



The Secret Of Unconditional Security

CONTENTS

- THE COMPANY 1**
 - THE TEAM.....2
 - OUR CLIENTELE.....2
 - OUR HISTORY3
- UNCONDITIONAL SECURITY..... 4**
 - HOW DOES IT WORK ?4
- PRODUCT OVERVIEW 5**
 - SECURE MESSAGING SOLUTIONS.....6
 - RANDOM KEY PRODUCTION.....8
 - TELEPHONE AND FAX ENCRYPTION.....9
 - CUSTOM SOLUTIONS..... 10
- SUMMARY 11**

mils electronic is a major player in the field of communications- and information security. Our product range includes message cipher systems, telephone and fax encryption devices and random key production equipment. Ever since our founding, the cryptographic functions in our products have relied on the strongest possible encryption algorithms and the unbreakable **One Time Key**¹⁾ encryption method.

As an independent and privately held Austrian company, we are in a unique position to provide our customers worldwide with this highest standard of security.

Private &
Independent



mils electronic is situated in the village of Mils, which gave the company its name. Mils is near the Olympic town of Innsbruck, in Austria's mountainous province of Tyrol.

The excellent reputation that **mils electronic** has gained in the world of information security is based on our principles:

- We use the decades of experience we have gathered to find the best solution for each customer's security demands.
- Our products provide top level security. They are reliable and simple to use.
- We optimize our products to meet each customer's specific needs rather than just selling off-the-shelf merchandise.
- Our relationship with our customers does not end with the product purchase. We provide customer support and consultations for the entire life of the product.

¹⁾ see chapter "Unconditional Security"

THE TEAM

In **mils electronic**, a team of highly qualified information security experts is ready to provide confidentiality for your sensitive data. With its manageable number of employees, **mils electronic** offers a high degree of flexibility and innovation for your projects.

Our sales managers, with their years of experience in the field of message and information security, will identify the right solution for your security demands. They are backed up by a world-wide network of representatives who provide additional pre-sales and after-sales support.

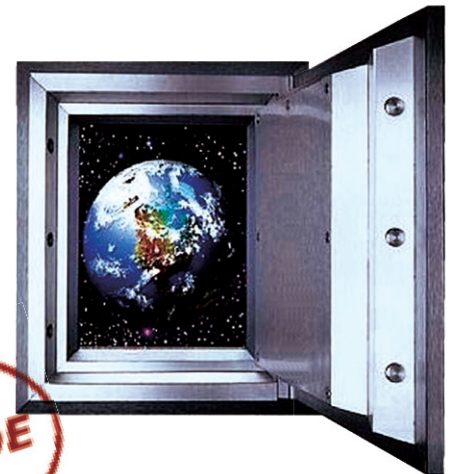
Today's technology must be prepared for the realities of tomorrow; it must identify future trends and pinpoint the opportunities and risks involved. The engineers in our research and development team are continually working on finding solutions and developing concepts to meet these challenges.

The Logistics team guarantees punctual delivery and worldwide lifetime service, including technical adaptations, product training, customer service and follow-up orders.



OUR CLIENTELE

mils electronic is a highly respected adviser to and supplier of clients in more than fifty countries around the globe. Ministries, diplomatic services, military commands, heads of state, intelligence services and law enforcement agencies trust the unbreakable security of our products.



1948

The company was founded by two German experts. The **6723 Key Tape Perforator** was the first product ready for the market.

1967

To avoid export restrictions, the company moved to Austria, a neutral nation, and established a new home in the village of Mils.

1976

Introduction of computerized equipment for key production and data encryption. **mils electronic** presents its first family of microprocessor-controlled random key generators and cipher machines.

1982

In addition to **One Time Key** encryption, stream cipher algorithms of the highest level of security are introduced in the cipher equipment of the company.

1989

mils electronic releases **System 800**, its first cipher system that supports various transmission services.

1993

System 700, mils' first PC-based cipher system is born. The advantages of **System 700** are that it is compatible with standardized hardware and can be used with any telecommunication service.

1998

Introduction of the 3rd generation of key production equipment, the **M615 Key Generator** and the **M650 Tape Puncher**.

1999

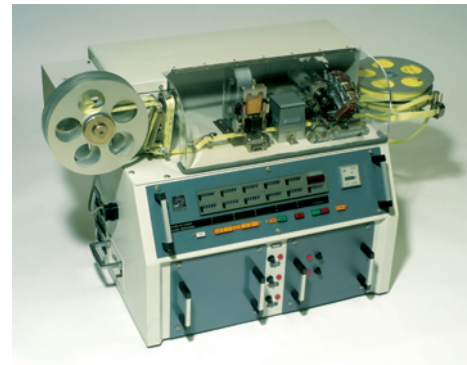
The **M111**, a high speed cryptographic security controller (ASIC) is launched.

2001

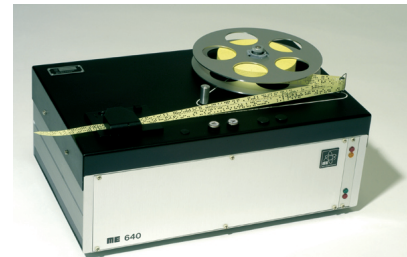
Introduction of **MilsMail** and **MilsFile**. These encryption plugins provide for secure e-mail exchange and protected file storage on PC's.

2004

Release of **MilsMessage**. This Windows application provides secure transmission of sensitive messages via any telecommunication service.



How it all began. The 6723 Key Tape Perforator.



The M640, mils electronics first microprocessor controlled cipher machine.



An M730 Cipher Machine, connected to a telephone modem and an HF - radio.

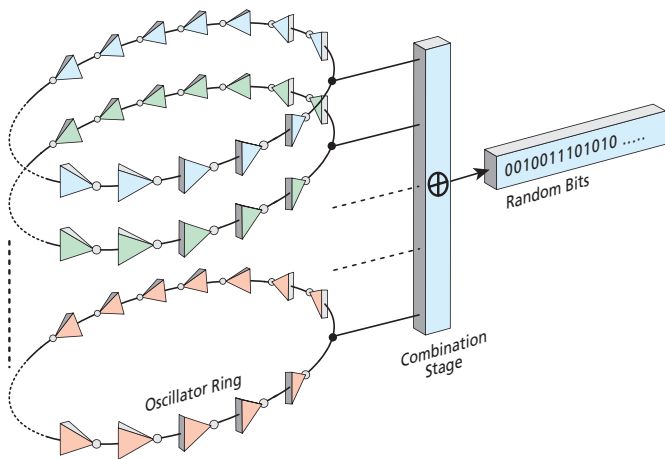


The MilsCard supports all messaging applications with unbreakable security.

UNCONDITIONAL SECURITY

For decades, **mils electronic** has used the **One Time Key (OTK)** method in its cipher systems for encrypting sensitive data. OTK is the only truly unbreakable encryption method. In order to be able to offer our customers the highest degree of secrecy, **mils electronic** applies the OTK method to secure applications such as e-mail, personal data files, and messages.

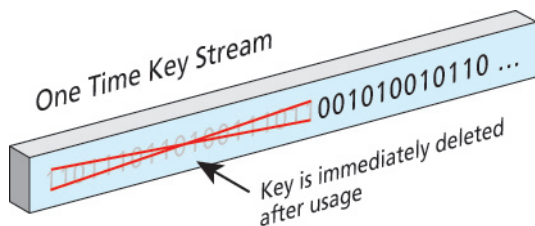
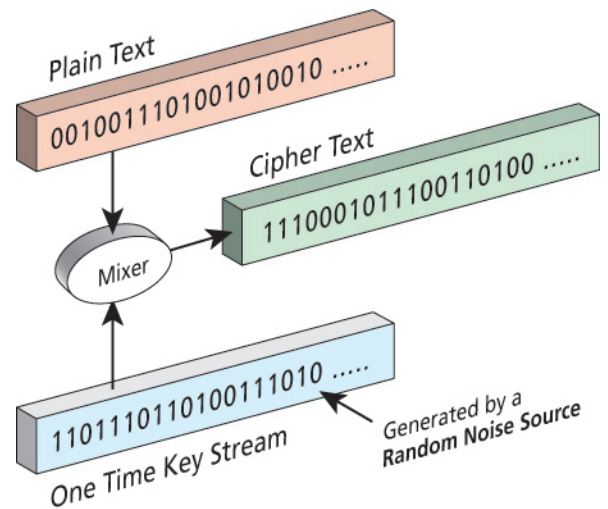
HOW DOES IT WORK ?



The basis of an OTK system is a string of random characters known only to the sender and the intended recipient. This random key stream does not come from an algorithm or mathematical formula. Instead, it is obtained from a true random noise source which derives its randomness from thermal drift and timing jitter effects. This ensures that One Time Keys cannot be reproduced.

The Secret of Unconditional Security

This random key stream is then used for encryption, whereby each bit of the plain text is mixed with one bit of the random key stream. This results in a truly random cipher text that cannot be broken by any power in the world. The cipher text is then posted to the recipient of the message who reverses the process of encryption by using the same random key stream.



Once the One Time Key stream has been used for encryption or decryption, it is immediately destroyed. This guarantees that the same key cannot be reapplied by mistake.

Secure Messaging Solutions

Secure Messaging is one of the core competencies of **mils electronic**. Our long-standing experience in this field has been summarized in a range of personal computer based messaging products:



- **MilsMessage** is a dedicated messaging client for the secure transmission of sensitive messages via e-mail and any other telecommunication service.
- **MilsMail** is a security plug-in for Microsoft Outlook and provides encrypted e-mail exchange at the highest security level.
- **MilsFile** adds unbreakable security to the Windows Explorer. It allows the encryption of files and folders on local or remote storage media.
- **MilsAdministrator** is a Windows application that allows the setup and management of a secure messaging network.
- **MilsCard** is a tamper-proof security module (USB or PC-card) developed by **mils electronic**. It provides hardware-based security for all messaging applications.

Random Key Production

mils electronic offers equipment for the production and distribution of random key sequences for all kinds of cryptographic applications. Windows-based programs generate key sequences of variable size and format which can be printed or stored on removable storage media.



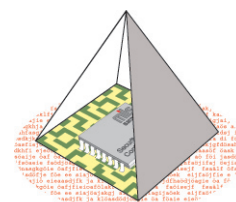
Telephone and Fax Encryption



For the protection of speech, fax and data on various telephone services, **mils electronic** offers secure telephones and stand-alone fax encryption equipment.

Custom Solutions

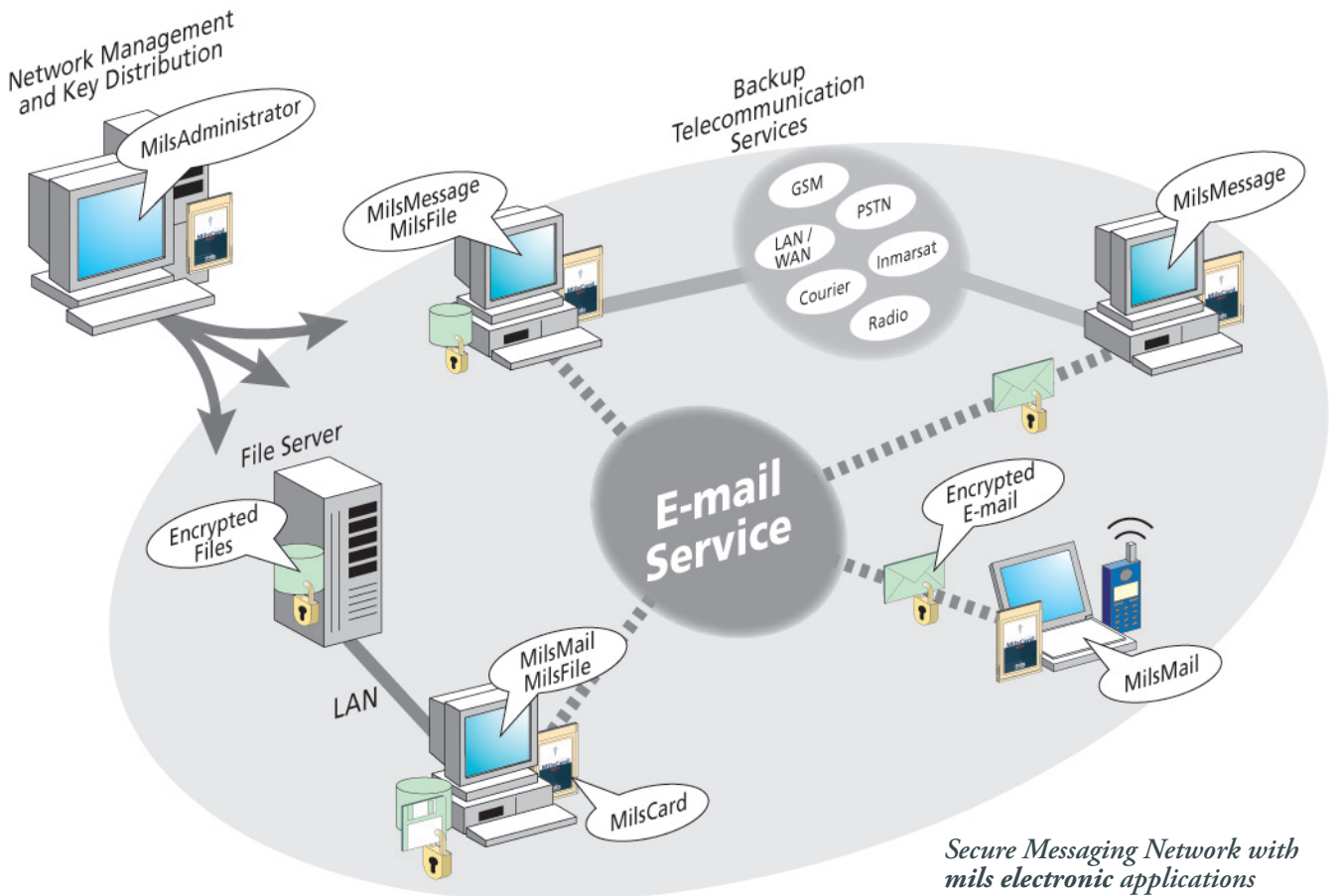
As a responsible provider of top-of-the-line products for protected message exchange, **mils electronic** places high priority on responding to each customer's particular wants and needs. Designing tailor-made solutions for specific requirements and fulfilling special requests are integral parts of **mils electronic's** service.



SECURE MESSAGING SOLUTIONS

Messaging solutions of the highest possible security level have always been the center of **mils electronic's** product strategy. While in former times telecommunication services like tel-ex or direct modem connections played an important role, nowadays communication more and more shifts towards e-mail services.

Taking this development into consideration, **mils electronic** is now ready to provide its customers with a comprehensive range of e-mail centered solutions that additionally support other telecommunication services as backup.



Secure Messaging Network with mils electronic applications

Key Features

- Message exchange is protected by means of the unbreakable **One Time Key** encryption method, by a proprietary stream cipher algorithm from **mils electronic** or by a proprietary block cipher algorithm.
- Key production and network management are completely customer controlled. Encryption algorithms are individually customized.
- All security-related functions are executed in a tamper-proof cryptographic security module (**MilsCard**).
- A **mils electronic** developed security controller (an ASIC chip in the **MilsCard**) provides true random key production and top speed encryption.
- The applications run on all commercially available personal computers (desktops, notebooks, tempest and ruggedized equipment) and the latest Windows version.

MilsMessage

MilsMessage can be considered as a proprietary „e-mail client“ for Windows personal computers. It offers a set of security, transmission and management functions which makes it a complete and top-secure messaging product for government applications. MilsMessage offers:

- Comprehensive message management functions by providing automatically encrypted folders and encrypted message archives
- Transmission via any SMTP / POP3 based e-mail system (Internet standard)
- The use of alternative message transmission services such as HF-Radio, PSTN / ISDN dial-up connections, GSM / Satellite services, ...
- Encrypted e-mail exchange with **MilsMail** users.

MilsMail

MilsMail is a security plug-in for the Microsoft Outlook e-mail client. It provides encrypted e-mail exchange of highest security level while working in the familiar Outlook environment. Encrypted e-mails can be exchanged with other **MilsMail** and with **MilsMessage** users.

MilsFile

MilsFile is an application used for secure file storage. It is an extension of the Windows Explorer and can be applied for encryption and decryption of single files or entire folders on local or remote storage devices.

MilsAdministrator

MilsAdministrator is a Windows application within the messaging network. Its main purposes include network management and the generation and distribution of cryptographic keys.

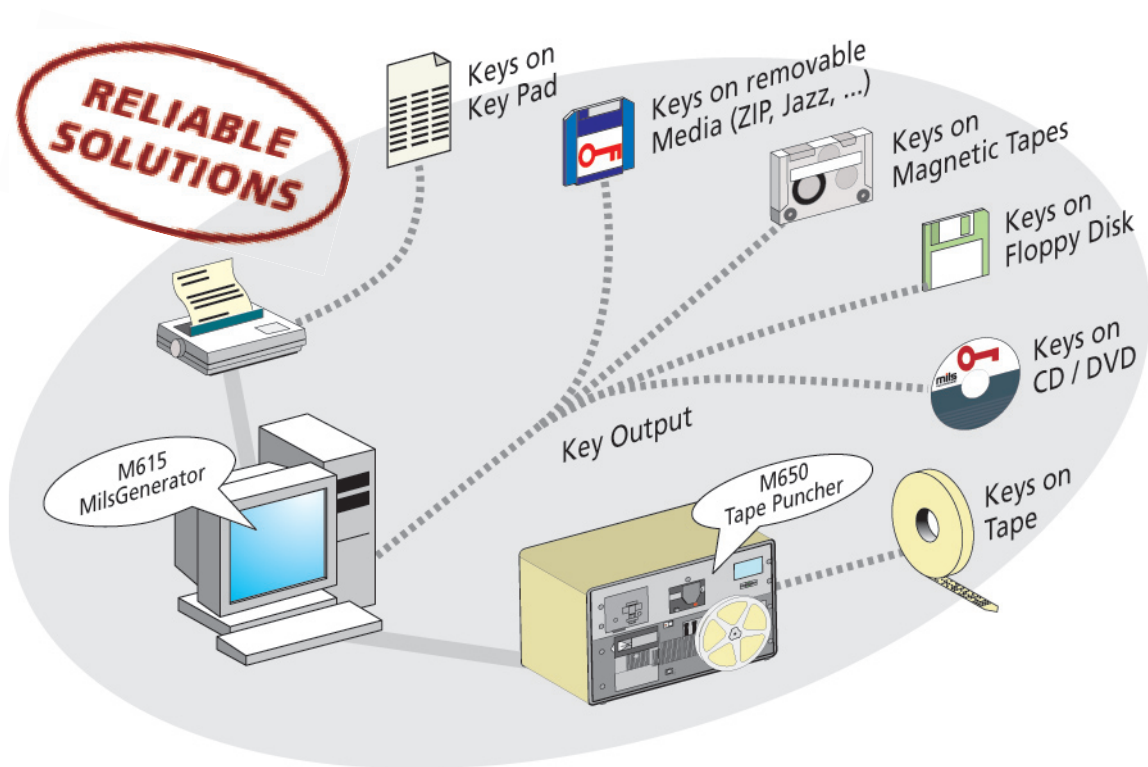


MilsCard

MilsCard is a cryptographic security module, implemented as a USB device or a PC-Card. It works in conjunction with the above mentioned applications and provides secure storage of cryptographic keys and execution or cryptographic algorithms in a protected environment. Every user is provided with an individual **MilsCard**.

RANDOM KEY PRODUCTION

The security level of cryptographic applications is strongly influenced by the quality of the keys that are used. The key production equipment from **mils electronic** relies on hardware-based noise sources that provide true random key sequences. Extensive statistical testing and great flexibility in terms of key size and format makes this equipment the first choice for random key production.



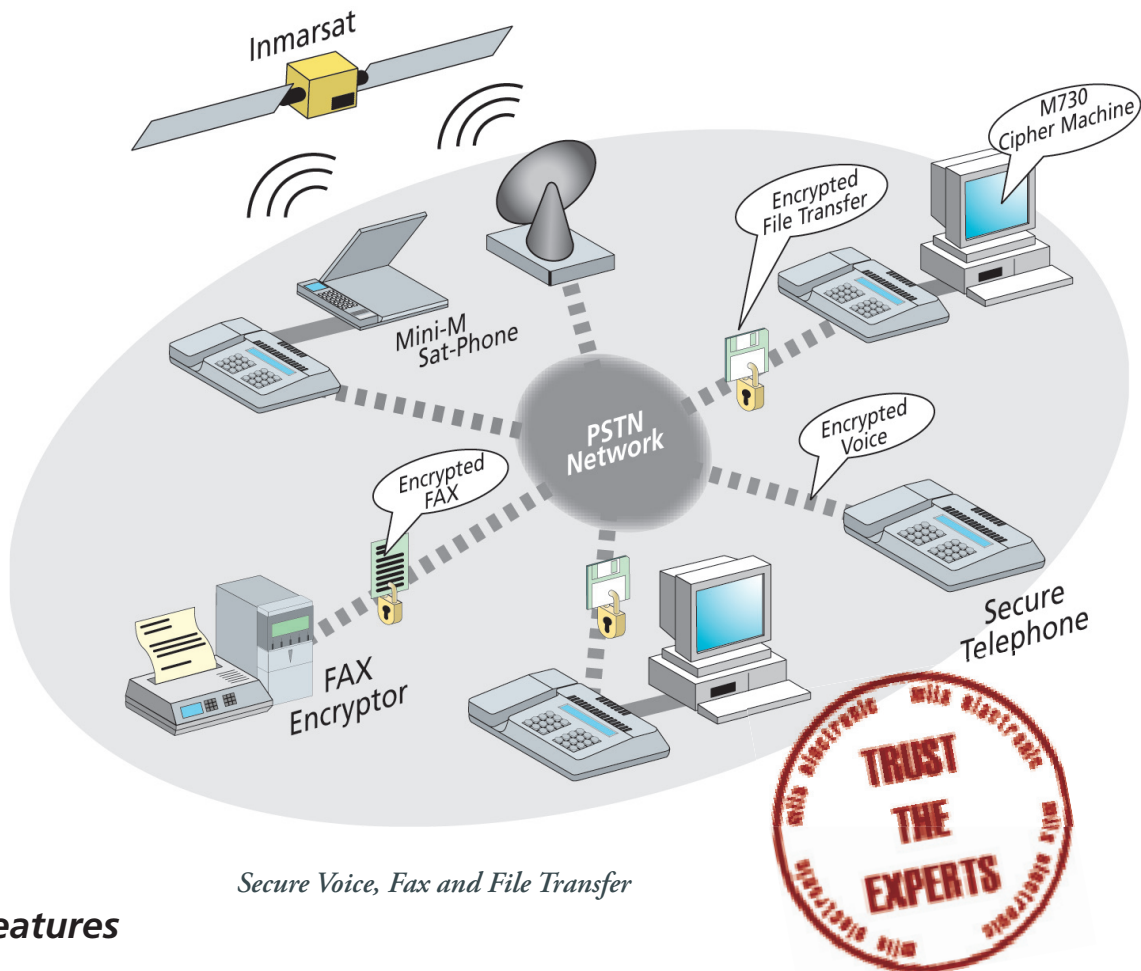
Random Key Production and Distribution with the M615 MilsGenerator

Key Features

- The key production is based on a hardware noise source which guarantees a perfect randomness of the keys.
- Extensive statistical testing ensures the quality of each individual key.
- The size, character set and format of the keys can be varied in many different ways.
- Because the random key generator supports a large number of peripheral devices, the keys can be distributed and used as punched tapes, key pads, key disks and key files.
- Standard personal computers and peripheral devices can be employed.
- Specialized equipment – like the **M650 Tape Puncher** - allows the production of key tapes in a great variety of formats.

TELEPHONE AND FAX ENCRYPTION

To protect speech and data on various telephone services, **mils electronic** offers secure telephones with excellent voice quality. Stand-alone fax encryption equipment is also available and can be used with any Group 3 fax machine.



Secure Voice, Fax and File Transfer

Key Features

Secure Telephone

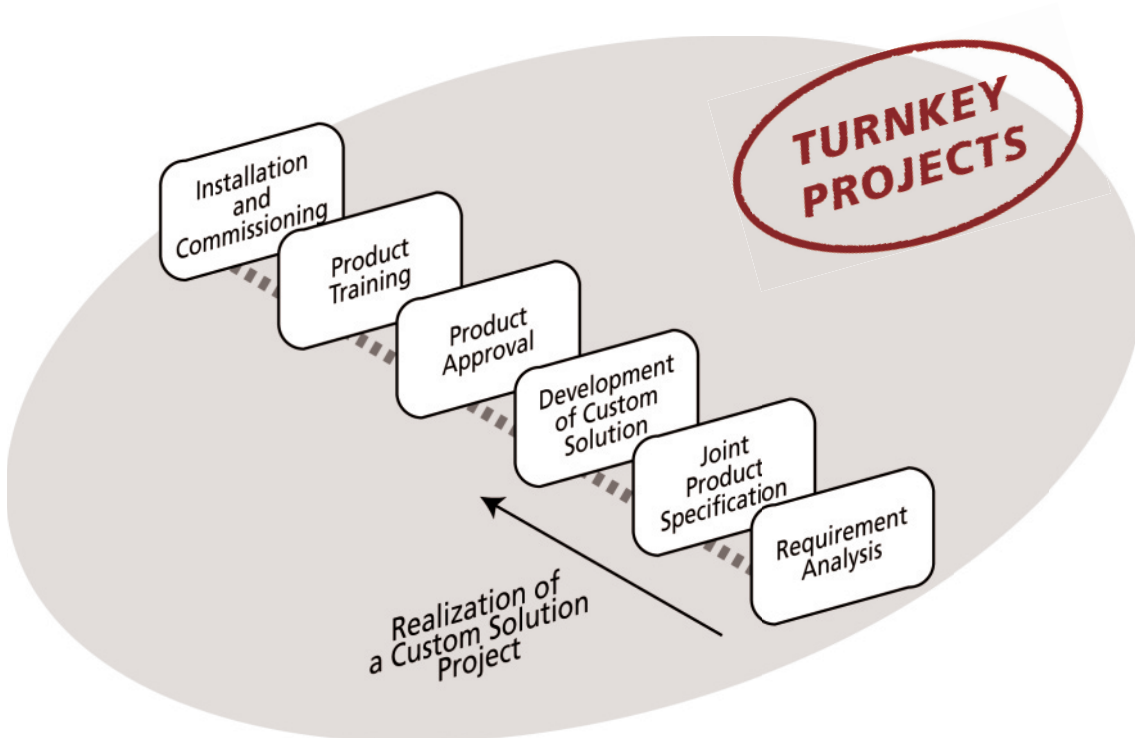
- High security end-to-end protection of voice, data and fax over PSTN telephone lines.
- Excellent voice quality in full duplex, even in encrypted mode.

FAX Encryptor

- Secure fax messaging, compatible with any Group 3 machine and PC fax.
- Compatible with all kinds of telephone channels (PSTN) and with INMARSAT satellite channels.

CUSTOM SOLUTIONS

At **mils electronic**, we welcome the challenge of designing and producing unique solutions for secure data communication and storage. We can work with you to understand your needs and tailor a solution to your exact specifications. Our staff of experienced engineers and cryptology experts can develop customized solutions to satisfy the most demanding security requirements.



Experience

- Development and production of unique message encryption systems according to customers specifications.
- Adaptation of the user interface to several latin and non-latin (e.g. Arabic) languages.
- Implementation of customer specific message management and transmission requirements.
- Adaptation of encryption algorithms according to customers demands.
- Implementation of customer specific statistical tests into key production equipment.
- Hardware adaptations to achieve compatibility with customers existing equipment.

The perfect solution for your security demands not only requires unbreakable encryption. It is rather a question of finding a partner who understands your particular wants and needs and is able to act accordingly.

With **mils electronic** as your supplier, you are on the safe side for now and for the future.

*Private &
Independent*

*Specialized in
One Time Key
Encryption*

*Worldwide
Lifetime
Support*

*Customized
Solutions*



*Top Level
Security*

*Reliable and
Simple to Use
Products*

*More than
50 Years of
Experience*

*Flexibility
& Innovation*





For more information please contact us or visit our homepage:

www.mils.com



Headquarters:

mils electronic gesmbh & cokg

leopold-wedl-strasse 16 • A-6068 mils • austria

tel: +43 (5223) 577 10-0 e-mail: info@mils.com

fax: +43 (5223) 577 10-1 internet: www.mils.com

Apac:

tiara communication sdn bhd (303514-K)

21-2, jalan 65c, pekeling business centre,

off jalan pahang barat, 53000 kuala lumpur, malaysia

tel: +60 (3) 4023 87 33 email: info@tiaracomasia.com

fax: +60 (3) 4023 92 66 internet: www.tiaracomasia.com