TELETEC
CORPORATION

General System Features

Architecture and Network

Fax Encryption Appliance

Highly secured store-and-forward encryption gateway. The TelFaxEncryption *ix* is placed between a standard fax device and the communication line. Physical communication between the local fax device and the FaxEncryptor is based on Fax G3 operation.

Analog Line Connectivity (PSTN)

This feature enables the transmission of encrypted faxes over the analog PSTN.

Digital Line Connectivity (ISDN)

(optional)

This feature enables the transmission of encrypted faxes over a digital subscriber line (ISDN).

IP Network Connectivity

(optional)

This feature enables the transmission of encrypted faxes over IP-based networks. E.g., public networks as the Internet or closed networks as a satellite-based transmission infrastructure.

Key Management Server

Central management unit for the creation, personalization and certification of secure tokens. Appliances are managed offline and via secure tokens. No local configuration is necessary.

Standards adherence

FaxEncryptor adheres to a maximum to international standards:

- ITU-T T.30 (interoperable with fax devices according to G3 Fax standards)
- ITU-T V.34 (for analog-line transmission)
- ITU-T I.430/431, ITU-T Q.921, ITU-T Q.931 (for digital-line transmission)
- RFC2460 et al. (for IP-based transmission)
- ITU-T X.509v3 (for digital certificates)

Review of Source Code

Under a special agreement, any customer can review all the cryptographic source code and source code compilation may be jointly executed within the customer's premises.

Management

Overall concept

The appliances are designed to be operated with minimal management efforts. They are stateless and integrate an auto-configuration while boot-up.

The secure authentication of devices and users are based on security tokens that are managed by a central management unit. The management unit takes over the role of a certification authority (CA) and integrates a fully-operational public-key infrastructure (PKI).

Key creation

Secure tokens in physical form of a USB dongle are generated by the key management server. These tokens provide identity as a key prerequisite for each fax encryption appliance.

Administrator Access

Administrators have access to the key management server via a simple GUI. Administrator access to any fax encryption appliance is neither necessary nor permitted.

Reporting

All activities of the fax encryption appliance are reported as an appliance generated fax document transmitted to the local fax device. A local phone directory can be generated on user request while reports on received but waiting fax documents and transmission protocols for fax documents sent are generated automatically.

Provisioning

The fax encryption appliance acts as a ready-to-run store-and-forward device. The rollout of firmware updates for appliances is fully automated and deployment takes place via a signed and encrypted update file applied with a USB storage stick.

PKI Service

The key management server acts also as integrated PKI server. Certification Authorities are created for each fax encryption community and locally generated key pairs are certified centrally by signing the respective public key. The CA is based on a 8192 bit long RSA key pair. All such activities are provided with full automation and require no administrator effort or initiation whatsoever.

Security features

General operation

Device based encryption

Encrypted fax communication is based on the presence of a device specific security token at each end of the line. A secured transmission cannot start without this prerequisite while the receiving side will immediately forward the decrypted fax towards the remote fax device.

User based encryption

The system can additionally support individual security tokens on a user basis. The sender can then specify a specific user at the remote site for whom a document shall be destined.

The document is delivered towards the remote fax device only if the specific user token is present. If not, the document stays encrypted at the receiving fax encryption appliance and a report is printed on the fax device.

Once the respective user applies his security token the document is decrypted and forwarded to the local fax machine.

The following figure shows the multi-level, hybrid cryptographic design of the system:

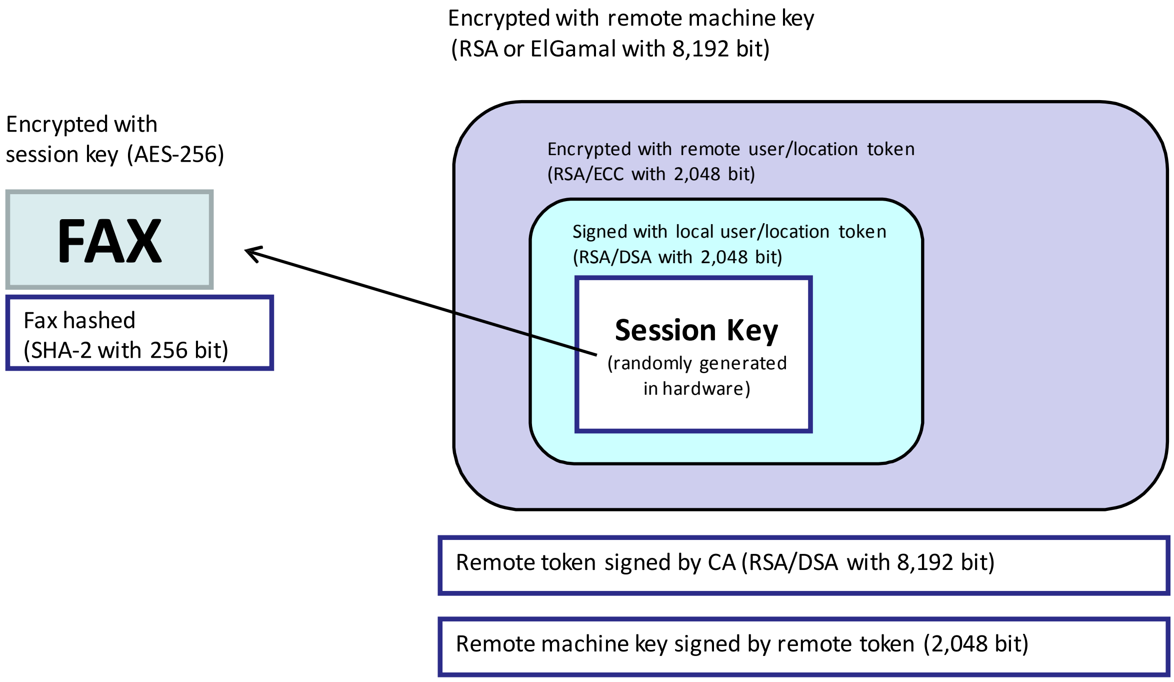
Encrypted with remote machine key
(RSA or ElGamal with 8,192 bit)
Encrypted with
session key (AES-256)
FAX
Fax hashed
(SHA-2 with 256 bit)
Encrypted with remote user/location token
(RSA/ECC with 2,048 bit)
Signed with local user/location token
(RSA/DSA with 2,048 bit)
Session Key
(randomly generated
in hardware)
Remote token signed by CA (RSA/DSA with 8,192 bit)
Remote machine key signed by remote token (2,048 bit)

Figure 1

System security

Stateless design

All relevant cryptographic keys are stored either in the security token or in the security module inside the device. Key handling occurs solely inside these tamper-resistant security devices and never leave them. This includes only keys for authentication purposes and integrity check.

Keys for encryption are not stored persistently inside the device. They are generated right before use, refreshed regularly and are discarded in case of power down / reboot fax encryption.

Persistently stored are only the phone book and received yet not forwarded documents in encrypted form.

On-board security module

The appliance is equipped with an onboard security module, covering 3 crucial security requirements:

a) Trusted Boot and integrity proof of firmware,

b) processing and storage of cryptographic keys and

c) secure random number generation.

The TPM chip holds within its tamper resistant security hardware a cryptographic authentication key enabling a strong identity of each appliance. All long-term key material is stored solely inside the secure hardware module.

Trusted Boot

Based on the TPM chip, a Trusted Boot process is implemented which ensures that the appliance can only be booted with its original firmware or updated with original non-manipulated version.

Hardware based tokens for device and user authentication and user-specific fax document encryption.

The system employs security tokens for user and device authentication and for user-specific fax document encryption.

The security tokens are tamper-protected, the respective private keys are solely processed inside the security token and never leaves them. The keys on the security tokens are certified by the certification authority, provided inside the management unit.

Secure Random Number Generator

The appliances contain a hardware-based (RNG)random number generator inside the security module.

Permanent storage encryption

The appliance is delivered with an integrated full-encryption for its permanent storage. The respective encryption key is secured by the TPM which will only handout this key upon a proper Trusted Boot.

No local access

No local management access at the appliances necessary. Configuration can be loaded by secure tokens.

Communication security

Hybrid encryption

The encryption is realized according to hybrid encryption, using a highly-efficient symmetric cipher for the actual fax encryption and a modern asymmetric (public-key) scheme for key, device and user authentication.

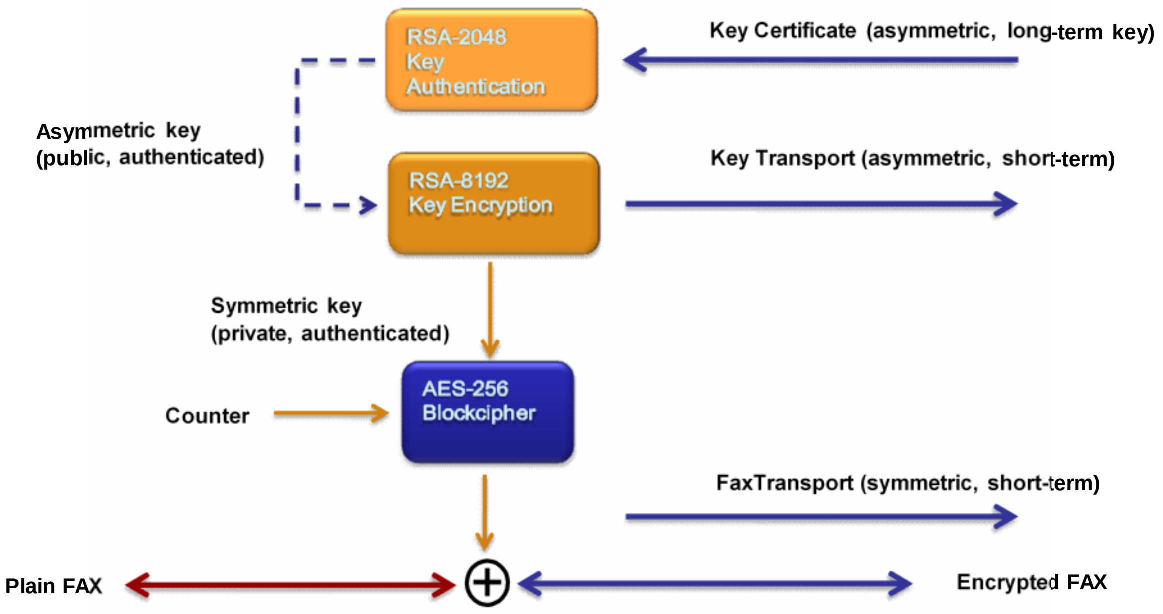
RSA-2048 Key Authentication
Key Certificate (asymmetric, long-term key)
Asymmetric key (public, authenticated)
RSA-8192 Key Encryption
Key Transport (asymmetric, short-term)
Symmetric key (private, authenticated)
Counter
AES-256 Blockcipher
FaxTransport (symmetric, short-term)
Plain FAX
Encrypted FAX

Figure 2

Fax encryption

The actual fax document to be secured is encrypted using an AES-256 key which is continuously freshly generated for each single document on the basis of a hardware security-module generated random number.

Transport key encryption

Transport keys are encrypted, using an asymmetric encryption scheme with 8,192 bit.

Device or user key authentication

User and devices are authenticated, by using an asymmetric encryption scheme and X.509-certificates.

The keys are generated within the security tokens and certified by the certification authority (CA), which is part of the public-key infrastructure (PKI), integrated in the key management server.

User-specific encryption

Faxes can be encrypted for a dedicated receiver. In that case, the transport key is additionally encrypted with the public-key of the receiver (user or device). Then, the received fax can only be decrypted with the respective user/device token.

Asymmetric authentication

RSA 2,048 bit, DSA and ECC on request

Key pair is generated within the secure token. Key is certified by central CA.

Asymmetric encryption (device and user key)

Asymmetric encryption (appliance key) RSA 2,048 bit, ECC on request

Key pair is generated within the secure token. Key is certified by central CA.

RSA 8,096 bit, ElGamal and ECC on request

Key pair is generated within the appliance using the hardware- based random generator. Key is regenerated every 24 hours or on reboot, automatically.

Symmetric encryption

AES256, other on request

Hash functions

SHA-2 256, other on request

Ease of use differentiation	
Design	
Basic operation	The system is used solely via a locally connected standard fax device. No user intervention is required at the fax encryption appliance itself except optionally plugging one's own security token into one of the respective ports.
Sending an encrypted fax	Sending a fax requires no different action when compared with using the same fax device directly on the phone line. The fax encryption appliance works as a transparent black box in between. The device related security token must be present. Additional user based tokens may be attached to the appliance.
Sending an encrypted fax to a specific user	Sending a fax to a specific user is done easily by pre-pending a respective short dial code to the fax number when dialing at the fax machine. The short dial codes are stored inside and are automatically generated and amended upon receiving any fax from the remote user.
Sending a plain text fax	Sending a plain text fax is also possible as an option which is invoked by pre-pending the control sequence to the fax number. The system helps prevent sending unintended plain text faxes to this same number by using the redial button.
Receiving an encrypted fax	No special action is required. The device related security token must be present. Additional user based tokens may also be attached to the appliance. If the sender has destined the fax document generally to the receiving device the appliance forwards it decrypted towards the local fax machine and it simply gets printed. If the sender has destined the fax document towards a specific user the appliance forwards it decrypted towards the local fax machine if (or once) the specific user token is attached to the receiving appliance.
Deployment of new appliances	If an appliance has to be exchanged (e.g. in case of hardware breakdown) the replacement appliance can simply be cabled equivalently at the location of the former appliance. Security tokens shall be plugged off the replaced appliance and are to be attached to the new one. The system is immediately operational and needs no configuration. The phone book will be rebuilt automatically with operating the system.

FaxEncryptor (PSTN-Version) - Appliance Features

Basic data	
Form factor	Gateway appliance
Processor	Intel Atom 1,6 GHz
RAM	512 MB
Interfaces	
Communication ports	FXS port for connection to local fax device FXO port for connection to phone line
Optional ports	ISDN (4x BRI) Ethernet (100Base-T)
Token connectors	2 x USB
Physical	
Dimensions (W/H/D) in mm	320x270x75 mm
Weight	2,5 kg
Power supply	External 90W, 100 - 240V
Security module	integrated, Infineon TPM v1.2 (SLB9535TT)

Offer notes

Used symmetric key length: The system uses for payload encryption the symmetric crypto scheme AES-256 (Advanced Encryption Standard, **standardized by NIST with 256-bit keys).**

Used asymmetric key length: The system uses for key exchange the asymmetric crypto scheme RSA-8192 (RSA Public Key scheme with 8192-bit keys).

Used signature key length: The system uses for key exchange authentication the asymmetric crypto scheme RSA-2048 (RSA PKI with 2048-bit keys in hardware tokens)

Used hash function: The system uses for integrity purposes SHA2-256 with 256-bit keys.

No-Backdoor Warranty : **Teletec Corporation testifies that there are neither backdoors nor hidden channels on the system. Moreover, Teletec testifies that the protocol used in the encryption system is secure against both passive and active attacks, including Adaptive Chosen-Ciphertext and timing attacks.**