



Основни понятия - Черна и червена зона



- Червена зона – медни или оптични кабели, апаратура, компоненти и системи, които обработват **класифицирани некриптирани данни, както и пространствата, в които възникват класифицирани данни;**
- Черна зона – медни или оптични кабели, апаратура, компоненти и системи, които обработват **само некласифицирани или криптирани данни, както и пространствата, в които възникват некласифицирани данни.**



Различен слой – различен подход

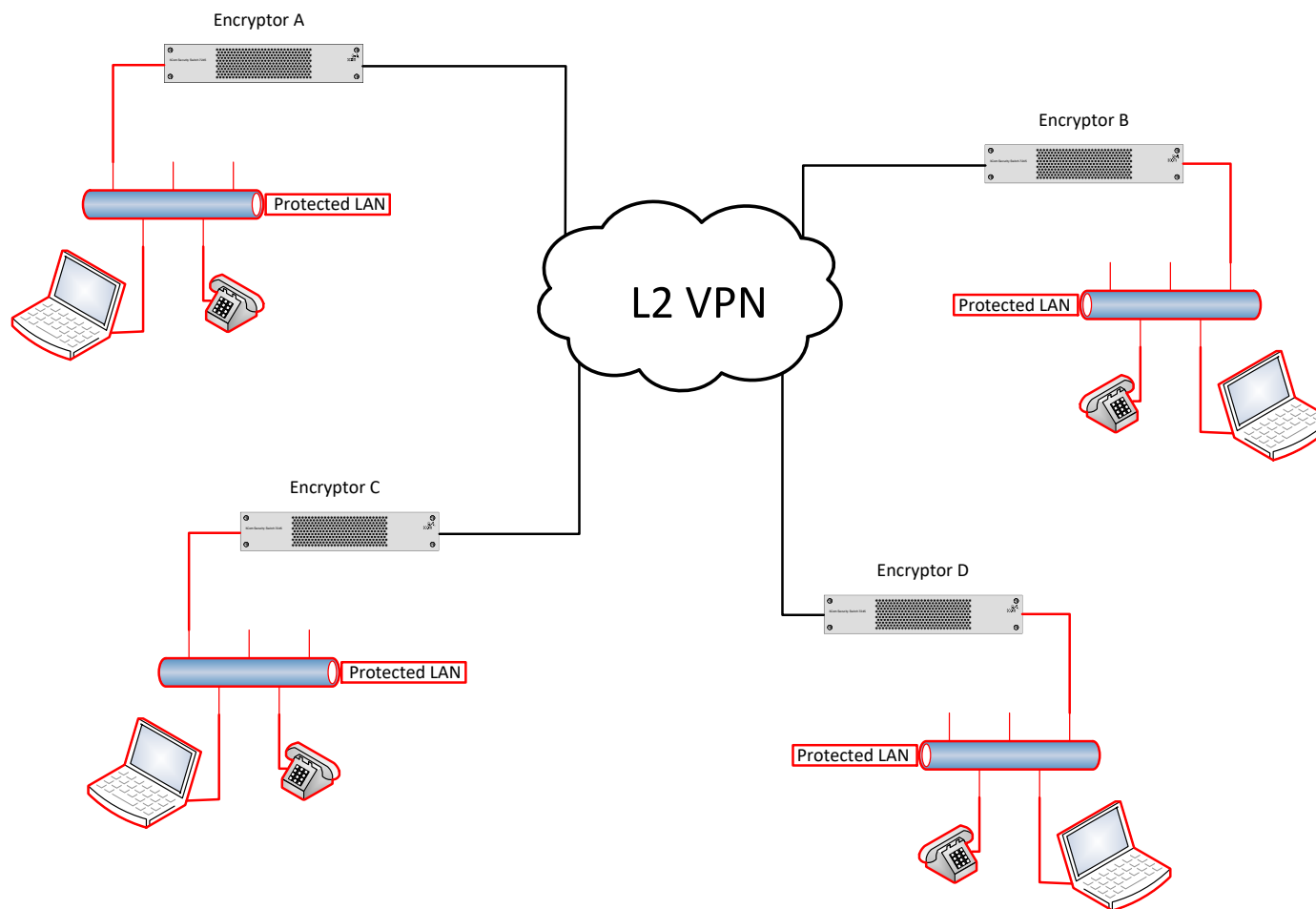
- Layer 1 енкриптори - предназначени за криптиране на директни връзки във физическия слой, (OTN – Optical Transport Network). Криптират всички протоколи от Layer 2 и по-високи, без да се интересуват от конкретния тип протокол. Метод с измерване на оптичното влакно.
- Layer 2 енкриптори – оптимизирани са за Ethernet и MPLS и не криптират IP пакетите. На практика понякога криптират Ethernet рамките и ги предават през IP мрежа в IP тунел;
- Layer 3 енкриптори – използват се за криптиране на IP Payload-а или криптиране на целия IP пакет. Ограничение в големината на MTU на криптирания пакет.
- GFE (Government Furnished Equipment) и RGFE (Radio GFE);

Layer 1 или Layer 2 криптиране точка-точка





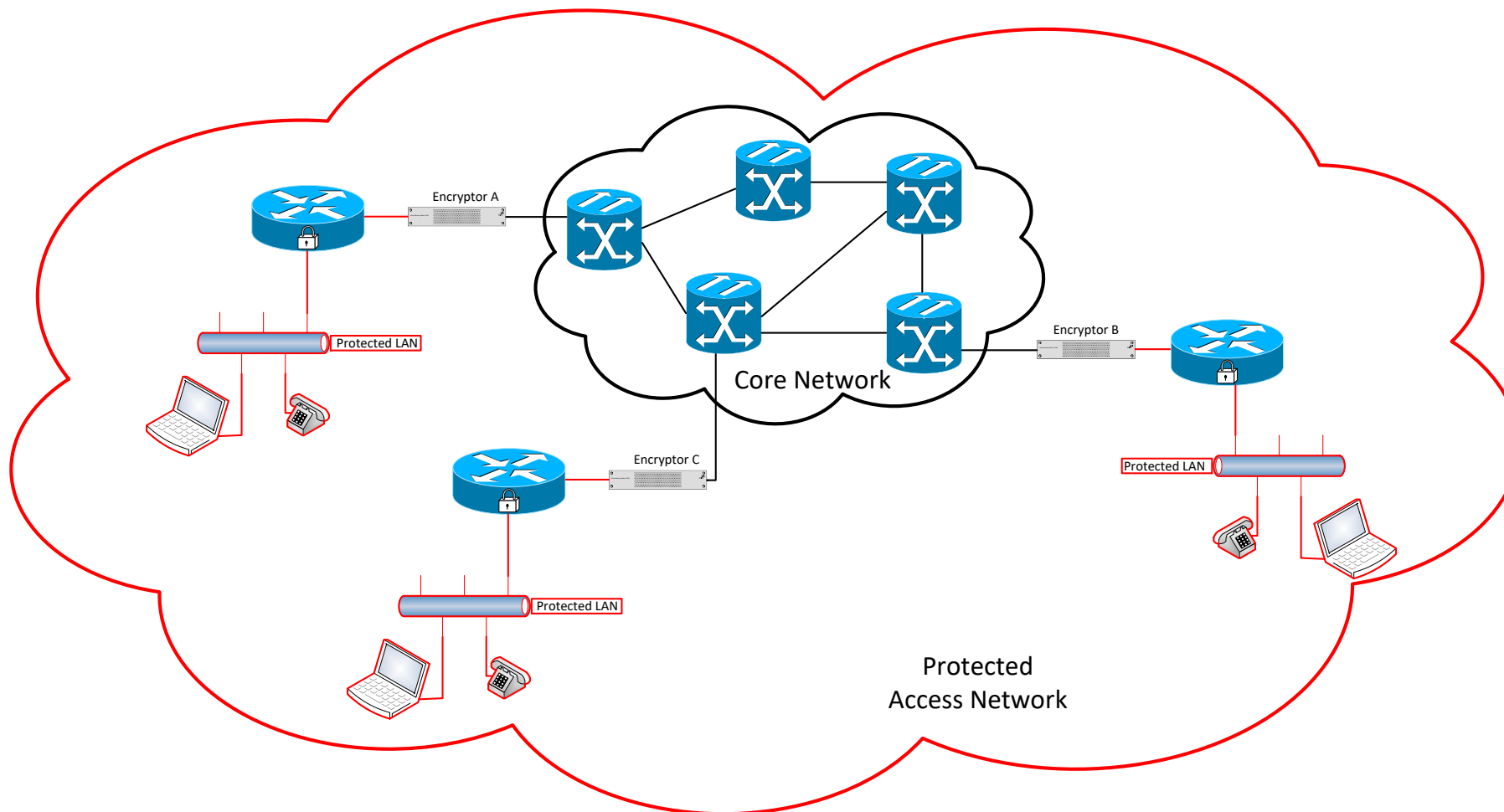
Layer 2 криптиране точка-много точки



www.euroqci.bg

Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейският съюз, нито съфинансиращият орган не носят отговорност за тях.

Layer 3 криптиране



www.euroqci.bg

Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейският съюз, нито съфинансиращият орган не носят отговорност за тях.



Практики при използване на енкрипторите

- ***Налагани изисквания при използване на криптиращи устройства:***
 - Отстояния между успоредно полагане на проводници – мин 10см;
 - Пресичането на проводниците да е под ъгъл 90°;
 - Допълнително заземление различно от това на останалото оборудване;
 - Поставяне на филтри на захранванията;
 - Дефиниране на наблюдавана зона и физическа охрана;
 - Регламентиране на зони – 1, 2 и 3;
 - Задължително екраниране на всички „червени“ медни проводници;
 - Недопускане на използването на оптични влакна от един и същ кабел за предаване на „червена“ и „черна“ информация.



Практики при използване на енкрипторите

- Често срещани проблеми при въвеждането в експлоатация:
 - Липса на синхронизация или NTP;
 - Jitter или Wander => Latency;
 - Наличието на тунел в тунела;
- Типове управление на енкрипторите – предимства и недостатъци:
 - Out-of-band управление – използване на отделна мрежа за управление;
 - In-band управление - обикновено управлението не се криптира от устройството;
 - In-line управление – има висока степен на сигурност, но ниска степен на надеждност.

Хардуерна реализация на крипто алгоритми

- Citadel - 1998г.
 - 64bit – 128bit ключ;
- Citadel II - 2004
 - 256bit ключ;
- Citadel и Citadel II не се използват от правителството и от армията на САЩ, но използват Siera и Siera II, които са Type1 алгоритми.



Хардуерна реализация на крипто алгоритми

- Sierra и Sierra II – програмируеми модули и поддържаните алгоритми
- Type 1 крипто алгоритми:
 - BATON/MEDLEY
 - SAVILLE/PADSTONE
 - KEESEE/CRAYON/WALBURN
 - GOODSPEED
 - ACCORDION
 - FIREFLY/Enhanced FIREFLY
 - JOSEKI Decrypt
- Type 3 крипто алгоритми:
 - DES / Tripple DES (3DES)
 - AES
 - Digital Signature Standard (DSS)
- Type 4 крипто алгоритми:
 - CITADEL – обратна съвместимост



Хардуерни криптиращи устройства със специално предназначение

- **Интеграция на хардуерен процесорен модул в корпус на SD карта – невидим за околните енкриптор на глас;**
- **Радио енкриптор за HF, VHF, UHF, SatCom – криптиране на глас и серийни данни и възможност за IP VPN**
- **IP VPN енкриптор – L2 и L3 енкриптор с възможност за повече от 2000 VPN тунела и организиране на групи в „Star“ и „Mesh“ топологии.**



Хардуерни криптиращи устройства със специално предназначение

- Крипто алгоритъм –
NATO Type A algorithm (Einride), NATO Type B algorithm (AES)
- PT (RED) и CT (BLACK)
интерфейси – **Ethernet 10/100BT, Optical (Option);**
- Скорост на криптиране /
декриптиране – **12Mbps;**
- MTBF/MTTF – **> 100 000 часа;**

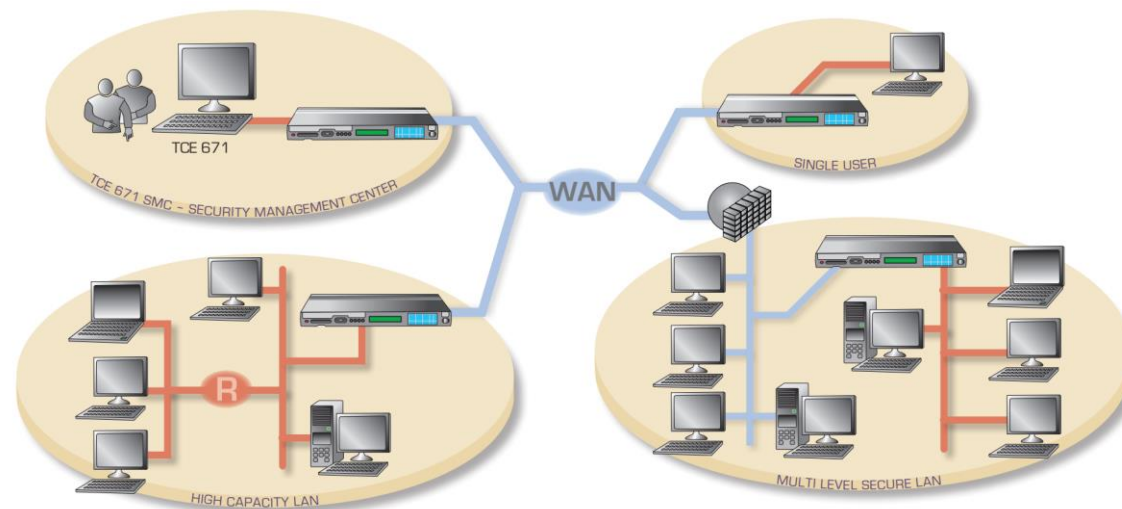


www.euroqci.bg

Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейският съюз, нито съфинансиращият орган не носят отговорност за тях.

Хардуерни криптиращи устройства със специално предназначение

- Крипто алгоритъм –
NATO Type A algorithm (Einride), NATO Type B algorithm (AES)
- PT (RED) и CT (BLACK) интерфейси – Ethernet 10/100/100BT, Opt. – MT-RJ/LC;
- Скорост на криптиране / декриптиране – 600Mbps;
- MTBF/MTTF – > 100 000 часа;



Хардуерни криптиращи устройства със специално предназначение

- Крипто алгоритъм – **AES-256**, режими **CTR, CFB, GCM**;
- Ключове – до **32** ключа на канал;
- РТ (RED) и СТ (BLACK) интерфейси – **LVDS**;
- Скорост на криптиране - **640Mbps**;
- MTBF/MTTF – **> 200 000** часа;



Хардуерни криптиращи устройства със специално предназначение

- Крипто алгоритъм – **Photoplay (Type1)**;
- Ключове – **до 128 ключа на канал**;
- РТ (RED) и СТ (BLACK)
интерфейси – **LVDS**;
- Скорост на криптиране /
декриптиране – **4Gbps**;
- MTBF/MTTF – **> 500 000 часа**;





Co-funded by
the European Union



Благодаря за вниманието!

www.euroqci.bg

*Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейският съюз, нито съфинансиращият орган не носят отговорност за тях.*