SafeNet. THE DATA PROTECTION COMPANY

gemalto security to be free

Сталевий бубен

Всеукраїнська конференція системних адміністраторів

# Gemalto&SafeNet Laeyr 2 Encryption

**Vladimir Zdor**
**Vladimir.Zdor@gemalto.com**

# What We Do.

We protect the **most money that moves**–over **80% of the world's intra-bank fund transfers** and nearly **$1 trillion per day.**

We control access to **the most sensitive corporate information**– more than **35 million identities protected** via tokens, smartcards, and mobile devices managed on-premise and in the cloud.

We are **the de facto root of trust**–deploying more than **86,000 key managers** and **protecting up to 750,000,000 encryption keys.**

gemalto security to be free

SafeNet. THE DATA PROTECTION COMPANY

# Who We Protect.

Gemalto IDP is trusted by **25,000 customers** and partners in **100 countries**, including blue-chip organizations

















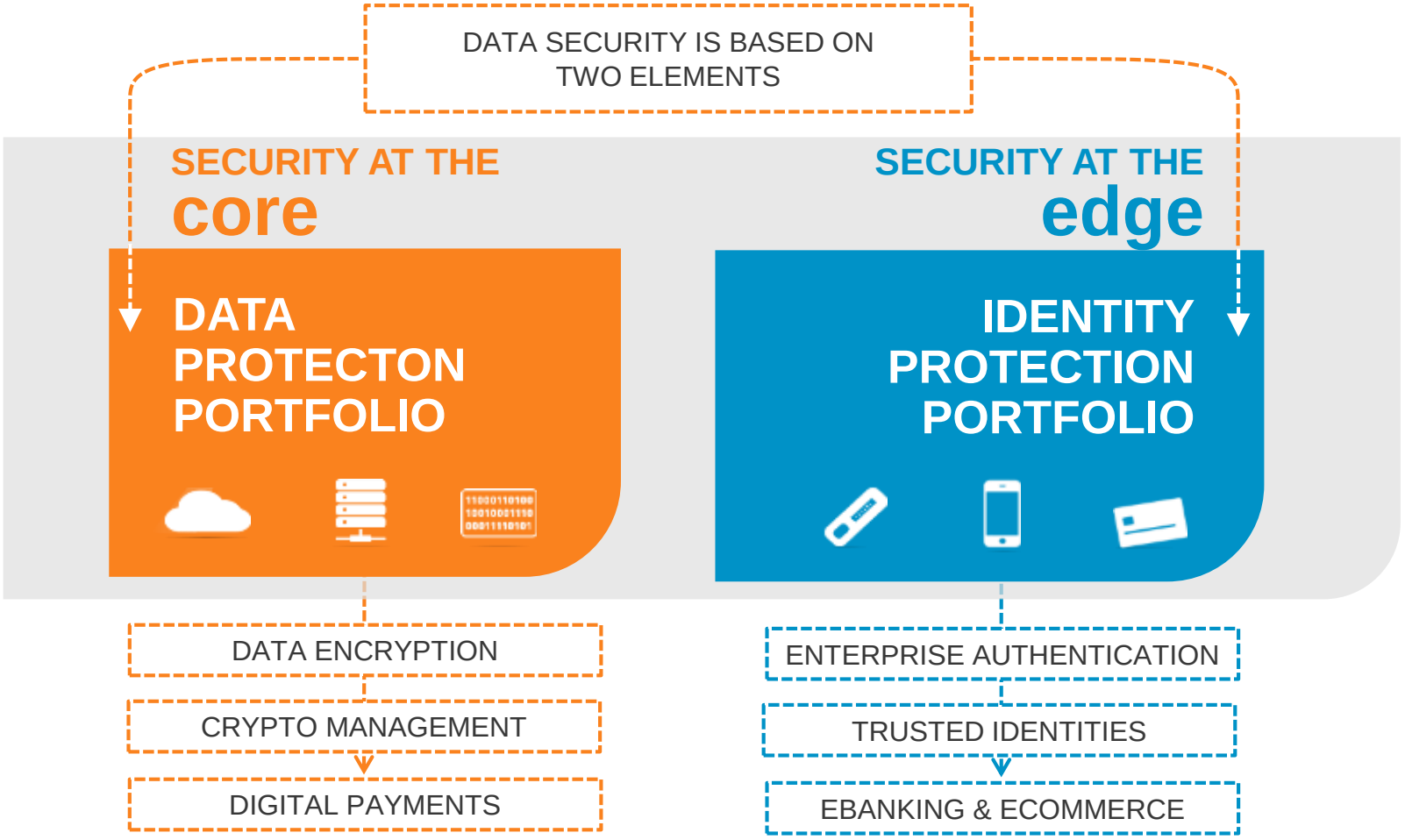


UK Government



THE DATA PROTECTION COMPANY

# Gemalto IDP Business Areas



# Our Digital World is Changing…

## More data…

Customer Personal Identifiable Information (PII)

**Social Security Numbers**

Data Encryption & Transaction Keys

**Account Numbers**

**Transaction History**

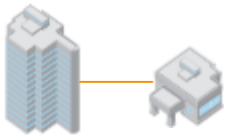
Sensitive Corporate Information

**Credit Card Numbers**

**Employee Records**

## In more places…

**Networks**



(Data-in-Motion)

**Servers**
On-premises/Cloud/Virtual

(Files, Databases, and Virtual Machines)

**Media**

(Drives and Tapes)

**Storage**

(Volumes or Shares)

## Facing more threats…

- Identity Theft
- Fraud
- BYOD
- Social Engineering

gemalto security to be free

SafeNet. THE DATA PROTECTION COMPANY

# The Reality: Data Breaches

2014

**1,023,108,267**

RECORDS EXPOSED

… as the result of 1,541 data breaches globally

| | |
|---|---|
| **128** | breaches per **month** |
| **32** | breaches per **week** |
| **5** | breaches per **day** |

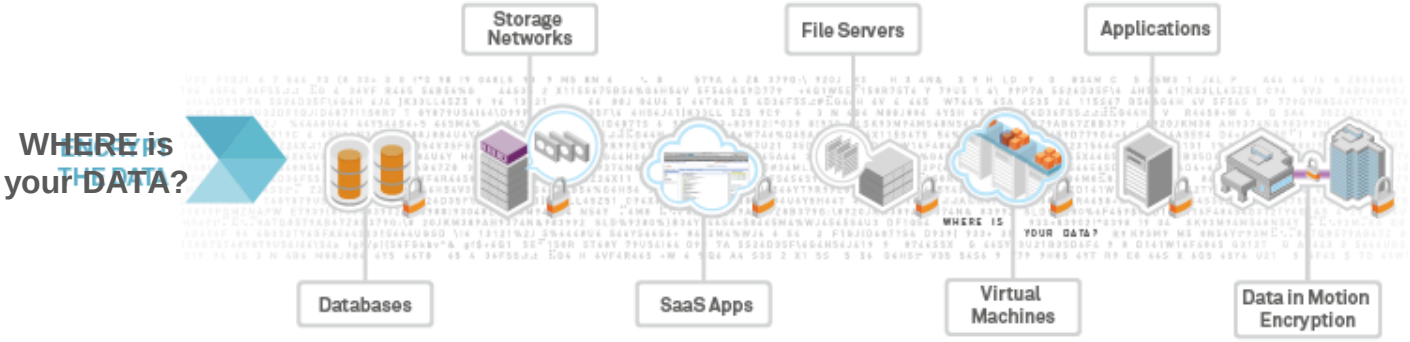
**>95% of all breaches involved data that was NOT ENCRYPTED**

http://breachlevelindex.com/

gemalto security to be free

SafeNet. THE DATA PROTECTION COMPANY

# Protect What Matters, Where it Matters





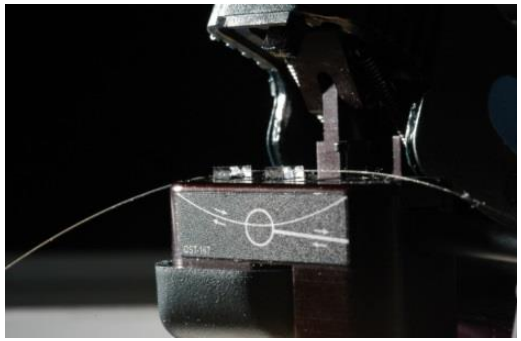
# SafeNet Today

| **Authentication**<br>- **eToken**<br>- **iKey**<br>- **IDCore, IDPrime**<br>- **eBanking**<br>- **Management Systems** | **High Security Module (HSM)**<br>- **Finance**<br>- **General Purpose (PKI)** | **Layer 2 Encryption (HSE)**<br><br>- **Fiber Channel**<br>- **Ethernet** |
|---|---|---|
| Protection for virtual infrastructure (ProtectV)<br><br>- VMWare<br>- Amazon | Enterprise Key Management Platform (KeySecure) | |

# Fibre is safe – so why should I Encrypt?

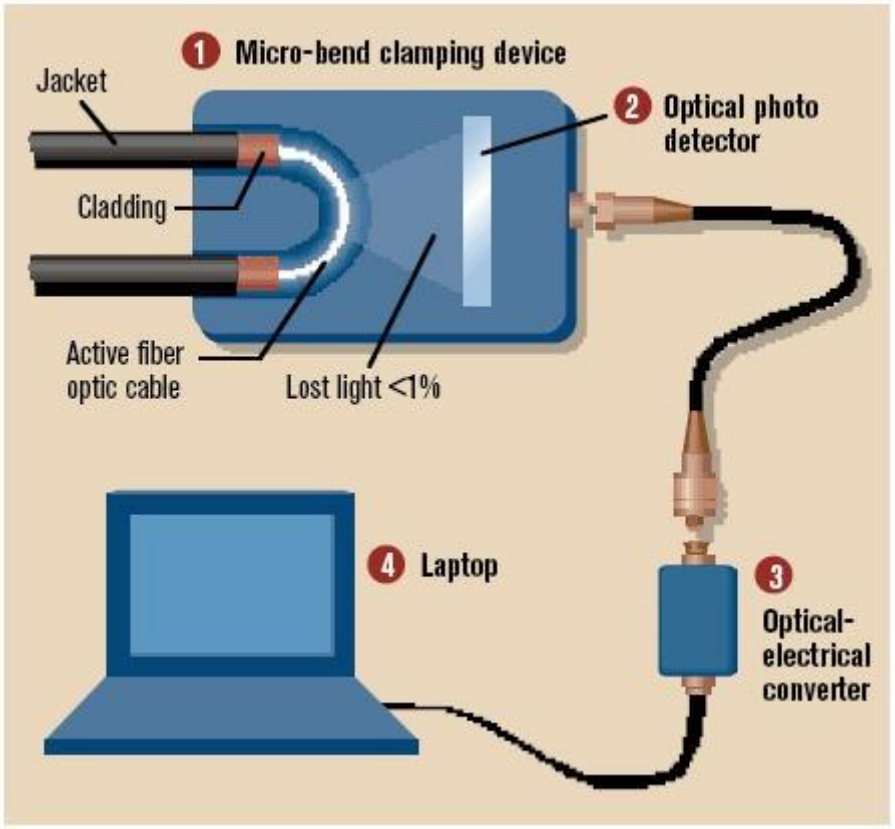
BBC security correspondent Gordon Corera says the Guardian is not accusing GCHQ of breaking the law but it does suggest the existing legislation is being very broadly applied to allow such a large volume of data to be collected.
OK, so Governments routinely 'legally' tap fibre – but surely only governments are in a position to do this, no one else could, could they?

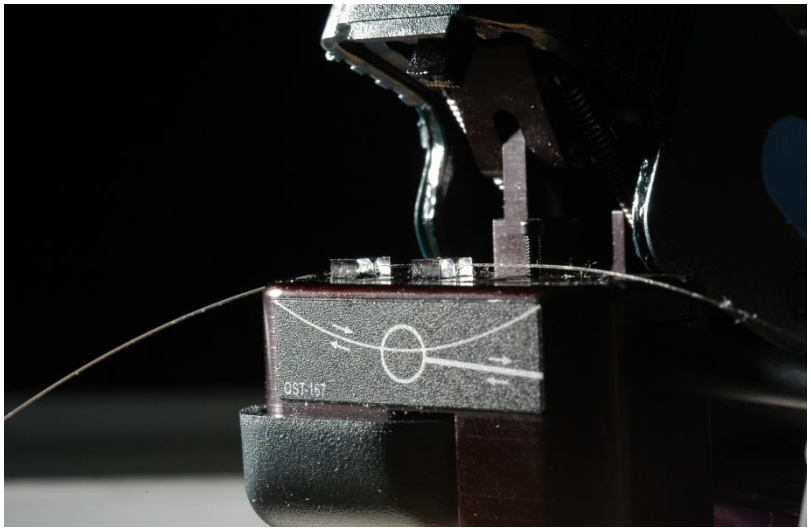
- Eavesdropping On Fibre Is Not Trivial
- - But it can be done!



- Fibres emit light which can be detected
- Some small signal attenuation (insertion loss <= 3dB) but risk of detection is low

# Simple example of a tapping device

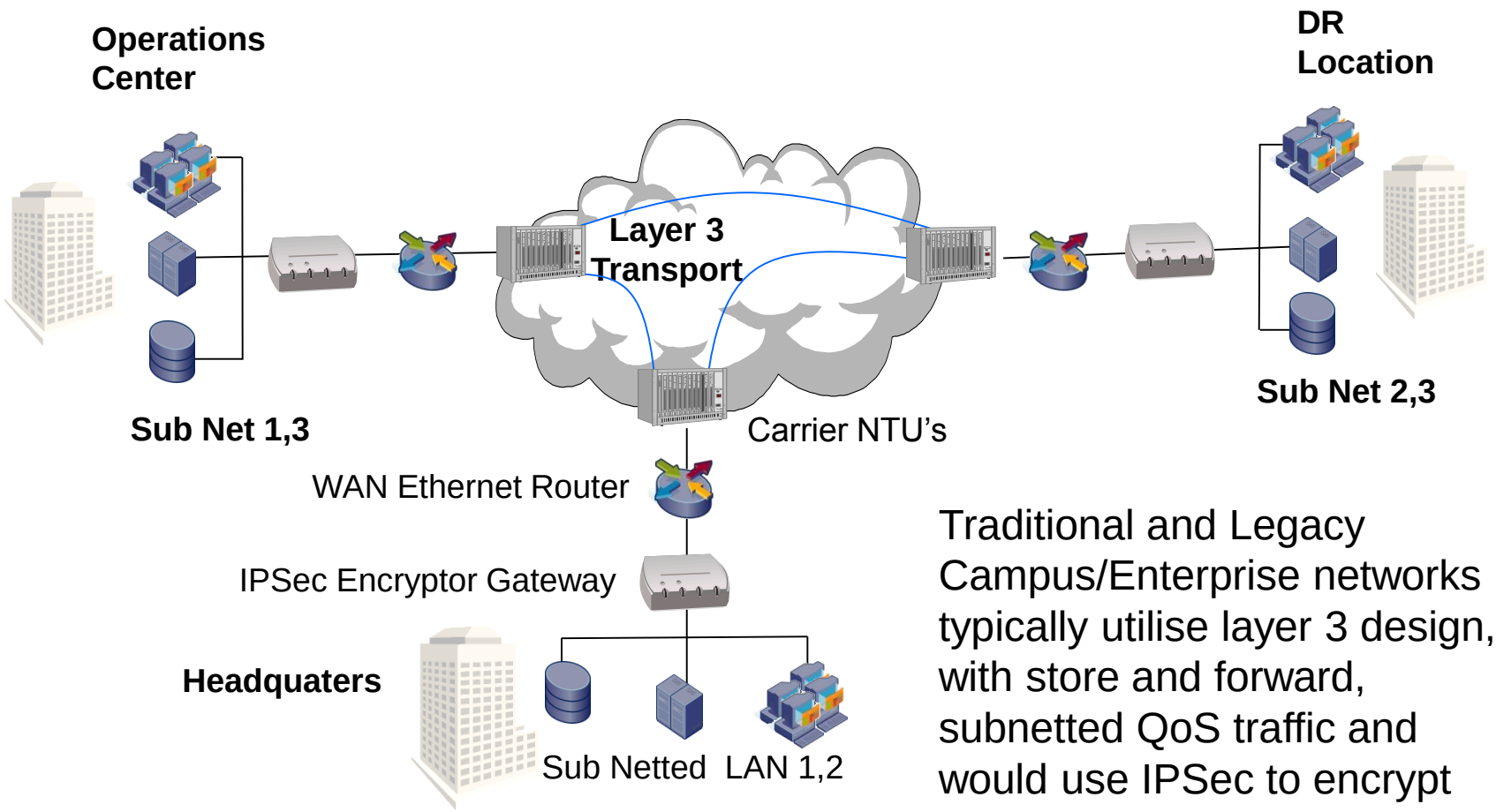


- Clip on clamping device
- Around £300

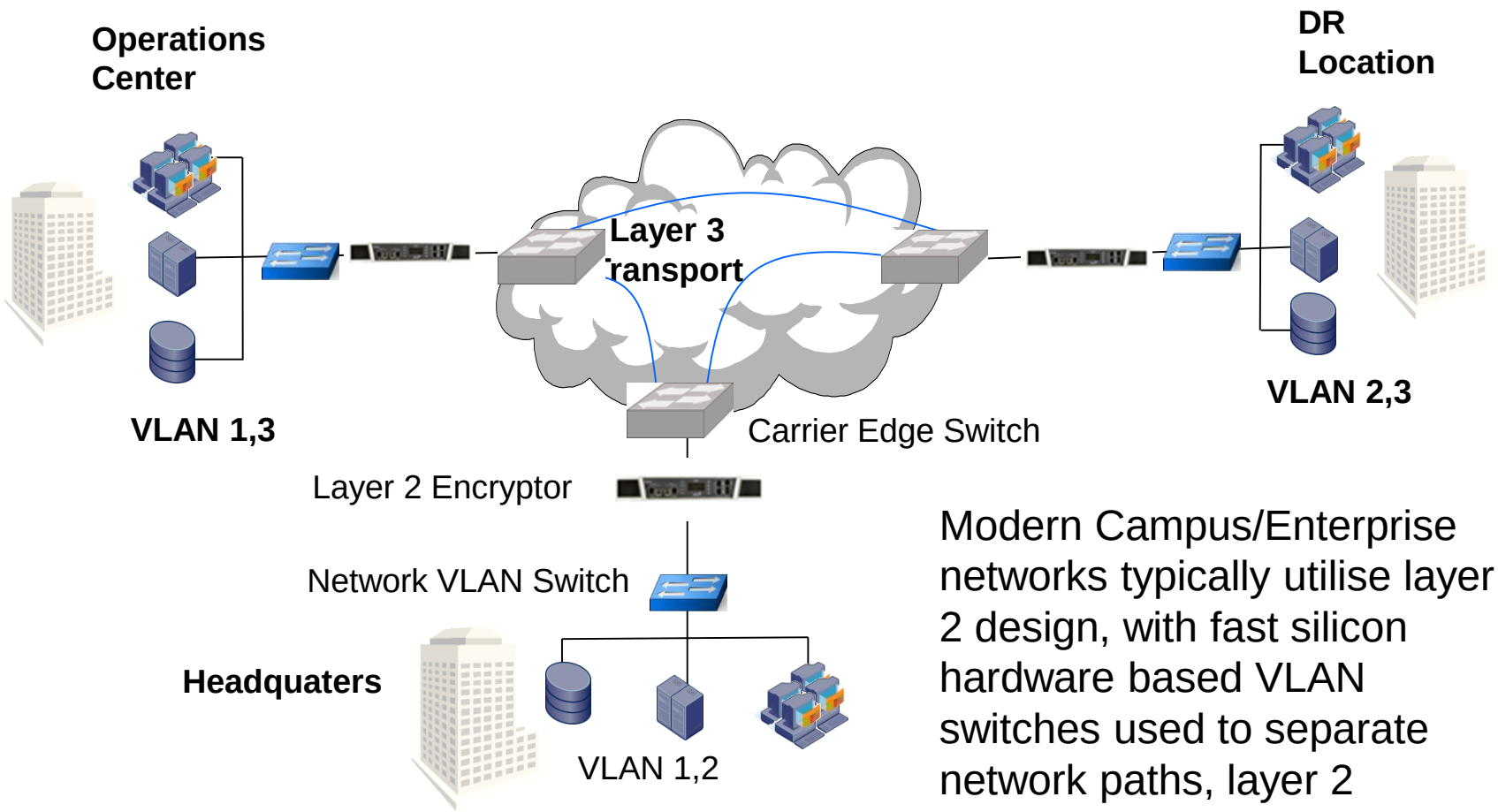
*Sandra Kay Millar *Information Security Magazine*

# Layer 3 Enterprise Network Architecture




Traditional and Legacy Campus/Enterprise networks typically utilise layer 3 design, with store and forward, subnetted QoS traffic and would use IPSec to encrypt the sensative traffic.

# Layer 3 Enterprise Network Architecture




Modern Campus/Enterprise networks typically utilise layer 2 design, with fast silicon hardware based VLAN switches used to separate network paths, layer 2 encryptors are used to secure sensitive data.

# Securing a L3 verses L2 Network

## *Layer 3 Cost and Performance*

- **Requires extra memory/blades in each router/VPN Gateway**
- **Causes loss of performance due to extra CPU overhead.**
- **Loss of throughput**
  - Layer 3 IPSec reduces throughput by as much as 40% for small packets (64 Bytes). Increased fragmentation on large packets.
- **Higher ongoing costs associated with IPSec key management**
- **Locked into Network Vendor**

## *Layer 2 Cost and Performance*

- **Separation of duties**
  - Let the network VLANs Switches do there job at wire speed
  - Let the encryptors do their job at wire speed
- **'Bump in the wire' cut through device**
  - **full bandwidth utilisation**
- Dedicated device
  - **no CPU overhead counts required.**
  - No vendor 'lock in'
- **Zero packet expansion in CFB mode**
  - CTR mode adds1 byte shim/32frames
  - GCM mode adds a 16 byte shim
- Very low latency – FPGA used to encrypt frame.

# Securing a Layer 2 Network

## *Layer 2 Cost and Performance*

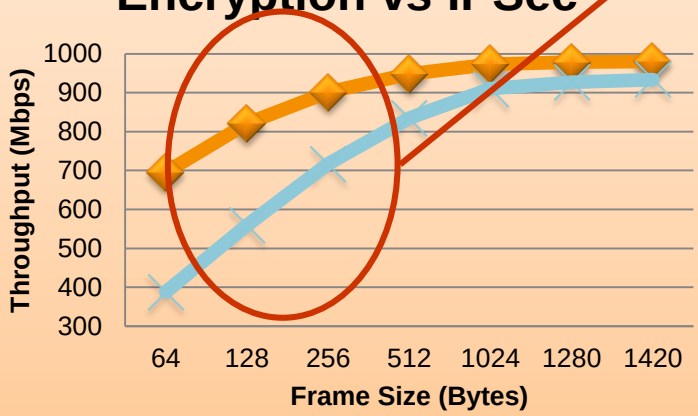
- **Separation of duties**
  - Let the network VLANs Switches do there job at wire speed
  - Let the encryptors do their job at wire speed
- **‘Bump in the wire’ cut through device – full bandwidth utilisation**
- **Dedicated device, therefore no CPU overhead counts required.**
- **Zero packet expansion in CFB mode**
  - CTR mode adds1 byte shim/32frames
  - GCM mode adds a 16 byte shim
- Very low latency – FPGA used to encrypt frame.

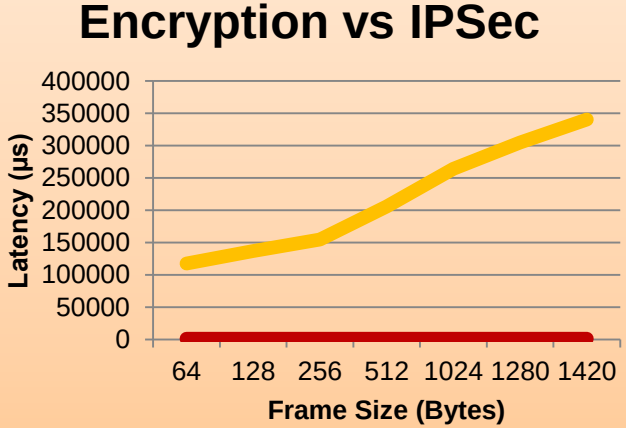
## *Security*

Policy against MAC address or VLAN ID
Encryptor is a ‘cut through’ design, encrypted frame is transmitted even before whole frame received.
Dedicated inband Management .
Tamper proof  certified Cryptographic device.

# Improved Performance

*Typical Network traffic Profile*




Ethernet Encryption at Layer 2 offers in excess of 2x Better Bandwidth Efficiency and 5x Better Speed…

Source: Rochester Institute of Technology

# Layer 2 Network Encryption – where safety is not an optical illusion

With proven reliability, high throughput, and low latency, network encryption security devices ensure safety is not an optical illusion.

**CC and FIPS certifications**

**CN6040**

Ethernet

Fibre Channel


**CN6100**

Ethernet


**CAPS**

**CN1000**

Ethernet

**CN3000**

Ethernet


gemalto
security to be free

SafeNet
THE DATA PROTECTION COMPANY

# A Quick Glance

| SafeNet CC and FIPS certified Dedicated High Speed Encryption Appliances | |
|---|---|
| Model Speeds | Scalable - From 100Mps to 10Gps |
| Protocols | Ethernet; Fiber Channel; SONET/SDH; E1/T1 |
| Size | 19” 1U |
| Pricing | Flexible – Pay as you grow |


# CN6000 Series

| SafeNet CC and FIPS certified Dedicated High Speed Encryption Appliances | |
|---|---|
| Model CN6040 eth | Scalable - From 250Mbps to 1Gbps |
| Certifications | CC EAL2+ and FIPS 140-2 Level 3 |
| Size | 19” 1U |
| Central Management | CM7 with integrated CA or external PKI certs |
| Dual PSU options | AC or DC dual integrated PSU and Fan tray |
| Network Access Ports | SFP or integrated Copper Local/Network ports |
| Management Connections | 10/100Mbps Eth, CLI, USB and front panel buttons |

# CN6000 Series

| SafeNet CC and FIPS certified Dedicated High Speed Encryption Appliances | |
|---|---|
| Model CN6040 FC | 1/2/4 Gbps |
| Certifications | CC EAL2+ and FIPS 140-2 Level 3 |
| Size | 19” 1U |
| Central Management | CM7 with integrated CA or external PKI certs |
| Dual PSU options | AC or DC dual integrated PSU and Fan tray |
| Network Access Ports | SFP or integrated Copper Local/Network ports |
| Management Connections | 10/100Mbps Eth, CLI, USB and front panel buttons |

# CN6000 Series

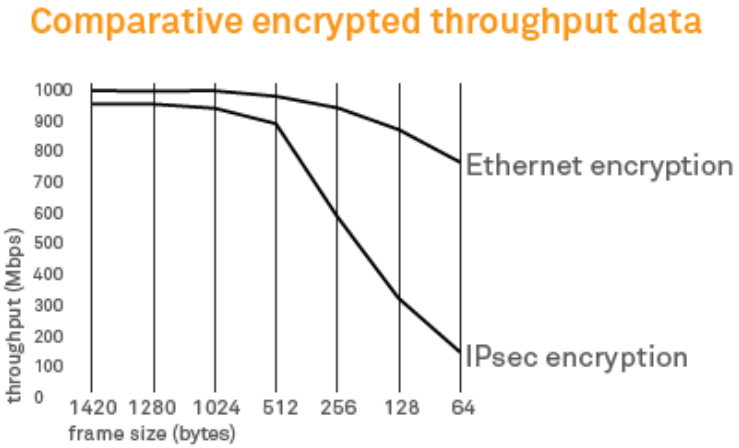
| SafeNet CC and FIPS certified Dedicated High Speed Encryption Appliances | |
|---|---|
| Model CN6100 eth | Scalable - From 1Gbps to 10Gbps |
| Certifications | CC EAL2+ and FIPS 140-2 Level 3 |
| Size | 19” 1U |
| Central Management | CM7 with integrated CA or external PKI certs |
| Dual PSU options | AC or DC dual integrated PSU and Fan tray |
| Network Access Ports | Front access XFP Local/Network ports |
| Management Connections | 10/100Mbps Eth, CLI, USB and front panel buttons |


gemalto security to be free

SafeNet THE DATA PROTECTION COMPANY

# Have it all with SafeNet

## Maximum throughput with zero protocol overhead




SafeNet high speed Layer 2 encryption technology =

- Zero protocol overhead for maximum bandwidth
- Up to 50% more efficient than competing technologies
- Fastest network encryption available, operating at true line speed, full duplex.
- No impact on latency ensures the high quality of real-time applications such as VoIP and video

# Security Can be Simple

- SafeNet high speed encryptors can be set up in minutes
  - No need for network reconfiguration and no need for routing table updates.
  - Routing updates are transparent to encryption.
  - No need to manually build complex addressing tables and policies because SafeNet encryptors automatically discover network MAC addresses.
- It's Layer 2 so it does not care about IP addresses
- Encryption based on VLAN tags or MAC address
- Can also just bulk encrypt

# Reclaim Your Bandwidth & Save Money

- Simple network topology
  - Bump in the Wire
  - Decreased complexity of network infrastructure, maintenance and admin
- Low Latency (in the micro seconds)
- Zero Overhead means you get the bandwidth you pay for

- Reclaiming your network bandwidth = $$$

# Strongest Security for Data in Transit

- Strongest cryptographic algorithm AES-256
- No Key Management Required
- Audit and Event logs
- X.509 Certificates for authentication
- Certified:
  - FIPS 140-2 level 3
  - Common Criteria
  - CAPS (UK)

- SafeNet devices are used by many government agencies
- SafeNet encryptors are designed and built from the ground up as security appliances

SafeNet. THE DATA PROTECTION COMPANY

gemalto security to be free

# Q&A

Vladimir.Zdor@gemalto.com