ATS - TELCOM PRAHA a.s.®
TELEKOMUNIKAČNÍ SPOLEČNOST

Zabezpečená videokonference a hlas v IP a GSM komunikačním prostředí

Jiří DOUŠA

Červen 2014

Agenda

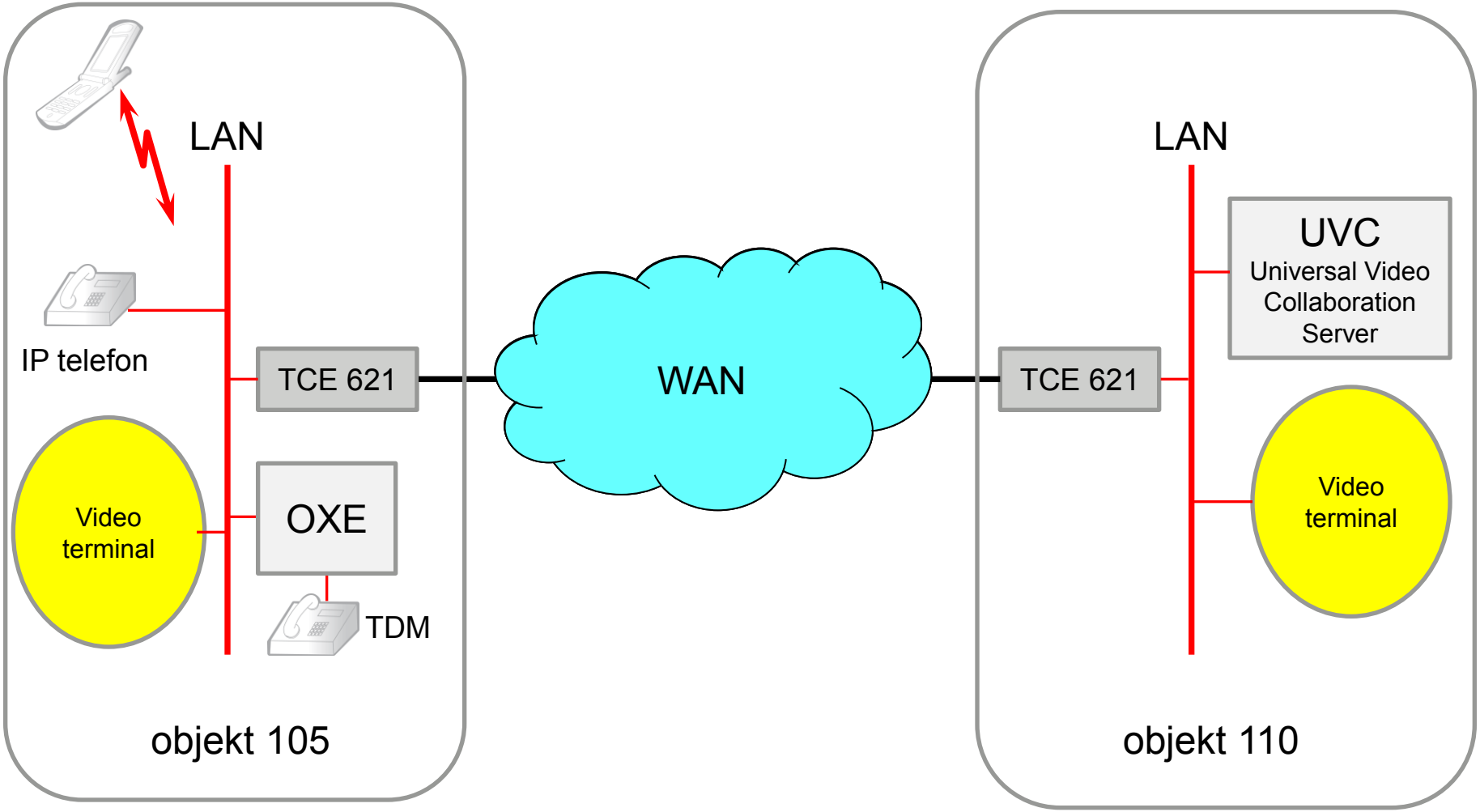
1. IP šifrátory pro zabezpečení videokonference
2. Požadavky na IP šifrátory
3. Cryptel IP® řešení
4. Zabezpečený hlas a SMS v GSM síti
5. Sectra Panthon® 3 řešení
6. Kontakty a služby

IP šifrátory pro zabezpečení videokonference

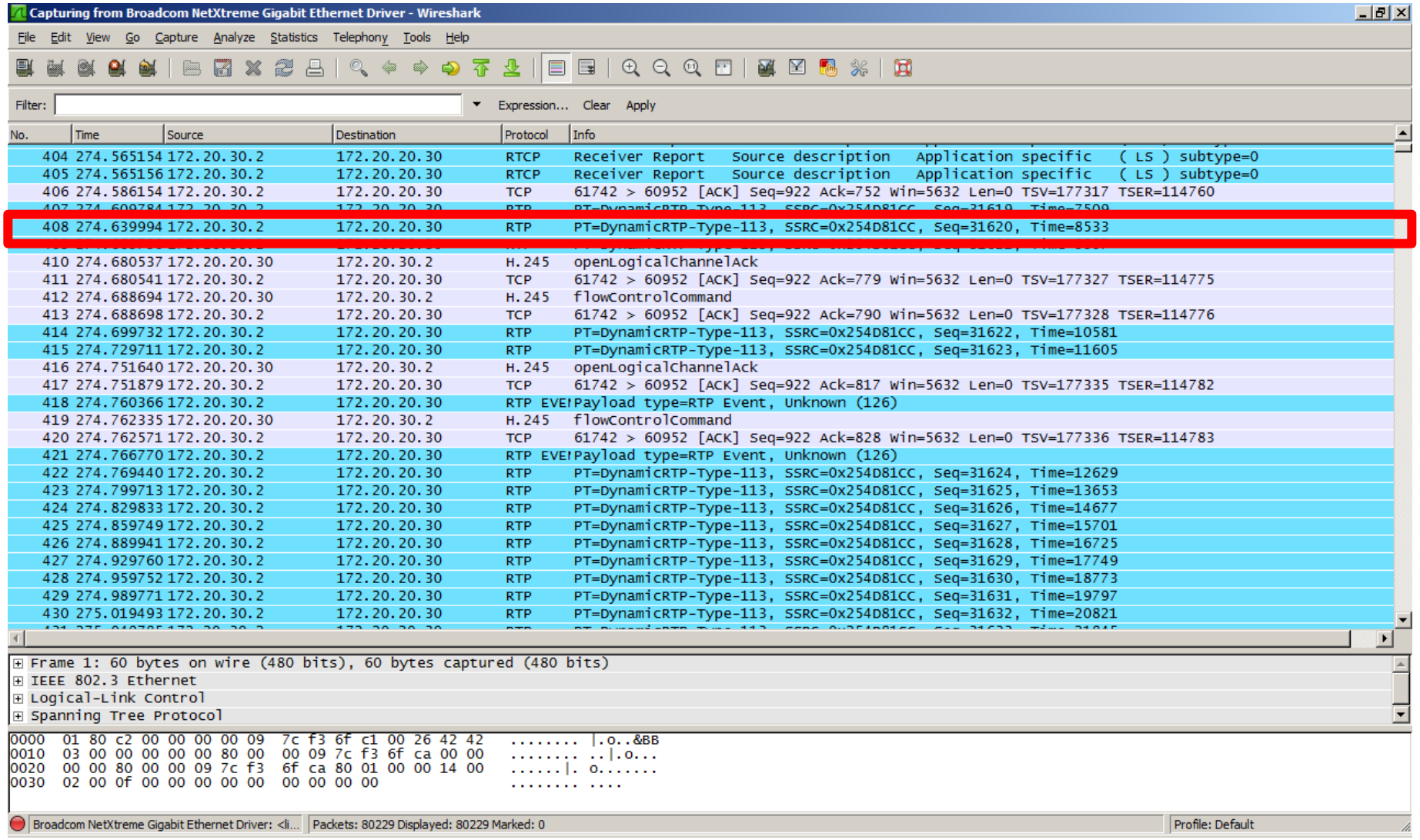
1. Proč utajovat videokonferenční datový přenos
   - modifikace dat během přenosu, podsunutí dat
   - virtuální jednací místnost - chybí osobní kontakt
   - únik informace
   - ochrana klasifikovaných informací podle zákona č. 412/2005 Sb.

2. V pevných IP datových sítích
   - IP šifrátor oddělující červenou LAN od černé WAN
   - data v červené síti chrání data další vrstva utajení (síťové prvky, videokonferenční terminál)
   - u klasifikovaných dat je vyžadováno fyzické zabezpečení
   - šifrátory mají nezávislou správu (jsou součástí zabezpečených IP sítí)

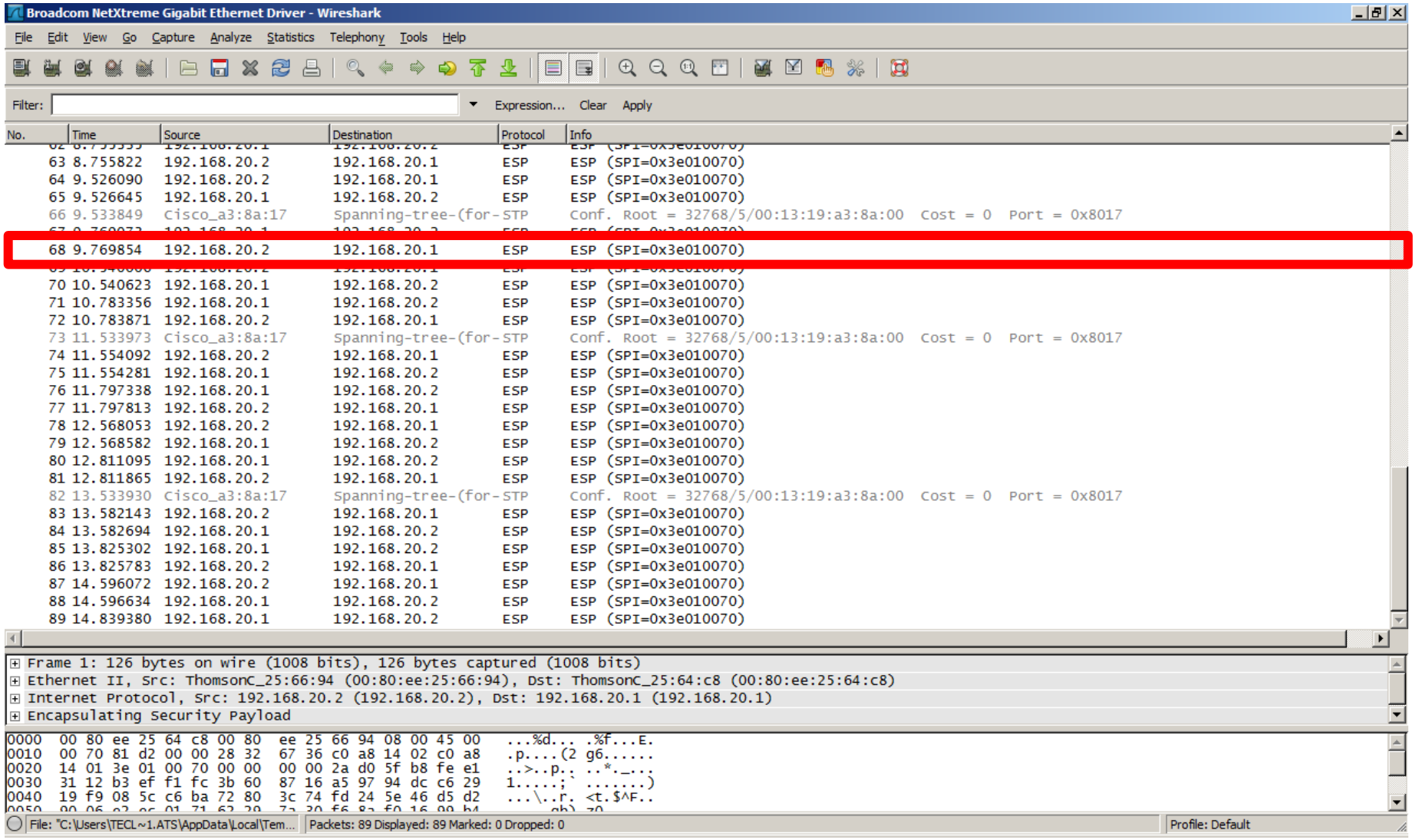
IP šifrátory pro zabezpečení videokonference



Nezabezpečená IP komunikace



Zabezpečená IP komunikace



Požadavky na IP šifrátory pro zabezpečení videokonference

1. Plná podpora multicastového provozu (point – to –multipoint), klíče a správa šifrátorů
2. Plná podpora QoS (priorita voice a video paketů), řazení paketů vč. sekvenčních čísel paketů
3. Plný duplex, podpora rychlostí 10/100/1000 Mbit/s
4. Pro klasifikovaná data certifikace od NBÚ
5. Požadavky na sítě
   - trastované sítě, podpora QoS, lze využívat pro klasifikovaná data vyšších stupňů utajení
   - veřejné sítě (internet) omezení z hlediska QoS a dostupnosti služeb

Využití kryptografického systému Cryptel®-IP

1. TCE 621B/C a TCE 621B/C CZ - IP kryptografické prostředky
2. plně HW on-line KP, určený pro kryptografickou ochranu informací na úrovni IP s přenosovou rychlosti do 100 Mbit/s (B), 1000 Mb/s (C)
3. CZ představují národní verzi na bázi komponent TCE 621
4. podpora IPv4 i IPv6 a NAT (pomocí UDP zapouzdření), zálohování vytvořením virtuálních KP, zabezpečený multicast
5. Mechanické provedení je v souladu s SDIP 27- level A (TEMPEST)
6. rozhraní Ethernet metalické/optické
7. v ČR certifikovány pro utajované informace od NATO Confidential, Confidentiel UE, Důvěrné až po Přísně Tajné, COSMIC TOP SECRET

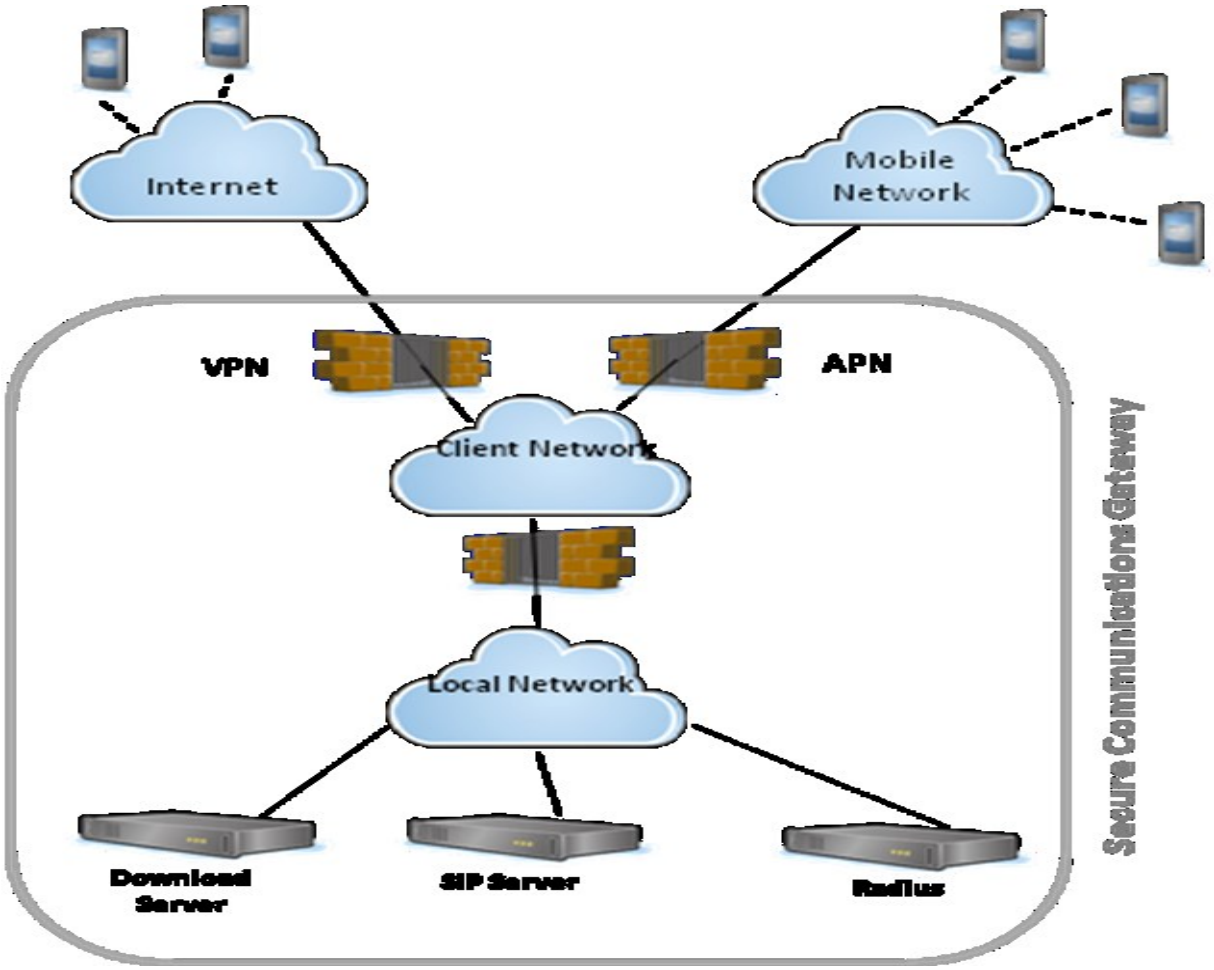
Mobilní IP šifrátory pro mobilní videokonferenční terminál

1. Pro mobilně zřizovaný terminál,
2. Mobilní IP kryptografický prostředek, plně kompatibilní s TCE 621 B (C)
3. Podporuje statické i dynamické přidělování IP adres na straně neutajované sítě
4. Na černé straně se připojí k datové síti (WiFi, GSM brána, metalika apod.)
5. mechanické provedení je v souladu s SDIP 27- level A
6. rozhraní Ethernet metalické/optické
7. v ČR v procesu certifikace; je certifikován v NATO do stupně SECRET

Zabezpečený hlas a SMS v GSM síti

1. Sítě GSM - omezení z hlediska přenosové rychlosti (od 2G), QoS a dostupnosti signálu, výpadky, přetížení sítě
2. IP šifrátor je součástí terminálu (mobilního telefonu, tabletu apod)
3. Utajení End-to End
4. Komunikace přes gateway (servery zajišťující spojení)
5. Možnost využití GSM i internetových sítí (WiFi)
6. Řešení IP šifrátoru kombinací SW a HW
7. Aplikace a SD karta do smartphonu
8. Požadavky na rychlosti přenosu IP paketů (voice, obraz)
9. Šifrované SMS je možno zasílat standardním SMS kanálem
10. Vyšší nároky na ochranu mobilních terminálů (organizační a technické)

Zabezpečený hlas a SMS v GSM síti



Sectra Panthon® 3

1. Utajovač Panthon ® 3 je implementován do standardních mobilních telefonů s operačním systémem Android
2. Bezpečnostně významné operace jsou zpracovávány a ukládány v přidaném HW
3. Aplikace Panthon je instalována v mobilním telefonu
4. Mobilní telefon lze využívat i jako standardní mobilní telefon
5. SMS zprávy šifrovány off-line a posílány standardním SMS kanálem v prostředí GSM
6. Hlasová komunikace on-line s utajením End-to-End
7. Panthon vyžaduje podpůrnou infrastrukturu - bezpečnostní komunikační bránu (SCGW),

Sectra Panthon® 3

1. Technická podpora ochrany
   - bezpečnostní brána SCGW (firewally, politika, audit)
   - CRL (black list)
   - správa kontaktů z SCGW
   - white list (brání instalaci nebezpečných aplikací a škodlivého SW)
   - otevřená data pouze po dobu aktivního stavu
   - omezení počtu pokusů o zadání PIN
   - automatické ukončování aplikace
2. Certifikováno NBÚ pro ochranu utajovaných informací
   - Vyhrazené (č. certifikátu K20154)
   - Vyhrazené, EU RESTRICTED (č. certifikátu K20163)

Kontakty a služby

ATS-TELCOM PRAHA a.s.

- Informace k systémům Cryptel®-IP a Sectra Panthon® 3
- Podpora při projektování, nasazování a provozu systémů
- Servis
- Školení správců a uživatelů
- Testovací sestavy
- Kontakty:

  Jiří Douša, tel: 602 573 270, e-mail: dousa@atstelcom.cz

  Karel Bouchner, tel: 602 390 903, e-mail: bouchner@atstelcom.cz

  Jiří Tecl, tel: 602 246 653, e-mail: tecl@atstelcom.cz

  Jan Sedlák, tel: 602 246 650, e-mail: sedlak@atstelcom.cz