

**Total Information Security<sup>®</sup>**  
**By Crypto AG**

---



© Crypto AG / HC6835-E.PPT / hy / 1

©2001 Crypto AG - all rights reserved.

---

**HC-6835**  
**Ruggedized**  
**Security Workstation**



© Crypto AG / HC6835-E.PPT / hy / 2

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation General Applications



- Message Handling
- Processing
  - Data
  - Graphics
  - Fax
  - Images
  - Video
  - Voice
  - Data
- C<sup>4</sup>-I<sup>2</sup> Applications

© Crypto AG / HC6835-E.PPT / hy / 3

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation



### General Specifications

- Ideal ruggedized security workstation for all types of electronic data processing applications, i.e. for E-Mail / Peer Messaging / PC Security (with HC-6360) or VPN Encryption (with HC-7830) or both installed in the same system HC-6835 (with HC-6378)
- Fully ruggedized and absolutely mobile
- Comprehensive Workstation Security including:
  - Access control
  - User identification
  - Disk, file and message encryption
  - Virtual memory encryption
  - VPN encryption

© Crypto AG / HC6835-E.PPT / hy / 4

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation



### Hardware / Software

- Hardware components
- Fully ruggedized Notebook, state-of-the-art Pentium III,  $\geq$  256 MB RAM,  $\geq$  12 GB HDD, DVD / CD ROM Drive / MPEG II, Ethernet 10 / 100 Mbit, 3.5" 1.44 MB FDD, PC Card Slot (Type II), 12.1" Monitor TFT 800x600, Backlight keyboard. Including one parallel, two serial and one Card Bus Type I interfaces.
- Microsoft Windows NT 4.0 operating system
- Microsoft Office 2000 application with integrated secure messaging

© Crypto AG / HC6835-E.PPT / hy / 5

©2001 Crypto AG - all rights reserved.



## HC-6835 Ruggedized Security Workstation Communications



- Public Network
- Private Network
- Telephone lines
- HF / VHF / UHF radio circuits
- Optionally
  - Satellite
  - GSM or ISDN
  - X.25, LANs
  - etc.

© Crypto AG / HC6835-E.PPT / hy / 6

©2001 Crypto AG - all rights reserved.



## HC-6835 Ruggedized Security Workstation

### Secure and Reliable Radio communication



- Built-in HF-Modem
- Point to point & broadcast
- Automatic error correction
- Automatic speed adaptation
- Automatic compensation of Tx/Rx frequency off-set
- Long range HF communication (up to 30,000 km) possible

© Crypto AG / HC6835-E.PPT / hy / 7

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation

### Public / Private Network communication



- Built-in Telephone-Modem
  - Point to point communication
  - E-Mail encryption
  - VPN encryption
- Built-in Ethernet 10 / 100 Mbit
  - E-Mail encryption
  - VPN encryption

© Crypto AG / HC6835-E.PPT / hy / 8

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Accessories



- Field carrying bag for HC-6835 basic unit and accessories
- External ruggedized portable printer
- DC adaptor 10 - 32 V dc
- AC adaptor 100 - 240V ac
- External battery charger
- LS-120 Floppy Drive
- Docking Station
- Mounting kit
- etc.

© Crypto AG / HC6835-E.PPT / hy / 9

©2001 Crypto AG - all rights reserved.



## HC-6835 Ruggedized Security Workstation Versions



- Versions:
  - English
  - French
  - Spanish
  - Arabic-enabled

© Crypto AG / HC6835-E.PPT / hy / 10

©2001 Crypto AG - all rights reserved.



## HC-6835 Ruggedized Security Workstation



### Compatibility



• The HC-6835 Ruggedized Security Workstation is compatible with:

- HC-6830
- HC-6950
- Standard Desktop PC with integrated PC Security
- Standard Notebook with integrated PC Security

© Crypto AG / HC6835-E.PPT / hy / 11

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Environmental Conditions / Climate



### Mil-Standard-810E

- Operating temperature 0°C...+50°C
- Storage temperature -20°C...+70°C
- Humidity 5%...95% RH
- Altitude operating <16,000 ft
- Salt fog 5% salt solution at 35°C, 48h
- Enclosure class IP 54 (IEC 529)

© Crypto AG / HC6835-E.PPT / hy / 12

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Environmental Conditions / Mechanical



### Mil-Standard-810E

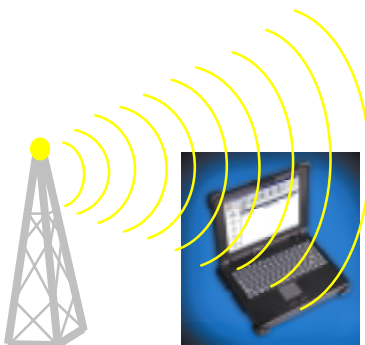
- Shock (operating)  
25g, 6ms (IEC 68-2-29)
- Vibration (operating)  
random 10...500Hz  
1.04g RMS
- Drop  
50 cm
- GB, GF, GMW, MP, NS,  
ARW, GMT

© Crypto AG / HC6835-E.PPT / hy / 13

©2001 Crypto AG - all rights reserved.



## HC-6835 Ruggedized Security Workstation Environmental Conditions / Susceptibility / EMC



### Radiated susceptibility

- Magnetic field
- Electric field

### MIL-STD-461C (RS103 limits)

Radiated susceptibility > 10V/m

© Crypto AG / HC6835-E.PPT / hy / 14

©2001 Crypto AG - all rights reserved.



# HC-6835 Ruggedized Security Workstation



## System Applications

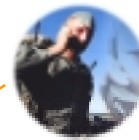
© Crypto AG / HC6835-E.PPT / hy / 15

©2001 Crypto AG - all rights reserved.

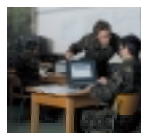
# HC-6835 Ruggedized Security Workstation Military Applications



**Vehicular Application**



**Manpack Application**



**Stationary Application**



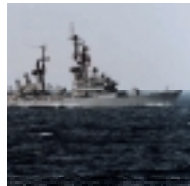
**Airborne Application**

© Crypto AG / HC6835-E.PPT / hy / 16

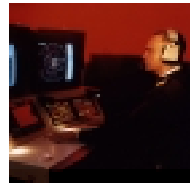
©2001 Crypto AG - all rights reserved.



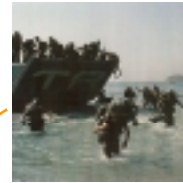
# HC-6835 Ruggedized Security Workstation Navy Applications



Ship Application



Shore Application



Manpack Application



Submarine Application

© Crypto AG / HC6835-E.PPT / hy / 17

©2001 Crypto AG - all rights reserved.

# HC-6835 Ruggedized Security Workstation MOFA Applications



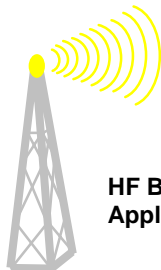
Vehicular Application



Portable Application



Stationary Application



HF Backup link  
Application

© Crypto AG / HC6835-E.PPT / hy / 18

©2001 Crypto AG - all rights reserved.

# Security and Administration

### Local Security

- Encryption of files stored locally or on server
- Automatic decryption upon selection of encrypted file (double-click)
- Wipe Function (secure delete)
- Transparent Disk Encryption for extended hard disk partitions and floppy disks
- Access Protection to encrypted drives and encryption / decryption services
- Swap File Clean-up
- Temp File Redirection

# HC-6835 Ruggedized Security Workstation

## The Security Services



### Message & File Encryption

Manual operation

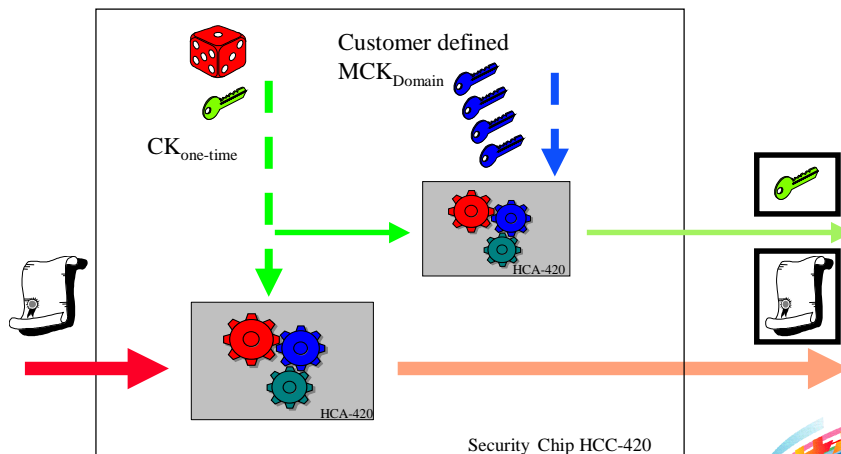
- Type and include files into CryptoPad application
- Select in Explorer context menu
- Drag & Drop files onto CryptoPad application
- Works with single or multiple files
- Decryption
  - Automatically on double-click
  - Manually in Explorer context menu
- Includes Compression and Integrity Check

© Crypto AG / HC6835-E.PPT / hy / 21

©2001 Crypto AG - all rights reserved.

# HC-6835 Ruggedized Security Workstation

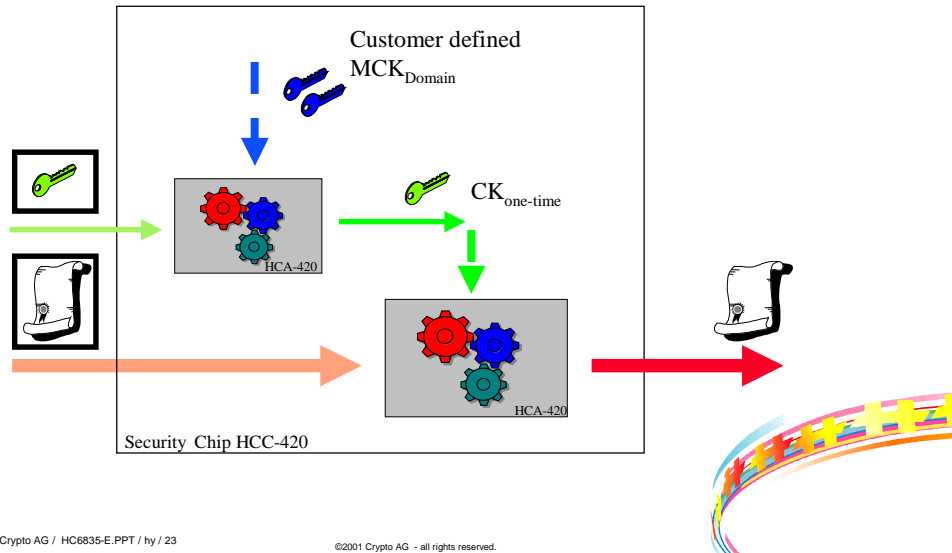
## Communication Security Mechanisms: Sender



© Crypto AG / HC6835-E.PPT / hy / 22

©2001 Crypto AG - all rights reserved.

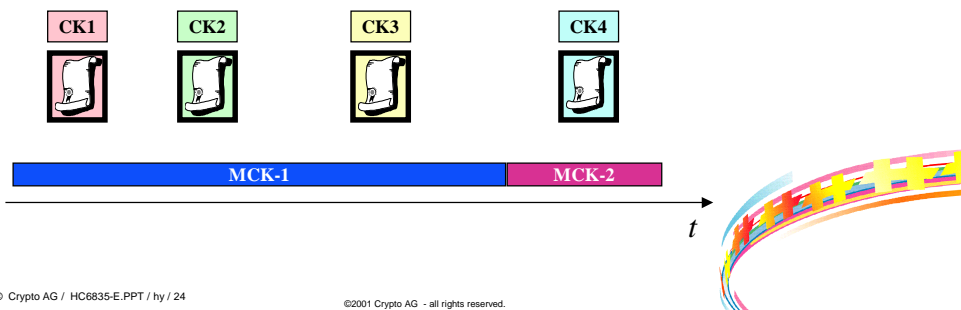
## HC-6835 Ruggedized Security Workstation Communication Security Mechanisms: Receiver



## HC-6835 Ruggedized Security Workstation Key Life Cycles



- Communication Key CK is randomly generated to encrypt only **one message**
- Master Communication Key MCK is generated by customer's security administrator and used until the next **key change**
- Validity duration for MCK is defined at generation time



## HC-6835 Ruggedized Security Workstation Algorithm in the HCC-420



### Cryptographical parameters

- Master communication key variety over  $10^{37}$
- Communication key variety over  $10^{37}$
- Storage key for disk encryption variety over  $10^{37}$

### Algorithm Customisation

- Customisation by CMP: variety over  $10^{38}$

### Customer Definitions

- Total variety of customer definition in security chip HCC-420 over  $10^{112}$

© Crypto AG / HC6835-E.PPT / hy / 25

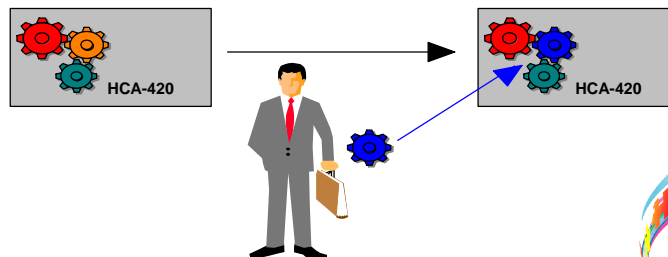
©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Detachment Philosophy



### Security elements fully under customer control:

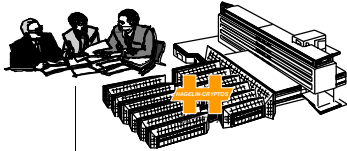
- The Master Communication Keys
- The Storage Key
- The Access Password
- A vital Part of the Algorithm



© Crypto AG / HC6835-E.PPT / hy / 26

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Cryptographic Algorithms



- Proprietary, customer-specific, secure handled cryptographic algorithms
- Possibility to set algorithm structure / parameters by customer

© Crypto AG / HC6835-E.PPT / hy / 27

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Algorithm



### Highly Sophisticated Algorithms

- HCA-420 for encryption / decryption embedded in Crypto AG's security chip HCC-420
- Hardware-based true random generator embedded in security chip HCC-420

© Crypto AG / HC6835-E.PPT / hy / 28

©2001 Crypto AG - all rights reserved.

# HC-6835 Ruggedized Security Workstation

## Elements of Seamless Security



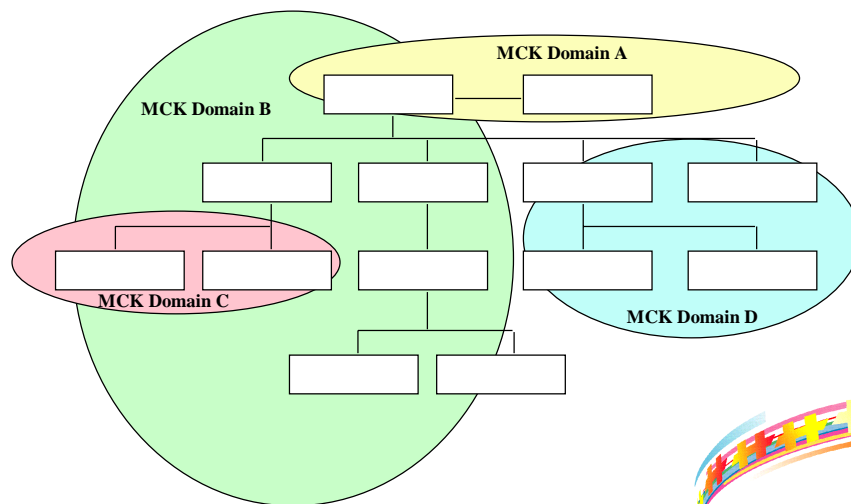
**A Security Chain is as strong as its weakest link !**

- Detachment from manufacturer:
  - Customer controlled algorithm
  - Access to terminal
- Highly sophisticated hardware-based algorithm
- Flexible security management
- Hardware-based access control mechanisms
- Easy and reliable operation
- High quality of COMPREM measures



# HC-6835 Ruggedized Security Workstation

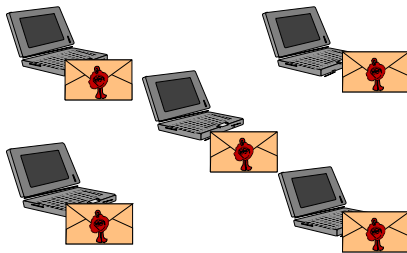
## Security Management: Communication Topology



## HC-6835 Ruggedized Security Workstation Traditional Security Management



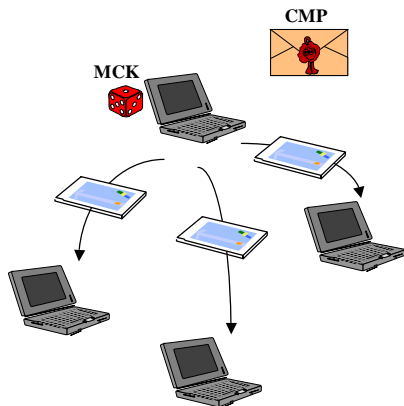
- Delivery of all HC-6835 to the customer
- HC-6835 are detached by customer
- Traditional key management by security manager of communication organisation (periodically)



© Crypto AG / HC6835-E.PPT / hy / 31

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Enhanced Security Management



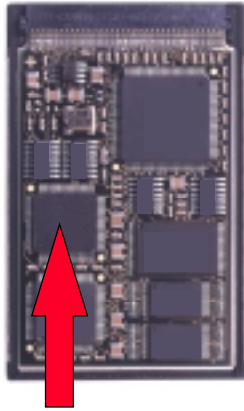
- Delivery of all HC-6835 to customer's communication organisations
- Detachment of first HC-6835 according to customer's centralized rules (CMP)
- Manual input of MCK into first HC-6835
- Distribution of securely copied security modules to the other communication partners (periodically)

© Crypto AG / HC6835-E.PPT / hy / 32

©2001 Crypto AG - all rights reserved.



## HC-6835 Ruggedized Security Workstation Security Module



**Crypto AG's security chip HCC-420**

- Tamper proof security chip HCC-420 with
  - cipher algorithm HCA-420
  - true random generation of keys
- Plain keys, Password and other classified data never leave the security chip
- Algorithm is fully protected against copying, readout, modifications
- High COMPREM quality due to metal housing of PC card

© Crypto AG / HC6835-E.PPT / hy / 33

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation

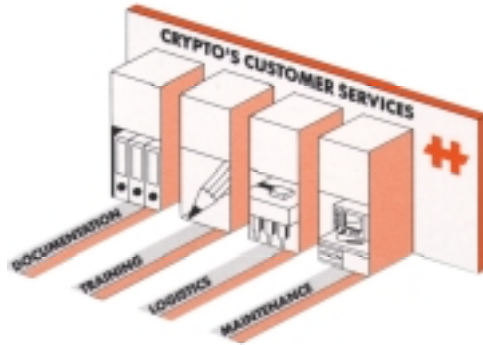


# Services

© Crypto AG / HC6835-E.PPT / hy / 34

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Maintenance / Concept



- Support for various levels
    - Level I (by operator)
    - Level II (module level)
- Tools and test equipment  
Spare parts  
Factory repair  
Documentation  
Training

© Crypto AG / HC6835-E.PPT / hy / 35

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Maintenance / Level I



### Level I (Operator)

- Performed by the operator or user
- Replacement of complete units or parts thereof
- No spare parts or tools required
- Part of optional basic training
- Level I is entirely covered with standard documentation (e.g. user manual)

© Crypto AG / HC6835-E.PPT / hy / 36

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Maintenance / Level II



Spare modules required !



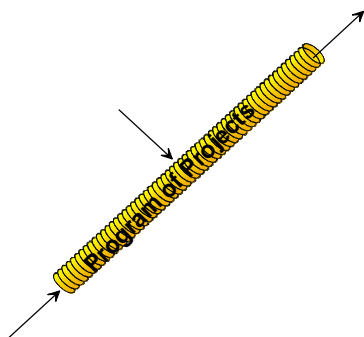
### Level II (Module Level)

- Performed by technicians
- Replacement of modules
- Diagnosis with off the shelf test equipment and BITE (built-in tests)
- Standard tool set (WOF)
- Service Handbook (Part of WOF)
- Optional Level II training available

© Crypto AG / HC6835-E.PPT / hy / 37

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Turn Key Aspects



### Crypto AG Capabilities

- Customer presentation
- Field trials
- Site survey
- Installation
- Commissioning
- Acceptance tests
- Training
- Customer service

© Crypto AG / HC6835-E.PPT / hy / 38

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation Capabilities as System Intergrator



### General contractor for a complete, secure system

On customer request we shall supply, install and commission the entire IT and security system on a turnkey basis.



© Crypto AG / HC6835-E.PPT / hy / 39

©2001 Crypto AG - all rights reserved.

## HC-6835 Ruggedized Security Workstation But Crypto AG will support ...



- The customer with
  - ideas
  - proposals
  - security know howif the new and the existing units have to be used
- The customer with hardware, software, brainware to use the existing and new units in an optimized configuration



© Crypto AG / HC6835-E.PPT / hy / 40

©2001 Crypto AG - all rights reserved.

## Your Benefits

---



- End-to-end communication security
- File, disk, virtual memory and message encryption
- Virtual Private Network (VPN) encryption
- Excellent performance (light, small, ruggedized)

