



Nabishi FaxEncryption Appliance

Quick Guide

February 3rd, 2010

Nabishi UK Ltd
16c Upton Road
Tilehurst
Reading, Berkshire RG30 4BJ
Tele: 0118 943 3311 – Fax: 0118 943 3311
Sales@nabishi.com
www.securevoice.co.uk

Quick Guide

Installation of the Nabishi FaxEncryption appliance

The solution consists of a black box (the Nabishi FaxEncryption appliance) which needs to be connected on the one hand to an analogue phone line (either directly to the Public Switched Telephone Network or indirectly via a local PBX) and on the other hand to a standard fax device. The fax device does not form part of the product and must be user supplied.



USB ports

Local fax device

The Nabishi FaxEncryption appliance comes with an external USB based modem which needs to be connected with one of the USB ports and the external phone line.

The user supplied fax device shall be connected to the second (from left to right) RJ11 port.

Finally the appliance requires a USB token to be plugged-in in order to allow encrypted fax transmission or reception.

The Nabishi FaxEncryption appliance needs no user intervention whatsoever when being installed as it comes pre-configured and ready to run. It has a power button on the lower right hand side. When pressed the green power indication LED will light up and the device needs approximately 2 minutes to boot up and perform self test functions before being operational. You will notice that the LCD screen will display "Nabishi - FaxEncryptor 2.0" at this moment.

Creation of USB tokens

A separate Key Management system is provided on a special notebook. It can be used to create machine tokens and optionally user tokens. Those tokens are implemented as smart cards which allow for RSA key generation as well as certificate storage. All tokens generated with this specific key management form a trust group enabling the secure communication with each other effectively precluding any 3rd party from maliciously participating in the encrypted communication.

For each fax appliance one needs a separate machine token however there is no specific allocation between those tokens and the appliances.

User tokens can also be generated and should be handed over solely to specific persons who could ensure with their user token that faxes destined specifically for them will not be decrypted and printed unless they plug in their user token.

Once the Key Management system is started, the Return button will activate the login screen. The user name is "CA" and the initial password is "Nabishi 09!". The following menu will be shown:

```
-- Nabishi FaxEncryption CA Main Menu -----  
  
1. Generate Token  
2. Show Token info  
3. Initialize CA  
4. Show CA info  
5. Change password  
6. Exit  
7. Poweroff  
  
Your choice?
```



The very first action is to initialize the Certification Authority (function 3) which creates new key material and a new trust group. Please be aware of this function. You cannot add further tokens for the same trust group if you create a new CA.

If you do initialize a new CA you must provide the following information:

```
-- Nabishi FaxEncryption Generate CA --  
  
Please enter your 2 letter country code :  
Please enter your province name       :  
Please enter your city name           :  
Please enter your organization name    :  
Please enter your email address       :
```

Once a CA is created you can then generate tokens for each of your appliances and each user with a private mailbox on the Nabishi FaxEncryption appliance. Please plug in one of your hardware tokens and use function 1 to invoke the following screen:

```
-- Nabishi FaxEncryption Generate Token -----  
  
1. Create user token  
2. Create machine token  
3. Abort  
  
Your choice? :
```



You will be asked to provide a user or machine identifier respectively. This will start the creation of a RSA key pair on the token device and the generation of a respective certificate by the CA. Any prior content of the token will be overwritten! Once the process is finished the tokens can be immediately used with any of the Nabishi FaxEncryption appliances.

Standard operation of the Nabishi FaxEncryption appliance

In order to transmit secured fax documents the user shall use the fax device according to its operating manual. There is no special configuration required to inter-work successfully with the Nabishi FaxEncryption appliance. When sending a document the user shall dial the remote fax number of the device he wants to reach.



It must be ensured though that a machine or user tokens (or both) are plugged into both the transmitting and receiving appliance during the transmission process.

The Nabishi FaxEncryption appliance acts as a fully automatic store and forward device. It will receive the fax document locally and convert it into a TIFF formatted document. Then it will dial the number as provided by the user originally on the fax machine. The connection will be made to the remote Nabishi FaxEncryption appliance using its V.34 data modem. The remote appliance will return its own public key which is then used on the local appliance to authenticate the remote appliance as legitimate member of the same trust group. Next this remote public key is used to encrypt the locally generated symmetric AES key. The above TIFF document will be signed on the local appliance using its own private key and then encrypted with the AES key as just generated. The result is transmitted in the same modem session together with the encrypted AES key and its own local certificate.

The remote Nabishi FaxEncryption appliance will decrypt the TIFF document and use the sender's certificate to authenticate the sender as member of the same trust group and verify the signature of the TIFF document to ensure its integrity. As a next step the remote Nabishi FaxEncryption appliance will deliver the document in a standard fax transmission to the remote fax machine.

As a result the user will just send and receive fax documents ordinarily using his own fax devices. He will not notice any deviation from a procedure without the Nabishi FaxEncryption appliance involved at all. The overall transmission process from end to end lasts slightly longer but the actual transmission over the Public Switched Telephone Network will effectively be much faster than usual.

User specific operation of the Nabishi FaxEncryption appliance

Additionally to the above standard method of sending/receiving encrypted faxes a sender can also address individual users as identified by their specific user tokens. In such case the sender dials a user specific prefix to the remote fax number of the device he wants to reach.

Example:

Remote User ID:	001
Remote Fax number:	0123456
Dial sequence:	001#0123456

Thus if one wants to reach the remote fax machine in general then dial "0123456", but if one wants to ensure that only user "001" can see the document then dial "001#0123456".

On the receiving end the fax document will remain encrypted within the Nabishi FaxEncryption appliance until such time that the user token "001" is plugged into the appliance. Only then the decryption will take place and the document is printed on the local fax machine.