Grange Bacstel-iP for iSeries

Setting up a new PC in an existing Bacstel-iP installation

This document describes setting up a new 'signing' PC in an existing Bacstel-iP installation and assumes that there is a PC available that is already configured for use in the Bacstel-iP environment.

The following pre-reqs and items must be available
PC with Windows2000 or XP attached to network that can access the iSeries
Spare USB port
Smart card reader
Smart cards with pin numbers
Smart card signing solution software e.g. Gemsafe or Schlumberger

1. Install the Bank's smart card signing solution software (e.g. Gemsafe or Schlumberger)
2. Reboot the PC and attach the smart card reader
3. Locate the smart card tool from the signing solution software just installed. For Gemsafe this is called the Gemsafe Card Details Tool or Gemsafe Toolbox, for Schlumberger this is called COVE. For each smart card, register the smart card certificate into Windows. This differs between signing solutions, but they are all similar. For Gemsafe, the registration link is under the 'Card' tab or Certificates, then register certificates. You will need the smart card pin number to do this. If a warning dialogue box appears asking if a trusted CA certificate should be installed, take 'YES' option to install it (the default is no).
4. Create a mapped drive or other link (e.g. UNC) to the iSeries IFS folder 'grange'
5. Copy the Bacstel-iP PC folder 'grbacsip1' or its equivalent from an existing PC to the new PC
6. Copy the following dll's from the grbacsip1 folder or subfolder into the Windows folder (WINDOWS for W2K, WINNT for W2000)
   ch_com.dll
   capicom.dll
   capicomseesure.dll
7. Register the dll's in Windows. For each dll:
   (RUN) regsvr32.exe <dll name>
8. From the grbacsip1 folder run the Checker_Admin.exe program. Ignore warning message regarding ch_com.dll being in multiple directories. Click the browse button '…' in the Path to data files panel, highlight one of the Checker files, press Open, then Apply, then OK.
9. Run the gr_svr.exe program. When started, it will probably display a red cross against the second line in the display when it tries to contact the IFS – just ignore. Take menu option Tools/Settings and use password ADMIN to get into the server set-up. The directory locations need to be changed to the correct location for that PC. For

mapped drives (e.g. drive X is mapped to the iSeries folder \grange) the Directory locations are:

(Zip dir) x:\reports\zip
(Output dir) x:\reports\html
(Home dir) x:

For UNC links to the IFS, the locations would be:

(Zip dir) \\<iSeries server>\grange\reports\zip
(Output dir) \\<iSeries server>\grange\reports\html
(Home dir) x: \\<iSeries server>\grange

10 Hit OK, then stop and start the server. This time there should be 2 green ticks in the display. If not, the correct mappings or links have not been applied, or the links are not active. This must be resolved for the system to work. Take a note of the PC name as displayed in the server window. The name is on the first line: 'Started on THISPC (192.168….)' where THISPC is the PC name.

11 On the iSeries, go into the Maintenance Menu (option 70 from the User menu) and check the PC names in option 17. The new PC name should be displayed with its current IP address.

12 This PC can now be used in the Bacstel-iP system. The name of the PC must be entered either as the default PC (Option 1 Maintenance menu) or specific to an application (option 5 Maintenance menu).

13 If there are smart card certificates to be used on this PC that were NOT registered on the original source PC, they must be registered in the Grange server program as follows. Perform this for each new smart card to be added.

Go into the tools/settings menu option of the server and click Certificates tab

If the smart card to be added does NOT exist in the list of certificates, click Add button. Select the Certificate to be added and hit OK. Then hit OK to return to main server window.

Note: When adding certificates, if two certificates are displayed from the card and one is 'Utility' and the other is 'Identity', **ONLY** select the 'Identity' certificate. **NEVER** select a 'Utility certificate.