

## Sirrix. FaxEncryption Appliance

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

#### Features

The Sirrix.FaxEncryption appliance has been designed as a store-and-forward device. Independent of the fax machine connected to it, the Sirrix.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 (ISDN) and IP

transmission (Fax over IP) of G3 Fax documents. Finally, it can optionally act as a Fax to E-mail gateway and deliver the fax documents encrypted to any E-mail address.

A separate key management device provides for the generation and distribution of digital certificates. The Sirrix.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 the RSA private/public key pair method with a key length of 8192 bits for the purpose of key encryption. This very long appliance-based RSA key pair is regenerated from scratch each time when the appliance reboots.

SHA-2 is used as hash function for the purpose of assuring the integrity and authenticity of data transmitted. The actual encryption takes place on the basis of the AES-256 method with a protection of the respective symmetric keys by the above RSA key.

The key management system is used to initiate the creation of an individual private/public key pair with a key length of 2048 bits directly on and by a USB-based tamper-proof smart card device. The public key is then provided to the key management system, while the private key never leaves it. The management system

creates a X.509 certificate by digitally signing the public key using an 8192 RSA key pair and providing it back to the smart card. In result, each appliance can authenticate every other appliance belonging to the same group as defined by the key management device. Each appliance can encrypt faxes towards any other appliance in the same group and the respective counter part can decrypt the message and verify its integrity.

The sending device will create new AES-256 symmetric keys for each individual fax transmission and encrypts one with the public key (2048 bits) of the receiving USB smart card and the other with the public key (8192 bits) of the receiving device. This combination ensures a top level encryption during the transmission phase and the use of a separate security token for the local protection of sensible documents.

#### Optional Features

The smart card devices can also be personalized on a per user basis. In such case the sender can specify a special extension to the normal fax number and thus ensure that only the targeted person will be able to receive the facsimile. Instead of forwarding the document directly to the fax device, the receiving appliance will store it. Just upon plugging the right USB device into the appliance, the stored fax document will be decrypted and forwarded to the locally connected fax device.

## Sirrix. FaxEncryption Appliance



### Technical specification

#### Operational Mode

- Fully automatic at send and receive side
- Send/receive clear faxes possible
- Store-and-forward architecture
- Plug&Play installation
- No user intervention required
- Optional addressee-dependent encryption (Decryption only by addressee via secure token)
- Persistent storage fully encrypted

#### Symmetric Encryption

- AES-256, optionally customer-specific

#### Asymmetric Encryption and Authentication

- RSA (8192 bits) key pair on appliance
- RSA (2048 bits) key pair on smart card
- Key generator included in appliance
- X.509-based certificate management

#### Random Key Generation

- Hardware-based random key generator
- Build-in security module

#### Key Management

- Certification Authority/PKI supported management system, on- or offsite

#### Communication

- Fax transmission according to CCITT/ITU G3 recommendation
- Works with any Super G3 and G3 fax unit
- V.34 modem supports up to 33,6 kBit/s
- Supports fax transport over digital lines (ISDN) and over Internet Protocol (IP) (optionally)

#### Conformity

- Conforms to EN 55024, EN 55022 and 60950

#### Processing Unit

- Dimensions: 323 x 69 x 254 mm
- Weight: 4,5 kg
- Internal CompactFlash-Memory
- Interfaces:
  - 2 x analogue lines
  - 1 x digital BRI (optionally)
  - 1 x Ethernet 100BaseT
- External AC adapter 115-220V