings Grant (Grant) applications and financial transactions to Human Resources and Skills Development Canada (HRSDC)'s, Canada Disability Savings Program (CDSP). The CDSP accepts and returns electronic reporting through a dedicated, secure Internet-based, Public Key Infrastructure (PKI). No other means of information exchange is accepted by the CDSP.

1.1 Purpose

The purpose of this document is to provide detailed information about how to set up secure encrypted bi-directional telecommunications operations between an Issuer and the CDSP.

1.2 Scope

This document describes the nature of and mechanisms for the transmission of information between an Issuer and the CDSP. The *Data Interface Operations and Connectivity* document provides the following information:

- How organizations connect and transmit information to the CDSP;
- When organizations send and receive information; and
- Who to contact for technical support concerning problems with information exchanges with the CDSP.

This document does not cover general business requirements of organizations managing RDSPs or business rules surrounding the CDSP.

Business issues are covered in other documents which include the:

- *Canada Disability Savings Act*
- *Income Tax Act*
- Canada Disability Savings Regulations
- CDSP Interface Transaction Standards
- Issuer Agreement for the purposes of the exchange of information and the payment of the Grant and Bond

1.3 Terms

The following are definitions of terms used in this document:

Issuer

A trustee that is licensed or authorized to offer its services in Canada and who offers an RDSP to the public has ultimate responsibility for the administration of the RDSP which includes securing the approval of the Canada Revenue Agency for the particular RDSP specimen plan.

Agent

An organization that has entered into an agreement to act as an administrative agent for the RDSP Issuer. For the purpose of this document a Service Provider is not considered an Agent.

Service Provider

An organization that provides a service, on behalf of a financial organization, to compile and submit electronic transaction information to the CDSP.

2 Non-technical Connectivity Requirements

This section outlines non-technical requirements that must be arranged by an Issuer or Agent to transmit files to the CDSP.

2.1 PKI Subscription Basics

PKI certification facilitates the transmission of secure, encrypted, and authenticated electronic mail over the Internet. PKI encrypted media ensures that no sensitive Issuer or Agent information is exposed during transmission to or from the CDSP. All PKI transmissions receive acknowledgement in both directions.

The PKI Certification and Managed Secure File Transfer (MFST) account set-up must be completed prior to submitting any data files to the CDSP. The Issuer or Agent must fill out a PKI External Subscriber application form in order to obtain PKI certification.

An External Subscriber Application form can be found at the Public Works and Government Services Canada (PWGSC) website:

http://www.tpsgc-pwgsc.gc.ca/gji-icm/documents/formulaires-forms/13923-eng.pdf

The completed form can be faxed to the CDSP's authorized Local Registration Authority (LRA). See section 2.5 for LRA's fax number.

Each Issuer or Agent is limited to two PKI user accounts. One user account should be designated the primary user, and the second as a back-up to the primary user account. Once an account becomes activated, reports already received through the primary user should be deleted. Reports not retrieved or deleted after three 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 user must be replaced, the active user must advise the CDSP Electronic Services Section along with all the LRA's listed below, that they wish to have their account disabled. Replacement users must submit a PKI External Subscriber Application form and continue through the certification process as a new user.

2.2 The Guarantor Model

PWGSC has agreed to a new method for issuing PKI certificates, called the "Guarantor Model". This allows the creation of a key without an LRA being present.

In most instances, the Guarantor (defined below) will be an Office Manager or current PKI key holder. Others who may be considered as a Guarantor include Judges, Lawyers, Police Officers, Chartered Accountants, Doctors, Dentists, and other registered professionals - much like the required Guarantor when someone applies for a Canadian passport. It is the subscriber's responsibility to find someone who can act as a Guarantor.

2.3 Local Registration Authority & the Guarantor

Local Registration Authority (LRA): Provides assistance to the subscriber of the PKI key on behalf of PWGSC.

Guarantor: Provides assistance to the LRA in the form of validating the identity of the PKI key subscriber in person.

The LRA & Guarantor participate in the PKI key creation process in the following manner:

- PKI User Initialization: Upon initial subscription, the Guarantor is required to identify each user in person. The LRA and Guarantor are responsible for completing their specified sections of the External Subscriber Application form. The LRA is also responsible for providing the Authorization Code to the user to allow the user to perform the initialization process.

- User Key Recovery: Key recovery is necessary when a user forgets their password, when the profile is compromised due to loss of a personal computer (PC), when there is suspected unauthorized access, or when one's common name is changed due to a name change or organizational change. In order to request a key recovery the user must submit a PKI Change Request Application form to their authorized LRA. This form can be downloaded from the PWGSC website:

http://www.tpsgc-pwgsc.gc.ca/gji-icm/05/13922-eng.html

The LRA will request that the Certificate Authority (CA) set up the user for recovery. The Guarantor will be required to repeat physical identification of the user; the LRA will provide the new authorization code for key recovery via registered mail. Until key recovery is complete, users can not submit new files to the CDSP or access the report files returned from the CDSP.

2.4 PKI User Requirements

All PKI users must identify themselves to a Guarantor, showing at least two pieces of identification, including one with a picture and both with a signature, such as a driver’s license or building pass. Subsequent to authentication by the Guarantor, the LRA provides the subscriber with half of the initialization

codes (the authorization code) via registered mail. The reference code, the other half from the CA, is sent directly to the subscriber by electronic mail. Both codes are required to enable the actual initialization.

If there is a problem receiving the authorization code, contact the authorized LRA or Information Technology Services Branch (ITSB) at the numbers noted below. ITSB is responsible for facilitating secure communications of sensitive information for the federal government.

2.5 LRA & PWGSC Contact Information

LRA – Main Contact

Compliance and Monitoring
Canada Disability Savings Program
Human Resources and Skills Development Canada
140, Promenade du Portage, Phase IV Mailstop: Bag 4
Gatineau, Quebec
K1A 0J9

Fax: (819) 953-6500

E-mail: cesg-pcee.indtest@hrsdc-rhdcc.gc.ca

PWGSC – National Service Desk

- **Information Technology Services Branch (ITSB)**
- Tel: (613) 738-7782

3 Technical Connectivity Requirements

This section outlines the technical requirements that an Issuer or Agent must fulfill to establish telecommunications with the CDSP.

3.1 PWGSC MSFT (Managed Secure File Transfer) Service

An Issuer or Agent must use MSFT software to send data to the CDSP via the Internet. MSFT is Entrust enabled, and is recognized by HRSDC as a secure method of data encryption. MSFT is the only file transmission technology that the CDSP accepts.

MSFT software is provided free to an Issuer or Agent by the CDSP. MSFT software and installation instructions are sent to an Issuer or Agent by ITSB as part of the PKI subscription process, however, the PKI certification process must be completed 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 Entrust Client works on any IBM-compatible personal computer equipped with the following:

- Pentium 166 MHz microprocessor or better
- At least 32 Mbytes of RAM
- At least 12 Mbytes of free disk space on the user's hard disk for software
- At least 5 times the disk space estimated for data files (ie. 10MB file requires 50MB of free disk space to process through MSFT agent)
- Network Card or Dial-up Modem

Operating system: Windows 95/98, Windows NT Workstation 4.0, Windows XP, Windows 2000 and Windows 2003

Note:

This is a Web based application and requires Internet Explorer 5.5 or above.

Pop-ups should be enabled for this site.

Client needs to have Java Runtime Environment 1.4.02_13 or above (versions 5 or 6 should use the version that has the new daylight savings time (DST) patches).

3.3 Network Requirements

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

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

3.3.1 Access to ITSB MFST Services

Internet Protocol (IP) connectivity must exist from the MSFT Agent PC to the ITSB MSFT service. If the Sender 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 CDSP will receive information from an RDSP Issuer or Agent, in the electronic format defined by the specifications outlined in the current CDSP *Interface Transaction Standards* (ITS).

An Issuer will submit encrypted data representing transactions within an RDSP to ITSB. The data will be decoded by ITSB and transferred to the CDSP for processing. The CDSP will return reports, indicating transaction events and associated errors, to an Issuer or Agent by the same encrypted method.

4.1 Industry Testing

An Issuer or Agent must submit data to the CDSP Industry Testing Unit to be certified compliant with the current CDSP ITS specifications.

Until an Issuer or Agent test data is certified compliant, their production data will not be accepted by the CDSP. This policy prevents format errors in Issuer or Agent data and increases data integrity.

The CDSP *Industry Testing Guide* will provide detailed information on the guidelines for Industry Testing.

4.2 Standard Production Runs

The CDSP will receive files containing transaction information representing activities within an RDSP and process them monthly based on calendar year and processing period. A production run will typically be the monthly timeframe within which the CDSP will process an Issuer or Agent data files.

4.3 Processing Period

An Issuer or Agent will report all RDSP activity that occurred during a processing period to the CDSP by the production run cut off date. Processing periods, which will be similar to the Canada Education Savings Program, will extend from the first day of the month to the last day of the same month. The cut off date for an Issuer or Agent to submit a data file for a production run will fall on the fourth business day following the processing period's end date.

Example: The January 2009 production run has a processing period of December 1, 2008 to December 31, 2008. The production run cut off date for December is January 7, 2009.

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

Example: A transaction dated January 3, 2009 received by CDSP on January 4, 2009 for the December 1 to 31, 2008 processing period will be rejected.

4.4 Report Timing

The CDSP system will use the date the file is received by the Government of Canada and the event date of the transaction to determine a beneficiary's entitlement. Therefore, an Issuer or Agent should ensure that transactions which occur in a given processing period are reported to the CDSP before the production run cut-off date for that particular processing period. Information contained in files received by the CDSP system, after the production run cut-off date, will be stored and processed in the next processing period unless the Issuer or Agent requests that the file be removed.

If transmission to the CDSP is delayed due to CDSP technical difficulty, deadline dates will be extended and an Issuer or Agent will be notified via ListServ notification.

4.5 Monthly Processing

The CDSP system will process RDSP transactions to calculate the amount of Grant and/or Bond awarded by or owed to the CDSP.

During processing there will be an order in which certain transactions will be processed. Non-financial transactions, which provide information on the RDSP contract, beneficiary and holder, will be processed first. Financial transactions (Record type "401") such as Grant and Bond requests will be

processed after the non-financial transactions. Please refer to the current CDSP ITS for details on record and transaction types.

4.6 Production Schedules

An Issuer or Agent transaction data will not be processed until after the production run cut off date. After the data is processed, payment of Grant and/or Bond to the Issuer or Agent typically will occur on the last business day of the month.

Production schedules for transaction processing and any other relevant information will be issued periodically by the CDSP via ListServ notification.