INSTALLATION GUIDE

BP CODE SERVICE CONNECTOR

BP Code 7.26.X.X

Buypass OPEN

Version: 1.0
Document date: 25.02.2014

Buypass AS
Nydalsveien 30A, PO Box 4364 Nydalen
N-0402 Oslo, Norway
Tel.: +47 23 14 59 00
Fax: +47 23 14 59 01
E-mail: kundeservice@buypass.no
VAT: NO 983 163 327
www.buypass.no

History of change

Version	Date	Status	Description/Change
1.0	25.02.2014	First version	First version
1.1	13.03.2014	Updated	Added upgrade information

Contributors

Company name	Name
Buypass AS	Oskar Otterskog

Table of content

Overview

Buypass Code Service Connector (SC) is the physical access point to the Buypass Coe solution for merchants. The SC uses a regular SSL certificate issued by Buypass to perform point-to-point encryption when communicating with Buypass Code Servers located centrally at Buypass.

A unique signing certificate is used to identify a SC. The signing certificate is generated by Buypass and should be used on all SC's so that all requests are signed.

The SC is a light weight access point for Radius traffic, and mostly routes the traffic to Buypass Code Servers for further processing. It also handles directory lookup using instructions based on configurations that the merchant enters into Buypass Code Manager.

SC supports the following authentication protocols: PAP, CHAP, MSCHAPv2.

1.1 Technical requirements

1.1.1 Software requirements

- Windows 2003 SP1 (32 or 64 bit) / Windows 2008 (R2) / Windows 2012 (R2)
- Active internet connection

1.1.2 Hardware requirements

- CPU – Pentium class processor 1 GHz or faster
- HD – 200Mb of available hard disk space
- RAM – 120Mb of available ram

1.1.3 Network connectivity

- Buypass SC needs read access to your Directory Server via LDAP. Service account credentials are entered in Buypass Code Manager.
- Buypass SC needs to communicate with Buypass Code Servers via https (port 443).
- The access point/Radius client needs to communicate with the SC via Radius (default port 1812).

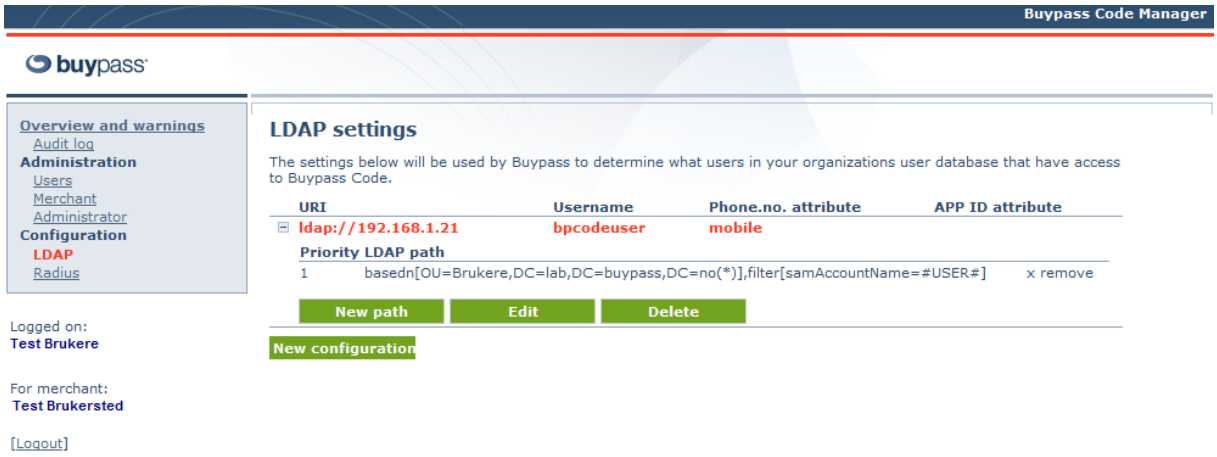
Installation and configuration

There are three phases for installation/configuration of the SC. Radius and LDAP configurations have to be established in Buypass Code Manager. The point of access (RAS, NAS, VPN etc.) has to be configured to use the SC. And finally the SC has to be installed and configured.

2.1 Buypass Code Manager

2.1.1 LDAP configuration

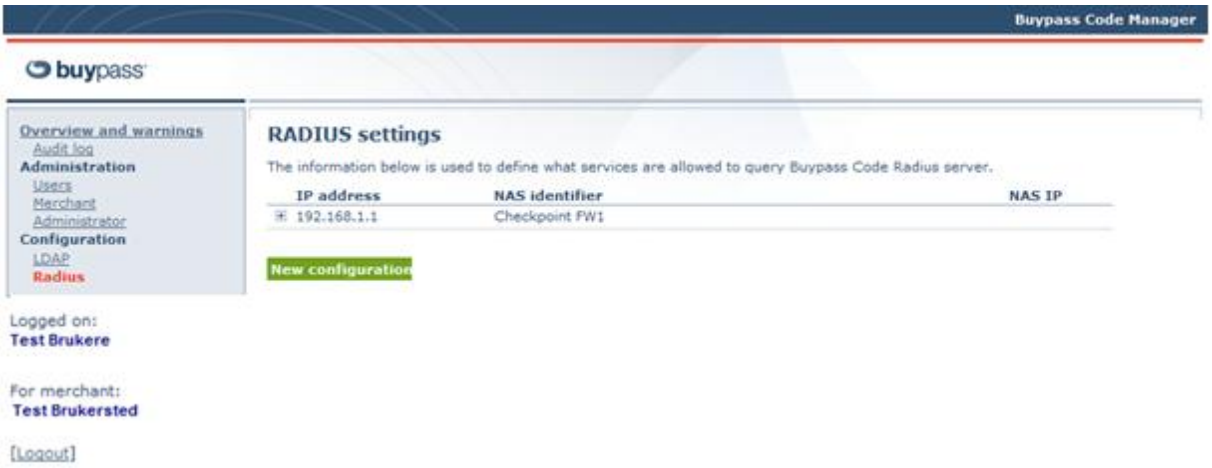
The LDAP configuration is used to lookup user information using a Directory Service via LDAP, e.g. Active Directory (AD) from Microsoft. The Directory Service should contain mobile numbers and/or App-ID for users.



For more information about LDAP configuration, see
BP Code Manager7.25.0.25_AdminGuide_EN.pdf.

2.1.2 Radius configuration

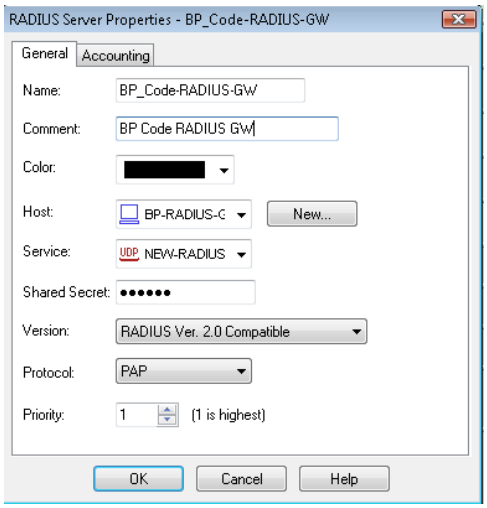
The Radius configurations define which access points/Radius clients are allowed to send requests to the SC.



For more information about Radius configuration, see
BP Code Manager7.25.0.25_AdminGuide_EN.pdf.

2.2 Point of access/Radius client

The local point of access/Radius client has to be configured to communicate with the SC via Radius. The IP-address has to point to the SC and the PSK (pre-shared key) has to be the same as the one in the Radius configuration in Buypass Code Manager.



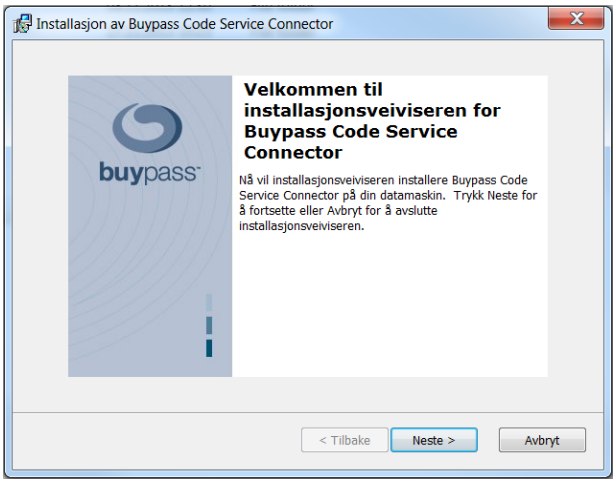
For more information about integrating Buypass Code with other products, see Integration Guides at Buypass Ekstranett.

2.3 Installation of Buypass Code Service Connector

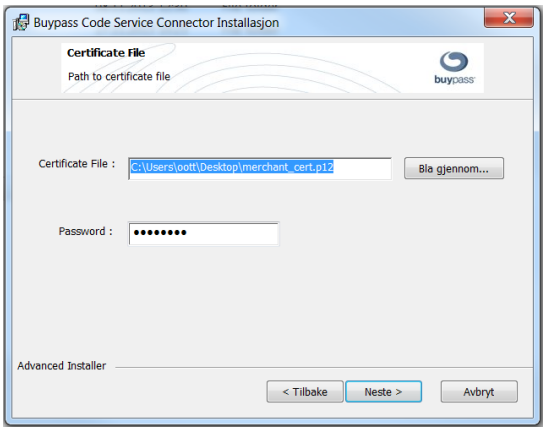
A Service Connector install wizard can be downloaded from Buypass Ekstranett. Please make sure you have access to the signing certificate sent by e-mail and the certificate password sent by SMS from number 1960. Also make sure you have admin access.

2.3.1 Installation guide

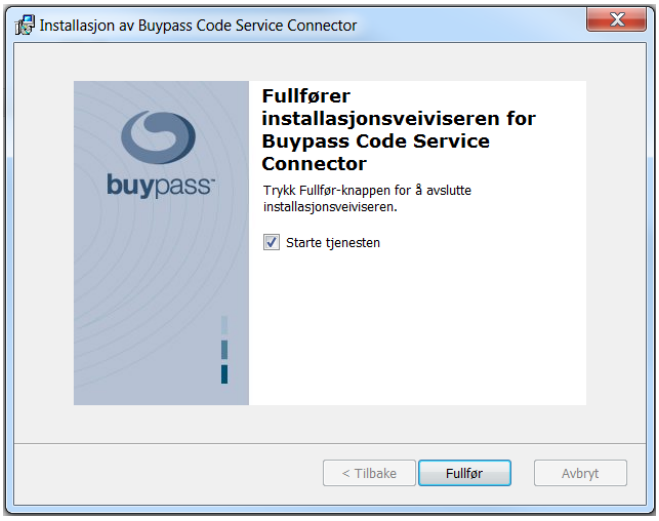
1. Start the install wizard and press "**Next**".



2. Find the signing certificate and enter the certificate password. Press “**Next**” and then “**Install**”. The necessary files will be installed in C:\bps\ and a service named “sc” will be installed.



3. Check the ”**Start service**” checkbox and press ”**Finish**”.



4. Verify that the SC has started by opening C:\bps\log\trace\sc_trace_TIMESTAMP.log and check that the last rows look like the following:

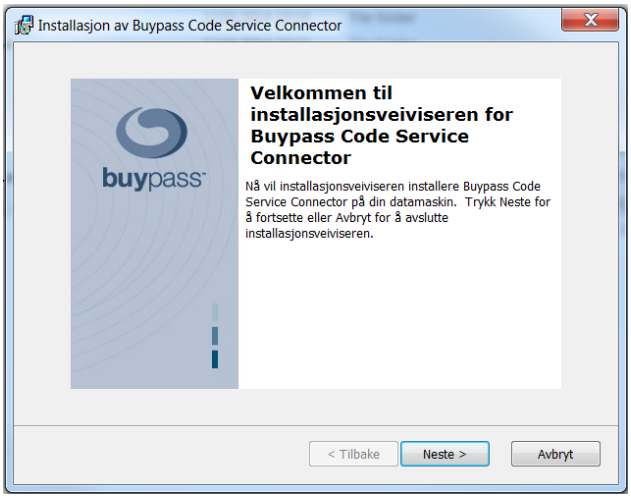
```
1: 2014.02.25 12:57:28,151 Starting SC Resources ...
1: 2014.02.25 12:57:28,151 Starting SC Encryption Manager
1: 2014.02.25 12:57:28,382 SC Encryption Manager started (cryptographic configuration OK)
1: 2014.02.25 12:57:28,382 Starting SC Communication Manager
1: 2014.02.25 12:57:28,810 SC authenticated and security context established
1: 2014.02.25 12:57:28,811 SC Communication Manager started
1: 2014.02.25 12:57:28,811 Starting SC Radius Proxy Manager
1: 2014.02.25 12:57:28,811 SC Radius Proxy Manager started
1: 2014.02.25 12:57:28,811 SC User Resolver Manager started
1: 2014.02.25 12:57:28,811 All SC Resources started successfully
1: 2014.02.25 12:57:28,811 Starting SC servers
1: 2014.02.25 12:57:28,812 Starting SC authentication server on UDP port: 1812
1: 2014.02.25 12:57:28,818 SC authentication server was successfully started
1: 2014.02.25 12:57:28,818 All SC servers started
```

5. You can also try to authenticate and verify that it is logged in C:\bps\log\trace\sc_trace_TIMESTAMP.log.

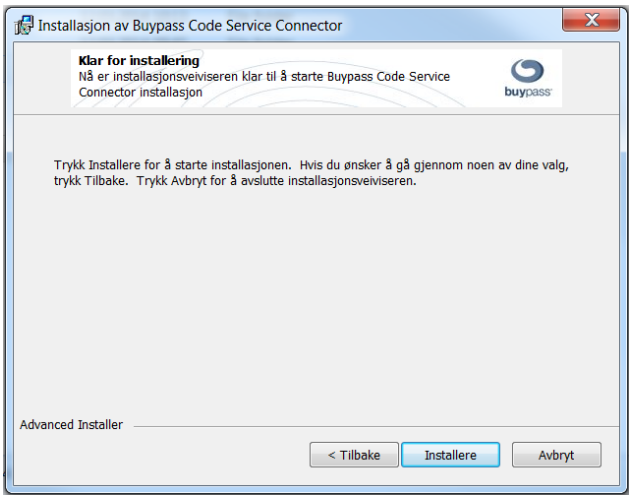
2.3.2 Upgrading guide

This section describes how to upgrade from an earlier version of the Service Connector.

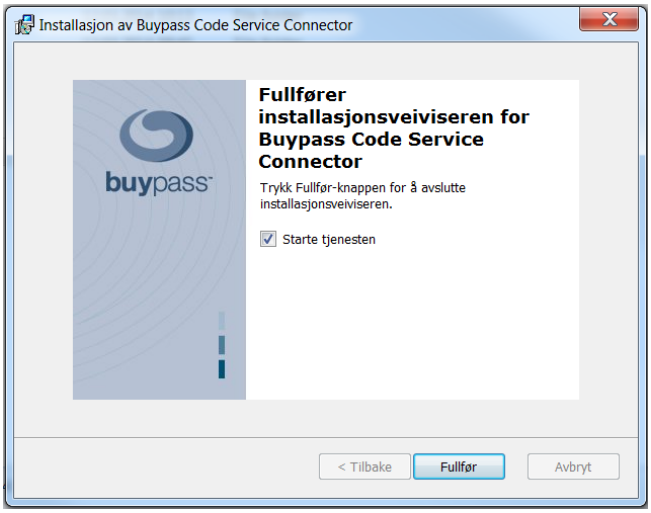
1. Start the install wizard and press ”**Next**.



2. The install wizard will automatically find your certificates and config, press ”**Install**”.



3. The upgrade is finished. Check the ”Start service” box and press ”**Finish**” to start the service.



4. Verify that the SC has started by opening C:\bps\log\trace\sc_trace_TIMESTAMP.log and check that the last rows look like the following:

```
1: 2014.02.25 12:57:28,151 Starting SC Resources ...
1: 2014.02.25 12:57:28,151 Starting SC Encryption Manager
1: 2014.02.25 12:57:28,382 SC Encryption Manager started (cryptographic configuration OK)
1: 2014.02.25 12:57:28,382 Starting SC Communication Manager
1: 2014.02.25 12:57:28,810 SC authenticated and security context established
1: 2014.02.25 12:57:28,811 SC Communication Manager started
1: 2014.02.25 12:57:28,811 Starting SC Radius Proxy Manager
1: 2014.02.25 12:57:28,811 SC Radius Proxy Manager started
1: 2014.02.25 12:57:28,811 SC User Resolver Manager started
1: 2014.02.25 12:57:28,811 All SC Resources started successfully
1: 2014.02.25 12:57:28,811 Starting SC servers
1: 2014.02.25 12:57:28,812 Starting SC authentication server on UDP port: 1812
1: 2014.02.25 12:57:28,818 SC authentication server was successfully started
1: 2014.02.25 12:57:28,818 All SC servers started
```

5. You can also try to authenticate and verify that it is logged in C:\bps\log\trace\sc_trace_TIMESTAMP.log.

2.3.3 Configuration parameters

If you wish to modify the default SC configurations this is done in C:\bps\release\[version]\config\properties\cnl\bpc\sc\scconfig-local.properties. The “sc” service has to be restarted before new configurations become active.

Parameter and default value	Description
Log paramater	
cfg.gen.general.logger_type=1	Specifies what logger type to use 0 - void logger 1 - console logger (stdout/stderr) 2 - file logger, specified by file_log_dir
cfg.gen.general.file_log_dir=/bps/log/	Specify log path for log, only used if logger_type is 2
cfg.gen.general.tracer_type=1	Specifies what tracer type to use 0 - void tracer 1 - console tracer (stdout/stderr) 2 - file tracer, path specified by file_trace_dir
cfg.gen.general.trace_level=8	Trace lever for the server, primary used for debuging 0 - no trace .. 8 - maximum trace
cfg.gen.general.file_trace_dir=/bps/log/trace/	Specify log path for trace, only used if tracer_type is 2
cfg.gen.general.print_properties=true	Specifies if configurations should be written to trace on start up of Service Connector.
Networking configuration	
cfg.gen.io.client_socket_read_wait=30000	Specifies socket timeout for read operations against Buypass Code Server – in milliseconds
cfg.gen.io.max_raw_message_bytesize=2097152	Maximum packet size between the SC and the Buypass Code Server server (in bytes)
cnl.bpc.sc.rasurl=https://ras.buypass.no/ras2/	Specifies the Buypass Code Server (RAS) URL
cnl.bpc.sc.auth_port=1812	Specifies the Radius Authentication port
cfg.gen.io.bind_ip=	Can be used on a multi-homed host for only accepting connect requests to one of its addresses. If not set, it will default accepting connections on any/all local addresses
Start up	
cnl.bpc.sc.halt_on_startup_remote_initialization_error=true	Specifies if SC should stop if it can’t contact the Buypass Code Server
Radius duplicate handling	

cnl.bpc.sc.duplicate_window_time=30000	Duplicate package handle timeout in milliseconds
cnl.bpc.sc.duplicate_window_size=5000	Duplicate package handle max cache size
Key and certificate configuration	
cnl.bpc.sc.keystore.path= /bps/tools/jarsigning/512keystore	Specifies the physical path to the signing certificate used by the service connector. This file authenticates this instance of the service connector
cnl.bpc.sc.keystore.alias=AUTO	Specifies the key file alias. If the key file contains only one entry, please set this value to AUTO. If the key file contains more than one entry, the correct alias must be specified
cnl.bpc.sc.keystore.type=AUTO	Specifies key file type JKS - Java Key Store PKCS12 - PKCS12 key file AUTO - auto detect key file type based on file extension (PKCS12 files has .p12 extensions, JKS has no extension)
cnl.bpc.sc.keystore.password=test123	Specifies the signing certificate password
cnl.bpc.sc.encryption_certificate.path= /bps/tools/jarsigning/512.crt	Physical path to encryption certificate used to encrypt kommunication between the SC and Buypass Code Server
cnl.bpc.sc.node_id=0	Specify when you use more than one Service Connector per Service Connector certificate to guarantee unique ID per SC

2.3.4 Server logging

All trace log files can be found in C:\bps\log\trace\
All access log files can be found in C:\bps\log\access\
Error log files can be found in C:\bps\log\error\ or C:\bps\release\[version]\log\

2.3.4.1 Configuration parameters for log rotation

The SC can rotate/archive log files based on time and/or size. The table shows configuration parameters and examples of different configurations. Choose one for each type of log and put it in C:\bps\release\[version]\config\properties\cnl\bpc\sc\scconfig-local.properties.

Parameters and example configurations	**Description**
Trace log	
cfg.gen.general.tracer_type=6	Specifies type of log rotation 6 = Time based (or time and size based) 7 = Size based
cfg.gen.general.tracer_history=3	Specifies the number of archive files to store

cfg.gen.general.tracer_rollover_pattern=hourly	Specifies how often rotation should happen minutely = Every minute hourly = Every hour daily = Every day weekly = Every week monthly = Every month
cfg.gen.general.tracer_max_size=5mb	Specifies maximum size of active file before rotation happens. Size in km, mb or gb
Example of configurations for trace log	
Time dependent	
cfg.gen.general.tracer_type=6 cfg.gen.general.tracer_history=3 cfg.gen.general.tracer_rollover_pattern=hourly	Rotates every hour with maximum 3 archive files
Size dependent	
cfg.gen.general.tracer_type=7 cfg.gen.general.tracer_history=10 cfg.gen.general.tracer_max_size=5mb	Rotates when active file is 5mb with maximum 10 archive files
Time dependent with size limit	
cfg.gen.general.tracer_type=6 cfg.gen.general.tracer_history=3 cfg.gen.general.tracer_rollover_pattern=hourly cfg.gen.general.tracer_max_size=5mb	Rotates every hour or when active file is 5mb with maximum 4 archive files
Access log	
cfg.gen.general.access_logger_type=6	Specifies type of log rotation 6 = Time based (or time and size based) 7 = Size based
cfg.gen.general.access_history=3	Specifies the number of archive files to store
cfg.gen.general.access_rollover_pattern=hourly	Specifies how often rotation should happen minutely = Every minute hourly = Every hour daily = Every day weekly = Every week monthly = Every month
cfg.gen.general.access_max_size=5mb	Specifies maximum size of active file before rotation happens. Size in km, mb or gb
Example of configurations for access log	
Time dependent	
cfg.gen.general.access_logger_type=6 cfg.gen.general.access_history=3 cfg.gen.general.access_rollover_pattern=hourly	Rotates every hour with maximum 3 archive files

Size dependent	
cfg.gen.general.access_logger_type=7 cfg.gen.general.access_history=10 cfg.gen.general.access_max_size =5mb	Rotates when active file is 5mb with maximum 10 archive files
Time dependent with size limit	
cfg.gen.general.access_logger_type=6 cfg.gen.general.access_history=3 cfg.gen.general.access_rollover_pattern=hourly cfg.gen.general.access_max_size =5mb	Rotates every hour or when active file is 5mb with maximum 4 archive files
Error log	
cfg.gen.general.logger_type=6	Specifies type of log rotation 6 = Time based (or time and size based) 7 = Size based
cfg.gen.general.logger_history=3	Specifies the number of archive files to store
cfg.gen.general.logger_rollover_pattern=hourly	Specifies how often rotation should happen minutely = Every minute hourly = Every hour daily = Every day weekly = Every week monthly = Every month
cfg.gen.general.logger_max_size=5mb	Specifies maximum size of active file before rotation happens. Size in km, mb or gb
Example of configurations for error log	
Time dependent	
cfg.gen.general.logger_type=6 cfg.gen.general.logger_history=3 cfg.gen.general.logger_rollover_pattern=hourly	Rotates every hour with maximum 3 archive files
Size dependent	
cfg.gen.general.logger_type=7 cfg.gen.general.logger_history=10 cfg.gen.general.logger_max_size=5mb	Rotates when active file is 5mb with maximum 10 archive files
Time dependent with size limit	
cfg.gen.general.logger_type=6 cfg.gen.general.logger_history=3 cfg.gen.general.logger_rollover_pattern=hourly cfg.gen.general.logger_max_size=5mb	Rotates every hour or when active file is 5mb with maximum 4 archive files

2.3.5 Troubleshooting

If the installation fails for some reason, start by looking for error messages in the log files

C:\bps\log\trace\
C:\bps\log\error\
C:\bps\release\[version]\log\

The following are examples of error messages, what they mean and how to solve the error.

2.3.5.1 Wrong password

```
gen.util.bpc.error.BpcException: Failed to load keyfile /bps/tools/jarsigning/oottgateway.p12
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.loadPrivateKeyCertificate(DataEncryptionServiceFactory.java:127)
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.createDataEncryptionService(DataEncryptionServiceFactory.java:67)
    at cnl.bpc.sc.server.handler.ScEncryptionManager.doStart(ScEncryptionManager.java:52)
    at cnl.bpc.sc.server.handler.ServiceManager.awaitRunning(ServiceManager.java:25)
    at cnl.bpc.sc.server.handler.ScResourceManager.startResources(ScResourceManager.java:27)
    at cnl.bpc.sc.server.socket.ScServer.startup(ScServer.java:36)
    at cnl.bpc.sc.server.socket.ScServer.main(ScServer.java:55)
Caused by: gen.util.bpc.error.BpcException: Failed to load keyfile /bps/tools/jarsigning/oottgateway.p12
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.loadKeyStore(DataEncryptionServiceFactory.java:142)
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.loadPrivateKeyCertificate(DataEncryptionServiceFactory.java:124)
    ... 6 more
Caused by: java.io.IOException: failed to decrypt safe contents entry: javax.crypto.BadPaddingException: Given final block not properly padded
    at sun.security.pkcs12.PKCS12KeyStore.engineLoad(PKCS12KeyStore.java:1304)
    at java.security.KeyStore.load(KeyStore.java:1214)
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.loadKeyStore(DataEncryptionServiceFactory.java:137)
    ... 7 more
Caused by: javax.crypto.BadPaddingException: Given final block not properly padded
    at com.sun.crypto.provider.CipherCore.doFinal(CipherCore.java:811)
    at com.sun.crypto.provider.CipherCore.doFinal(CipherCore.java:676)
    at com.sun.crypto.provider.PKCS12PBECipherCore.implDoFinal(PKCS12PBECipherCore.java:355)
    at com.sun.crypto.provider.PKCS12PBECipherCore$PBEWithSHA1AndRC2_40.engineDoFinal(PKCS12PBECipherCore.java:462)
    at javax.crypto.Cipher.doFinal(Cipher.java:2087)
    at sun.security.pkcs12.PKCS12KeyStore.engineLoad(PKCS12KeyStore.java:1295)
    ... 9 more
```

Above error means that the signing certificate password is wrong. Verify that the password sent to you by SMS is the same as the password found in C:\bps\release\[version]\config\properties\cnl\bpc\sc\scconfig-local.properties for attribute cnl.bpc.sc.keystore.password. Note that 0 (zero) and O as well as I (upper case i) and l (lower case L) can easily be mixed.

2.3.5.2 Unable to load certificate

```
gen.util.bpc.error.BpcException: Failed to load keyfile /bps/tools/jarsigning/oottgateway.p12
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.loadPrivateKeyCertificate(DataEncryptionServiceFactory.java:127)
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.createDataEncryptionService(DataEncryptionServiceFactory.java:67)
    at cnl.bpc.sc.server.handler.ScEncryptionManager.doStart(ScEncryptionManager.java:52)
    at cnl.bpc.sc.server.handler.ServiceManager.awaitRunning(ServiceManager.java:25)
    at cnl.bpc.sc.server.handler.ScResourceManager.startResources(ScResourceManager.java:27)
    at cnl.bpc.sc.server.socket.ScServer.startup(ScServer.java:36)
    at cnl.bpc.sc.server.socket.ScServer.main(ScServer.java:55)
Caused by: gen.util.bpc.error.BpcException: Key file /bps/tools/jarsigning/oottgateway.p12 not found
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.loadKeyStore(DataEncryptionServiceFactory.java:140)
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.loadPrivateKeyCertificate(DataEncryptionServiceFactory.java:124)
    ... 6 more
Caused by: java.io.FileNotFoundException: \bps\tools\jarsigning\oottgateway.p12 (The system cannot find the file specified)
    at java.io.FileInputStream.open(Native Method)
    at java.io.FileInputStream.<init>(FileInputStream.java:138)
    at java.io.FileInputStream.<init>(FileInputStream.java:97)
    at cnl.bpc.common.adapter.DataEncryptionServiceFactory.loadKeyStore(DataEncryptionServiceFactory.java:135)
    ... 7 more
```

Above error means that the signing certificate can't be loaded by the SC. Verify that the signing certificate that was sent by mail is located in C:\bps\tools\jarsigning\ and that the cnl.bpc.sc.keystore.path attribute in C:\bps\release\[version]\config\properties\cnl\bpc\sc\scconfig-local.properties points to the certificate.

2.3.5.3 Port in use

```
ERROR:
2014.02.25 12:41:37,155 Unable to start SC authentication server at port 1812
Address already in use: Cannot bind
java.net.BindException: Address already in use: Cannot bind
    at java.net.DualStackPlainDatagramSocketImpl.socketBind(Native Method)
    at java.net.DualStackPlainDatagramSocketImpl.bind0(DualStackPlainDatagramSocketImpl.java:81)
    at java.net.AbstractPlainDatagramSocketImpl.bind(AbstractPlainDatagramSocketImpl.java:95)
    at java.net.DatagramSocket.bind(DatagramSocket.java:376)
    at java.net.DatagramSocket.<init>(DatagramSocket.java:231)
    at java.net.DatagramSocket.<init>(DatagramSocket.java:284)
    at gen.io.server.socket.ServerSocketAcceptor.startServer(ServerSocketAcceptor.java:133)
    at gen.io.server.socket.ServerSocketAcceptor.startUdpServer(ServerSocketAcceptor.java:111)
    at gen.io.server.socket.SocketServer.startUdpServer(SocketServer.java:70)
    at gen.io.server.socket.SocketServer.startUdpServer(SocketServer.java:58)
    at cnl.bpc.sc.server.socket.ScServer.startAuthenticationServer(ScServer.java:77)
    at cnl.bpc.sc.server.socket.ScServer.startServers(ScServer.java:86)
    at cnl.bpc.sc.server.socket.ScServer.startup(ScServer.java:37)
    at cnl.bpc.sc.server.socket.ScServer.main(ScServer.java:55)
```

Above error means that the port that the SC is trying to use for Radius communication is already in use by another application. Close the application that is using the port or set another port that the SC can use for Radius communication by specifying it for attribute cnl.bpc.sc.auth_port in C:\bps\release\[version]\config\properties\cnl\bpc\sc\scconfig-local.properties (requires version 7.26.X.X).