AEP Networks Capabilities

# 1. By technology function

## 1.1 Secure Network Communications

### 1.1.1 Site-to-site encryption (ED20, ED100, SCOPE)

### 1.1.2 Secure Remote Access (ED20, ED100, Net Remote)

### 1.1.3 Secure Deployable Communications

## 1.2 Secure Applications

### 1.2.1 Secure Application Access (A+K)

### 1.2.2 Secure Virtual Desktop Deployment

### 1.2.3 Secure Video Conferencing

AEP Networks’ Series E CAPS Enhanced Grade Certified or CISPS certified IPSEC ESP tunnelling mode encryption system and AEP Networks’ Series V communications routers are combined to provide a package to secure VC systems. The solution is appropriate for Video Conferencing products supporting Unicast.

The diagram illustrates 4 types of deployment together with the management infrastructure for the encryption, communications and VC systems (if required):

* An installation in a conference suite at a data centre where it is possible permanently to install a protectively marked encryptor (the master site)
* An installation in a conference suite at a headquarters site where it is possible permanently to install a protectively marked encryptor
* An installation in a conference suite at a fixed site that does not offer the level of security necessary for an unsupervised encryption device
* An installation in a deployable conferencing system

The solution can also offer packages to secure single user fixed and deployable systems (see below).

It is assumed that a typical customer’s requirements will comprise a mixture of these deployment types. The solution will need to be capable of fully meshed configuration or hub and spoke / star or any combination of these options. Architectures for different configurations are described in subsequent sections.

It is also assumed that the solution may need to offer an assured level of data separation between domains within the VC system. This is addressed in the Cryptographic Communities of Interest section below.

***For more detail on AEP Networks Secure Video Conferencing Solution please see <Steve’s datasheet or a variation thereof>***

### 1.2.4 “Protecting Cloud “

## 1.3 Secure Network Infrastructure

### 1.3.1 Infrastructure Security (DNSSEC – K)

## 1.4 Optimised Communications

### 1.4.1 Ship-to-shore communications (inc ASR, etc)

### 1.4.2 Optimising low bandwidth links (

### 1.4.3 Internet backup via satellite

--

# 2. By sector

((See Thales’ website – goes into detail))

Emergency services

Maritime

Enterprise

Finance

Government

Armed services

Infrastructure providers (ISPs – DNSSEC)

## 2.X Critical infrastructure

### 2.X.1 Airports and Ports

### 2.X.2 Energy and Utilities / Sensitive sites and events /

## 2.Y Government

((Loads here))

Government

Industry and Finance

Radiology

Radio Frequency and Maritime Services