Example of How to Create a Secure Channel

* Given a PlainTCPChannel object *ch* do:
* Create a Mac object *mac*.
* Set *mac* with a suitable secret key. (The same key has to be used by both parties using the channel).
* Create an AuthenticatedChannel object with *ch* and *mac*.

//Decorate a PlainTcpChannel with authentication and then with encryption - order is important for security:

Mac mac = null;

try {

mac = MacFactory.getInstance().getObject(""CBCMacPrepending(TripleDES)" ");

} catch (FactoriesException e) {

e.printStackTrace();

}

SecretKey keyMac = mac.generateKey(168);

try {

mac.setKey(keyMac);

} catch (InvalidKeyException e) {

e.printStackTrace();

}

AuthenticatedChannel authenChannel = new AuthenticatedChannel(ch, mac);

SymmetricEnc aesEnc = null;

try {

aesEnc = SymmetricEncFactory.getInstance().getObject("CBCEncRandomIV");

} catch (FactoriesException e) {

e.printStackTrace();

}

SecretKey keyEnc = aesEnc.generateKey(128);

try {

aesEnc.setKey(keyEnc);

} catch (InvalidKeyException e) {

e.printStackTrace();

}

**EncryptedChannel secureChannel = new EncryptedChannel(authenChannel, aesEnc);**