



Crypto Mobile Client HC-7835

For a modern, more mobile working style from frequently changing locations, access to a central infrastructure and data of one's own organisation is an integral part of "daily business". What needs to be considered when using the Internet for communication is that data can easily be tapped by unauthorised parties. This risk can be avoided by setting up a safe, encrypted connection (IP VPN tunnel). Before e-mails are sent from (unsafe) Internet connections, they should be encrypted end-to-end. And because sensible data is often stored on a laptop computer, it should only be stored in an encrypted manner. The new Crypto Mobile Client HC-7835 provides the mobile user with the perfect basic technology to ensure seamless information security.

Ad-hoc access to the Internet or other IP networks is available almost anywhere these days, for instance via WLAN hotspots in hotels, Ethernet interfaces in regional offices, satellite terminals outdoors or ADSL connections in private homes. Furthermore, a Bluetooth mobile phone in a GSM/UTMS network could also be used for access. With most applications converging on IP today, providers offer bandwidths enabling triple-play applications (voice, data, and video).

Crypto AG addresses the potential security risks of ad-hoc communication with its new Crypto Mobile Client HC-7835 which sets up an IP tunnel (secure IP VPN) for protected data transport and utilises IP encryption to render all communications in the network unreadable by unauthorised parties. The Crypto Mobile Client also offers "thin client" functions for processing ultra-sensitive data on your laptop computer or PC. Any data that is processed in this mode never leaves the central infrastructure and remains fully protected.

Especially in a mobile working environment e-mail is still one of the most important means for communication. The Crypto Mobile Client provides the ideal solution with its e-mail message encryption function (including attachments).

But where do you store sensitive data when travelling? The best option is directly on the HC-7835 – with the optional Secure Data Storage function. This way, data and information can also be transported outside your laptop computer – e.g. when crossing borders this can be very important.

The Crypto Mobile Client is a small, portable all-in-one solution for use while travelling with virtually any laptop or PC and regardless of operating system. You simply connect it to the computer with a USB and Ethernet cable and then connect to the communication network via Ethernet cable or, optionally, via WLAN or Bluetooth.

The Crypto Mobile Client is compatible with the other IP VPN units from Crypto AG. The same holds true for the Security Management Centre SMC-1100 and the Remote Access Device RAD-1100 (remote configuration of the network parameters), all without any additional system administration effort on your part.

Key features

- Small, portable, multi-application, high-performance unit with several application options
- Optional IP VPN for secure remote access via public IP networks (e.g. the Internet)
- Optional message/file encryption for sending and receiving encrypted e-mails
- Optional Secure Data Storage for transport of confidential data
- Easy connection to laptop computer or PC (USB/Ethernet) regardless of operating system
- Network access via Ethernet and optionally via WLAN or Bluetooth
- Encryption in tamper-proof hardware module with your own secret algorithms

Cryptography & Security

Algorithm

- Customer-specific cipher algorithm
- Customer managed profiling of algorithm by CMP
- Mutual key agreement scheme for generation of short-term Communication Keys (CKs)
- Built-in high-quality true random generator

Keys

- Customer-defined Master Communication Keys (MCKs, for CK generation) stored in tamper-proof security module

Key management

- Manual key input via user interface
- Copy / backup of key and installation data by Security Data Carriers (SDCs)

Tamper-proof design

- Role based access control
- Block function
- Emergency clear
- Tamper evidence
- Tamper detection & response (reset to ex-factory state)
- Metal housing
- Built-in security module

Services

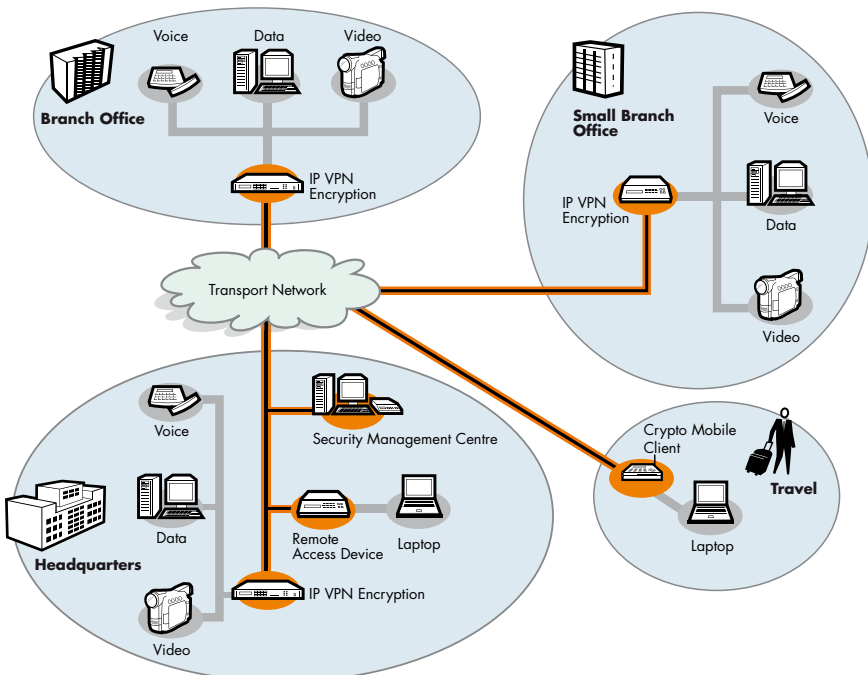
Home-side services

- DHCP server
- Static routing or RIP-II

World-side services

- DHCP client
- NAT support

IP VPN



Features

User interfaces

- Keypad
- LCD display
- Status LEDs

Payload (home/world) interfaces

- Home IEEE 802.3 Ethernet, 10BASE-T/100BASE-TX, RJ45
- World:
 - IEEE 802.3 Ethernet, 10BASE-T, RJ45
 - WLAN, IEEE 802.11 b/g (optional)
 - Bluetooth version 2.0 (optional)

USB Memory

- USB Memory (4GB) with write protection
- Possible to boot the notebook with an operating system (thin client)

Management interfaces

- Diagnostics interface RS-232, RJ45
- Built-in smart card reader

Management

- Local management via keypad and display
- Local management via browser based user interface
- Remote software update
- Time Server Support (SNTP)
- Network Management System (NMS) integration support (SNMPv1/Standard MIB II)

Maintenance

- Built-in test equipment (BITE)

Power supply

- Via USB (from laptop/PC)
- Or via power socket: 6...18VDC
- (Optional external power supply 100...240 VAC/50...60 Hz)
- Power consumption < 3W

Mechanical

- Small mobile housing
- 116 x 70 x 25 mm W/D/H
- 0.3 kg

Reliability

- MTBF: > 50,000 hrs

Environmental data

- Operating temperature: -5 °C...+50 °C
- Storage temperature: -25 °C...+70 °C

EMC / Safety

- EN 55022 class B/EN 55024
- EN 60950-1

Quality system / Conformity

- ISO 9001:2000
- CE (European conformity)

Accessories / options

- External power supply
- Transportation case
- Security Management Centre SMC-1100 IP VPN
- Remote Access Device RAD-1100
- Security Data Carriers SDCs

Application IP VPN

Services supported

- Unicast IP VPN tunnels (tunnel mode)
- Multicast IP VPN tunnels (tunnel mode)
- Optional: Throughput approx. 1, 4 or 8 Mbps with 1500 byte IP packets (limited with Bluetooth)
- Up to 8 tunnels (1 Mbps) or 32 tunnels (4 / 8 Mbps)
- Star and/or mesh topologies
- Traffic types: data/voice/video

Quality of service (QoS) support

- TOS/DSCP forwarding
- Configuration of TOS/DSCP for key agreement
- Replay protection window size 64 packets

Management

- Security Management Centre SMC-1100 IP VPN, online or offline with Security Data Carrier
- Remote Access Device RAD-1100

Application Message/File Encryption

- User-friendly Windows® applications
- Message Encryption: Use with prevalent e-mail clients possible
- File Encryption: For files stored locally or on a server
- Backward compatibility with HC-6360 / 6378
- Simple management

Message Encryption



Application Secure Data Storage

- Encrypted file storage in Flash memory (2GB)
- Transparent operation (as with a file server SMB / CIFS)
- Data transfer via drag & drop in a file manager

Secure Data Storage

