



FaxEncryption Appliance

Problem

The communication infrastructure forms a fragile foundation of our information society. In particular, insufficient security on the information highway causes substantial financial damage to our economy due to industrial espionage. Therefore, it is essential to protect sensitive information from unauthorized access or manipulation and to prevent severe consequences. Telephone and facsimile services on connection-oriented networks - still the most widely deployed communication medium - are particularly exposed to attacks.

Solution

The Nabishi FaxEncryption appliance developed by Nabishi UK, provides secure authentication and encryption as front-end device to any regular fax machine. In a user-friendly and easy manner, the Nabishi FaxEncryption secures your communications and protects your assets from eavesdropping and manipulation by both passive and active attackers.

Features

The Nabishi FaxEncryption appliance has been designed as a store-and-forward device. Independent of the fax machine connected to it, the FaxEncryption appliance will always attempt to forward the fax message at full V.34 speed of 33,6 kbit/s over the PSTN lines. In addition to its standard analogue mode of operation the appliance supports optionally digital transmission (ISDN)

of G3 Fax documents. Finally it can optionally act as a Fax to Email gateway and deliver the fax documents encrypted using IP protocols.

A separate key management device provides for the generation and distribution of digital certificates. The FaxEncryption appliances can be delivered without this management station and pre-configured certificates. Customers have also the option to purchase the management station and take care for the key management independently.

The appliance uses RSA or ElGamal private/public key pair methods with a key length of 3072 bits for the purpose of signing and encrypting. SHA-2 is used as hash function for the purpose of assuring the integrity of data transmitted and preventing thus any man-in-the-middle attack. The actual encryption takes place on the basis of AES-256 while the respective symmetric keys are protected by the above RSA or ElGamal methods.

The key management device is used to initiate the creation of an individual private/public key pair directly on and by the Fax Encryption appliance. The public key is then transferred back to the key management device which creates a X.509 certificate by digitally signing this public key. The certificate is returned to the appliance while the private key never leaves it. In result each appliance can authenticate each other appliance belonging to the same group as defined by the key

management device. Each appliance can encrypt faxes towards any other appliance individually and the respective counter part can decrypt the message and verify its integrity.

Optional Features

Smart Card technology can be used to further strengthen the security provided by the solution.

A USB dongle device will act as smart card reader and smart cards personalized on a per device and/or per user basis are delivered as a bundle. When equipped with this option the Nabishi FaxEncryption appliance will use the smart card to generate the private/public key pairs and the decryption process of the symmetric keys used in the AES-256 encryption will take place on the smart card. This method ensures that the private keys of the RSA process will never leave the smart card.

When user based smart cards are created and delivered the Nabishi FaxEncryption appliance is enabled for a mailbox approach to receiving fax documents. The sender can specify a special extension to the normal fax number thus addressing a personal mailbox at the receiving end. Instead of forwarding the document directly to the fax device the appliance will store it on behalf of the person selected by the sender. Just upon plugging his/her USB dongle into the appliance all stored fax documents of the respective mailbox will be forwarded to the locally connected fax device.



Technical specification

Operational Mode

- Fully automatic encryption/ decryption
- Store-and-Forward architecture
- Plug&Play installation
- No user intervention required
- Secure Token Option

Symmetric Encryption

- AES-256

Asymmetric Encryption

- RSA or ElGamal (3072bits key)
- Key generator included in appliance

Authentication

- X.509 key certificate

Key Management

- Pre-configured or by management system on- or offsite

Communication

- V.34 modem supports up to 33,6 kbit/s

Conformity

- Conforms to EN 55024, EN 55022 and 60950

Processing Unit

- Dimensions: 323 x 69 x 254 mm
- Weight: 4,5 kg
- Internal CompactFlashMemory
- Interfaces: 2 x analogue lines RJ11
1 x Ethernet 100BaseT
- External AC adapter 220V

Nabishi UK Ltd
16c Upton Road,
Tilehurst, Reading, Berks,
RG30 4BJ. England,
United Kingdom.
Tele +44 (0) 118 943 3311
Fax +44 (0) 118 943 3366