# Table of Contents

## Implementation Models for Institutions with SPEEDE/ExPRESS

| Model 1: Texas EDI System – Overview, Pros/Cons, and Implementation Steps | 3 |
| Model 2: NJ TRANSFER ET System – Overview, Pros, and Implementation Steps | 4 |

| Appendix A: Sample Texas Server Registration Authorization Form | 5 |
| Appendix B: Electronic Transfer FTP/SFTP Access Application | 6 |
| Appendix C: PGP Guide | 7 |
| Appendix D: FTP Guide | 11 |
Implementation Models for Institutions with SPEEDE/ExPRESS

Model 1: Dedicated to NSC SPEEDE

Overview:
Institutions employing this model will be able to send/receive transcripts via the NSC SPEEDE Server. Community colleges currently registered with the NSC SPEEDE Server, who have developed their own automation processes, can use this model. Four-year participating institutions interested in taking advantage of the automatic course articulation feature of NJ TRANSFER should not use this model.

Pros:
- Seamless
- Minor or no changes to processes established by your institution

Cons:
- Institution is responsible for maintaining communication with the NSC SPEEDE Server
- Institution is responsible for maintaining an adequate level of security
- Participating four-year institutions will not be able to use the automatic course articulation feature of NJ TRANSFER

Implementation Steps:
Please visit https://studentclearinghouse.org/colleges/speede for more information
Model 2: Dedicated to NJ TRANSFER ET System

Overview:
Institutions employing this model will be able to send/receive transcripts via the NJ TRANSFER ET system. Participating four-year colleges/universities will receive the added benefit of the automatic course articulation feature. In order to use the NJ TRANSFER ET system, schools must be registered with the NSC SPEEDE Server under the NJ TRANSFER umbrella account. College/University Presidents were asked to grant the NJ Statewide Transfer Initiative Office permission to register their institution with the UT Texas EDI Server*. (See sample form, Appendix A). Institutions already registered with the Texas Server would be re-registered under NJ TRANSFER. This may require the reconfiguration of settings on your institution.

Pros:
- Straightforward processes
- Maximum security enforced via PGP, Firewall and ACL. Institutions will need to acquire PGP software capable of generating RSA Keys. (See Appendix C: PGP Guide)
- NJ TRANSFER will be responsible for maintaining communication with the NSC SPEEDE Server and for security/PGP encryption on transcripts going out to out-of-state institutions

Implementation Steps:
2) Create a public PGP key for your institution and e-mail it to Sewon Kim at swkim@rcbc.edu. Upon receipt of items 1 and 2, we will e-mail the NJ TRANSFER public key and FTP/sFTP access account. Please see Appendix C: PGP Guide for more detailed information about PGP.
3) Sending transcripts: Please see Appendix C: Section 8 - Sending Encrypted Transcripts to NJ TRANSFER and Appendix D: FTP Guide.
4) Receiving transcripts: Please see Appendix D: FTP Guide.

* The SPEEDE server was designed and developed by University of Texas at Austin, hence the name “UT Texas EDI Server” and had maintained the free service until the SPEEDE team transferred the technology and operations to National Student Clearinghouse in 2012. SPEEDE server, as of October 1, 2019, is maintained by National Student Clearinghouse (referred as NSC SPEEDE Server).
Appendix A: Authorization Form

Authorization Form For NJ TRANSFER To Register Institutions
With The University of Texas at Austin EDI Internet Server

I authorize the NJ Statewide Transfer Initiative Office to register Institution XXX with the University of Texas at Austin EDI Internet Server (Texas Server), and understand NJ TRANSFER will serve as the portal for any transcripts this institution sends/receives through the Server. If my institution is currently registered with the Texas Server, I authorize the NJ Statewide Transfer Initiative Office to change that registration so it is included under NJ TRANSFER.

_________________________________________  ______________________________________
(Signature)                                (Please Print Name)

_________________________________________  ______________________________________
(Please Print Title)                        (E-mail Address)

_________________________________________
(Date)

Please designate which code NJ TRANSFER should use when registering your institution with the Texas Server:

_____ Please use our CEEB Code XXXX

_____ Please use our FICE Code XXXXXX

We would appreciate receiving your completed form no later than Friday, March 12, 2004. You may respond by e-mail to John Scott at jscott@bcc.edu, or fax your form to (609) 894-0638. If you have questions, or wish to receive further information, please contact Sewon Kim, Computer Systems Engineer, at swkim@bcc.edu or (609) 694-9311, ext 7410.
Appendix B: Electronic Transcript FTP/SFTP Access Application

Please provide the following information:

1. Name of Institution: ________________________________

2. [ ] FTP [ ] SFTP

3. User Information (person responsible for sending/retrieving files via FTP):
   Name: ________________________________ Title: ________________________________
   Email: ___________ @ ________________ Telephone: ________________________________

4. System IP Address: ________________________________

Please return this form to:

Théa Olsen
tolsen@rcbc.edu
Associate Director – New Jersey Statewide Transfer Initiative
Rowan College at Burlington County
900 College Circle
Mount Laurel, New Jersey 08054

---

1 Additional SFTP authentication public key exchange may be required.
2 The system that sends/retrieves files to/from ftp.njtransfer.org via FTP.
Appendix C: PGP Guide

This guide is based on The University of Texas at Austin’s publication, “PGP: A Beginner’s Guide”, and PGP command line version 2.6.2. It is intended for use by institutions with SPEEDE/ExPRESS, who want to employ the NJ TRANSFER ET System outlined in Model 2.

1. PGP Software
You will need PGP software, version 2.6.2 or later, capable of generating RSA keys. Please visit http://www.philzimmermann.com for a brief history of PGP and a summary of the differences among the various available products. Please note: PGP version 2.6.2 only supports ‘the 8.3 convention’. In order to work with files having long filenames, PGP 6.5.8 or above needs to be used.

We recommend you use one of the sources listed on Phil Zimmermann’s page (as of October 1, 2019, the listing is no longer available on Philip Zimmermann’s site) or below. Do not download a copy from a bulletin board or other web site.

Whether you download a distribution package from one of the links below or purchase a commercial product, please read the manual or README file before proceeding.

<table>
<thead>
<tr>
<th>Name of Product</th>
<th>URL for more information</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>International PGP</td>
<td><a href="https://www.openpgp.org/">https://www.openpgp.org/</a></td>
<td>Freeware</td>
</tr>
<tr>
<td>FileCrypt</td>
<td><a href="https://sourceforge.net/projects/filecrypt/">https://sourceforge.net/projects/filecrypt/</a></td>
<td>Freeware</td>
</tr>
<tr>
<td>Gnu Privacy Guard (GPG)</td>
<td><a href="http://www.gnupg.org/">http://www.gnupg.org/</a></td>
<td>Open source/ Command Line</td>
</tr>
</tbody>
</table>

2. Installing PGP Software
Install your PGP software according to the instructions. For UNIX, you will have to compile the source code for your particular flavor of UNIX. Installation for Win32 environment may only require you to unzip the application to a desired folder or follow an installation wizard.

3. Generating a Public/Private Key Pair
For command-line PGP 2.6.2 or above, the command is pgp –kg. PGP will then walk you through the process.

For other PGP versions please follow the steps outlined below. Please note: the exact wording may differ slightly depending on the PGP version you are using.

- Start-up the PGP application
- Open ‘PGPkeys’, or select the ‘Key Menu’
- Select the ‘New Keys’ or ‘Generate Key’ option
You will be prompted to:
- Enter login ID and e-mail address
- If you are using a PGP version above 2.6.2, or a PGP clone, you will have the option of selecting RSA or DSS/Diffie-Hellman keys. Please Note: You must select RSA keys.
- Recommended key size: at least 1024 bits
- Create a password consisting of a minimum of 8 characters. It should be something you will remember and would not be obvious to others.
- Enter random keystrokes as prompted (This step is not required of all PGP software).

4. Extracting Your Public Key With ASCII Armor

For command-line PGP 2.6.2, the command is `pgp -kxa`. Enter either your user ID and a file to save your key in, or `pgp -kxa userID filename`. (The ‘-a’ option = ASCII armored output.) Under ‘Extract Keys from What Key Ring?’ in the dialogue box, select ‘Your Public Key Ring’. Choose your public key from the list and check the box to ‘Asciify the Output’. Select the location/ filename for your key to be saved in.

![Image of command-line PGP output](image)

For other PGP versions pull down the ‘Key Menu’ and select ‘Extract Keys’ or ‘Export Keys’. Select the location/ filename for your key to be saved in. For PGP 5+, select ‘PGP Keys’ and choose your public key from the list.

For all PGP versions, check that the file you created contains an ASCII armored RSA key, not a binary key. To do this, open the file in a text editor. If the file does not begin with ‘----BEGIN PGP PUBLIC KEY BLOCK’, and end with ‘-----END PGP PUBLIC KEY BLOCK-----’ it is not an ASCII armored file. If you have successfully extracted your public key in an ASCII armored file, e-mail the file to Sewon Kim at swkim@rcbc.edu. Please send it as an attachment, or within the body of the message. Please do not ZIP the file.
5. **Adding the NJ TRANSFER ET System’s Public Key to Your Public Key Ring**

   You will receive the NJ TRANSFER ET System’s public key as an attachment via e-mail. Save the attachment as a file. For command-line PGP 2.6.2, the command is `pgp -ka keyfile` (keyfile = the name of the file containing the NJ TRANSFER public key).

   For other PGP versions, choose ‘Add Keys’ from the ‘Key Menu’. When prompted to locate a key file, select the file that contains the NJ TRANSFER public key and then select your public key ring. Some PGP software may ask if you want to certify the key, which means to add your signature to the key to certify you know it is genuine. As you will not be distributing this key, it is not necessary to certify it.

6. **Encrypting Your Transcript With the NJ TRANSFER ET System’s Public Key**

   For command-line PGP 2.6.2m, enter the command: `pgp -se filename Server’s-user ID`. The Server’s-user ID is `njtransfer@bcc.edu`.

   The options equate to the following:
   - `–s = sign`
   - `–e = encrypt`
   - `–a = ASCII armored output file`
   - `–t = use recipient’s textline conventions`

   For other PGP versions, click ‘Encrypt/Sign’ from the ‘File’ or ‘PGP Tools’ menu. Select the file to be encrypted. Choose NJ Statewide Transfer as the recipient. Specify either ‘Treat Source As Text’ and ‘Text Output’, or ‘Produce ASCII Output’. The exact wording will vary depending the PGP version/distribution. Next enter your pass phrase as prompted, and select a location/file name for the encrypted file to be saved to. The Server’s-userID is `njtransfer@bcc.edu`.

   If everything was done correctly, the encrypted file will begin with ‘-----BEGIN PGP MESSAGE ’, and end with ‘-----END PGP MESSAGE ’.
7. Sending the Encrypted Transcript to NJ TRANSFER

FTP into the NJ Transfer ET server at ftp.njtransfer.org or 130.156.140.21. Please note: to access the server, you must complete the Electronic Transfer FTP/SFTP Access Application form. (Appendix B) Submit the encrypted transcripts into the folder ‘OUTBOX.’

If you experience technical difficulties, please contact Sewon Kim at swkim@rcbc.edu.
Appendix D: FTP Guide

The following illustrates how to exchange files with the ftp.njtransfer.org server via FTP. We are using Microsoft WIN32 command line FTP, however any FTP client in any OS platform can be used. Additionally, most EDI software contains a FTP mechanism component.

1. Logon to ftp.njtransfer.org.

You will be brought to the “/” directory. Use the CD (Change Directory) command and your institution’s CEEB code to reach your home directory.

As illustrated above, there will be two directories; 1) INBOX and 2) OUTBOX. Files sent from other institutions will be deposited in your INBOX. Files being sent by you to other institutions will be uploaded to your OUTBOX, where they will be retrieved and processed each hour.
2. Uploading Transcript Files Using \textit{PUT} Command

- PUT [Local File location and name] [Remote File location and name]  
- Files must be \textbf{encrypted with ‘njtransfer@bcc.edu’ PGP public key} first.  
- Files in your INBOX will be picked up and processed every hour.

3. Downloading Received Files Using \textit{MGET} Command

- To download files in your INBOX use MGET: \texttt{mget *}  
- To remove files in INBOX use MDEL: \texttt{mdel *}  
- Decrypt downloaded files (\textbf{Please note:} All files in your INBOX are encrypted with your institution’s PGP public key.)

File Types in INBOX:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Contents</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>SENDERS</td>
<td>List of institutions that can send transcripts to your institution</td>
<td>Updated list is delivered every hour</td>
</tr>
<tr>
<td>RECEIVERS</td>
<td>List of institutions that can receive transcripts from your institution</td>
<td>Updated list is delivered every hour</td>
</tr>
<tr>
<td>TS130.YYMMDD.HHMMSS</td>
<td>Transcript in TS130 with date/time stamp as part of file name</td>
<td></td>
</tr>
<tr>
<td>TS131.YYMMDD.HHMMSS</td>
<td>Acknowledgement in TS131 from other institution that they have received transcript</td>
<td></td>
</tr>
</tbody>
</table>