HAGELIN-CRYPTOS
CRYPTO AG

Crypto Mobile Client HC-7835 IP VPN

For travelling members of defence and government organisations, military attachés, ambassadors, senior civil servants and executives, remote access to a central infrastructure and the data of their organisations is an integral part of daily work. Data are generally exchanged over an Internet access, so they can easily be tapped by unauthorised parties. This risk can be avoided by setting up a safe, encrypted connection (IP VPN Tunnel). The new Crypto Mobile Client HC-7835 IP VPN now provides the perfect basic technology for mobile users as well. Small and simple to run, this unit can be utilised in multi-location operation with virtually any laptop or PC.

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. With most applications today converging on IP, providers offer bandwidths enabling triple-play applications (voice, data, and video).
However, ad-hoc communication can only be used if the security of the information is guaranteed. Crypto AG is addressing these very security problems with its new Crypto Mobile Client HC-7835 IP VPN. This product sets up an IP tunnel (secure IP VPN) for secure data transport and utilises IP encryption to render all communications in the network unreadable by unauthorised parties.
The Crypto Mobile Client is a compact mobile/portable unit you can use with any of your notebooks or PCs regardless of operating system. You simply hook it up 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. From that point forward, you encrypt all calls conducted or information exchanged between yourself and your organisation's infrastructure (or another client). Confidentiality, authenticity and integrity are assured.
The Crypto Mobile Client also offers you "thin client" functions for processing your organisation's ultra-sensitive data on your laptop or PC. Any data you process in this mode never leave the central infrastructure and remain fully protected.
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, mobile high-performance unit for secure data transmission via IP networks
- All applications, e.g. E-mail, VoIP, data or video, are protected
- Easy to connect to notebooks or PCs (USB/Ethernet), regardless of operating system
- Once the basic configuration is set up, the Crypto Mobile Client can be used as a plug-and-play unit for immediate encryption of communication
- Network access via Ethernet and optionally via WLAN or Bluetooth
- Encryption in tamper-proof hardware module with your own secret algorithms
- Crypto Mobile Client is compatible with all other IP VPN units by Crypto AG

General data

Housing
- Small mobile unit

User interfaces
- Built-in user interface:
  - Keypad with 16 buttons
  - 2 lines x 16 characters LCD with backlight
  - Status LEDs
- Browser-based user interface
- Built-in smart card reader for reading / writing key and setup data
- Diagnostic user interface

Line interfaces
- Home: Ethernet/RJ45, IEEE 802.3, 10BASE-T/100BASE-TX
- World: Ethernet/RJ45, IEEE 802.3, 10BASE-T
- World: WLAN, IEEE 802.11 b/g (optional)
- World: Bluetooth version 2.0 (optional, release 2)

Throughput
- Optional: 1, 4 or 8 Mbps (limited with Bluetooth)

Control interface
- Serial RS-232 RJ45 (diagnostics)

Management
- Security Management Centre SMC-1100 IP VPN
- Remote Access Device RAD-1100
- Out-of-band management via world interface
- Local management via keypad and display or via web-based user interface
- SNMPv1, standard MIB II

Test facilities
- Built-in test equipment (BITE)
- Diagnostics

EMC
- EN 55022 class B/EN 55024

Safety
- EN 60950

Power supply
- Via USB (from notebook)
- Or via power socket: 6…18VDC, max. 3W
- (Optional external power supply 100…240 Vac/50/60 Hz)

Dimensions
- 116 x 70 x 25 mm W/D/H

Weight
- Approx. 0.3 kg

Reliability
- MTBF: 50,000 hrs

Quality system
- ISO 9001:2000

Conformity
- CE (European conformity)

Cryptographic data

Algorithm
- HCA-480, customer-specific cipher algorithm
- Customer managed profiling of algorithm by CMP with variety > 10^{506}
- Sophisticated mutual key agreement scheme based on HCA-480 for generation of short-term Communication Keys (CK)
- Built-in high-quality true random generator

Keys
- 160 customer-defined Master Communication Keys (MCK, for CK generation) stored in tamper-proof security module
- Master Communication Keys and Communication Keys with variety > 10^{38}

Key management
- Manual key input via local user interface
- Copy / backup of key and installation data by Security Data Carrier (SDC)
- Offline by Security Management Centre SMC-1100 IP VPN and Security Data Carrier
- Online by Security Management Centre SMC-1100 IP VPN

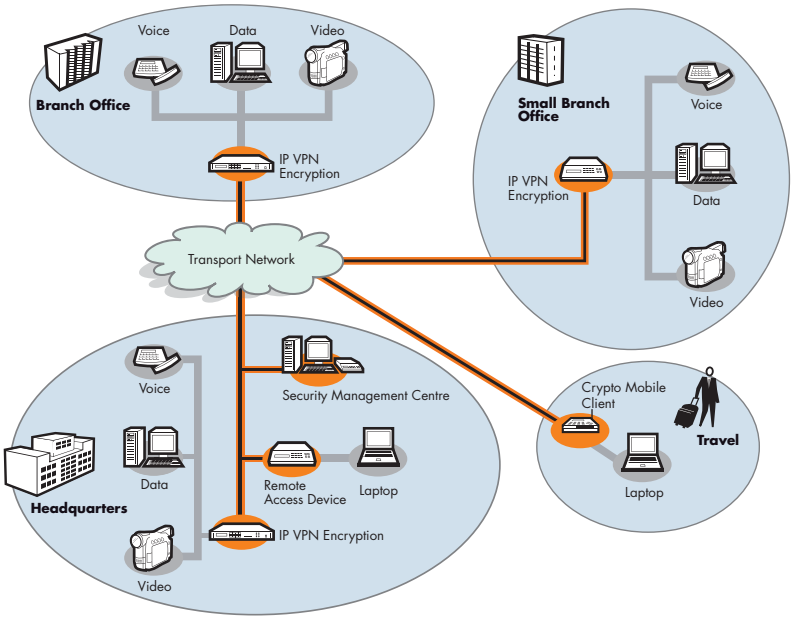
Access protection
- Tamper-proof design
- Password protection, user level specific
- Block / unblock function
- Emergency clear

Environmental data
- Operating temperature: -5 °C…+45 °C
- Storage temperature: -25 °C…+70 °C
- Humidity: < 93 %, non-condensing

Accessories / options
- External power supply
- Transportation case
- Security Management Centre SMC-1100 IP VPN
- Remote Access Device RAD-1100
- Security Data Carrier SDC

Applications (release 2)
- E-mail / file encryption
- Encrypted memory drive

Crypto Mobile Client



Crypto AG, P.O. Box 460, CH-6301 Zug, Switzerland, www.crypto.ch